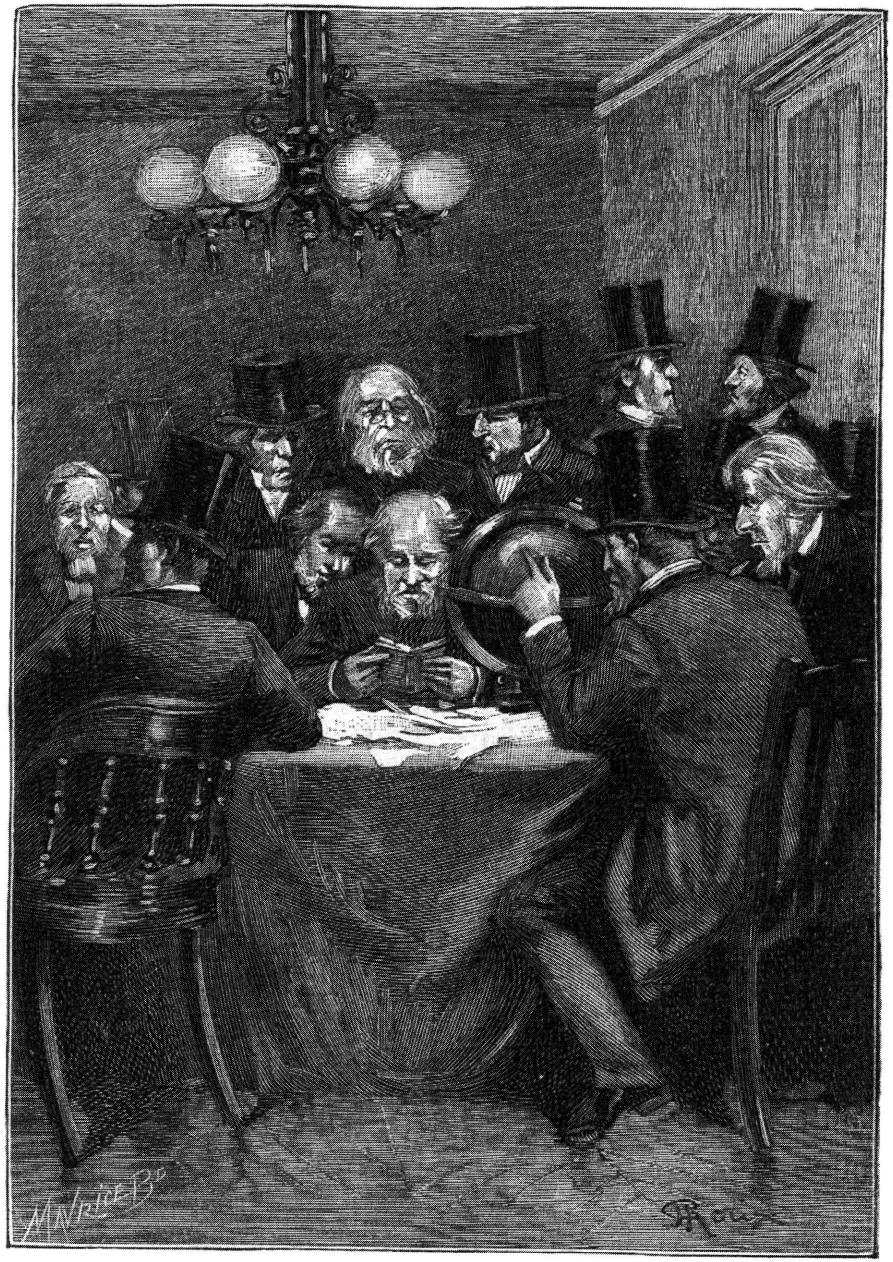
Jiří Matoušek • Jaroslav Nešetřil

Kapitoly z diskrétní matematiky

Univerzita Karlova v Praze
Nakladatelství Karolinum
2009

MZK – UK Brno
2610434082

1094663 | 2024910
MORAVSKÁ ZEMSKÁ KNIHOVNA
sign 2-1243.020



Jen matematikové dovedli ocenit tuto práci...

Recenzenti: prof. RNDr. Zdeněk Ryjáček, DrSc.
doc. RNDr. Václav Nýdl, CSc.

© Jiří Matoušek, Jaroslav Nešetřil, 2009

ISBN 978-80-246-1740-4

Obsah

Předmluva ke čtvrtému vydání **11**

Předmluva **13**

1 Základní pojmy a označení **19**
1.1 Ochutnávka problémů 19
1.2 Přirozená čísla, množiny 24
1.3 Matematická indukce 31
1.4 Relace 34
1.5 Funkce 39
1.6 Další druhy relací, zvláště ekvivalence 44

2 O uspořádaných množinách **51**
2.1 Uspořádání a jejich znázorňování 51
2.2 Uspořádání a lineární uspořádání 57
2.3 Uspořádání pomocí inkluze 61
2.4 O dlouhém a širokém 64

3 Kombinatorické počítání **69**
3.1 Funkce a podmnožiny 69
3.2 Permutace a faktoriály 72
3.3 Binomické koeficienty 76
3.4 Odhady funkcí: faktoriál 85
3.5 Odhady: binomické koeficienty 94
3.6 Princip inkluze a exkluze 99

3.7 Šatnářka a ti druzí 105

4 Grafy: úvod **111**
4.1 Pojem grafu; isomorfismus 111
4.2 Podgrafy, souvislost, metrika, matice sousednosti . . . 118
4.3 Hledání nejkratší cesty 124
4.4 Skóre grafu 129
4.5 Jednotažky – eulerovské grafy 135
4.6 Eulerovské orientované grafy 142
4.7 2-souvislost 147
4.8 Grafy bez trojúhelníků: extremální úloha poprvé . . . 154

5 Stromy **159**
5.1 Definice a charakteristika stromů 159
5.2 Isomorfismus stromů 164
5.3 Problém minimální kostry 170
5.4 Jarníkův algoritmus a Borůvkův algoritmus 180

6 Rovinné kreslení grafů **187**
6.1 Úvod do rovinných grafů 187
6.2 Proč a jak definovat rovinné nakreslení grafu 189
6.3 Jordanova věta o kružnici 194
6.4 Stěny a Eulerův vztah 201
6.5 Maximální počet hran rovinného grafu 204
6.6 Platónská tělesa 214
6.7 Kuratowského věta 218
6.8 Barvení map – problém čtyř barev 220
6.9 Kreslení grafů na plochách 231

7 Počítání dvěma způsoby **237**
7.1 Princip sudosti 238
7.2 Spernerova věta o nezávislém systému množin 245
7.3 Extremální věta: grafy bez čtyřcyklů 252

8 Počet koster **259**
8.1 Cayleyho formule 259
8.2 Důkaz přes skóre 260
8.3 Důkaz s obratlovci 262
8.4 Důkaz pomocí Prüferova kódu 265
8.5 Důkaz pracující s determinanty 268
8.6 Důkaz zatím asi nejjednodušší 278

9 Konečné projektivní roviny **281**
9.1 Definice a vlastnosti konečné projektivní roviny 281
9.2 Konstrukce projektivních rovin 289
9.3 Ortogonální latinské čtverce 294
9.4 Použití konečných projektivních rovin 298

10 Pravděpodobnostní důkazy **301**
10.1 Důkazy počítáním 301
10.2 Konečné pravděpodobnostní prostory 307
10.3 Střední hodnota 317
10.4 Několik aplikací 322

11 Řád z nepravidelnosti: Ramseyova věta **331**
11.1 Večírky se šesti 332
11.2 Ramseyova věta pro grafy 334
11.3 Dolní odhad Ramseyových čísel 336

12 Vytvořující funkce **341**
12.1 Kombinatorické aplikace mnohočlenů 341
12.2 Rozšíření na nekonečné řady 345
12.3 Fibonacciho čísla a zlatý řez 354
12.4 Binární stromy 360
12.5 O házení kostkou 365
12.6 Náhodná procházka 366
12.7 Rozklady 368

13 Aplikace lineární algebry **377**
13.1 Bloková schémata 377
13.2 Fisherova nerovnost 382
13.3 Pokrývání úplnými bipartitními grafy 386
13.4 Prostor kružnic grafu 388
13.5 Cirkulace a řezy: prostor kružnic podruhé 393

Dodatek: opakování algebry **399**

Literatura **409**

Rejstřík **413**

Návody ke cvičením **427**

Předmluva ke čtvrtému vydání

Toto je oficiálně čtvrté české vydání Kapitol z diskrétní matematiky. Oproti vydání třetímu z roku 2007 jsme podstatně přepracovali kapitolu o rovinných grafech (za její pročtení a řadu užitečných připomínek děkujeme Petru Kolmanovi a Heleně Nyklové) a jako obvykle opravili drobné chyby.

Třetí vydání bylo proti vydání předchozímu významně rozšířeno: přidali jsme kapitolu 2 o částečných uspořádáních, část 4.8 o Turánově větě, několik důkazů Cauchyho-Schwarzovy nerovnosti v části 7.3, další důkaz determinantové formule pro počítání koster v části 8.5, geometrickou interpretaci konstrukce projektivní roviny v části 9.2, krátkou kapitolu 11 o Ramseyově větě a oddíl 12.7 o počtu rozkladů čísla n.

Praha, říjen 2009

Jiří Matoušek *Jaroslav Nešetřil*

Předmluva

Čtenář, kterého jsme si při psaní této učebnice představovali, byl studentem prvního ročníku matematiky nebo informatiky. Text je ovšem určen i pro posluchače vyšších ročníků, kterým se dostává úvodního kursu diskrétní matematiky později, a může být užitečný i pro jiné zájemce o snadné a rychlé úvodní poučení o kombinatorice, například pro odborníky z četných oblastí, kde se diskrétní matematika využívá. Hlavně jsme však mysleli na našeho studenta prvního ročníku, a tomu jsme podání přizpůsobili. Ne snad vypuštěním všech těžších věcí, nýbrž hlavně důrazem na některé rysy výkladu:

- *Rozvoj matematického myšlení.* Chceme čtenáře seznámit se základy kombinatoriky a teorie grafů. Hlavně mu ale chceme pomoci naučit se matematickému způsobu myšlení, přesnému formulování myšlenek a řešení matematických problémů vyžadujících více rozmyslu než jen dosazení do vzorečku. Volba konkrétního materiálu pro takovou průpravu patrně není klíčová – uchvacuje-li vás algebra, rozhodně vás od ní nebudeme zrazovat! Domníváme se však, že kombinatorika je pro takové první samostatnější ponoření do matematiky zvlášť vhodná, poněvadž problémy a pojmy v ní studované jsou, přinejmenším ze začátku, elementárnější než např. v matematické analýze, která již od úvodního kursu začíná jako dosti hluboká a jednolitá teorie.

- *Radost.* Kniha je psána pro onoho ideálního čtenáře, který aspoň někdy zažil potěšení z důvtipného řešení matematické úlohy či hádanky. Je ovšem též naším smělým přáním, aby tato kniha

pomohla podobný pocit vzbudit u těch, u nichž dosud jen dřímal. Domníváme se, že taková občasná radost z elegantní myšlenky, někdy dokonce smíšená s pocitem dobře vykonané práce, je pro studium matematiky nesmírně důležitá. Ne každý byl obdařen takovým talentem, stejně jako ne každý má rád hudbu. Ale bez podobného pocitu je studium matematiky nejspíš velmi nudné.

- *Karty na stůl.* Látku se snažíme vyložit v úplnosti. Řekneme-li, že něco je jednoduché, myslíme to vážně, a jestliže to čtenáři při pozorném studiu tak nepřipadá, pak je patrně něco v nepořádku: Možná jsme situaci špatně odhadli, ale možná to naznačuje, že čtenář nepochopil něco z předchozí látky.

- *Souvislosti a aplikace.* Probíraná látka dává několik příležitostí ukázat pojmy a výsledky z jiných oblastí matematiky v akci, a tyto souvislosti se snažíme zdůraznit. Takové partie demonstrují vzájemnou provázanost základních matematických oborů, a podle našich zkušeností je studenti mají rádi, pokud se celá aplikace probere důkladně, včetně připomenutí pojmů z příslušného jiného odvětví.

- *A co informatika?* I když dnes mnoho posluchačů kursů diskrétní matematiky studuje informatiku, chtěli jsme text učinit přístupným i pro ty, kteří shledávají počítače a programování odpudivými, a proto jsme se informatické terminologii spíše vyhýbali (např. místo „NP-úplná úloha“ říkáme vágněji „algoritmicky těžká úloha“). Přesto kniha obsahuje několik pasáží o efektivních algoritmech a řadu cvičení na sestavení programů, od krátkých až po menší softwarové projekty.

Náplň. Náš text je úvodem do kombinatoriky a teorie grafů. Vychází z koncepce úvodního kursu diskrétní matematiky pro první ročník matematického a informatického studia na Matematicko-fyzikální fakultě University Karlovy v Praze, vypracované druhým z autorů, a pokrývá látku kursu v podobě, v jaké ho autoři řadu let přednášeli.

V jednosemestrálním kursu se určitě neprobírá celý tento text. Připsali jsme hodně rozšiřujícího (a někdy trochu pokročilejšího) materiálu, hlavně v naději, že čtenář si kromě toho, co je zrovna povinné k přednášce, třeba mimoděk přečte i jiné věci. Navíc některé kapitoly slouží aspoň jako úvod k specializovanějším kursům, např. o pravděpodobnostní metodě nebo o aplikacích lineární algebry.

Vložili jsme i dodatek shrnující základní pojmy a některé výsledky z lineární algebry. Nemůže samozřejmě nahradit řádný kurs, ale kromě připomenutí základních pojmů může být snad užitečný i pro studium lineární algebry jako jistý pohled z ptačí perspektivy.

V jednotlivých částech je rozšiřující nebo specializovanější materiál vyznačen takovýmhle menším písmem. Řadu dalších souvisejících informací jsme se snažili propašovat i do cvičení.

O literatuře. V českém jazyce existuje několik knih o teorii grafů, např. [23], i knihy pojednávající o základech kombinatorického počítání (třeba [30]), ale nemusí být snadno dostupné, a značná část zde probrané látky se patrně najde jen v zahraničních učebnicích. O matematice obecně a o tom, jak a na čem dnes matematici pracují, se lze dočíst ve vynikající populární knížce Gowersově [12].

V citacích neuvádíme zdaleka všechny prameny, z nichž jsme čerpali. Chtěli bychom ale vyzdvihnout (a doporučit) jeden z pramenů, totiž velkou sbírku řešených kombinatorických problémů Lovász [21], odkud jsme převzali část materiálu a část těžších cvičení (naše těžší cvičení jsou Lovászovy lehčí problémy). Tato knížka je vynikající pro pokročilejší studium kombinatoriky, i jako soupis spousty kombinatorických výsledků a metod. Dobrá učebnice kombinatoriky, vhodná jako pokračování našeho spisu, je Van Lint a Wilson [19]. Umění kombinatorického počítání a asymptotických odhadů je znamenitě zpracováno v knize Graham, Knuth, Patashnik [13] nebo též v monografii Knuthově [18]. Nedávno vyšla také obsáhlá kniha Flajolet a Sedgewick [10]. Dobrá moderní učebnice teorie grafů je např. Diestel [9]. Další zmínky o doporučené literatuře jsou roztroušeny po jednotlivých kapitolách. (Učebnic kombinatoriky existuje spousta, zde jsme jen zmínili některé naše oblíbené.)

O cvičeních. Za jednotlivými částmi najde čtenář větší či menší nabídku cvičení (některá souvisí s probraným tématem jen volně, a jsou zařazena spíš pro oživení a pro všeobecný matematický rozhled). Uspěchanost moderního života a utváření lidské psychologie asi málokomu dovolí, aby si pro vlastní uspokojení a sebevzdělání systematicky vyřešil větší část z uvedených 373 cvičení, i když by to byla asi nakonec časově nejúspornější cesta, jak probírané věci aktivně zvládnout.

Nezařazovali jsme cvičení zcela rutinní (spočívající v aplikaci nějakého probraného „receptu", např. „aplikujte probraný algoritmus na tento konkrétní graf"), věříme, že takovým způsobem si své porozumění látce může ověřit každý sám (apelujeme ale na vedoucí cvičení, aby takové příklady také zařazovali).

Cvičení jsme rozdělili na tři skupiny obtížnosti: bez hvězdičky, s jednou a se dvěma hvězdičkami. Představujeme si, že dobrý student matematiky by měl po pochopení příslušného článku být schopen vyřešit velkou většinu bezhvězdičkových cvičení. Jednohvězdičková cvičení většinou vyžadují nějaký nápad, na nějž člověk přijít může a nemusí, a konečně dvouhvězdičková chtějí asi nápad poměrně neotřelý. Skoro všechna cvičení mají krátké řešení – pokud víme, nikde nejsou potřeba dlouhé a úmorné výpočty. Naše rozdělení podle obtížnosti je ovšem subjektivní, a cvičení, které je pro někoho zcela snadné, protože třeba již viděl nějaký matematický obrat použitelný v podobné situaci, může být pro jiného nepřekonatelné. Rozhodli jsme se zařadit i krátké návody na řešení některých cvičení. Přečtením návodu si čtenář může zkazit radost ze samostatného vyřešení problému, ale i za pomoci návodu dá formulace úplného řešení často ještě hodně práce.

O rejstříku. Pokud se pojem, na nějž se v rejstříku odkazuje, vyskytuje v číslovaném odstavci (např. v definici), číslo tohoto odstavce je v závorce za číslem stránky, něco jako 56(3.2.2). Podobně odkazy na cvičení jsou typu 123(cv. 2). U většiny pojmů, zejména všeobecně matematického charakteru (jako např. relace, graf) rejstřík odkazuje pouze na místo jejich definice. Matematické symboly vytvořené z latinských písmen (např. C_n) jsou zařazeny pod příslušným písmenem, před ostatními slovy. Značení zahrnující speciální symboly (jako $X \setminus Y$, $G \cong H$) a řecká písmena je uvedeno na začátku rejstříku.

Historie. Tento text vznikl na katedře aplikované matematiky Matematicko-fyzikální fakulty University Karlovy Praha. Předběžnou verzi vydala katedra v prosinci 1995. První vydání vyšlo v nakladatelství Matfyzpress koncem roku 1996. Rozšířená anglická verze byla publikována nakladatelstvím Oxford University Press v roce 1998 pod názvem *Invitation to Discrete Mathematics*, a postupně byla přeložena do několika dalších jazyků. Další dvě česká vydání vyšla v Nakladatelství Karolinum. Každé z nich má proti předchozímu něco navíc a jsou v něm opraveny další chyby.

Autorství některých ilustrací. Obrázky na obálce jsou dílem Jiřího Načeradského a Jaroslava Nešetřila. Úvodní ilustrace je rytina G. Rouxe z knihy Julese Verna: Zmatek nad zmatek, vydané nakladatelem J. Vilímkem v Praze roku 1931.

Poděkování. Mnoho našich spolupracovníků z KAM a studentů spoluvytvářelo příjemnou stimulující atmosféru, v níž se nám dobře psalo. Jan Kratochvíl napsal první verze části 4.3 (za chyby, které jsme tam vyrobili dalším jejím přepracováváním, ovšem nenese žádnou zodpovědnost!). Naši kolegové, vedoucí cvičení a někteří studenti přispěli drobnými připomínkami k textu a náměty na cvičení. Velké množství chyb v předchozích vydáních nalezli zejména Pavel Socha, Eva Matoušková, Tomáš Holan, Robert Babilon a Jana Chlebíková. Martin Klazar a Jiří Otta sestavili sbírku cvičných příkladů, z nichž většinu jsme použili. Aleš Pultr laskavě přispěl k vylepšení dodatku o algebře několika připomínkami, a Martin Klazar nás upozornil na slabosti jednoho z důkazů i na možnosti nápravy. Jana Chlebíková a Karel Horák velmi pomohli prvnímu autorovi radou při zápolení s typografií knížky. S Jaroslavem Jirsou a Kamilou Schüllerovou z nakladatelství Karolinum byla radost spolupracovat na přípravě druhého vydání. Všem zmíněným (jakož i těm, na které jsme bez zlého úmyslu mohli zapomenout) děkujeme.

Jménem lidstva též děkujeme Otfriedu Cheongovi za napsání grafického editoru Ipe, jímž byla vyrobena většina obrázků. Zmíněný editor je názorným dokladem významu matematického vzdělání pro zdánlivě nematematické činnosti, jako v tomto případě psaní složitého

MORAVSKÁ ZEMSKÁ BRNO KNIHOVNA

software – stačí tento teoretickým informatikem napsaný program porovnat s chaotičností mnohého komerčního software.

Prosba na závěr. V každém textu jsou nějaké chyby. Už jsme jich spoustu odstranili, ale určitě ne všechny. Zejména se může stát, že některá cvičení jsou nevhodně formulována, nebo že nefunguje řešení, které jsme si představovali. Prosíme čtenáře, který nějaká nedopatření odhalí, aby je sdělil autorům (e-mail `jiri.matousek@mff.cuni.cz` nebo `jaroslav.nesetril@mff.cuni.cz`). Aktuální seznam objevených chyb vystavujeme na internetové stránce přístupné z adresy `http://kam.mff.cuni.cz/~matousek`.

1

Základní pojmy a označení

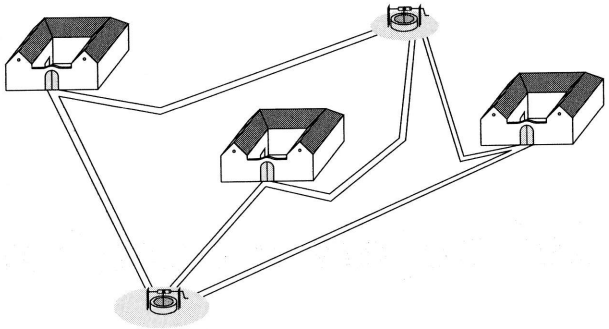
V této úvodní kapitole zavedeme mnoho pojmů. Věříme, že se jimi čtenář nenechá odradit; předpokládáme, že jich většinu dobře zná nebo aspoň již slyšel. Takže vlastně pojmy většinou pouze připomínáme a (hlavně) ukazujeme jejich přirozené souvislosti, různé možné způsoby jejich zavedení apod. A i když, jakkoliv nepravděpodobně, čtenář nikdy nic podobného neslyšel, jedná se zde o pojmy základní, snadno pochopitelné a názorné. Vynechat je nemůžeme: Matematika má svůj jazyk, a kdo chce porozumět a domluvit se, musí zvládnout aspoň základní slovíčka.

1.1 Ochutnávka problémů

Nejdříve se podívejme na několik úloh, jimiž se budeme v této knížce zabývat. Zde je zformulujeme jako matematické hádanky, a je dost dobře možné, že se čtenář s některými z nich již setkal v populární literatuře.

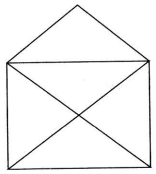
Známý problém pojednává o třech domech a třech studnách. V daleké zemi stály tři pěkné domy, a tři blízké studny jim dávaly čistou chladnou vodu. Všichni tam žili spokojeně, až jednoho dne vypukl spor, a nikdo jej nedokázal rozsoudit. Od každého domu chtěli mít tři cesty, jednu ke každé ze tří studen, a nejen to, s jejich cestami že se nesmí křížit žádná z cest jejich sousedů.

Může někdo někdy najít takové cesty? Kdyby byly studny jenom dvě, řešení by bylo snadné:

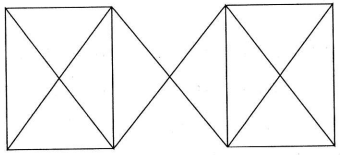


Ale pro tři studny není žádná naděje (pokud by ti zatvrzelci nepřistoupili na chození po mostě nebo tunelem, ale to se asi čekat nedá). Uměli byste úlohu zformulovat jako matematický problém, a třeba dokonce ukázat, proč je neřešitelný?

Tohle byla v podstatě otázka o kreslení v rovině. Mnoho jiných úloh studovaných v naší knize lze také formulovat pomocí kreslení. Dá se následující obrázek nakreslit jedním tahem, aniž bychom zvedli tužku z papíru, a aniž bychom některou z čar obtáhli vícekrát?

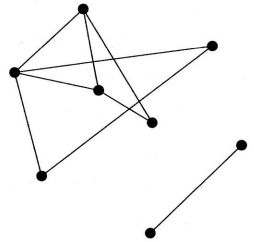


A co tenhle obrázek?

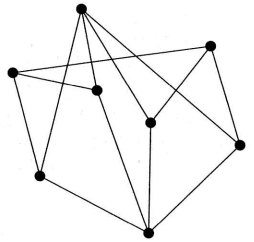


Jestli ne, tak proč? Je nějaký jednoduchý způsob, jak odlišit obrázky, které jdou tak nakreslit, od těch, které nejdou?

K následující sérii problémů si nakreslíme 8 puntíků tak, aby žádné 3 neležely na přímce (číslo 8 je celkem libovolné, obecně bychom mohli uvažovat n takových puntíků). Spojíme některé dvojice puntíků úsečkami, například takto:

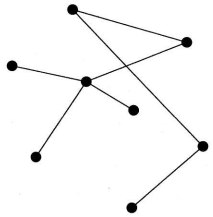


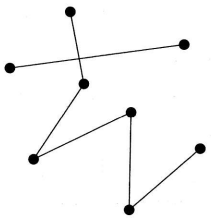
Kolik nanejvýš lze do obrázku s 8 puntíky nakreslit spojnic, když nesmí vzniknout žádný trojúhelník s vrcholy v puntících? Zde je obrázek se 13 spojnicemi:



Dovedete pro 8 puntíků nakreslit větší počet spojnic? Asi ano. Ale uměli byste dokázat, že váš počet už nejde zlepšit?

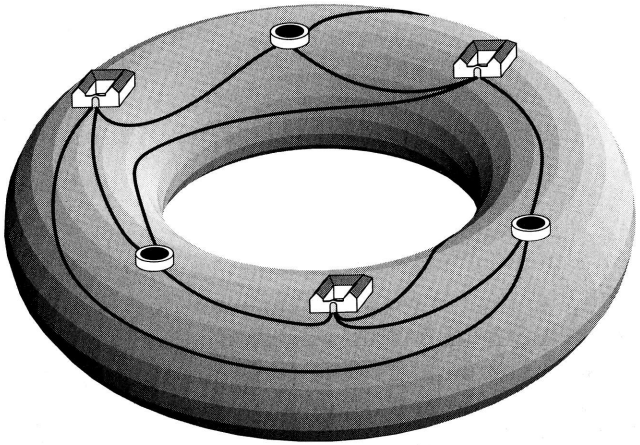
Teď pro změnu chceme nakreslit nějaké spojnice (úsečky) tak, aby se mezi každými dvěma puntíky dalo přejít po cestě, sestávající z nakreslených úseček. Taková cesta nesmí zatáčet mimo puntíky, v místech, kde se úsečky jen kříží. Tedy levý obrázek je správné řešení, zatímco pravý nikoliv:





Jaký je nejmenší počet úseček, které je třeba nakreslit? A kolik existuje různých řešení s tímto minimálním počtem úseček? A jak bychom našli řešení, pro něž je celková délka nakreslených úseček co nejmenší?

Všechny tyhle úlohy jsou populární verze jednoduchých základních otázek *teorie grafů*, což bude jedno z našich hlavních témat (budeme se jí zabývat v kapitolách 4, 5 a 6). Je snadno vidět, že u problémů s 8 puntíky, až na ten poslední, vůbec nesejde na tom, jak jsou puntíky rozmístěny. Záleží jedině na tom, které z dvojic puntíků jsou spojeny a které ne. Většina teorie grafů pojednává o otázkách, které se dají geometricky znázornit, ale v nichž geometrie ve skutečnosti nehraje roli. Naproti tomu úloha o domech a studnách náleží do „opravdu geometrické" části teorie grafů. Je podstatné, že cesty se mají vytyčit v rovině. Kdyby domy a studny byly na maličké planetě tvaru duše z pneumatiky, tak by se požadované cesty daly navrhnout:



Dalším důležitým tématem této knížky je *kombinatorické počítání*, probírané v kapitolách 3 a 12. Úlohy z této oblasti většinou začínají „Kolika způsoby..." nebo nějak podobně. Jednu takovou otázku jsme zmínili v sérii úloh s 8 puntíky (a je to pěkná a nesnadná otázka – je jí zasvěcena celá kapitola 8). Čtenář nepochybně viděl už řadu úloh takového typu. Tady je ještě jedna: Kolika způsoby lze natřít čtyřicetipatrový mrakodrap, když každé ze 40 pater se může natřít buď zeleně

nebo růžově, ale každá dvě růžová patra musejí být oddělena aspoň jedním zeleným?

Ačkoli výše uvedené úlohy mohou vypadat jako pouhé hříčky, každá z nich se dá považovat za výchozí bod zajímavé teorie, s mnoha použitími jak v matematice samé, tak v mnoha jiných odvětvích.

Rozlišit dobré matematické problémy od špatných není snadné. Co je dobrý problém? Je to takový, jehož řešení vede k novým pohledům na známé věci, novým trikům a metodám, či dokonce k celé nové teorii. Mnohé z úloh rekreační matematiky z tohoto hlediska dobré nejsou, i když k jejich vyřešení může být potřeba značný důmysl.

Čtenář může namítnout, že problémy z této sekce jsou pro praxi k ničemu. Proč by se o nich člověk měl učit, když je taková spousta důležitých znalostí, které budou určitě potřeba v budoucím zaměstnání?

Jedna možná odpověď na takové námitky je, že ke každé z uvedených úloh–hříček lze uvést důležitý praktický problém, jehož řešení je založeno na podobných principech. Řekněme, že pošťák má doručit poštu do všech domů v nějaké čtvrti, což znamená aspoň jednou projít každou z ulic. Jaká je nejkratší možná trasa obchůzky? Dá se v rozumném čase najít pomocí stolního počítače? Aby člověk porozuměl tomuto pošťáckému problému, měl by se napřed seznámit s poměrně jednoduchými výsledky o kreslení obrázků jedním tahem.

Podobně úloha o domech a studnách je úvodem například k problémům rozmístění a propojení prvků integrovaného obvodu, a když ji člověk pochopí, je pak mnohem snadnější proniknout do algoritmů pro návrh integrovaných obvodů.

V naší knize se takovými „praktickými" problémy přímo zabývat nebudeme, ale aby člověk porozuměl řešením, popsaným v jiných knihách, nebo dokonce nějaké dobré řešení sám vymyslel, je potřeba se nejdřív seznámit se základními pojmy a myšlenkovými obraty.

Zdůrazněme také, že ačkoliv má matematika odjakživa působivé aplikace, nejkvalitnější matematický výzkum byl zřídkakdy přímo motivován praktickými problémy. Aplikace matematických objevů přicházejí často s velkým časovým odstupem a v překvapivých souvislostech.

K tomuto oddílu nejsou potřeba žádná cvičení. Podaří se vám vyřešit nějakou z uvedených úloh, nebo dokonce všechny?

1.2 Přirozená čísla, množiny

Číselné obory. Pro množinu všech přirozených čísel, tj. množinu $\{1, 2, 3, \ldots\}$, vyhradíme symbol **N**. Písmena n, m, k, i, j, p (a případná další) budou většinou rezervována pro přirozená čísla.

Pomocí přirozených čísel se konstruují další, větší číselné obory: čísla celá, racionální a reálná (a také čísla komplexní, ale ta téměř potřebovat nebudeme).

Celá čísla vzniknou z přirozených čísel přidáním záporných čísel a nuly. Množinu všech celých čísel označíme **Z**. *Racionální čísla* jsou zlomky s celočíselným čitatelem a jmenovatelem; zpravidla se značí písmenem **Q**, ale v tomto textu pro ně žádný symbol zavádět nepotřebujeme. Konstrukce množiny **R** všech *reálných* čísel je složitější a probírá se zpravidla v úvodním kursu analýzy. Známými příklady reálných čísel, jež nejsou racionální, jsou čísla jako $\sqrt{2}$, některé důležité konstanty jako π, a obecně čísla mající v dekadickém zápisu za desetinnou čárkou nekonečnou a neperiodickou posloupnost číslic, třeba $0.12112111211112\ldots$. *Uzavřený interval* od a do b na reálné ose budeme značit $[a, b]$, *otevřený interval* s týmiž koncovými body zapisujeme (a, b).

Operace s čísly. Většina označení pro číselné operace, jako například $+$ pro sčítání, $\sqrt{\ }$ pro odmocninu atd., je všeobecně známa. *Dělení* budeme zapisovat buď zlomkovou čarou, nebo někdy (pro úsporu místa) lomítkem, tedy ve tvaru $\frac{a}{b}$ nebo a/b.

Zavedeme dvě méně běžné funkce. Pro reálné číslo x se symbol $\lfloor x \rfloor$ nazývá[1] *dolní celá část* x a jeho hodnota je největší celé číslo, které je menší nebo rovno x. Podobně $\lceil x \rceil$, *horní celá část* x, označuje nejmenší celé číslo, které je větší nebo rovno x. Tak například: $\lfloor 0.999 \rfloor = 0$, $\lfloor -0.1 \rfloor = -1$, $\lceil 0.01 \rceil = 1$, $\lceil \frac{17}{3} \rceil = 6$, $\lfloor \sqrt{2} \rfloor = 1$.

Později zavedeme další číselné funkce a symboly, které budeme pro jejich kombinatorický význam zkoumat podrobněji. Patří sem např. $n!$, $\binom{n}{k}$, $\check{s}(n)$.

Sumy a součiny. Jsou-li $a_1, a_2, \ldots, a_n$ reálná čísla, jejich součet

[1] Zejména ve starší literatuře se někdy ve stejném významu používá symbol $[x]$.

$a_1 + a_2 + \cdots + a_n$ se zapisuje také pomocí *sumačního znaménka* $\sum$, ve tvaru

$$\sum_{i=1}^{n} a_i.$$

Tento zápis je trochu podobný `FOR` cyklu z různých programovacích jazyků. Ještě několik příkladů jeho použití:

$$\sum_{j=2}^{5} \frac{1}{2j} = \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{10}$$

$$\sum_{i=2}^{5} \frac{1}{2j} = \frac{1}{2j} + \frac{1}{2j} + \frac{1}{2j} + \frac{1}{2j} = \frac{2}{j}$$

$$\sum_{i=1}^{n} \sum_{j=1}^{n} (i+j) = \sum_{i=1}^{n} ((i+1) + (i+2) + \cdots + (i+n)) =$$

$$\sum_{i=1}^{n} (ni + (1 + 2 + \cdots + n)) = n \left(\sum_{i=1}^{n} i \right) + n(1 + 2 + \cdots + n)$$

$$= 2n(1 + 2 + \cdots + n).$$

Podobně jako součty se zapisují pomocí $\sum$ (což je velké řecké písmeno „sigma“, od slova *s*uma), součiny se vyjadřují užitím znaménka $\prod$ (velké řecké písmeno „pí“, od slova *p*rodukt), kupříkladu

$$\prod_{i=1}^{n} \frac{i+1}{i} = \frac{2}{1} \cdot \frac{3}{2} \cdot \cdots \cdot \frac{n+1}{n} = n + 1.$$

Množiny. Jiným základním pojmem, který budeme používat, je pojem množiny. S tímto pojmem jste se patrně setkali již na střední škole (a díky snaživosti pedagogických modernizátorů možná i na základní škole). Množiny budeme označovat zpravidla pomocí písmen velké abecedy:

$$A, B, \ldots, X, Y, \ldots, M, N, \ldots$$

a podobně, a prvky množin budeme značit většinou malými písmeny $a, b, \ldots, x, y, \ldots, m, n, \ldots$.

Skutečnost, že množina X obsahuje prvek x, se označuje tradičně pomocí symbolu $\in$ (což je trochu stylizované řecké písmeno ε – „epsilon“); $x \in X$ čteme „x (je) prvkem X“.

Je třeba si uvědomit, že pojem množiny a symbol „$\in$“ nedefinujeme (pomocí jiných, dříve zavedených pojmů). Jsou to tzv. primitivní pojmy. Předpokládáme, že ve všech konkrétních případech bude smysl uvažovaných množin a jejich prvků jasný. Jak se ukázalo začátkem století, používá-li se pojem množiny zcela svobodně a bezuzdně, může to vést k různým podivným situacím, tzv. paradoxům[2]. V tomto textu se však něčeho takového obávat nemusíme, většina námi uvažovaných množin bude mít dokonce konečný počet prvků.

Množina s prvky 1, 37 a 55 se zapíše $\{1, 37, 55\}$. To i zápisy $\{37, 1, 55\}$ a $\{1, 37, 1, 55, 55, 1\}$ znamenají všechny totéž (tedy vícenásobný výskyt téhož prvku se ignoruje, týž prvek se nemůže v jedné množině vyskytovat dvakrát). Tři tečky v zápisu množiny $\{2, 4, 6, 8, \ldots\}$ znamenají ovšem „a dále podobně, podle stejné zákonitosti“, tj. v uvedeném případě množinu všech sudých přirozených čísel (příslušná zákonitost by ovšem měla být na první pohled patrná, tak například $\{2^1, 2^2, 2^3, \ldots\}$ je srozumitelné jako množina všech mocnin dvojky, $\{2, 4, 8, \ldots\}$ je už možná srozumitelné méně).

Složitější a zajímavější množiny se zpravidla tvoří ze známých množin pomocí nějakého pravidla. Množinu všech druhých mocnin přirozených čísel bychom mohli zapsat například

$$\{i^2;\ i \in \mathbf{N}\}$$

nebo také

$$\{n \in \mathbf{N};\ \text{existuje } k \in \mathbf{N} \text{ tak, že } k^2 = n\}$$

či totéž pomocí symbolu $\exists$ pro „existuje“

$$\{n \in \mathbf{N};\ \exists k \in \mathbf{N} : k^2 = n\}.$$

[2]Nejznámější je asi tzv. paradox holiče: vojenský holič má holit všechny vojáky, kteří se neholí sami – má se, jakožto jeden z vojáků, holit, nebo ne? To se dá přeložit do matematické řeči a ukazuje to spornost pojmů jako „množina všech množin“ a podobně.

Důležitá je množina neobsahující žádný prvek. Taková množina existuje pouze jedna a je zvykem ji značit $\emptyset$ a nazývat *prázdná množina*. Poznamenejme, že prázdná množina může být prvkem jiné množiny. Například, $\{\emptyset\}$ je množina, obsahující prázdnou množinu jako prvek, a není to tedy totéž jako $\emptyset$!

Počet prvků, neboli *mohutnost*, množiny X budeme značit symbolem $|X|$ (jako absolutní hodnota). Cizím slovem se mohutnosti říká také *kardinalita*. Mohutnost se definuje i pro nekonečné množiny; my ji ale budeme uvažovat jen pro množiny konečné.

V matematice máme dost často co dělat s množinami, jejichž prvky jsou jiné množiny. Můžeme třeba definovat množinu

$$M = \{\{1, 2\}, \{1, 2, 3\}, \{2, 3, 4\}, \{4\}\},$$

jejímiž prvky jsou 4 množiny přirozených čísel, přesněji řečeno 4 podmnožiny množiny $\{1, 2, 3, 4\}$. V diskrétní matematice se s takovými množinami setkáváme běžně. Aby se nemuselo říkat „množina množin“, používá se někdy výraz *množinový systém*[3], řekli bychom tedy, že M je systém množin na množině $\{1, 2, 3, 4\}$. Takové množiny množin neboli množinové systémy se někdy označují ozdobnými typy velkých písmen, třeba $\mathcal{M}$. Je ale vidět, že takové rozlišení pomocí typů písma nemůže být úplně důsledné, co třeba když bychom narazili na množinu množin množin?

Množinu všech možných podmnožin nějaké množiny X budeme značit symbolem 2^X. (Jiné v literatuře běžné označení je $\mathcal{P}(X)$, písmeno $\mathcal{P}$ je od anglického „power set“).

Obecnější zápis sum a součinů. Někdy je výhodný obecnější způsob zápisu sumy než podle vzoru $\sum_{i=1}^{n} a_i$. Například

$$\sum_{i \in \{1,3,5,7\}} i^2$$

znamená součet $1^2 + 3^2 + 5^2 + 7^2$; pod sumační znaménko se napíše nejdříve proměnná, podle které se sčítá, a potom se nějakým způsobem zapíše množina hodnot, přes něž se sčítá. Ve způsobu zápisu

[3]V angličtině se někdy používá roztomilejší výraz *family of sets*, tedy rodina množin.

této množiny je značná libovůle, někdy se může i zčásti popsat slovy. Třeba:

$$\sum_{\substack{i;1\le i\le 10\\ i \text{ prvočíslo}}} i = 2+3+5+7.$$

Pokud je množina hodnot, přes kterou se má sčítat, prázdná, definuje se hodnota sumy jako 0, tedy například

$$\sum_{i=1}^{0}(i+10) = 0\,, \qquad \sum_{\substack{i\in\{2,4,6,8\}\\ i \text{ liché}}} i^4 = 0.$$

Podobný „množinový zápis“ můžeme uplatnit i pro součiny. Prázdný součin, například $\prod_{j;2\le j<1} 2^j$, se definuje jako 1 (tedy ne 0 jako pro prázdnou sumu).

Operace s množinami. Pomocí primitivního pojmu náležení, $\in$, můžeme definovat další vztahy mezi množinami a operace s nimi. Tak například dvě množiny X a Y budeme pokládat za stejné (totožné), jestliže mají stejné prvky. V tom případě budeme psát $X = Y$.

Vztah $X = Y$ tedy definujeme pomocí platnosti výroku „pro každý prvek x platí: $x \in X$, právě když $x \in Y$“. Tento výrok můžeme symbolicky zapsat

$$\forall x : (x \in X \Leftrightarrow x \in Y),$$

ale tímto směrem se nebudeme ubírat. Formální (formalizované) teorii množin jsou věnovány jiné texty (v češtině např. kniha Balcara a Štěpánka [4]).

Podobným způsobem můžeme definovat další množinové vztahy. Jsou-li X, Y množiny, znamená $X \subseteq Y$ (slovy „X je podmnožinou Y“) to, že každý prvek X je také prvkem Y.

Pomocí $X \subset Y$ se někdy vyznačuje, že X je podmnožina Y, přičemž ale X není rovno Y. Toto značení nebývá v literatuře zcela jednotné.

Průnik množin X a Y, čili množinu všech prvků náležejících zároveň do X i do Y, píšeme $X \cap Y$. Zápis $X \cup Y$ znamená *sjednocení* X a Y, což je množina všech prvků ležících v X nebo v Y (či v obou zároveň!). Chceme-li vyznačit, že sjednocujeme disjunktní množiny X a Y (tj. $X \cap Y = \emptyset$), píšeme $X \dot\cup Y$. Výraz $X \setminus Y$ je *rozdíl* množin X a Y, tj. množina všech prvků ležících v X a nikoliv v Y.

Zvětšené symboly $\cup$ a $\cap$ se používají podobně jako symboly $\sum$ a $\prod$. Jsou-li tedy $X_1, \ldots, X_n$ množiny, můžeme jejich sjednocení napsat

$$\bigcup_{i=1}^{n} X_i \tag{1.1}$$

a podobně pro průnik.

Uvědomte si, že tento zápis je možný (nebo korektní, správný) jen díky tomu, že operace sjednocení a průniku množin jsou *asociativní*. Jinými slovy, že platí (pro každou trojici množin X, Y, Z) vztahy

$$X \cap (Y \cap Z) = (X \cap Y) \cap Z,$$

$$X \cup (Y \cup Z) = (X \cup Y) \cup Z.$$

V důsledku toho nezávisí na způsobu „uzávorkování“ sjednocení (libovolných) tří, a obecně n, množin, takže můžeme společnou hodnotu označit symbolem (1.1). Operace $\cup$ a $\cap$ jsou ovšem i *komutativní*, neboli splňují vztahy

$$X \cap Y = Y \cap X,$$

$$X \cup Y = Y \cup X.$$

Komutativita a asociativita operací $\cup$ a $\cap$ je doplněna ještě jejich *distributivitou:*

Jestliže X, Y, Z jsou množiny, potom platí:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),$$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

Platnost těchto vztahů můžeme ověřit např. pomocí Vennova diagramu pro příslušné tři množiny. Zmíněné vztahy je možno zobecnit na více množin (dokážou se indukcí, viz oddíl 1.3). Např. takto

$$A \cap \left(\bigcup_{i=1}^{n} X_i\right) = \bigcup_{i=1}^{n} (A \cap X_i) \quad \text{nebo}$$

$$A \cup \left(\bigcap_{i=1}^{n} X_i\right) = \bigcap_{i=1}^{n} (A \cup X_i)$$

Jiné populární vztahy pro množiny jsou

$$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B) \quad \text{a} \quad X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B)$$

(tzv. *de Morganovy vzorce*), a jejich zobecnění na více množin

$$X \setminus \left(\bigcup_{i=1}^{n} A_i \right) = \bigcap_{i=1}^{n} (X \setminus A_i)$$

$$X \setminus \left(\bigcap_{i=1}^{n} A_i \right) = \bigcup_{i=1}^{n} (X \setminus A_i).$$

Cvičení

1. Které z následujících vztahů jsou správné?
   (a) $\lfloor \frac{(n+1)^2}{2} \rfloor = \lfloor \frac{n^2}{2} \rfloor + n$,
   (b) $\lfloor \frac{n+k}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + \lfloor \frac{k}{2} \rfloor$,
   (c) $\lceil (\lfloor x \rfloor) \rceil = \lceil x \rceil$ (pro reálné číslo x),
   (d) $\lceil (\lfloor x \rfloor + \lfloor y \rfloor) \rceil = \lfloor x \rfloor + \lfloor y \rfloor$.

2. (a) Pro která přirozená čísla n je pravda, že jejich zápis v desítkové soustavě má $\lceil \log_{10} n \rceil$ číslic?
   (b) Najděte „správnou“ formuli pro počet číslic v desítkovém zápisu čísla n.

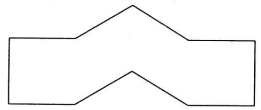
3.* Dokažte, že pro každé reálné číslo $x > 0$ platí $\lfloor \sqrt{x} \rfloor = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$.

4. Zapište výraz $\bigcap_{i=1}^{n} \bigcup_{j=1}^{m} A_{ij}$ jako sjednocení průniků.

5. (a) Podejte definici „uzávorkování“ pro sjednocení n množin $\bigcup_{i=1}^{n} X_i$ a „uzávorkování“ pro součet n čísel $\sum_{i=1}^{n} a_i$.
   (b) Dokažte, že každá dvě uzávorkování výrazu $\bigcap_{i=1}^{n} X_i$ dávají stejný výsledek.
   (c) Kolika způsoby lze uzávorkovat sjednocení 4 množin $A \cup B \cup C \cup D$?
   (d)** Pokuste se odvodit, kolika způsoby lze uzávorkovat sjednocení n množin $\bigcup_{i=1}^{n} X_i$.

6. Je pravda, že pro každé dvě množiny X a Y platí $2^X = 2^Y$, právě když $X = Y$?

7. Na následující úloze si můžete otestovat svou schopnost nacházet jednoduchá leč skrytá řešení. Rozdělte následující obrazec na 7 navzájem shodných částí (všechny ohraničující úsečky mají délku 1 a úhly jsou 90, 120 a 150 stupňů).



1.3 Matematická indukce

Řekněme, že chceme spočítat třeba součet

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n = \sum_{i=0}^{n} 2^i$$

(a že si nevybavujeme vzorec pro součet geometrické posloupnosti). Výpočtem číselných hodnot pro několik malých hodnot n můžeme odhalit, že uvedený součet bude nejspíš roven $2^{n+1} - 1$. I kdybychom to ale ověřili na počítači pro miliony konkrétních hodnot n, nebude to ještě důkaz. Správnost tohoto vztahu pro všechna n se dá ukázat tzv. *matematickou indukcí* (jiný používaný název je *úplná indukce*). V tomto případě bychom postupovali takto:

1. Vztah $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ je správný pro $n = 1$, jak se přesvědčíme dosazením.

2. Předpokládejme, že uvedený vztah platí pro nějakou hodnotu $n = n_0$. Dokážeme, že platí i pro $n = n_0 + 1$. Skutečně,

$$\sum_{i=0}^{n_0+1} 2^i = \left(\sum_{i=0}^{n_0} 2^i \right) + 2^{n_0+1};$$

   suma v závorce je podle předpokladu rovna $2^{n_0+1} - 1$, takže

$$\sum_{i=0}^{n_0+1} 2^i = 2^{n_0+1} - 1 + 2^{n_0+1} = 2 \times 2^{n_0+1} - 1 = 2^{n_0+2} - 1.$$

   To je ale požadovaný vztah pro $n = n_0 + 1$.

Tím jsme dokázali platnost vztahu pro libovolné n: Podle kroku 1 totiž vztah platí pro $n = 1$, podle kroku 2 platí i pro $n = 2$ (použijeme krok 2 s $n_0 = 1$), opět podle kroku 2 platí pro $n = 3, \ldots$, a takto můžeme pokračovat libovolně daleko.

Krok 2 v tomto typu důkazu se jmenuje *indukční krok*. Předpoklad, že dokazované tvrzení již platí pro nějaké $n = n_0$, se nazývá *indukční předpoklad*.

Obecně se princip matematické indukce dá formulovat například takto:

1.3.1 Tvrzení. *Nechť X je množina přirozených čísel, pro niž platí:*

(i) Číslo 1 je prvkem X.

(ii) Je-li číslo n prvkem X, potom rovněž číslo $n + 1$ je prvkem X.

Potom X je množina všech přirozených čísel (tedy $X = \mathbf{N}$).

V aplikacích bude X množina všech n, pro něž platí dokazované tvrzení.

Schéma důkazu indukcí má mnoho různých obměn. Například, chceme-li nějaké tvrzení dokazovat pro všechna $n \geq 2$, bude první krok důkazu patrně ověření platnosti tvrzení pro $n = 2$. Jako indukční předpoklad můžeme někdy využívat nejen platnosti tvrzení pro $n = n_0$, ale i pro všechna $n \leq n_0$. A tak dále.

Matematickou indukci můžeme pokládat buď za základní vlastnost přirozených čísel (tj. axiom, který nedokazujeme), nebo ji můžeme dokázat z jiné základní vlastnosti (axiomu), totiž že každá neprázdná podmnožina přirozených čísel má nejmenší prvek (to se vyjadřuje obratem, že uspořádání přirozených čísel podle velikosti je *dobré uspořádání*).

Důkaz tvrzení 1.3.1 z vlastnosti dobrého uspořádání: Předpokládejme pro spor, že X splňuje (i) a (ii), ale neobsahuje všechna přirozená čísla. Nechť tedy přirozené číslo n nenáleží X. Mezi všemi takovými přirozenými čísly n (nenáležejícími X) zvolme číslo nejmenší a označme ho n_0. Podle podmínky (i) víme, že $n_0 > 1$, a protože n_0 bylo minimální, je číslo $n_0 - 1$ prvkem množiny X. Použitím (ii) však dostaneme, že n_0 je prvkem X, což je spor. □

Poznamenejme, že tento typ úvahy, kde řekneme „Nechť n_0 je nejmenší číslo, pro které dokazované tvrzení neplatí“ a odvodíme spor – jmenovitě že musí existovat ještě menší číslo, pro nějž tvrzení neplatí – někdy nahrazuje matematickou indukci. Oba způsoby (právě zmíněný a matematická indukce) v podstatě dělají totéž a který z nich použijeme je hlavně věc vkusu.

Matematickou indukci budeme často používat, bude to jeden z našich základních důkazových prostředků. Spoustu příkladů a cvičení na indukci najde tedy čtenář v dalších kapitolách.

Cvičení

1. Dokažte indukcí vztahy
   (a) $1 + 2 + 3 + \cdots + n = n(n + 1)/2$
   (b) $\sum_{i=1}^{n} i2^i = (n - 1)2^{n+1} + 2$.

2. Čísla $F_0, F_1, F_2, \ldots$ jsou zadána takto: $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ pro $n = 0, 1, 2, \ldots$. Dokažte, že pro každé $n \geq 0$ platí
   $$F_n \leq ((1 + \sqrt{5})/2)^{n-1}$$
   (viz též část 12.3).

3. (a) Nakresleme n přímek v rovině tak, že žádné 2 nejsou rovnoběžné a žádné 3 se neprotínají v jednom bodě. Dokažte, že rovina je tím rozdělena na přesně $n(n + 1)/2 + 1$ částí.
   (b)* Podobně uvažte n rovin v třírozměrném prostoru, z nichž každé 3 mají právě jeden společný bod a žádné 4 nemají společný bod. Zjistěte, na kolik oblastí rozdělují prostor.

4. Dokažte indukcí *de Moivreovu větu*:
   $$(\cos\alpha + \mathrm{i}\sin\alpha)^n = \cos(n\alpha) + \mathrm{i}\sin(n\alpha)$$
   (kde i je imaginární jednotka, $\mathrm{i}^2 = -1$).

5.* Nechť $M \subseteq \mathbf{R}$ je množina reálných čísel taková, že každá její neprázdná podmnožina má nejmenší prvek a také největší prvek. Dokažte, že M je nutně konečná.

6. Dokážeme indukcí následující tvrzení: *Nechť $p_1, p_2, \ldots, p_n$ je $n \geq 2$ různých přímek v rovině, žádné 2 nejsou rovnoběžné. Potom všechny tyto přímky mají společný bod.*

   1. Pro $n = 2$ tvrzení platí, protože každé 2 různoběžné přímky se protínají.

   2. Nechť tvrzení platí pro $n = n_0$, mějme $n = n_0+1$ přímek $p_1, \ldots, p_n$. Podle indukčního předpokladu mají všechny přímky kromě poslední, tj. $p_1, p_2, \ldots, p_{n-1}$, společný nějaký bod, označme jej x. Podobně přímky $p_1, p_2, \ldots, p_{n-2}, p_n$ mají společný bod, označíme jej y. Přímka p_1 leží v obou skupinách, proto obsahuje jak x, tak y. Totéž platí pro přímku p_{n-2}. Poněvadž jsou p_1 a p_{n-2} podle předpokladu různoběžné a tedy se protínají jen v jednom bodě, platí $x = y$. Tedy všechny přímky $p_1, \ldots, p_n$ mají společný bod.

   Kde je zádrhel?

7. Obyvatelé staroegyptské říše zapisovali zlomky jako součty zlomků s čitatelem 1 a s navzájem různými jmenovateli, např. $\frac{3}{5} = \frac{1}{2} + \frac{1}{10}$. Uvažte následující algoritmus pro zápis zlomku $\frac{m}{n}$ v tomto tvaru ($1 \leq m < n$): napiš zlomek $\frac{1}{\lceil n/m \rceil}$, vypočítej zlomek $\frac{m}{n} - \frac{1}{\lceil n/m \rceil}$, a je-li nenulový, vyjádři jej v požadovaném tvaru týmž algoritmem. Dokažte, že tento algoritmus vždy skončí.

1.4 Relace

Je pozoruhodné, jak mnoho matematických pojmů je možno vyjádřit pomocí množin a rozličných množinových konstrukcí. Je to nejen pozoruhodné, ale i překvapivé, neboť teorie množin, a dokonce pojem množiny, jsou pojmy zařazené do matematiky vlastně nedávno, a ještě před 100 lety byla teorie odmítána i některými předními vědci. Dnes se však teorie množin stala součástí běžného matematického vyjadřování, stala se jazykem matematiky (a matematiků), jazykem, který napomohl chápat současnou matematiku při vší její různorodosti jako jeden celek se společnými základy.

Ukažme si, jak pomocí nejjednodušších množinových prostředků můžeme definovat další matematické pojmy.

Jestliže x a y jsou prvky (nějaké množiny), potom symbol $\{x, y\}$ označuje množinu obsahující právě prvky x a y, a nazývá se *neuspořádaná dvojice* prvků x a y. Připomeňme, že $\{x, y\}$ je totéž jako $\{y, x\}$,

a pokud $x = y$, potom $\{x, y\}$ je jednoprvková množina.

Zavedeme rovněž označení (x, y) pro *uspořádanou dvojici* prvků x a y. Při této konstrukci závisí na pořadí prvků x a y. Předpokládáme tedy, že platí

$$(x, y) = (z, t) \text{ právě když } x = z \text{ a } y = t. \tag{1.2}$$

Je zajímavé, že uspořádanou dvojici lze již vytvořit pomocí pojmu neuspořádané dvojice, následovně:

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

Ověřte, že takto definované uspořádané dvojice splňují podmínku (1.2). V tomto textu však bude pro nás jednodušší považovat (x, y) za další primitivní (tedy známý) pojem.

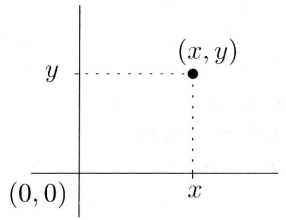
Podobně definujeme *uspořádanou n-tici* prvků $x_1, \ldots, x_n$, již označujeme[4] $(x_1, \ldots, x_n)$.

1.4.1 Definice. *Nechť X a Y jsou množiny. Symbolem $X \times Y$ označíme množinu všech uspořádaných dvojic tvaru (x, y), kde $x \in X$ a $y \in Y$. Formálně zapsáno*

$$X \times Y = \{(x, y);\ x \in X,\ y \in Y\}.$$

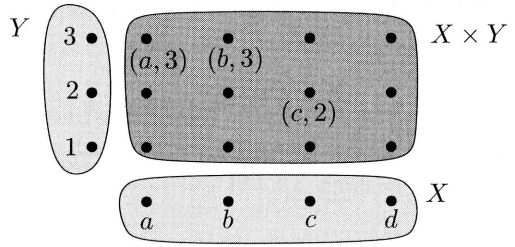
$X \times Y$ se nazývá (kartézský) součin *množin X a Y.*

Název „kartézský součin" pochází z geometrické interpretace (a původně tedy ze jména Descartes): Když např. $X = Y = \mathbf{R}$, potom $X \times Y$ můžeme interpretovat jako všechny body roviny, a v tomto případě x a y jsou (kartézské) souřadnice bodu (x, y) roviny:



[4] Stejný zápis používáme i pro n-rozměrný vektor se složkami $x_1, \ldots, x_n$, jsou-li x_i např. reálná nebo komplexní čísla.

Tohoto názoru používáme nejenom pro číselné množiny, ale například i pro kartézský součin konečných množin:



Kartézský součin $X \times X$ někdy zapisujeme jako mocninu, tj. X^2, a podobně $X^3 = X \times X \times X$ atd.

Dostáváme se nyní k jednomu z klíčových pojmů celé matematiky. Pojem relace, který nyní zavedeme, zobecňuje tak rozdílné pojmy, jako jsou ekvivalence, funkce a uspořádání.

1.4.2 Definice. Relace[5] *R je množina uspořádaných dvojic. Jsou-li X a Y množiny, nazývá se libovolná podmnožina kartézského součinu $X \times Y$* relací mezi X a Y. *Zdaleka nejdůležitější případ je $X = Y$, v takovém případě mluvíme o* relaci na X, *což je tedy libovolná podmnožina $R \subseteq X^2$.*

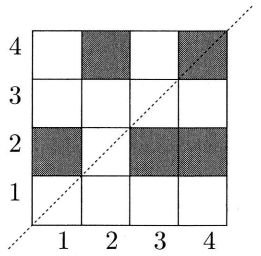
Náleží-li dvojice (x, y) relaci R, tj. $(x, y) \in R$, říkáme také, že x a y *jsou v relaci* R, a zapisujeme též xRy.

Jako relace v tomto smyslu můžeme interpretovat některé čtenáři dobře známé symboly. Tak například, „=“ (rovnost) i „$\geq$“ (neostrá nerovnost) jsou relace na množině $\mathbf{N}$ všech přirozených čísel. První z nich sestává z dvojic $(1,1), (2,2), (3,3), \ldots$, druhá z dvojic $(1,1), (2,1), (2,2), (3,1), (3,2), (3,3), (4,1), \ldots$. Mohli bychom tedy psát i třeba $(5,2) \in \geq$ místo $5 \geq 2$, což ovšem neděláme. Všimněte si, že jsme museli říci, na jaké množině např. relaci $\geq$ uvažujeme; jako relace třeba na $\mathbf{R}$ by to byla jiná množina dvojic.

Slovo „relace“ pochází z kořene znamenajícího „(příbuzenský) vztah“. Příbuzenské vztahy (např. „býti matkou“, „býti otcem“, „býti sourozencem“) skutečně poskytují řadu (netriviálních) příkladů relací na množině všech lidí.

[5]Obšírněji *binární relace* (poněvadž dává do vztahu dvojice prvků). Někdy se definují i relace n-ární pro $n > 2$.

Relaci R na množině X můžeme obrázkově vystihnout dvěma naprosto rozdílnými způsoby. Pro relaci $R = \{(1,2), (2,4), (3,2), (4,2), (4,4)\}$ na množině $\{1,2,3,4\}$ dává první způsob takovýto obrázek:



Čtvercová políčka odpovídají uspořádaným dvojicím v kartézském součinu, a pro dvojice náležející do relace jsme příslušná políčka vybarvili. V tomto obrázku zdůrazňujeme definici relace na X a vystihujeme její „celkový tvar“.

Tento obrázek má rovněž velmi blízko k alternativnímu popisu relace na množině X pomocí pojmu matice[6]. Jestliže R je relace na nějaké n-prvkové množině $X = \{x_1, \ldots, x_n\}$, potom R je úplně popsána $n \times n$ maticí $A = (a_{ij})$, kde

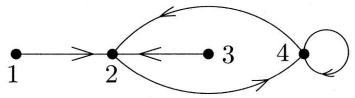
$$\begin{aligned} a_{ij} &= 1 \quad \text{jestliže } (x_i, x_j) \in R \\ a_{ij} &= 0 \quad \text{jestliže } (x_i, x_j) \notin R. \end{aligned}$$

Matici A nazýváme *matice sousednosti* relace R. Například, pro relaci R zobrazenou výše je příslušná matice sousednosti (pro $x_i = i$, $i = 1,2,3,4$)

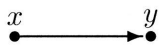
$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Jiný způsob znázornění téže relace je takovýto:

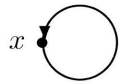
[6]Matice $n \times m$ je obdélníková tabulka čísel s n řádky a m sloupci; viz dodatek o algebře.



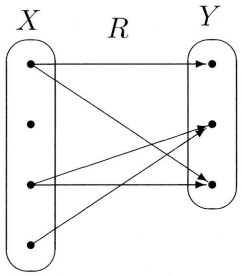
Puntíky odpovídají jednotlivým prvkům množiny X. Skutečnost, že daná uspořádaná dvojice prvků (x, y) náleží relaci R, vyznačíme nakreslením šipky z x do y:



a v případě $x = y$ smyčkou

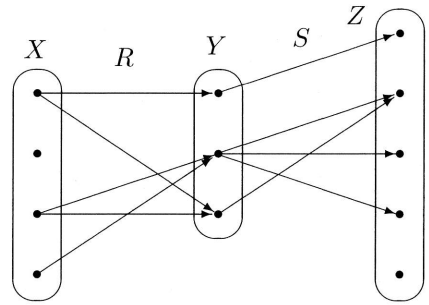


Oba způsoby znázornění budeme v dalším používat. Podobně můžeme znázorňovat relaci mezi X a Y, například takto:



Skládání relací. Nechť X, Y, Z jsou množiny, $R \subseteq X \times Y$ nějaká relace mezi X a Y, a $S \subseteq Y \times Z$ relace mezi Y a Z. *Složením relací* R *a* S nazveme relaci $T \subseteq X \times Z$, definovanou následovně: xTz (pro $x \in X$, $z \in Z$) platí právě tehdy, když existuje nějaké $y \in Y$ takové, že xRy a ySz. Složení relací R a S se značí zpravidla $R \circ S$.

Skládání relací se dá dobře schematicky znázornit pomocí šipek. Na následujícím obrázku bude dvojice (x, z) v relaci $R \circ S$, kdykoli lze z x do z projít po šipkách (přes nějaké $y \in Y$):



Všimněme si, že složení není definováno pro každé 2 relace: abychom mohli skládat, musí mít relace společnou „prostřední“ množinu (již jsme v definici značili Y). Jsou-li však R i S relace na téže množině X, je jejich složení vždy dobře definováno. I v tomto případě výsledek skládání relací záleží na pořadí; $R \circ S$ je obecně něco jiného než $S \circ R$, viz cvičení 2.

Cvičení

1. Popište relaci $R \circ R$, označuje-li R
   (a) relace rovnosti „=“ na množině $\mathbf{N}$ všech přirozených čísel,
   (b) relaci „menší nebo rovno“ („$\leq$“) na $\mathbf{N}$,
   (c) relaci „ostře menší“ („$<$“) na $\mathbf{N}$,
   (d) relaci „ostře menší“ („$<$“) na množině $\mathbf{R}$ všech reálných čísel.
2. Najděte relace R a S na nějaké množině X takové, že $R \circ S \neq S \circ R$.
3. Pro relaci R na množině X definujeme indukcí symbol R^n: $R^1 = R$, $R^{n+1} = R \circ R^n$.
   (a) Ukažte, že je-li X konečná množina a R relace na ní, potom existují $r, s \in \mathbf{N}$, $r < s$ taková, že $R^r = R^s$.
   (b) Najděte relaci R na konečné množině takovou, že $R^n \neq R^{n+1}$ pro každé $n \in \mathbf{N}$.
   (c) Ukažte, že je-li X nekonečná, tvrzení (a) platit nemusí (tj. existuje relace R taková, že všechny relace tvaru R^n jsou navzájem různé).

1.5 Funkce

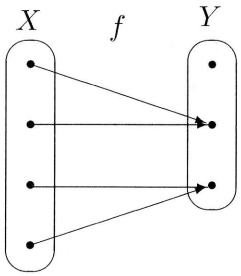
Pojem funkce je jeden ze základních pojmů v matematice. Trvalo dlouho, než se dospělo k dnešnímu chápání funkce (jakožto speciálního typu

relace); například v době, kdy byl objeven diferenciální počet, se uvažovaly pouze reálné nebo komplexní funkce, a „poctivá“ funkce musela být vyjádřena nějakou formulí nebo součtem nekonečné řady (jako třeba $f(x) = x^2 + 4$, $f(x) = \sqrt{\sin(x/\pi)}$, nebo $f(x) = \int_0^x (\sin t/t)\mathrm{d}t$, $f(x) = \sum_{n=0}^{\infty}(x^n/n!)$). To, že například reálná funkce může přiřazovat každému reálnému číslu nějaké zcela libovolné reálné číslo, je celkem moderní vynález.

1.5.1 Definice. Funkce *z množiny X do množiny Y je relace $f \subseteq X \times Y$, splňující dodatečnou podmínku, že pro každý prvek $x \in X$ existuje právě jediný prvek $y \in Y$ tak, že xfy.*

Místo „funkce“ se také říká „zobrazení“[7].

Při znázornění relace pomocí šipek předchozí definice znamená, že z každého bodu množiny X vychází právě jedna šipka, jako na následujícím obrázku:



To, že f je funkce z množiny X do množiny Y, zapisujeme takhle:

$$f : X \to Y.$$

A to, že funkce f přiřazuje nějakému prvku x jistý prvek y, zapisujeme

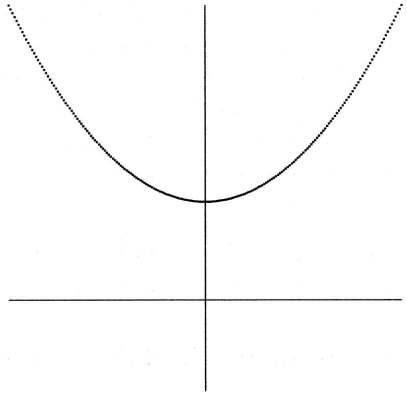
$$f : x \mapsto y.$$

Tento symbol je výhodný, chceme-li mluvit o nějaké funkci aniž bychom ji pojmenovali, například „uvažme funkci $x \mapsto 3a\sin(bx)$“ (z tohoto

[7] V některých odvětvích matematiky se slovo funkce rezervuje pro funkci do reálných (nebo komplexních) čísel, a slovo zobrazení se používá pro funkce do libovolné množiny. Pro nás budou „funkce“ a „zobrazení“ synonyma.

zápisu je vidět, že míníme zkoumat závislost na x a nikoli na a nebo na b).

Funkce, jakožto podmnožina kartézského součinu $X \times Y$, se také kreslí pomocí *grafu*. To je způsob znázornění, který se nejvíce používá na střední škole i v matematické analýze. Následující obrázek to ukazuje pro funkci $f : \mathbf{R} \to \mathbf{R}$ danou předpisem $f(x) = x^2 + 1$:



Pro funkce se ovšem nepoužívá značení, zavedeného pro relace. Je-li $f \subseteq X \times Y$ relace, která je funkcí, $f(x)$ označuje to jediné $y \in Y$, pro něž xfy. Dále, množinu $\{f(x);\, x \in X\}$ označujeme $f(X)$.

Zavádějí se i další termíny (X je *definiční obor*, Y je *obor hodnot*), ale v tomto textu se snažíme používat minimálně formalismu a terminologie.

Skládání funkcí. Funkce se skládají stejně jako relace, ale používá se přitom jiné značení! Definici skládání funkcí můžeme odvodit ze skládání relací, pro jistotu ji zformulujme:

1.5.2 Definice. *Jsou-li $f : X \to Y$ a $g : Y \to Z$ funkce, potom můžeme definovat novou funkci $h : X \to Z$ předpisem*

$$h(x) = g(f(x))$$

pro každé $x \in X$.

Funkce h (přesvědčete se, že h je opravdu funkce) se nazývá složení funkcí g a f *a značí se* $g \circ f$. *Tedy platí*

$$\big(g \circ f\big)(x) = g(f(x))$$

pro každý prvek $x \in X$.

Tady je zmíněná odlišnost od skládání relací. Pro *relace* je zvykem psát skládání „zleva doprava", pro funkce „zprava doleva". Jsou-li tedy $f : X \to Y$ a $g : Y \to Z$ funkce, jejich složení zapíšeme $g \circ f$, kdybychom je ale chápali jako *relace*, psali bychom pro totéž $f \circ g$! Oba zápisy mají své důvody, takto se značení historicky ustálilo a nemá asi smysl se snažit ho měnit. K nejasnostem by dojít nemělo. V tomto textu budeme téměř výhradně mluvit o skládání funkcí.

Skládání funkcí je asociativní, ale není komutativní. Má-li $g \circ f$ smysl, potom $f \circ g$ nemusí být vůbec definováno.

1.5.3 Definice (Důležité druhy funkcí). *Funkci $f : X \to Y$ nazýváme*

- prostá funkce, *jestliže pro $x \neq y$ je $f(x) \neq f(y)$,*
- funkce na, *jestliže pro každé $y \in Y$ existuje $x \in X$ splňující $f(x) = y$,*
- vzájemně jednoznačná funkce, *jestliže f je prostá a na.*

Cizími slovy se funkce na nazývá *surjektivní* (z francouzštiny, čte se „syrjektivní"), prostá funkce je *injektivní*, a vzájemně jednoznačná funkce se jmenuje *bijektivní* nebo *bijekce*. „Bijekce" je pro svou krátkost možná vhodnější termín než „vzájemně jednoznačná funkce".

V obrázkovém znázornění funkce pomocí šipek se tyto druhy funkcí poznají takto:

- pro prostou funkci vchází do každého bodu $y \in Y$ *nejvýš jedna* šipka,
- pro funkci na vchází do každého bodu $y \in Y$ *aspoň jedna* šipka,

- pro bijekci vchází do každého bodu $y \in Y$ *právě jedna* šipka.

Jak už jsme řekli, funkci f z X do Y značíme $f : X \to Y$. Fakt, že funkce f je prostá, vyznačujeme někdy zápisem

$$f : X \hookrightarrow Y,$$

funkci f, která je *na*, značíme

$$f : X \twoheadrightarrow Y,$$

a konečně funkci vzájemně jednoznačnou značíme

$$f : X \hookrightarrow\!\!\!\!\!\!\rightarrow Y.$$

(Tohle značení není v literatuře příliš běžné.)

Platí následující:

1.5.4 Tvrzení. *Nechť $f : X \to Y$ a $g : Y \to Z$ jsou funkce.*

(i) Jsou-li f, g prosté funkce, je rovněž $g \circ f$ funkce prostá;

(ii) Jsou-li f, g funkce na, *je rovněž $g \circ f$ funkce* na;

(iii) Jsou-li f, g funkce vzájemně jednoznačné, je rovněž $g \circ f$ funkce vzájemně jednoznačná.

(iv) Pro každou funkci $f : X \to Y$ existuje množina Z, prostá funkce $h : Z \hookrightarrow Y$ a funkce na *$g : X \twoheadrightarrow Z$ tak, že $f = h \circ g$. (Tedy každou funkci lze napsat jako složení funkce prosté a funkce na.)*

Důkaz. Části (i), (ii), (iii) se dostanou přímým ověřením definice. Dokažme např. (ii). Zvolme $z \in Z$, hledáme $x \in X$ splňující $\big(g \circ f\big)(x) = z$. Protože g je funkce *na*, existuje nejprve $y \in Y$ tak, že $g(y) = z$. A protože f je funkce *na*, existuje poté $x \in X$ splňující $f(x) = y$. Takový x je hledaný prvek splňující $\big(g \circ f\big)(x) = z$.

Nejzajímavější je bod (iv). Buď $Z = f(X) = \{f(x);\, x \in X\}$ (je tedy $Z \subseteq Y$). Definujme zobrazení $g : X \to Z$ a $h : Z \to Y$ předpisem:

$$\begin{aligned} g(x) &= f(x) \quad \text{pro } x \in X \\ h(z) &= z \quad\;\; \text{pro } z \in Z. \end{aligned}$$

Zřejmě g je funkce *na* (čili $g : X \twoheadrightarrow Z$), h je funkce prostá (čili $h : Z \hookrightarrow Y$) a $f = h \circ g$. □

Cvičení

1. Ukažte, že je-li X konečná množina, potom funkce $f : X \to X$ je prostá, právě když je na.
2. Najděte příklad
   (a) prosté funkce $f : \mathbf{N} \hookrightarrow \mathbf{N}$, která není na,
   (b) funkce $f : \mathbf{N} \twoheadrightarrow \mathbf{N}$ (na), která není prostá.
3. Označme $i_X : X \to X$ funkci, která zobrazuje každý prvek množiny X na něj samotný (tato funkce se nazývá *identická* nebo *identita* na X). Nechť $f : X \to Y$ je nějaká funkce. Ukažte, že
   (a) funkce $g : Y \to X$ taková, že $g \circ f = i_X$, existuje právě když f je prostá.
   (b) funkce $g : Y \to X$ taková, že $f \circ g = i_Y$, existuje právě když f je na.
4. (a) Je-li $g \circ f$ funkce na, musí g být na? Musí f být na?
   (b) Je-li $g \circ f$ prostá funkce, musí g být prostá? Musí f být prostá?

1.6 Další druhy relací, zvláště ekvivalence

Každý jazyk má své zvláštnosti. Některé jazyky milují samohlásky, jiné souhlásky (mezi ně asi patří čeština) a ještě jiné se vyznačují spřežkami. Některé jsou jednoduché z hlediska gramatiky, u jiných se snadno učí výslovnost. Podobně tomu je i v matematice. Sám matematický jazyk má své podstatné vlastnosti (je přesný a záleží v něm snad až příliš na detailech), ale i jednotlivé části matematiky se odlišují stylem a jazykem. Tak například pro algebru se zdá být typické množství pojmů a definic, které se zpravidla vyskytují na počátku, předtím než se přikročí k vlastnímu studiu. Mnoho z těchto pojmů se však vyskytuje i při studiu jiných disciplín a patří do jazykového fondu celé matematiky. Zde uvedeme takový příklad tvorby pojmů. Tato část náleží do obecné algebry a týká se různých druhů relací.

V odstavci 1.5 nám již speciální relace posloužily k definici pojmu funkce. Nyní zavedeme další 4 druhy.

1.6.1 Definice. *Řekneme, že relace R na množině X je*

- reflexivní, *jestliže pro každé $x \in X$ platí xRx,*
- symetrická, *jestliže kdykoli xRy, pak i yRx,*
- antisymetrická, *jestliže pro každé $x, y \in X$ platí, že pokud xRy a zároveň yRx, potom $x = y$,*
- transitivní, *jestliže ze vztahů xRy a yRz plyne xRz.*

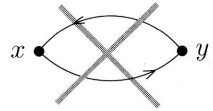
Samozřejmě jsme mohli zavést i další druhy, ale vystačíme si s uvedenými 4 druhy a jejich rozličnými kombinacemi.

Ve znázornění jako str. 37 obsahuje reflexivní relace všechny čtverečky na diagonále, a ve znázornění se šipkami má smyčky u všech bodů.

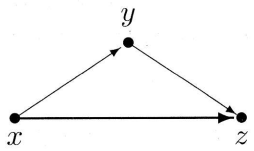
Obrázek jako str. 37 pro symetrickou relaci je symetrický podle diagonály. Ve znázornění pomocí šipek jdou vždy šipky oběma směry:



Pro antisymetrickou relaci naopak víme, že se v ní takový obrázek nevyskytuje:



Podmínka transitivity se dá dobře vyjádřit pomocí šipek: jsou-li v relaci šipky $x \to y$ a $y \to z$, musí tam být i $x \to z$:



Uvedené znázornění zdůrazňuje skutečnost, že všechny 4 vlastnosti je možno snadno ověřit; jsou to vlastnosti definované pomocí dvouprvkových a tříprvkových podmnožin.

Vlastnosti z definice 1.6.1 můžeme rovněž zapsat pomocí operace skládání relací (zavedené v odstavci 1.4) a následujících dvou pojmů:

Pro relaci R definujeme relaci R^{-1} předpisem

$$R^{-1} = \{(y, x);\ (x, y) \in R)\}.$$

Nazýváme ji relace *inverzní* k relaci R.

Symbolem Δ_X označíme nejmenší reflexivní relaci na množině X:

$$\Delta_X = \{(x, x); x \in X\}.$$

Relace Δ_X se jmenuje *diagonála* (na množině X). Tento název je motivován maticovým znázorněním relace, uvedeném v části 1.4.

Použitím těchto nástrojů můžeme zapsat definici 1.6.1 krátce takto:

(1) R je reflexivní, jestliže $\Delta_X \subseteq R$.

(2) R je symetrická, jestliže $R = R^{-1}$.

(3) R je antisymetrická[8], jestliže $R \cap R^{-1} \subseteq \Delta_X$.

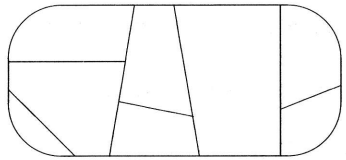
(4) R je transitivní, jestliže $R \circ R \subseteq R$.

Kombinací těchto pojmů dostaneme některé ze základních typů relací.

1.6.2 Definice.

- *Řekneme, že relace R na X je* ekvivalence *na X, jestliže je reflexivní, symetrická a transitivní (tj. ekvivalence splňuje (1), (2) a (4)).*
- *Řekneme, že relace R na X je* uspořádání *na X, jestliže je reflexivní, antisymetrická a transitivní (tj. uspořádání splňuje (1), (3) a (4)).*

[8]To, čemu my říkáme antisymetrická relace, se někdy v literatuře nazývá *slabě antisymetrická relace.*



Obrázek 1.1: Schematické znázornění relace ekvivalence na množině.

- *Řekneme, že relace R na X je* lineární uspořádání *na X, jestliže je to uspořádání a navíc $R \cup R^{-1} = X \times X$.*

Na první pohled se může zdát, že rozdíly v jednotlivých částech definic jsou nepodstatné, ale příklady přesvědčí každého snadno o opaku (viz rovněž cvičení 7): relace $(\mathbf{N}, =)$ (rovnost přirozených čísel) je ekvivalence, relace $(\mathbf{N}, |)$ (dělitelnost přirozených čísel) je uspořádání, relace $(\mathbf{N}, \leq)$ (nerovnost přirozených čísel) je lineární uspořádání.

Každé lineární uspořádání je také uspořádání, ale to je jediný vztah, který obecně platí pro uvedené tři druhy relací. Ve skutečnosti je podobnost pouze zdánlivá. Pojmy ekvivalence a uspořádání jsou tak vzdálené, že se studují odděleně. Učiníme tak i my. V tomto článku pojednáváme o ekvivalencích, zatímco uspořádáním a lineárním uspořádáním bude věnována kapitola 2.

O ekvivalencích. Pojem ekvivalence je střechový pojem pro všechny pojmy vyjadřující stejnost, podobnost, isomorfismus atd. Relace ekvivalence se zpravidla značí symboly jako $=, \equiv, \simeq, \approx, \cong, \pi, \rho$ a podobně.

Přestože ekvivalence R na množině X je speciální relace a můžeme ji tedy znázornit libovolným ze dvou výše uvedených způsobů, častěji se používá znázornění jako na obr. 1.1.

Klíčem k tomuto znázornění je následující pojem třídy ekvivalence: Nechť R je ekvivalence na množině X, nechť x je libovolný prvek množiny X. Označme symbolem $R[x]$ množinu všech prvků y, které jsou ekvivalentní s x, tj. $R[x] = \{y;\ xRy\}$. Toto $R[x]$ se nazývá *třída ekvivalence R určená prvkem x.*

1.6.3 Tvrzení. *Pro každou ekvivalenci R na X platí*

(i) $R[x]$ *je neprázdná množina pro každý prvek* $x \in X$.

(ii) Pro každé dva prvky x, y *množiny* X *platí buď* $R[x] = R[y]$, *nebo* $R[x] \cap R[y] = \emptyset$.

(iii) Třídy ekvivalence jednoznačně určují (popisují) relaci R.

Předtím, než přistoupíme k důkazu, bychom měli vysvětlit smysl bodu (iii). Přesný význam je následující: Jsou-li R a S dvě ekvivalence na množině X a platí-li pro každý prvek x množiny X rovnost $R[x] = S[x]$, potom $R = S$.

Důkaz je jednoduchý použitím všech tří požadavků v definici ekvivalence.

(i) Množina $R[x]$ vždy obsahuje prvek x, protože R je relace reflexivní.

(ii) Nechť x, y jsou dané prvky. Rozlišíme dvě možnosti:

(a) Jestliže xRy, potom dokážeme nejprve $R[x] \subseteq R[y]$. Skutečně, je-li $z \in R[x]$, potom víme rovněž že zRx (použitím symetrie relace R) a tudíž zRy (použitím transitivity R). Proto i $z \in R[y]$. Opětovným použitím symetrie R dostáváme, že z platnosti xRy plyne $R[x] = R[y]$.

(b) Nechť neplatí xRy. Ukážeme, že $R[x] \cap R[y] = \emptyset$. Postupujme sporem: Nechť existuje $z \in R[x] \cap R[y]$. Potom xRz a zRy (použitím symetrie R), a tedy xRy (opětovným použitím transitivity R), což je spor.

(iii) Tato část tvrzení je zřejmá, neboť třídy ekvivalence R určují R vztahem

$$xRy \text{ právě když } \{x, y\} \subseteq R[x].$$

□

Toto tvrzení vysvětluje obrázek 1.1. Podmnožiny dané množiny X, které jsou navzájem disjunktní a které obsahují (dohromady) všechny prvky, tvoří *rozklad množiny* X. Tvrzení 1.6.3 potom zaručuje, že třídy ekvivalence tvoří rozklad množiny a že vztah mezi všemi ekvivalencemi na dané množině X a všemi rozklady X je vzájemně jednoznačný.

Cvičení

1. Formulujte podmínky pro reflexivitu relace, pro symetrii relace a pro její transitivitu v řeči matice sousednosti relace.
2. Dokažte, že relace R na množině X je transitivní, právě když $R \circ R \subseteq R$.
3. Dokažte, že $R \cap R^{-1} = \Delta_X$, právě když R je reflexivní a antisymetrická.
4. (a) Dokažte, že pro libovolnou relaci R na nějaké množině X je relace $T = R \cup R \circ R \cup R \circ R \circ R \cup \ldots$ (sjednocení všech mnohonásobných složení R) transitivní.
   (b) Dokažte, že každá transitivní relace obsahující R obsahuje i T.
   (c) Dokažte, že je-li $|X| = n$, pak $T = R \cup R \circ R \cup \ldots \cup \underbrace{R \circ R \circ \ldots \circ R}_{(n-1)\times}$.
5. Nechť R a S jsou libovolné ekvivalence na množině X. Rozhodněte, které z následujících relací jsou nutně také ekvivalence.
   (a) $R \cap S$
   (b) $R \cup S$
   (c) $R \setminus S$
   (d) $R \circ S$.
   (e) $R^{-1} \circ S^{-1}$.
6. Nechť R a S jsou libovolná uspořádání na množině X. Rozhodněte, které z následujících relací jsou nutně také uspořádáními.
   (a) $R \cap S$
   (b) $R \cup S$
   (c) $R \setminus S$
   (d) $R \circ S$.
7. Dokažte, že Δ_X je jediná relace na množině X, která je současně ekvivalence i uspořádání.

8. Nechť R a S jsou relace na nějaké množině X. Řekneme, že R a S jsou *isomorfní*, pokud existuje bijekce $f: X \to X$ taková, že pro každé $x, y \in X$ platí xRy, právě když $f(x)Sf(y)$.

   (a) Vypište všechny možné relace na dvouprvkové množině $X = \{a, b\}$. Určete, které jsou navzájem isomorfní.

   (b) Dokažte, pro libovolnou množinu X je vztah „býti isomorfní“ ekvivalence na množině všech relací na X.

2

O uspořádaných množinách

Čtenář jistě zná lineární uspořádání přirozených čísel i dalších číselných oborů podle velikosti. Takové uspořádání se v matematice chápe jako speciální typ relace, tj. jako vztah dvojic čísel. Tato relace se ve zmíněném případě zpravidla označuje symbolem „$\leq$“ („menší nebo rovno“). I na jiných množinách, třeba na množině všech slov v nějakém jazyku, se zavádějí různá uspořádání, a tutéž množinu lze uspořádat mnoha způsoby.

Obecný pojem uspořádání jsme již zavedli v definici 1.6.2: Relace R se nazývá uspořádání, jestliže je reflexivní, antisymetrická a transitivní. Dodejme ještě, že je-li X množina a R uspořádání na X, říká se dvojici (X, R) *uspořádaná množina.*

Uspořádané množiny mají mnoho zajímavých vlastností. V této kapitole uvedeme některé z nich a k dalším se vrátíme později, např. v kapitole 7.

2.1 Uspořádání a jejich znázorňování

Začneme několika poznámkami k pojmu uspořádání. Pro relace uspořádání se často používají symboly $\preceq$ nebo $\leq$. První z nich je užitečný, chceme-li např. mluvit ještě o nějakém jiném uspořádání množiny přirozených čísel, než je obvyklé uspořádání podle velikosti, nebo uvažujeme-li nějaké obecné uspořádání na libovolné množině.

Máme-li nějaké uspořádání $\preceq$, definujeme odvozenou relaci „ostré nerovnosti“ $\prec$ takto: $a \prec b$, právě když $a \preceq b$ a $a \neq b$. Dále můžeme definovat „obrácenou nerovnost“, tj. relaci $\succeq$, vztahem $a \succeq b \Leftrightarrow b \preceq a$.

Lineární uspořádání a částečná uspořádání. Připomeňme, že relace R se nazývá lineární uspořádání, jestliže je to uspořádání a navíc pro každé x, y platí xRy nebo yRx. Lineární uspořádání se také někdy nazývá *úplné uspořádání*. Když se mluví o uspořádání, které nemusí být nutně lineární, říká se někdy obšírněji *částečné uspořádání*. Částečné uspořádání tedy znamená přesně totéž, co uspořádání (bez dalších přívlastků), a podobně místo uspořádaná množina se často říká *částečně uspořádaná množina*[1].

Příklady. Několik příkladů uspořádaných množin jsme už zmínili – byly to $(\mathbf{N}, \leq)$, $(\mathbf{R}, \leq)$ a podobně, kde $\leq$ značí obvyklé uspořádání podle velikosti (formálně chápané jako relace).

Jak se snadno ověří, jestliže je R uspořádání na nějaké množině X a Y je podmnožina X, potom relace $R \cap Y^2$ je uspořádání na Y (pomocí relace R porovnáváme prvky z Y a na ostatní zapomeneme). Tím máme další příklady uspořádaných množin, totiž všelijakých podmnožin reálných čísel. To je poměrně obecný příklad lineárně uspořádané množiny – viz cvičení 2.3.6.

Myšlenku seřazení slov ve slovníku podle abecedy formálně zachycuje pojem *lexikografického uspořádání* (česky „slovníkového“). Uvažme napřed speciální případ: buď $X = \mathbf{N} \times \mathbf{N}$ kartézský součin dvou kopií přirozených čísel, tj. množina všech uspořádaných dvojic (a_1, a_2), kde a_1 a a_2 jsou přirozená čísla. Na X definujeme relaci $\leq_{\text{lex}}$ lexikografického uspořádání následovně: $(a_1, a_2) \leq_{\text{lex}} (b_1, b_2)$, právě když $a_1 < a_2$ nebo když $a_1 = a_2$ a zároveň $a_2 \leq b_2$.

Obecněji, jsou-li $(X_1, \leq_1)$, $(X_2, \leq_2)$,..., $(X_n, \leq_n)$ libovolné lineárně uspořádané množiny, definujeme relaci $\leq_{\text{lex}}$ lexikografického uspořádání na kartézském součinu $X_1 \times X_2 \times \cdots \times X_n$ takto: máme

$$(a_1, a_2, \ldots, a_n) \leq_{\text{lex}} (b_1, b_2, \ldots, b_n),$$

[1] Což má i pěknou zkratku. Ostatně v angličtině se plný termín *partially ordered set* také zkracuje na umělé slovo *poset*.

pokud buď $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$, nebo existuje index i, $1 \leq i \leq n$, takový, že $a_j = b_j$ pro všechna $j < i$ a $a_i <_i b_i$. Čtenář snadno nahlédne, že uspořádání slov podle abecedy je příkladem lexikografického uspořádání v našem smyslu (i když při bližším pohledu jsou v tom drobné zádrhele, například slova jsou různě dlouhá, nemluvě o jemnůstkách jako že van Beethovena najdete ve slovníku pod B).

Příklady částečných uspořádání. Jak mohou vypadat uspořádání, která nejsou úplná? Jeden příklad je relace $\Delta_X = \{(x, x); x \in X\}$ (diagonála). Vyhovuje definici uspořádání, ale pro $|X| > 1$ to není uspořádání lineární.

Popišme zajímavější příklady částečně uspořádaných množin.

2.1.1 Příklad. *Představme si, že chceme koupit třeba ledničku. Složitou skutečnou situaci si zjednodušíme matematickou abstrakcí a předpokládáme, že u ledniček hledíme jen na 3 číselné parametry: cenu, spotřebu elektřiny a objem. Máme-li dva typy ledniček, a první typ je dražší, více spotřebuje a méně se do něj vejde, potom lze považovat druhý typ za lepší – na tom by se shodla asi velká většina kupců ledniček. Na druhé straně, někdo dá přednost menší a levnější ledničce, jiný preferuje větší, i když je dražší, a kdo očekává vzestup cen elektřiny, možná si koupí drahou ledničku s malou spotřebou. Relace „být jednoznačně horší“ (označíme ji $\preceq$) v tomto pojetí je tedy částečné uspořádání na ledničkách, matematicky formulováno na množině všech trojic (a, b, c) reálných čísel, definované takto:*

$$(a_1, b_1, c_1) \preceq (a_2, b_2, c_2) \Leftrightarrow a_1 \geq a_2,\ b_1 \geq b_2 \text{ a } c_1 \leq c_2. \tag{2.1}$$

Následující příklad jsme už zmínili, ale připomeňme jej:

2.1.2 Příklad. *Pro přirozená čísla a, b symbol $a|b$ znamená „a dělí b“, neboli že existuje přirozené číslo c takové, že $b = ac$. Relace „$|$“ (dělitelnost) je částečné uspořádání na $\mathbf{N}$ (k ověření už jsme čtenáře vyzývali).*

2.1.3 Příklad. *Nechť X je nějaká množina. Relace „$\subseteq$“ (býti podmnožinou) definuje částečné uspořádání na množině 2^X, tj. na systému všech podmnožin množiny X.*

Znázorňování částečně uspořádaných množin. Konečné částečně uspořádané množiny můžeme znázorňovat pomocí šipek jako kterékoliv jiné relace. V takových obrázcích bude typicky spousta šipek, například pro 10-prvkovou lineárně uspořádanou množinu bychom museli nakreslit $9 + 8 + \ldots + 1 = 45$ šipek a ještě 10 smyček. Řada šipek se ale dá zrekonstruovat z transitivity: Víme-li, že $x \preceq y$ a $y \preceq z$, potom už také $x \preceq z$ a šipku z x do z můžeme vynechat. Podobně není třeba kreslit smyčky. Pro konečné uspořádané množiny všechnu potřebnou informaci zachycuje relace „být bezprostředním předchůdcem“, kterou teď definujeme.

Nechť $(X, \preceq)$ je uspořádaná množina. Řekneme, že prvek x je *bezprostředním předchůdcem* prvku y, pokud platí

- $x \prec y$, a
- neexistuje žádné $t \in X$ takové, že $x \prec t \prec y$.

Právě zavedenou relaci bezprostředního předchůdce můžeme označit třeba $\lhd$.

Tvrzení, že uspořádání $\preceq$ lze rekonstruovat z relace $\lhd$, můžeme přesně formulovat takto:

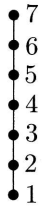
2.1.4 Tvrzení. *Nechť $(X, \preceq)$ je konečná uspořádaná množina a $\lhd$ je příslušná relace bezprostředního předchůdce. Potom pro libovolné dva prvky $x, y \in X$ platí $x \prec y$, právě když existují prvky $x_1, x_2, \ldots, x_k \in X$ takové, že $x \lhd x_1 \lhd \cdots \lhd x_k \lhd y$ (případně může být i $k = 0$, tj. přímo $x \lhd y$).*

Důkaz. Jedna implikace je snadno vidět: Máme-li $x \lhd x_1 \lhd \cdots \lhd x_k \lhd y$, potom podle definice bezprostředního předchůdce je i $x \prec x_1 \prec \cdots \prec x_k \prec y$, a z transitivity relace $\prec$ plyne $x \prec y$.

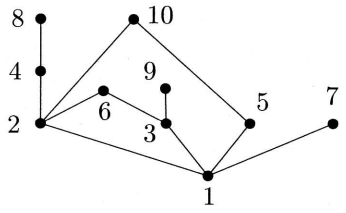
Ani opačná implikace není těžká, dokážeme ji indukcí. Budeme dokazovat toto: *Nechť $x, y \in X$, $x \prec y$, jsou dva prvky takové, že existuje nejvýš n prvků $t \in X$ splňujících $x \prec t \prec y$. Potom existují $x_1, x_2, \ldots, x_k \in X$ takové, že $x \lhd x_1 \lhd \cdots \lhd x_k \lhd y$.* Pro $n = 0$ předpoklad tohoto tvrzení říká, že neexistuje žádné t, $x \prec t \prec y$, a proto $x \lhd y$, čili tvrzení platí (volíme $k = 0$).

Nechť tvrzení platí pro všechna n až do n_0, a mějme $x \prec y$ takové, že množina $M_{xy} = \{t \in X;\ x \prec t \prec y\}$ má $n = n_0 + 1$ prvků. Vyberme jeden prvek $u \in M_{xy}$, a uvažme množiny $M_{xu} = \{t \in X;\ x \prec t \prec u\}$ a podobně M_{uy}. Z transitivity $\prec$ plyne, že $M_{xu} \subset M_{xy}$, $M_{uy} \subset M_{xy}$. Jak M_{xu}, tak M_{uy} mají aspoň o 1 prvek méně než M_{xy} (protože $u \notin M_{xu}, M_{uy}$), a podle indukčního předpokladu najdeme prvky $x_1, \ldots, x_k$ a $y_1, \ldots, y_\ell$ tak, že $x \lhd x_1 \lhd \ldots \lhd x_k \lhd u$ a $u \lhd y_1 \lhd \ldots \lhd y_\ell \lhd y$. Spojením obou těchto „řetízků“ dostaneme požadovanou posloupnost spojující x a y. □

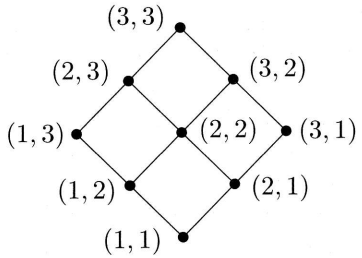
Pro znázornění konečné částečně uspořádané množiny tedy stačí nakreslit šipkami jen relaci bezprostředního předchůdce. Přijmeme-li konvenci, že v obrázku povedou všechny šipky směrem nahoru (tj. je-li $x \prec y$, bude x nakresleno níž než y), nemusíme ani zakreslovat směr šipek, stačí kreslit spojnice bodů. Takové znázornění částečně uspořádané množiny se nazývá její *Hasseův diagram.* Následující obrázek zachycuje sedmiprvkovou lineárně uspořádanou množinu, např. $(\{1, 2, \ldots, 7\}, \leq)$:



Další obrázek ukazuje množinu $\{1, 2, \ldots, 10\}$ uspořádanou relací dělitelnosti (viz příklad 2.1.2):



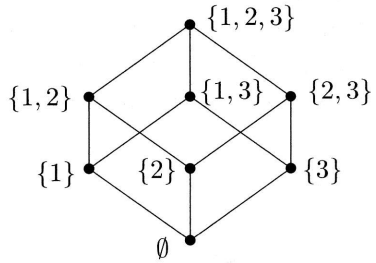
Na tomto náčrtku



je množina $\{1,2,3\} \times \{1,2,3\}$ s uspořádáním $\preceq$ daným předpisem

$$(a_1, b_1) \preceq (a_2, b_2) \text{ právě když } a_1 \leq a_2 \text{ a } b_1 \leq b_2.$$

Konečně toto



je Hasseův diagram množiny všech podmnožin množiny $\{1,2,3\}$, uspořádaných relací $\subseteq$.

Cvičení

1. Ověřte podrobně, že vztah (2.1) v příkladu 2.1.1 skutečně definuje částečné uspořádání.
2. * Nechť R je relace na množině X taková, že neexistuje konečná posloupnost prvků $x_1, x_2, \ldots, x_k$ splňujících $x_1 R x_2, x_2 R x_3, \ldots, x_{k-1} R x_k$, $x_k R x_1$ (říkáme, že taková R *nemá cyklus* nebo že je *acyklická*). Dokažte, že pak existuje uspořádání $\preceq$ na množině X takové, že $R \subseteq \preceq$. (Pomůže-li vám to, předpokládejte, že X je konečná.)
3. Ukažte, že tvrzení 2.1.4 neplatí pro nekonečné množiny.

4. Nechť $(X, \leq)$, $(Y, \preceq)$ jsou uspořádané množiny. Říkáme, že tyto uspořádané množiny jsou *isomorfní* (tj. z hlediska uspořádání „vypadají stejně"), pokud existuje nějaké vzájemně jednoznačné zobrazení $f : X \hookrightarrow\!\!\!\rightarrow Y$ takové, že pro každé $x, y \in X$ platí $x \leq y$ právě když $f(x) \preceq f(y)$.

   (a) Nakreslete všechny navzájem neisomorfní tříprvkové částečně uspořádané množiny.

   (b) Dokažte, že každé dvě n-prvkové *lineárně uspořádané* množiny jsou navzájem isomorfní.

   (c)* Najděte dvě navzájem neisomorfní lineární uspořádání množiny všech přirozených čísel.

   (d)** Dokážete najít nekonečně mnoho navzájem neisomorfních lineárních uspořádání $\mathbf{N}$? Nespočetně mnoho?

2.2 Uspořádání a lineární uspořádání

Každé lineární uspořádání je rovněž (částečné) uspořádání. Opačné tvrzení (tedy „každé částečné uspořádání je lineární uspořádání") jistě neplatí, jak jsme viděli na několika příkladech. Na druhé straně platí následující důležitá věta:

2.2.1 Věta. *Nechť (X, R) je konečná částečně uspořádaná množina. Potom existuje lineární uspořádání S množiny X takové, že $R \subseteq S$.*

Každé částečné uspořádání lze tedy rozšířit na lineární uspořádání. Takové lineární uspořádání se nazývá *lineární rozšíření*.

Před důkazem věty 2.2.1 zavedeme ještě jeden pojem, který je důležitý sám o sobě.

2.2.2 Definice. *Nechť $(X, \preceq)$ je uspořádaná množina. Prvek $a \in X$ nazveme* minimálním prvkem *$(X, \preceq)$, pokud neexistuje žádné $x \in X$ takové, že $x \prec a$.* Maximální prvek *a definujeme podobně (neexistuje žádné $x \succ a$).*

2.2.3 Věta. *Každá neprázdná konečná částečně uspořádaná množina $(X, \preceq)$ má (alespoň jeden) minimální prvek.*

Důkaz. Zvolme $x_0 \in X$ libovolně. Jestliže x_0 je minimální, jsme hotovi. Není-li x_0 minimální v $(X, \preceq)$, potom existuje nějaké $x_1 \prec x_0$. Je-li x_1 minimální, jsme hotovi, jinak najdeme nějaké $x_2 \prec x_1$, atd. Po konečně mnoha krocích nalezneme minimální prvek, protože jinak by X měla nekonečně mnoho různých prvků $x_0, x_1, x_2, \ldots$. □

Poznamenejme, že věta 2.2.3 neplatí pro nekonečné množiny. Například množina všech celých čísel $(\mathbf{Z}, \leq)$ (s přirozeným uspořádáním) nemá žádný minimální prvek.

Možná se výše uvedený (algoritmicky motivovaný) důkaz věty 2.2.3 zdá čtenáři podezřelý. Místo toho, abychom jej vysvětlovali, připojme jinou (běžnější) verzi:

Druhý důkaz. Uvažujme uspořádanou množinu $(X, \preceq)$ a pro prvek $x \in X$ definujme $L_x = \{y \in X;\ y \preceq x\}$. Všimneme si, že pokud $x \preceq y$, potom $L_x \subseteq L_y$.

Zvolme nyní $x \in X$ tak, aby množina L_x měla nejmenší možný počet prvků. Jestliže $|L_x| = 1$, jsme hotovi, neboť x je nutně minimální prvek – platí totiž $L_x = \{x\}$. Kdyby $|L_x| > 1$, pak by existovalo $y \in L_x$, $y \neq x$, a pro něj potom $|L_y| < |L_x|$, což je ve sporu s výběrem prvku x. □

Větu 2.2.3 použijeme pro důkaz věty 2.2.1.

Důkaz. Postupujeme indukcí. Pro $|X| = 1$ není třeba nic dokazovat, máme $R = \Delta_X$ a stačí položit $S = R$. Uvažme tedy uspořádanou množinu (X, R), $|X| > 1$. Nechť $x_0 \in X$ je minimální prvek (X, R). Položme $X' = X \setminus \{x_0\}$ a nechť R' je relace R zúžená na množinu X'. Víme již, že (X', R') je uspořádaná množina, a tedy podle indukčního předpokladu existuje lineární uspořádání S' na X' takové, že $R' \subseteq S'$. Definujme relaci S na množině X následujícím způsobem:

$$\begin{array}{lll} x_0 S y & \text{pro každé} & y \in X; \\ x S y & \text{kdykoliv} & x S' y. \end{array}$$

Ověřte sami, že S je lineární uspořádání. Je rovněž zřejmé, že $R \subseteq S$. □

Existence lineárního rozšíření je důležitá a užitečná v mnoha aplikacích. V informatice je pro dané částečné uspořádání často potřeba najít nějaké lineární rozšíření. Tento algoritmický problém se jmenuje *topologické třídění.*

Věta 2.2.1 platí rovněž pro nekonečné množiny. Nejde to však dokázat tak snadno. Ve skutečnosti to nejde vůbec, protože existence lineárního rozšíření je možno považovat za jeden z axiomů teorie množin (podobně jako tzv. axiom výběru, s nímž je tento axiom spřízněn).

Na závěr tohoto článku připojme varování (lingvistické). Pojmu minimálního prvku je zdánlivě příbuzný pojem nejmenšího prvku. Jedná se však o podobnost pouze zdánlivou a vlastně jen jazykovou, jak ukazuje definice tohoto pojmu.

2.2.4 Definice. *Nechť $(X, \preceq)$ je uspořádaná množina. Prvek $a \in X$ nazveme* nejmenším prvkem *$(X, \preceq)$, jestliže pro každé $x \in X$ platí $a \preceq x$. Podobně definujeme* největší prvek.

Nejmenší prvek je zřejmě rovněž minimální. Například pro množinu všech přirozených čísel uspořádanou relací dělitelnosti, neboli $(\mathbf{N}, |)$, je 1 jak nejmenší, tak minimální prvek. Ale minimální prvek nemusí zdaleka vždycky být nejmenší: Kupříkladu je-li X aspoň dvouprvková množina uspořádaná relací diagonály Δ_X (tj. žádné dva různé prvky nejsou porovnatelné), pak každý prvek je minimální, ale žádný není nejmenší. Jiným příkladem je $(\mathbf{N} \setminus \{1\}, |)$, tj. přirozená čísla bez jedničky uspořádaná relací dělitelnosti, která také nemá nejmenší prvek, a přitom má nekonečně mnoho minimálních prvků, viz cvičení 7.

Cvičení

1. (a) Ukažte, že největší prvek je maximální, a ukažte příklad uspořádané množiny, která má maximální prvek, ale nemá největší prvek.

   (b) Najděte uspořádanou množinu, která nemá ani nejmenší, ani minimální prvek, ale má největší prvek.

2. (a) Uvažte množinu $\{1, 2, \ldots, n\}$ uspořádanou relací dělitelnosti $|$ (viz příklad 2.1.2). Kolik nejvýše prvků může mít podmnožina $X \subseteq$

$\{1, 2, \ldots, n\}$, která je relací | uspořádána lineárně (takové podmnožině se někdy říká *řetězec*)?

(b) Řešte tutéž otázku pro množinu $2^{\{1,2,\ldots,n\}}$ uspořádanou relací $\subseteq$ (viz příklad 2.1.3).

3. Označme symbolem $\mathrm{lr}(X, \preceq)$ počet lineárních rozšíření částečně uspořádané množiny $(X, \preceq)$. Dokažte

   (a) $\mathrm{lr}(X, \preceq) = 1$, právě když $\preceq$ je lineární uspořádání;

   (b) $\mathrm{lr}(X, \preceq) \leq n!$ pro $n = |X|$ (tady může být užitečné si napřed přečíst kapitolu 3).

4. Dokažte, že nejmenší prvek, pokud existuje, je určen jednoznačně.

5. Dokažte, že pro lineárně uspořádané množiny je každý minimální prvek rovněž prvek nejmenší.

6. Dokažte nebo vyvraťte: Má-li $(X, \preceq)$ jediný minimální prvek, potom je to také prvek nejmenší.

7. (a) Dokažte, že uspořádaná množina $(\mathbf{N} \setminus \{1\}, |)$ má nekonečně mnoho minimálních prvků. O která čísla se jedná?
   (b) Kolik minimálních prvků má množina $\{4k + 2; k \geq 2\}$ uspořádaná relací dělitelnosti? Poznamenejme, že podobná otázka pro množinu $\{4k + 1; k \geq 2\}$ je mnohem obtížnější.

8. Nechť (X, R) je částečně uspořádaná množina. Dokažte:

   (a) Potom (X, R^{-1}) je rovněž částečně uspořádaná množina.

   (b) Prvek $x \in X$ je maximální v (X, R), právě když x je minimální v (X, R^{-1}).

   (c) Prvek $x \in X$ je největší v (X, R), právě když x je nejmenší v (X, R^{-1}).

   Vzhledem k tomu, že $(R^{-1})^{-1} = R$, vidíme, že pojmy pro uspořádané množiny se vyskytují ve dvojicích: minimální a maximální prvek, nejmenší a největší prvek apod. Některé definice a důkazy se tak dají zkrátit tím, že se provedou jen pro jeden z příslušné dvojice pojmů. Tak například stačí dokázat větu 2.2.3 (o existenci minimálního prvku) a analogická věta o existenci maximálního prvku se dostane automaticky, důkaz se dá „přeložit". Tato metoda se nazývá, poněkud nepřesně, *princip duality* uspořádaných množin.

9. Buď $(X, \preceq)$ uspořádaná množina, $A \subseteq X$ její podmnožina. Prvek $s \in X$ nazveme *supremum* množiny A, pokud platí:

   (i) $a \preceq s$ pro každé $a \in A$.

   (ii) Pro každé $s' \in X$ platí: jestliže $a \preceq s'$ pro každé $a \in A$, potom $s \preceq s'$.

   Podobně, ale se všemi nerovnostmi v obráceném směru, se definuje *infimum* podmnožiny $A \subseteq X$.

   (a) Jaký prvek je supremem prázdné množiny?

   (b) Najděte příklad uspořádané množiny, jejíž každá neprázdná podmnožina má supremum, ale ne každá neprázdná podmnožina má infimum.

   (c)* Nechť $(X, \preceq)$ je uspořádaná množina, jejíž každá podmnožina (včetně prázdné) má supremum. Dokažte, že každá podmnožina má též infimum.

10. Uvažme množinu $\mathbf{N}$ uspořádanou relací | (dělitelnost).

    (a) Rozhodněte, zda každá podmnožina $\mathbf{N}$ má supremum.

    (b) Rozhodněte, zda každá konečná podmnožina $\mathbf{N}$ má supremum.

    (c) Rozhodněte, zda každá neprázdná podmnožina má infimum.

2.3 Uspořádání pomocí inkluze

V článku 1.5 jsme ukázali, jak je možno ekvivalenci na množině X popsat pomocí rozkladu množiny. Tento vztah je vzájemně jednoznačný (můžeme také říci, že rozklady představují ekvivalentní popis ekvivalencí). Existuje něco podobného pro částečná uspořádání?

Zdá se, že nikoliv. Pojem uspořádání je složitější než pojem ekvivalence, a také proto jsme mu věnovali zvláštní kapitolu. Přesto v tomto článku ukážeme, že si každou částečně uspořádanou množinu lze představit tak, že relace je vytvořena pomocí inkluze, tedy (zdánlivě) jednoduše. Klíčem k tomuto výsledku je následující pojem:

2.3.1 Definice. *Nechť (X, R) a (X', R') jsou uspořádané množiny. Zobrazení $f: X \to X'$ nazveme* vnoření (X, R) *do* (X', R'), *jestliže platí*

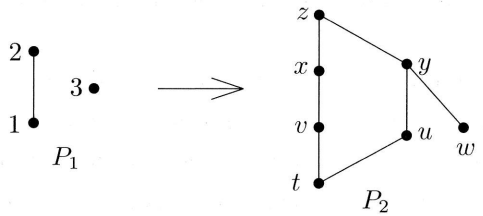
(i) f *je prosté zobrazení;*

(ii) $f(x)R'f(y)$ *pro každé* xRy*;*

(iii) jestliže $f(x)R'f(y)$*, potom i* xRy*.*

Připojme pár poznámek: Jestliže f je vnoření, které je rovněž zobrazení na, potom f je isomorfismus, o kterém jsme již pojednali ve cvičení 2.1.4. Jestliže isomorfismus uspořádaných množin vyjadřuje skutečnost, že příslušné množiny „vypadají stejně", potom vnoření (X, R) do (X', R') vyjadřuje skutečnost, že nějaká část, totiž část určená množinou $\{f(x); x \in X\}$, „vypadá stejně" jako (X, R).

Následující obrázek znázorňuje dvě uspořádané množiny:



Příklady vnoření P_1 do P_2 jsou zobrazení $f\colon 1 \mapsto v, 2 \mapsto x, 3 \mapsto y$ a také $f'\colon 1 \mapsto t, 2 \mapsto x, 3 \mapsto w$, zatímco třeba $g\colon 1 \mapsto t, 2 \mapsto v, 3 \mapsto y$ ani $g'\colon 1 \mapsto t, 2 \mapsto w, 3 \mapsto u$ vnoření nejsou.

2.3.2 Věta. *Pro každou uspořádanou množinu* $(X, \preceq)$ *existuje vnoření do uspořádané množiny* $(2^X, \subseteq)$*.*

Důkaz. Ukážeme navíc, že hledané vnoření je velmi snadné najít. Definujeme zobrazení $f\colon X \to 2^X$ předpisem $f(x) = \{y; y \preceq x\}$. Ověříme, že takto definované zobrazení je skutečně vnoření. Přitom využijeme všech vlastností uspořádání.

1. Ověříme, že f je prosté. Předpokládejme, že $f(x) = f(y)$. Protože $x \in f(x)$ a $y \in f(y)$, dostáváme vzhledem k definici $f(x)$, že platí $x \preceq y$ a rovněž $y \preceq x$, a tedy $x = y$ (z antisymetrie $\preceq$).

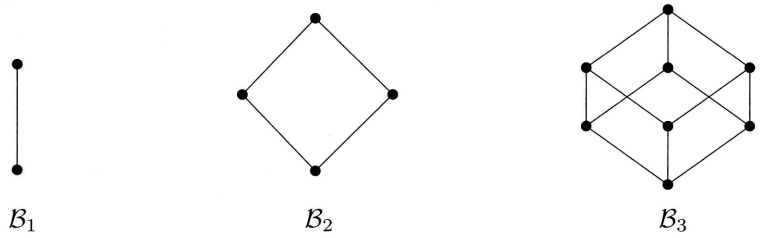
2. Ukážeme, že $f(x) \subseteq f(y)$ pro každé $x \preceq y$. Je-li $z \in f(x)$, potom $z \preceq x$, a tedy z transitivity $\preceq$ dostáváme rovněž $z \preceq y$. Poslední výraz značí, že $z \in f(y)$.

3. Nakonec dokážeme, že $x \preceq y$ pro každé $f(x) \subseteq f(y)$. Je-li $f(x) \subseteq f(y)$, potom $x \in f(y)$, a tedy $x \preceq y$. □

S definicí zobrazení f jsme se vlastně již setkali v důkazu věty 2.2.3, kde jsme množinu $f(x)$ označili L_x. Nevadí, že jsme ji v jiné souvislosti označili jinak. Konstrukce množiny L_x je v matematice častá a vyskytuje se pod různými jmény, např. dolní množina, dolní ideál apod.

Všimněte si, že výše uvedená věta i důkaz platí i pro nekonečné množiny.

Uspořádané množiny $(2^X, \subseteq)$ jsou tedy univerzální v tom smyslu, že obsahují všechny uspořádané množiny. Není divu, že jejich zkoumání byla věnována značná pozornost a že si vynutily zvláštní značení i pojmy. Speciálně pro množinu $X = \{1, 2, \ldots, n\}$ označíme uspořádanou množinu $(2^X, \subseteq)$ symbolem $\mathcal{B}_n$. Hasseovy diagramy uspořádání $\mathcal{B}_1$, $\mathcal{B}_2$, $\mathcal{B}_3$ jsou na obrázku.



O uspořádané množině $\mathcal{B}_n$ se v různých souvislostech mluví také jako o Booleově algebře, booleovském svazu nebo n-dimenzionální krychli.

Cvičení

1. Kolik mají uspořádání $\mathcal{B}_2$ a $\mathcal{B}_3$ lineárních rozšíření?

2. Modifikujte důkaz věty 2.3.2 pomocí *horních* množin, tj. množin tvaru $U_x = \{y \in X; xRy\}$.

3. Nalezněte příklad uspořádané množiny $P = (X, \preceq)$, pro niž existuje vnoření do $\mathcal{B}_n$ pro $n < |X|$.

4.* Dokažte, že každou konečnou uspořádanou množinu lze vnořit do $(\mathbf{N}, |)$.

5.* Dokažte, že ne každou konečnou uspořádanou množinu je možno vnořit do uspořádání trojic reálných čísel z příkladu 2.1.1.

6. (a) Popište nějaké vnoření množiny $\{1,2\} \times \mathbf{N}$ s lexikografickým uspořádáním do uspořádané množiny $(\mathbf{Q}, \leq)$, kde $\leq$ je obvyklé uspořádání podle velikosti.

   (b) Řešte obdobu (a) s množinou $\mathbf{N} \times \mathbf{N}$ s lexikografickým uspořádáním místo $\{1,2\} \times \mathbf{N}$.

   (c)* Dokažte, že dokonce libovolnou spočetnou lineárně uspořádanou množinu lze vnořit do $(\mathbf{Q}, \leq)$.

7.* Dokažte, že každá podmnožina uspořádané množiny $\mathcal{B}_n$ má jak supremum, tak infimum.

8. Spočtěte, kolik existuje vnoření P_1 do P_2, kde P_1 a P_2 jsou uspořádané množiny na obrázku nad větou 2.3.2.

2.4 O dlouhém a širokém

Nechť $(X, \preceq)$ je (konečná) uspořádaná množina. Pro stručnost ji označíme písmenem P, ve většině článku budeme uvažovat pouze jednu (zato libovolnou) uspořádanou množinu. Pojmy, které budeme zkoumat, jsou vyjádřeny následujícími definicemi.

2.4.1 Definice. *Množina prvků $A \subseteq X$ se nazývá* nezávislá v P, *jestliže pro žádné dva různé prvky $x, y \in A$ neplatí $x \preceq y$.*

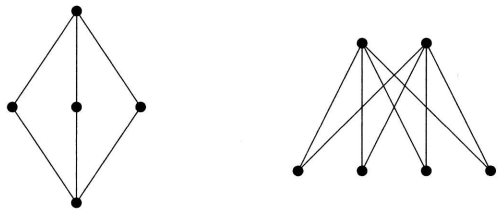
Nezávislé množině se někdy říká také *antiřetězec*.

Uvedenou definici je možno vyjádřit ještě jinak: Řekneme, že dva různé prvky x a y jsou *porovnatelné*, jestliže buď $x \prec y$, nebo $y \prec x$. Množina je tedy nezávislá, jestliže žádné dva její prvky nejsou porovnatelné.

Označme $\alpha(P)$ maximální velikost nezávislé množiny prvků v P. Symbolicky bychom to mohli zapsat takto:

$$\alpha(P) = \max\{|A|; A \text{ nezávislá v } P\}.$$

2.4.2 Příklad. *Pro uspořádané množiny P_1 a P_2 na obrázku platí $\alpha(P_1) = 3$, $\alpha(P_2) = 4$.*



P_1 P_2

2.4.3 Pozorování. *Množina všech minimálních prvků P tvoří nezávislou množinu.*

2.4.4 Definice. *Množina prvků $A \subseteq X$ se nazývá* řetězec v P, *jestliže každé dva prvky jsou porovnatelné (v P).*

Ekvivalentně, prvky A tvoří lineárně uspořádanou podmnožinu P. Označme $\omega(P)$ maximální velikost řetězce v P.

Pro výše uvedená uspořádání P_1 a P_2 platí $\omega(P_1) = 3$, $\omega(P_2) = 2$. Je snadné nahlédnout $\omega(\mathcal{B}_n) = n + 1$. Určit $\alpha(\mathcal{B}_n)$ je již obtížnější, tuto otázku zodpovíme v kapitole 7.

Z uvedených příkladů vidíme, že číslo $\alpha(P)$ můžeme považovat za jakousi abstraktní „šířku“ uspořádání P, zatímco $\omega(P)$ odpovídá jeho „výšce“. Následující výsledek dal tedy jméno tomuto článku:

2.4.5 Věta. *Pro každou konečnou uspořádanou množinu $P = (X, \preceq)$ platí*

$$\alpha(P) \cdot \omega(P) \geq |X|.$$

Důkaz. Definujeme množiny $X_1, X_2, \ldots, X_t$ indukcí: Nechť X_1 označuje množinu všech minimálních prvků uspořádání P. V indukčním kroku nechť jsou množiny $X_1, \ldots, X_\ell$ již definovány. Označme nejprve X'_ℓ množinu všech prvků nenáležejících žádné z množin $X_1, \ldots, X_\ell$. Symbolicky zapsáno $X'_\ell = X \setminus \bigcup_{i=1}^{\ell} X_i$. Jestliže X'_ℓ je prázdná množina, potom položme $t = \ell$ a konstrukci ukončíme. V opačném případě,

$X'_\ell \neq \emptyset$, označme $\preceq'$ uspořádání $\preceq$ zúžené na množinu X'_ℓ. Definujeme $X_{\ell+1}$ množinu všech minimálních prvků množiny $(X'_\ell, \preceq')$. Důkaz věty bude ukončen, jestliže se přesvědčíme o následujících skutečnostech:

(1) Množiny $X_1, \ldots, X_t$ tvoří rozklad množiny X.

(2) Každá z množin X_i je nezávislá (a tedy $\alpha(P) \geq |X_i|$).

(3) $\omega(P) \geq t$.

Tvrzení (1) a (2) plynou bezprostředně z konstrukce množin X_1, $X_2, \ldots, X_t$. Stačí tedy dokázat (3).

Postupujeme zpětnou indukcí. Pro $i = t, t-1, \ldots, 2, 1$ nalezneme prvky $x_i \in X$ takové, že množina $\{x_1, x_2, \ldots, x_t\}$ tvoří řetězec. Zvolme tedy $x_t \in X_t$ libovolně. Protože $x_t \notin X_{t-1}$, existuje nutně $x_{t-1} \in X_{t-1}$ takové, že platí $x_{t-1} \prec x_t$.Tato úvaha je základem celého postupu: jestliže jsme již sestrojili prvky $x_t \in X_t, x_{t-1} \in X_{t-1}, \ldots, x_{k+1} \in X_{k+1}$, potom $x_{k+1} \notin X_k$, a tedy existuje $x_k \in X_k$ splňující $x_k \prec x_{k+1}$. Prvek x_k je vždycky „důvodem", proč x_{k+1} nepřišel na řadu dřív.

Zkonstruovaná množina $\{x_1, \ldots, x_t\}$ tvoří řetězec. Tedy $\omega(P) \geq t$. (Ve skutečnosti ovšem $\omega(P) = t$, viz cvičení.) □

Věta 2.4.5 (o dlouhém a širokém) má řadu pěkných aplikací a souvislostí, jak je vidět z následujícího (slavného) použití.

2.4.6 Věta (Erdősovo-Szekeresovo lemma). *Libovolná posloupnost reálných čísel délky n^2+1 obsahuje monotónní podposloupnost délky $n+1$.*

Před důkazem definujme použité pojmy. Uvažme k-prvkovou posloupnost $(x_1, x_2, \ldots, x_k)$ reálných čísel. *Podposloupnost* délky m je určena indexy $i(1), \ldots, i(m)$, $i(1) < i(2) < \cdots < i(m)$, a je tvořena prvky $x_{i(1)}, x_{i(2)}, \ldots, x_{i(m)}$. Tato podposloupnost je *monotonní*, jestliže platí buď $x_{i(1)} \leq x_{i(2)} \leq \cdots \leq x_{i(m)}$, nebo $x_{i(1)} \geq x_{i(2)} \geq \cdots \geq x_{i(m)}$.

Důkaz. Nechť je posloupnost $(x_1, x_2, \ldots, x_{n^2+1})$ zadána. Položme $X = \{1, 2, \ldots, n^2+1\}$ a definujme relaci $\preceq$ na X předpisem

$$i \preceq j \text{ právě když } i \leq j \text{ a } x_i \leq x_j.$$

Není těžké ověřit, že takto definovaná relace $\preceq$ je (částečné) uspořádání množiny X.

Platí tedy $\alpha(X, \preceq) \cdot \omega(X, \preceq) \geq n^2+1$, a proto $\alpha(X, \preceq) > n$ nebo $\omega(X, \preceq) > n$. Nyní je snadné se přesvědčit, že řetězec odpovídá neklesající podposloupnosti a nezávislá množina odpovídá nerostoucí podposloupnosti. □

Cvičení

1. (a) Nechť $\preceq_i$, $i = 1, \ldots, k$, jsou uspořádání na nějaké množině X. Potom $\bigcap_{i=1}^{k} \preceq_i$ je opět uspořádání. (Uvědomte si, že každé $\preceq_i$, jakožto relace, je podmnožinou $X \times X$.)

   (b)* Dokažte, že libovolné částečné uspořádání $\preceq$ na konečné množině X se dá vyjádřit jako průnik *lineárních* uspořádání.

   Poznamenejme, že nejmenší možný počet lineárních uspořádání, jichž je dané uspořádání $\preceq$ průnikem, je velmi důležitým parametrem tohoto uspořádání a nazývá se jeho *Dushnikova-Millerova dimenze* nebo krátce *dimenze*.

2. Dokažte $\omega(\mathcal{B}_n) = n+1$.

3. Najděte posloupnost reálných čísel délky 17, která neobsahuje monotonní podposloupnost délky 5.

4. Dokažte následující zesílení věty 2.4.6: Každá posloupnost reálných čísel délky $k\ell+1$ obsahuje rostoucí podposloupnost délky $k+1$ nebo nerostoucí podposloupnost délky $\ell+1$.

5. Dokažte, že věta 2.4.5 a předcházející cvičení jsou nejlepší možné v následujícím smyslu: Pro každé k a ℓ existuje uspořádaná množina P s n prvky splňující $n = k\ell$, $\alpha(P) = k$ a $\omega(P) = \ell$.

6. (a) Uvažme dvě posloupnosti reálných čísel, $a = (a_1, a_2, \ldots, a_n)$ a $b = (b_1, b_2, \ldots, b_n)$, v nichž se žádné číslo neopakuje. Ukažte, že vždy existují indexy $i(1), \ldots, i(k)$, $1 \leq i(1) < \ldots < i(k) \leq n$, kde $k = \lceil n^{1/4} \rceil$, takové, že jimi určené podposloupnosti v a i b jsou rostoucí nebo klesající (připouští se všechny 4 možné kombinace, např. „rostoucí v a, rostoucí v b", „klesající v a, rostoucí v b" atd.).

   (b)* Ukažte, že odhad pro k v (a) obecně nelze zlepšit.

7.** (Dilworthova věta) Nechť $(X, \preceq)$ je n prvková částečně uspořádaná množina. Dokažte, že X lze vyjádřit jako (disjunktní) sjednocení nejvýš $\alpha = \alpha(X, \preceq)$ řetězců.

3

Kombinatorické počítání

V této kapitole budeme studovat úlohy „na počet konfigurací“ jako „Kolik je zobrazení dané n-prvkové množiny do m-prvkové?“ a podobně. Začneme jednoduchými příklady, které se dají vyřešit úvahou bez nějakých speciálních znalostí, ale později se dostaneme i k poněkud pokročilejším technikám.

3.1 Funkce a podmnožiny

3.1.1 Tvrzení. *Nechť N je nějaká n-prvková množina (případně i prázdná, tj. $n = 0, 1, 2, \ldots$), M je m-prvková množina, $m \geq 1$. Potom počet všech zobrazení (neboli funkcí) $f : N \to M$ (zobrazení množiny N do M) je m^n.*

Důkaz. Toto tvrzení asi řada čtenářů zná nebo si jeho pravdivost uvědomí bez velké námahy. Cvičně je nicméně dokážeme indukcí podle n.

Pro $n = 0$ uvažujeme zobrazení prázdné množiny. Podíváme-li se na definici zobrazení, je to relace (tedy podmnožina $N \times M$, čili v našem případě podmnožina prázdné množiny), splňující jistou podmínku – pro každý prvek $a \in N$ existuje v relaci právě jedna dvojice tvaru (a, b), kde $b \in M$. V našem případě N žádný prvek nemá, a proto uvedená podmínka nic nepožaduje, čili jediná možná relace,

totiž prázdná, je také zobrazením $N \to M$. Dokazované tvrzení platí pro $n = 0$.

Leckdo by namítl, že zobrazení prázdné množiny nemá žádný smysl a nebo že není potřeba se jím zabývat (opravdu bychom mohli indukci začít od $n = 1$). V matematických úvahách se většinou vyplatí si podobné „mezní" případy rozmyslet, uvážit, co přesně o nich říká obecná definice. Tím se potom vyhneme různým výjimkám a speciálním případům (nebo chybám) v důkazech.

Předpokládejme, že jsme tvrzení dokázali pro každé $n \leq n_0$ a pro každé m. Máme nyní $n = n_0+1$, n-prvkovou množinu N a m-prvkovou množinu M. Zvolme libovolně jeden prvek $a \in N$. Zadat zobrazení $f : N \to M$ je totéž, jako zadat hodnotu $f(a) \in M$ plus zobrazení $f' : N \setminus \{a\} \to M$ zbývajících prvků. Hodnotu $f(a)$ můžeme zvolit m způsoby, a pro volbu f' máme podle indukčního předpokladu m^{n-1} možností. Každou volbu $f(a)$ můžeme zkombinovat s libovolnou volbou f', takže celkem je počet možností pro f roven $m \cdot m^{n-1} = m^n$. □

Následuje jiné dobře známé tvrzení, k němuž podáme dva důkazy:

3.1.2 Tvrzení. *Libovolná n-prvková množina X má právě 2^n podmnožin.*

První důkaz (indukcí). Pro $X = \emptyset$ existuje jediná podmnožina, totiž prázdná, což souhlasí se vzorečkem, $2^0 = 1$. Pro $(n+1)$-prvkovou množinu X, zvolme jeden její prvek, a, a rozdělme podmnožiny X do dvou typů: ty které neobsahují a, a ty, které jej obsahují. První typ jsou právě všechny podmnožiny n-prvkové množiny $X \setminus \{a\}$, a podle indukčního předpokladu jich je 2^n. Pro každou podmnožinu A druhého typu uvažme množinu $A' = A \setminus \{a\}$. To je podmnožina $X \setminus \{a\}$. Zřejmě každá podmnožina $A' \subseteq X \setminus \{a\}$ se takto dostane právě z jedné množiny A, totiž z $A' \cup \{a\}$. Proto podmnožin A druhého typu je také 2^n, a celkem máme $2^n + 2^n = 2^{n+1}$ podmnožin $(n+1)$-prvkové množiny, jak to má být.

Druhý důkaz (převedením na známé tvrzení). Uvažme libovolnou podmnožinu A dané n-prvkové množiny X, a definujme zobrazení $f_A : X \to \{0,1\}$: pro prvek $x \in X$ položíme

$$f_A(x) = \begin{cases} 1 & \text{pokud } x \in A \\ 0 & \text{pokud } x \notin A \end{cases}$$

(toto zobrazení se v matematice často objevuje a nazývá se *charakteristická funkce* množiny A). Různým množinám A přísluší různá zobrazení f_A, a obráceně, pro libovolné zobrazení $f : X \to \{0,1\}$ existuje právě jedna množina $A \subseteq X$ taková, že $f = f_A$. Tudíž podmnožin X je stejný počet jako zobrazení $X \to \{0,1\}$, čili 2^n podle tvrzení 3.1.1. □

Teď trošku těžší tvrzení:

3.1.3 Tvrzení. *Nechť $n \geq 1$. Každá n-prvková množina má právě 2^{n-1} podmnožin liché velikosti a 2^{n-1} podmnožin sudé velikosti.*

Důkaz. Využijeme tvrzení 3.1.2. Zvolme pevně nějaký prvek $a \in X$. Libovolnou podmnožinu $A \subseteq X \setminus \{a\}$ můžeme doplnit na podmnožinu $A' \subseteq X$ s lichým počtem prvků: je-li $|A|$ liché, bude $A' = A$, a pro $|A|$ sudé $A' = A \cup \{a\}$. Je snadné zkontrolovat, že tím jsme našli bijekci mezi množinou všech podmnožin $X \setminus \{a\}$ a množinou všech podmnožin X liché velikosti, a tak posledně jmenovaných je 2^{n-1}. Pro podmnožiny sudé velikosti se postupuje stejně, nebo se řekne, že jich musí být doplněk do počtu všech podmnožin, tj. $2^n - 2^{n-1} = 2^{n-1}$. □

Vrátíme se k zobrazením.

3.1.4 Tvrzení. *Pro $n, m \geq 0$ existuje právě*

$$m(m-1)\cdots(m-n+1) = \prod_{i=0}^{n-1}(m-i)$$

prostých zobrazení n-prvkové množiny do m-prvkové množiny.

Důkaz. Zase indukcí podle n, budeme postupovat stručněji. Pro $n = 0$, prázdné zobrazení je prosté, tedy existuje jedno zobrazení, což odpovídá tomu, že hodnotu prázdného součinu jsme definovali jako 1. Pro $n > m$ žádné prosté zobrazení neexistuje, což souhlasí s dokazovaným vzorcem (vystupuje v něm totiž jeden činitel rovný 0).

Mějme n-prvkovou množinu N, $n \geq 1$ a m-prvkovou množinu M, $m \geq n$. Vyberme prvek $a \in N$ a zvolme jeho funkční hodnotu $f(a) \in M$ libovolně, jedním z m způsobů. Zbývá prostě zobrazit prvky $N \setminus \{a\}$ do $M \setminus \{f(a)\}$, pro což existuje podle indukčního předpokladu $(m-1)(m-2)\cdots(m-n+1)$ možností. Celkem dostaneme

$$m(m-1)(m-2)\cdots(m-n+1)$$

prostých zobrazení $N \to M$. □

Máme-li množinu M sestávající z m různých předmětů a vybereme-li z nich libovolně uspořádanou n-tici předmětů (tj. při výběru záleží na pořadí; takové výběry se někdy nazývají *variace*, obšírněji *variace n prvků z m prvků bez opakování*), máme $m(m-1)\ldots(m-n+1)$ možností takového výběru. Každý takový výběr můžeme chápat jako volbu prostého zobrazení $f : \{1, 2, \ldots, n\} \to M$: definujeme $f(1)$ jako první předmět z vybrané n-tice, $f(2)$ jako druhý předmět atd. Obráceně, volbu prostého zobrazení si můžeme představit jako výběr uspořádané n-tice z množiny, do níž zobrazujeme.

Cvičení

1. Určete počet všech uspořádaných dvojic (A, B), kde $A \subseteq B \subseteq \{1, 2, \ldots, n\}$.
2. (a) Kolik existuje $n \times n$ matic s prvky z množiny $\{0, 1, \ldots, q-1\}$?
   (b)* Předpokládejme, že q je prvočíslo. Kolik takových matic má determinant dělitelný q? (Jinými slovy, kolik matic nad tělesem $GF(q)$ je singulárních? Viz algebraický dodatek.)

3.2 Permutace a faktoriály

Prostá zobrazení konečné množiny X do sebe se nazývají *permutace* množiny X. Taková zobrazení jsou ovšem zároveň na.

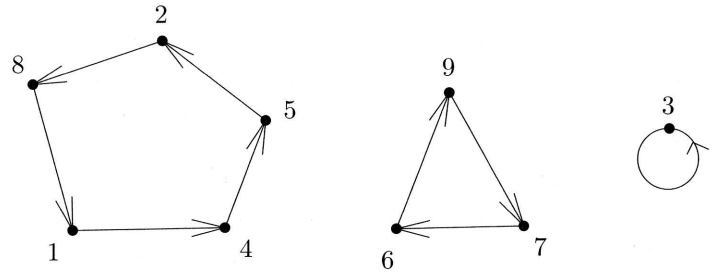
Máme-li prvky X srovnány v nějakém pořadí, můžeme si permutaci představovat jako nějaké jejich přerovnání. Například pro množinu $X = \{a, b, c, d\}$ je jedna možná permutace

$$\begin{pmatrix} a & b & c & d \\ b & d & c & a \end{pmatrix}$$

(v prvním řádku jsme vypsali prvky množiny X, a ve druhém jsme pod každý prvek napsali prvek, na nějž se uvažovanou permutací zobrazí). Nejčastěji se pracuje s permutacemi množiny $\{1, 2, \ldots, n\}$. Předpokládáme-li, že v prvním řádku budou tato čísla vždy zapsána v přirozeném pořadí, stačí uvést pouze druhý řádek; např. (2 4 3 1) by označovalo permutaci p s hodnotami $p(1) = 2$, $p(2) = 4$, $p(3) = 3$ a $p(4) = 1$.

V literatuře se někdy permutace množiny X chápou přímo jako rozložení prvků X v nějakém pořadí, tj. lineární uspořádání na X. To je někdy také užitečný pohled, my však budeme permutace chápat jako zobrazení, což má některé formální výhody, například že permutace lze přirozeně skládat.

Ještě jiný způsob zápisu permutace je pomocí jejích cyklů. Cykly permutace můžeme asi nejlépe definovat při znázornění permutace pomocí šipek (jako jsme znázorňovali relace v části 1.4, např. na str. 38). V případě permutace $p : X \to X$ znázorníme prvky množiny X body (puntíky), a nakreslíme šipku od každého bodu x k bodu $p(x)$. Například, pro permutaci $p = (4\ 8\ 3\ 5\ 2\ 9\ 6\ 1\ 7)$ (použili jsme jednořádkového zápisu pro permutace množiny $\{1, 2, \ldots, n\}$ vysvětleného výše) vypadá takové znázornění takto:



Z každého bodu vychází právě 1 šipka, a do každého bodu také právě 1 šipka vchází. Je snadné si rozmyslet, že za těchto podmínek je takové znázornění permutace vždy tvořeno několika disjunktními skupinami bodů, přičemž v každé ze skupin jsou body propojeny šipkami do cyklu (orientovaného, to znamená, že cyklus lze procházet kolem dokola

podél šipek) – jako na uvedeném obrázku. Tyto cykly budeme nazývat *cykly dané permutace.* Pomocí cyklů by se uvedená permutace zapsala $p = ((1,4,5,2,8)(3)(6,9,7))$. V každé vnitřní závorce jsou vypsány prvky jednoho z cyklů v pořadí podle jeho šipek, počínaje prvkem s nejnižším číslem.

K čemu mohou permutace sloužit? Studují se například při návrhu a analýze všelijakých algoritmů pro třídění. Některé efektivní algoritmy pro výpočty s grafy, s geometrickými objekty a podobně začínají tím, že rozestaví nějaké vstupní objekty do náhodného pořadí, tj. vlastně s nimi provedou náhodnou permutaci. Překvapivě komplikované vlastnosti permutací se uplatnily při matematické analýze míchání karet. V teorii grup jsou grupy permutací (se skládáním jako grupovou operací) jedním z hlavních předmětů studia. Prapříčina neřešitelnosti obecné algebraické rovnice pátého stupně je ve vlastnostech grupy všech permutací na 5-prvkové množině.

Podle tvrzení 3.1.4 je počet permutací n-prvkové množiny roven $n(n-1) \times \cdots \times 1$. Toto číslo jako funkce proměnné n se označuje $n!$ a nazývá se n *faktoriál.* Je tedy

$$n! = 1 \times 2 \times 3 \times \ldots \times n = \prod_{i=1}^{n} i.$$

Speciálně pro $n = 0$ je $0!$, jako prázdný součin, roven 1.

Cvičení

1. Kolik existuje permutací množiny $\{1, 2, \ldots, n\}$ s jediným cyklem?
2. Pro permutaci $p : X \to X$ značí p^k permutaci vzniklou k-násobným složením p, tj. $p^1 = p$, $p^k = p \circ p^{k-1}$. *Řádem* permutace p se rozumí nejmenší přirozené číslo k takové, že $p^k = id$, kde id označuje identickou permutaci, která každý prvek zobrazí na něj samotný.

   (a) Určete řád permutace (2 3 1 5 4 7 8 9 6).

   (b) Ukažte, jak se v obecnosti najde řád permutace pomocí délek jejích cyklů.
3. Buď π permutace na množině $\{1, 2, \ldots, n\}$, zapišme ji jednořádkovým zápisem, a vyznačme ve vzniklé posloupnosti jednotlivé *rostoucí úseky,* např. (4 5 7 2 6 8 3 1). Označme $f(n,k)$ počet permutací n-prvkové množiny s přesně k rostoucími úseky.

   (a)* Dokažte, že $f(n,k) = f(n, n+1-k)$, a odvoďte, že průměrný počet úseků permutace (přes všechny permutace) je $(n+1)/2$.

   (b)* Odvoďte rekurentní vzorec

$$f(n,k) = k\ f(n-1,k) + (n+1-k) f(n-1,k-1).$$

   (c) Pomocí (b) určete počet permutací se 2, resp. se 3 úseky, případně * s k rostoucími úseky.

   (d)* Pro náhodnou permutaci π určete pravděpodobnost, že počáteční rostoucí úsek má délku k. Ukažte, že pro velká n se průměrná délka počátečního rostoucího úseku blíží číslu $e - 1$.

   Poznámka: Podobné otázky se studují při analýze některých algoritmů pro třídění.
4. Buď π nějaká permutace množiny $\{1, 2, \ldots, n\}$. Řekneme, že dvojice $(i,j) \in \{1, 2, \ldots, n\} \times \{1, 2, \ldots, n\}$ je *inverze* π, pokud $i < j$ a zároveň $\pi(i) > \pi(j)$.

   (a) Dokažte, že množina $I(\pi)$ všech inverzí, chápaná jako relace, je transitivní. Ukažte, že také množina „neinverzí"

$$\{(i,j);\ i < j \text{ a } \pi(i) < \pi(j)\}$$

   je transitivní relace.

   (b) Uvažme nějaký třídicí algoritmus, který rovná n daných čísel podle velikosti, a přitom v každém kroku vymění pořadí některých dvou sousedních čísel (v momentálním pořadí). Dokažte, že pro setřídění některých posloupností je potřeba řádově aspoň n^2 kroků.

   (c)* Dokázali byste navrhnout algoritmus, který by spočítal počet inverzí dané permutace $\{1, 2, \ldots, n\}$ v podstatně méně než n^2 krocích? (Řešení viz např. [18].)
5. (a)* Zjistěte, jakou nejvyšší mocninou 5 je dělitelné číslo 50!. Kolik bude mít desítkový zápis 50! na konci nul?

   (b) Najděte obecný vzorec pro nejvyšší mocninu k takovou, že číslo $n!$ je dělitelné p^k, kde p je dané prvočíslo.
6. Ukažte, že pro každé $k, n \geq 1$, $(k!)^n$ dělí $(kn)!$.

3.3 Binomické koeficienty

Nechť $n \geq k$ jsou nezáporná celá čísla. *Binomický koeficient* nebo *kombinační číslo* $\binom{n}{k}$ (čteme „en nad ká“, nikoliv „en nad kátou“!) je funkce proměnných n, k, definovaná vzorcem

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{1 \times 2 \times \cdots \times k} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}. \qquad (3.1)$$

Čtenář možná zná i jinou formuli, totiž

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \qquad (3.2)$$

Ta je v naší situaci ekvivalentní (3.1). Z těchto dvou možných definic má (3.1) některé výhody. Číselná hodnota $\binom{n}{k}$ se z ní snadněji spočítá a při výpočtu vycházejí menší mezivýsledky. Navíc (3.1) má smysl pro libovolné reálné číslo n (o tom více v kapitole 12) a speciálně definuje hodnotu $\binom{n}{k}$ i pro přirozené číslo $n < k$; v takovém případě je hodnota $\binom{n}{k}$ rovna 0.

Základní kombinatorický význam kombinačního čísla $\binom{n}{k}$ je *počet všech k-prvkových podmnožin n-prvkové množiny.* To za chvilku dokážeme, nejdřív jedno označení.

3.3.1 Definice. *Nechť X je množina a k nezáporné celé číslo. Symbolem*

$$\binom{X}{k}$$

budeme značit množinu všech k-prvkových podmnožin množiny X.

Příklad:

$$\binom{\{a,b,c\}}{2} = \{\{a,b\},\{a,c\},\{b,c\}\}.$$

Symbol $\binom{x}{k}$ tedy má nyní dva významy, podle toho, zda x je číslo nebo množina. Následující tvrzení je dává do souvislosti:

3.3.2 Tvrzení. *Pro každou konečnou množinu X je počet všech jejích k-prvkových podmnožin roven $\binom{|X|}{k}$.*

V symbolech můžeme toto tvrzení zapsat

$$\left|\binom{X}{k}\right| = \binom{|X|}{k}.$$

Důkaz. Označme $n = |X|$. Budeme dvěma způsoby počítat všechny *uspořádané* k-tice, které lze utvořit z prvků množiny X (bez opakování). Na jedné straně tento počet je $n(n-1)\cdots(n-k+1)$ podle tvrzení 3.1.4 (viz poznámku za jeho důkazem). Na druhé straně, z jedné k-prvkové podmnožiny $M \in \binom{X}{k}$ můžeme vyrobit $k!$ různých uspořádaných k-tic, a každou uspořádanou k-tici dostaneme z nějaké podmnožiny právě jednou. Proto

$$n(n-1)\cdots(n-k+1) = k!\left|\binom{X}{k}\right|.$$

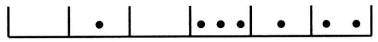
□

Ještě jedna základní úloha vedoucí ke kombinačním číslům. Kolika způsoby můžeme nezáporné celé číslo m zapsat jako součet r nezáporných celých sčítanců (přičemž záleží na pořadí sčítanců)? Jinak řečeno, chceme zjistit, kolik existuje uspořádaných r-tic $(i_1, i_2, \ldots, i_r)$ nezáporných celých čísel, splňujících rovnici

$$i_1 + i_2 + \cdots + i_r = m. \qquad (3.3)$$

Odpověď je kombinační číslo $\binom{m+r-1}{r-1}$. To se dá dokázat různými způsoby; zde popíšeme důkaz téměř ve stylu kouzelnického triku.

Představme si, že každé proměnné $i_1, i_2, \ldots, i_r$ odpovídá jedna z r přihrádek. Máme m nerozlišitelných kuliček, a chceme je do těchto přihrádek nějak rozmístit (předpokládáme, že do každé z přihrádek se v případě potřeby vejde i všech m kuliček najednou). Každé možné rozmístění kóduje jedno řešení rovnice (3.3). Zajímá nás tedy, kolika způsoby můžeme rozmístit kuličky do přihrádek. Jedno takové rozmístění, pro $m = 7$ a $r = 6$, vypadá takto:



Odpovídá rozkladu $0+1+0+3+1+2=7$. Necháme nyní zmizet dna přihrádek a dvě krajní stěny, takže zůstane jen m kuliček a $r-1$ přepážek, oddělujících přihrádky:

$$|\ \bullet\ |\ |\ \bullet\ \bullet\ \bullet\ |\ \bullet\ |\ \bullet\ \bullet$$

(navíc jsme pro lepší estetický dojem kuličky a přihrádky trochu posunuli). Tato situace stále obsahuje plnou informaci o rozdělení kuliček do přihrádek. Zvolit takové rozdělení tedy znamená vybrat pozice vnitřních přepážek mezi kuličkami. Jinak řečeno, máme $m+r-1$ předmětů, kuliček a vnitřních přepážek, srovnaných v řadě, a určíme, které pozice zaujmou kuličky a které přepážky. To odpovídá výběru $r-1$ pozic z $m+r-1$ možných, takže se to dá udělat $\binom{m+r-1}{r-1}$ způsoby. □

Jednoduché vlastnosti kombinačních čísel. Jedním dobře známým vzorcem je

$$\binom{n}{k} = \binom{n}{n-k}. \tag{3.4}$$

Jeho správnost (pro $n \geq k \geq 0$) je ihned vidět z již zmíněného vztahu $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ Kombinatoricky to znamená, že k-prvkových podmnožin n-prvkové množiny je stejně jako podmnožin s $n-k$ prvky, což můžeme nahlédnout bez odvolávání se na kombinační čísla – stačí každé k-prvkové podmnožině přiřadit její doplněk.

Dosti důležitý je vzorec pro součet kombinačních čísel

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}. \tag{3.5}$$

Jeden elegantní důkaz je založen na kombinatorické interpretaci obou stran (3.5). Pravá strana je počet k-prvkových podmnožin n-prvkové množiny X. Zvolme jeden prvek $a \in X$ a rozdělme všechny k-prvkové podmnožiny X do dvou skupin podle toho, zda obsahují a. Podmnožiny neobsahující a jsou právě všechny k-prvkové podmnožiny $X \setminus \{a\}$, a je jich tudíž $\binom{n-1}{k}$. Je-li A nějaká k-prvková podmnožina X obsahující prvek a, můžeme jí přiřadit $(k-1)$-prvkovou množinu $A' = A \setminus \{a\}$. Je snadno vidět, že toto přiřazení je bijekce mezi všemi k-prvkovými podmnožinami X obsahujícími prvek a a všemi $(k-1)$-prvkovými podmnožinami množiny $X \setminus \{a\}$. Posledně jmenovaných je $\binom{n-1}{k-1}$. Dohromady je tedy počet všech k-prvkových podmnožin X roven $\binom{n-1}{k} + \binom{n-1}{k-1}$. □

S identitou (3.5) je spojen tzv. Pascalův trojúhelník:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & \vdots & & & & & & \vdots & &
\end{array}$$

Každý další řádek v tomto schématu se vyrobí tak, že pod dvojici čísel z předchozího řádku se napíše jejich součet, a na kraje se doplní jedničky. Z (3.5) indukcí vyplývá, že v $(n+1)$-ním řádku jsou právě binomické koeficienty $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$.

Binomická věta. Rovnice (3.5) se také dá využít pro důkaz jiného známého tvrzení zahrnujícího binomické koeficienty – binomické věty (odtud i název „binomické koeficienty“). Tato věta praví, že pro nezáporné celé číslo n

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{3.6}$$

(je to rovnost dvou mnohočlenů v proměnné x, speciálně tedy platí pro každé konkrétní reálné číslo x).

Z binomické věty můžeme dostat všelijaké vztahy pro binomické koeficienty. Nejjednodušší z nich vznikne patrně posazením $x=1$ a zní

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n. \tag{3.7}$$

Kombinatoricky to ovšem není nic jiného než počítání všech podmnožin n-prvkové množiny; na levé straně jsme je napřed rozdělili podle velikosti.

Druhý důkaz tvrzení 3.1.3 (o počtu podmnožin liché velikosti). Dosazením $x = -1$ do binomické věty vyjde

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots = \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0. \qquad (3.8)$$

Sečteme-li tuto rovnost s (3.7), budou na levé straně jen binomické koeficienty se sudým k, a každý z nich bude vynásoben 2, tj.

$$2\left[\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots\right] = 2^n.$$

V hranaté závorce na levé straně stojí právě počet všech podmnožin n-prvkové množiny se sudým počtem prvků. Proto má n-prvková množina právě 2^{n-1} podmnožin sudé velikosti. □

Další identity s kombinačními čísly. Jsou známy doslova tisíce různých vztahů a identit pro kombinační čísla; jsou jim věnovány celé knihy. Zde si předvedeme ještě jednu formuli, která má pěkný kombinatorický důkaz. Další vzorce zmíníme ve cvičení a v kapitole 12.

3.3.3 Tvrzení.

$$\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}.$$

Důkaz. První trik je přepsat sumu pomocí (3.4) – symetrie kombinačního čísla – na

$$\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}.$$

Teď ukážeme, že tato suma vyjadřuje počet n-prvkových podmnožin $2n$-prvkové množiny (a tedy se rovná pravé straně v dokazovaném vzorci). Vezměme $2n$-prvkovou množinu X, a obarvěme n jejích prvků červeně a zbývajících n prvků modře. Zvolit podmnožinu množiny X znamená totéž, jako zvolit nějakou i-prvkovou podmnožinu červených prvků a nějakou $(n-i)$-prvkovou podmnožinu modrých prvků, kde

$i \in \{0, 1, \ldots, n\}$. Pro dané i máme pro výběr červené podmnožiny $\binom{n}{i}$ možností, a pro výběr modré podmnožiny $\binom{n}{n-i}$ možností, celkem tedy $\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i}$ možností volby červené a modré podmnožiny s dohromady n prvky. □

Multinomické koeficienty a multinomická věta. Jeden z oblíbených příkladů v amerických učebnicích je tenhle: Kolik různých slov (včetně nesmyslných) můžeme sestavit s použitím (všech) písmen slova MISSISSIPPI? (Tím doufáme čtenáře, v případě potřeby, i nenásilně poučit o pravopisu.) Nejdřív si představme, že stejná písmena v názvu otce řek odlišíme indexy: $M_1I_1S_1S_2I_2S_3S_4I_3P_1P_2I_4$. Tím máme 11 různých písmen, která lze rozestavit 11! různými způsoby. Uvažme nyní jedno (libovolné) slovo vyrobené z „neoindexované" MISSISSIPPI, např. SIPISMSIPIS. Z kolika „oindexovaných" rozestavení vznikne toto slovo vymazáním indexů? Indexy u čtyř písmen S mohou být rozmístěny 4! způsoby, nezávisle na tom indexy u čtyř I také 4! způsoby, pro dvě P máme 2! možností, a konečně pro jediné M jednu (neboli 1!) možnost. Tím pádem slovo SIPISMSIPIS (i každé jiné utvořené z MISSISSIPPI) lze oindexovat 4!4!2!1! způsoby, a proto počet neoindexovaných slov, tj. odpověď na úlohu, je $11!/(4!4!2!1!)$.

Stejnou úvahou se zjistí následující výsledek: máme-li předměty m druhů, k_i předmětů od i-tého druhu (a předměty jednoho druhu jsou nerozlišitelné), přičemž $k_1 + \cdots + k_m = n$, potom počet jejich různých seřazení je dán výrazem

$$\frac{n!}{k_1!k_2!\cdots k_m!}.$$

Tento výraz se někdy zapisuje symbolem

$$\binom{n}{k_1, k_2, \ldots, k_m}$$

a nazývá se *multinomický koeficient*. Speciálně pro $m = 2$ dostáváme binomický koeficient, tedy $\binom{n}{k,n-k}$ je totéž co $\binom{n}{k}$. Proč název multinomický koeficient? Vysvětlení dává následující věta:

3.3.4 Věta (Multinomická věta). *Pro libovolná čísla $x_1, \ldots, x_m \in \mathbf{R}$ a libovolné celé $n \geq 1$ platí rovnost*

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{\substack{k_1+\cdots+k_m=n \\ k_1,\ldots,k_m \geq 0}} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \ldots x_m^{k_m}.$$

Tato věta se dá dokazovat, podobně jako věta binomická, indukcí podle n (viz cvičení 21). Přirozenější důkaz vyplyne z metod části 12.1 (cvičení 3).

Cvičení

1. Dokažte součtový vzorec (3.5) použitím definice (3.1) pro kombinační čísla a početní úpravou.

2. (a) Dokažte vzorec

$$\binom{r}{r}+\binom{r+1}{r}+\binom{r+2}{r}+\cdots+\binom{n}{r}=\binom{n+1}{r+1}. \tag{3.9}$$

indukcí podle n (při pevném r). Uvědomte si, co říká pro $r=1$.

(b)* Dokažte týž vzorec kombinatoricky.

3.* Pro přirozená čísla $m \le n$ spočítejte (=vyjádřete jednoduchým vzorcem bez použití sumy) $\sum_{k=m}^{n} \binom{k}{m}\binom{n}{k}$.

4. Spočítejte (=vyjádřete jednoduchým vzorcem bez použití sumy)
(a) $\sum_{k=1}^{n} \binom{k}{m}\frac{1}{k}$,
(b)* $\sum_{k=0}^{n} \binom{k}{m}k$.

5.** Dokažte

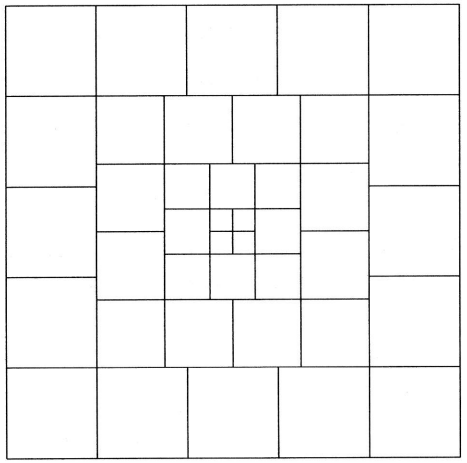
$$\sum_{k=0}^{m}\binom{m}{k}\binom{n+k}{m}=\sum_{k=0}^{m}\binom{m}{k}\binom{n}{k}2^k.$$

6.* Kolik existuje funkcí $f : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$, které jsou *monotonní*, tj. pro $i<j$ platí $f(i) \le f(j)$?

7. Kolik členů má rozvoj výrazu $(x_1+\cdots+x_m)^n$ podle multinomické věty?

8.* Kolik existuje k-prvkových podmnožin množiny $\{1,2,\ldots,n\}$, v nichž se nevyskytují žádná 2 po sobě jdoucí čísla?

9. (a) S použitím vzorce (3.9) pro $r=2$ vyjádřete součty $\sum_{i=2}^{n} i(i-1)$ a $\sum_{i=1}^{n} i^2$.
(b) S pomocí (a) a vzorce (3.9) pro $r=3$ spočítejte $\sum_{i=1}^{n} i^3$.
(c)* Odvoďte výsledek (b) podle takovéhoto obrázku:



10. Dokažte binomickou větu indukcí podle n.

11. Dokažte *Leibnizovu formuli* pro derivování součinu: nechť u, v jsou funkce jedné proměnné, $u^{(k)}$ značí k-tou derivaci funkce u. Potom

$$(uv)^{(n)}=\sum_{k=0}^{n}\binom{n}{k}u^{(k)}v^{(n-k)}$$

(za předpokladu že všechny uvedené derivace existují).

12. Buď p prvočíslo, n, k přirozená čísla.
(a) Dokažte, že pro $k<p$ je $\binom{p}{k}$ dělitelné p.
(b) Dokažte, že $\binom{n}{p}$ je dělitelné p právě když $\lfloor n/p \rfloor$ je dělitelné p.

13. (a)* Pomocí binomické věty odvoďte vztah pro počet podmnožin n-prvkové množiny, jejichž velikost je dělitelná 4.
(b)* Spočítejte počet podmnožin n-prvkové množiny velikosti dělitelné 3.

14. Máme n druhů předmětů, a chceme určit, kolika způsoby můžeme vybrat k-tici předmětů. Uvažujeme varianty jednak podle toho, zda vybíráme uspořádané nebo neuspořádané k-tice, a jednak podle toho, zda máme k dispozici od každého druhu jen 1 předmět nebo libovolně mnoho předmětů. Vyplňte počty v následující tabulce:

	Jen 1 předmět každého druhu	Libovolně předmětů každého druhu
Uspořádané k-tice		
Neuspořádané k-tice		

15. Máme k kuliček, rozmísťujeme je do n (očíslovaných) přihrádek. Vyplňte počty možných rozmístění ve variantách v následující tabulce:

	≤ 1 kulička do každé přihrádky	Libovolný počet kuliček do přihrádky
Kuličky jsou různobarevné (rozlišitelné)		
Kuličky jsou nerozlišitelné		

16.* Kolika způsoby lze rozestavit 5 vodníků a 7 čarodějnic do řady tak, že žádní 2 vodníci nestojí vedle sebe?

17. Na stole je prostřeno 13 velkých talířů, máme 5 vařených raků (nerozlišitelných) a 8 nadívaných hlemýžďů (též nerozlišitelných). Kolik je způsobů, jak servírovat raky a hlemýždě na talíře (podstatný je postup servírování, tj. jako bychom se ptali na počet různých filmových scénářů popisujících servírování, např. „nandat hlemýždě na talíř č.5, potom nandat raka na talíř č.7, ...)

(a) má-li se něco nadělit na každý talíř

(b) není-li žádné takové omezení, tj. např. všechno může přijít na jeden talíř.

18. V senátu zasedá 100 senátorů, po 2 z každého z 50 států. Kolika způsoby lze zvolit 4-členný výbor tak, aby v něm nebyli 2 senátoři z téhož státu?

19.* Uvažme pravidelný n-úhelník. Rozdělíme ho diagonálami na trojúhelníky tak, aby každý z nich měl aspoň jednu stranu společnou s naším n-úhelníkem. Kolik existuje takových rozdělení (triangulací)?

20. Najděte koeficient při x^2y^8z ve výrazu $(2x + y^2 - 5z)^7$.

21. (a) Dokažte rovnost

$$\binom{n}{k_1, k_2, \ldots, k_m} = \binom{n-1}{k_1 - 1, k_2, k_3, \ldots, k_m} + \binom{n-1}{k_1, k_2 - 1, k_3, \ldots, k_m} + \cdots + \binom{n-1}{k_1, k_2, \ldots, k_{m-1}, k_m - 1}$$

$(n \geq 1,\ k_1 + \cdots + k_m = n,\ k_i \geq 1)$.

(b) Dokažte multinomickou větu indukcí podle n.

3.4 Odhady funkcí: faktoriál

V této části budeme odpovídat na otázku „Jak rychle roste funkce $n!$ (faktoriál čísla n)?“.

Na první pohled se může zdát, že sama definice faktoriálu, $n! = 1 \times 2 \times \cdots \times n$, nám o této funkci říká všechno, co můžeme kdy potřebovat: Pro malé n lze $n!$ velmi rychle vyčíslit na počítači, a pro větší n by leckdo mohl prohlásit, že hodnoty faktoriálu již nemají v „reálném“ světě žádný smysl, neboť jsou příliš velké – např. již $70! > 10^{100}$, jak asi ví mnoho majitelů kalkulaček. V různých matematických úvahách však potřebujeme srovnat rychlost růstu funkce $n!$ s jinými funkcemi, a to i pro velmi velké hodnoty n. K tomu samotná definice není zvlášť vhodná, a často ani výpočet hodnot počítačem moc nepomůže. V takových situacích přijdou ke slovu *odhady*, které vyšetřovanou funkci, třeba $n!$, šikovně srovnávají s nějakou „jednodušší“ funkcí, například vhodnou mocninnou funkcí a podobně. V následujícím si několik takových odhadů předvedeme. Ukážeme několik metod a triků, jimiž se dají dělat odhady i pro jiné funkce, sumy, součiny apod. Nejdříve ale zavedeme užitečné značení pro porovnávání rychlosti růstu funkcí, hojně používané např. při analýze algoritmů.

Asymptotické porovnávání funkcí. Často je potřeba vyjádřit skutečnosti jako např. že funkce n^2 je „větší“ než funkce $10n+5$ a „zhruba

stejně velká“ jako funkce $n^2 + n\sqrt{n}$ (přitom chceme porovnávat rychlost růstu funkcí pro velká n). K tomu se zavádí následující definice.

Nechť f, g jsou reálné funkce jedné proměnné definované na přirozených číslech, přičemž zpravidla předpokládáme, že hodnoty f i g jsou nezáporné. Zápis

$$f(n) = O(g(n))$$

znamená, že existují konstanty n_0 a C takové, že pro všechna $n \geq n_0$ platí $|f(n)| \leq Cg(n)$. Místo $f(n)$ a $g(n)$ se v tomto zápise objevují i konkrétní formule; například můžeme psát $10n^2 + 5n = O(n^2)$. Zápisu $f(n) = O(g(n))$ tedy můžeme rozumět tak, že funkce f neroste podstatně rychleji než g, neboli že $f(n)/g(n)$ neroste do nekonečna. Zdůrazněme ještě, že ačkoliv se v zavedeném zápisu vyskytuje rovnítko, zápis je nesymetrický (ve své podstatě je to nerovnost). Nepíše se tedy $O(f(n)) = g(n)$!

Poznámky. Někdy se podobný zápis používá i pro funkce více proměnných; například $f(m, n) = O(g(m, n))$ znamená, že pro nějaké konstanty n_0, m_0, C a pro všechny hodnoty $m \geq m_0$ a $n \geq n_0$ platí

$$|f(n, m)| \leq Cg(m, n).$$

Pomocí symbolu $O(.)$ můžeme zapsat i přesnější srovnání funkcí. Třeba zápisu

$$f(n) = g(n) + O(n^3)$$

se má rozumět tak, že funkce f roste stejně rychle jako g, až na „chybu“ řádu n^3, neboli že $f(n) - g(n) = O(n^3)$. Jednoduchý konkrétní příklad je např.

$$\binom{n}{2} = \frac{n(n-1)}{2} = \frac{n^2}{2} + O(n).$$

V literatuře se běžně vyskytuje ještě několik symbolů pro jiné „nerovnosti“ mezi rychlostí růstu funkcí. Pro přehled uvedeme jejich definice ve formě tabulky:

Zápis	Definice	Význam
$f(n) = o(g(n))$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$	f roste podstatně pomaleji než g
$f(n) = \Omega(g(n))$	$g(n) = O(f(n))$	f roste aspoň tak rychle jako g
$f(n) = \Theta(g(n))$	$f(n) = O(g(n))$ a $f(n) = \Omega(g(n))$	f a g rostou řádově stejně rychle
$f(n) \sim g(n)$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$	$f(n)$ a $g(n)$ rostou asi stejně rychle

Odhady funkce faktoriál. Pro každé $n \geq 1$ je zřejmě pravda

$$n! \leq n^n$$

jak je vidět z definice faktoriálu.

Přesnější odhad ukázal pěkným trikem Gauss (neboli, německy psáno, Gauß):

3.4.1 Věta. *Pro každé $n \geq 1$*

$$n^{n/2} \leq n! \leq \left(\frac{n+1}{2}\right)^n.$$

Důkaz začneme nerovností mezi aritmetickým a geometrickým průměrem. Pro kladná reálná čísla a, b definujeme *aritmetický průměr* a a b výrazem $\frac{a+b}{2}$, a *geometrický průměr* a a b výrazem $\sqrt{ab}$.

3.4.2 Lemma. *Pro každou dvojici kladných reálných čísel a, b, geometrický průměr je nejvýše roven aritmetickému.*

Důkaz. Druhá mocnina reálného čísla je vždy kladná, speciálně tedy $(\sqrt{a} - \sqrt{b})^2 \geq 0$. Po rozepsání levé strany máme $a - 2\sqrt{ab} + b \geq 0$,

a přičtením výrazu $2\sqrt{ab}$ k oběma stranám nerovnosti a dělením 2 vyjde $\sqrt{ab} \leq (a+b)/2$, což je požadovaná nerovnost. □

Důkaz věty 3.4.1. Platí

$$\begin{aligned}(n!)^2 &= 1 \times 2 \times \cdots \times (n-1) \times n \times n \times (n-1) \times \cdots \times 2 \times 1 = \\ &= (1 \times n)(2 \times (n-1)) \cdots ((n-1) \times 2)(n \times 1) = \\ &= \prod_{i=1}^{n} i(n+1-i)\end{aligned} \tag{3.10}$$

(čísla v součinu jsme jenom přerovnali a sdružili do dvojic). Zvolíme-li v lemmatu 3.4.2 $a = i$, $b = n+1-i$, dostáváme

$$\sqrt{i(n+1-i)} \leq \frac{i+n+1-i}{2} = \frac{n+1}{2},$$

čili podle (3.11)

$$n! = \prod_{i=1}^{n} \sqrt{i(n+1-i)} \leq \prod_{i=1}^{n} \frac{n+1}{2} = \left(\frac{n+1}{2}\right)^n,$$

což dokazuje jednu z nerovností v tvrzení věty 3.4.1. Abychom ukázali druhou nerovnost, uvažme součin $i(n+1-i)$. Pro $i = 1$ a $i = n$ je roven n, a pro $2 \leq i \leq n-1$ máme součin dvou čísel, z nichž větší je aspoň $n/2$ a menší je nejméně 2, tedy součin je také nejméně n. Pokaždé tedy $i(n+1-i) \geq n$, a odtud

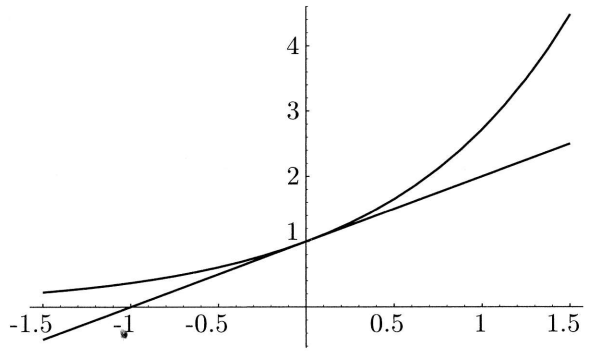
$$(n!)^2 = \prod_{i=1}^{n} i(n+1-i) \geq \prod_{i=1}^{n} n = n^n,$$

a proto $n! \geq \sqrt{n^n} = n^{n/2}$, jak jsme chtěli dokázat. □

Příklad. Každý z n lidí si z osudí obsahujícího čísla $1, 2, \ldots, n$ vylosuje jedno číslo, zapamatuje si ho a vrátí do osudí. Jaká je pravděpodobnost, že žádní dva nemají totéž číslo? Řečeno matematicky, jaká je pravděpodobnost, že náhodně zvolené zobrazení množiny $\{1, 2, \ldots, n\}$ do sebe bude permutace? Všech zobrazení je n^n, permutací je $n!$, hledaná pravděpodobnost je $n!/n^n$. Z horního odhadu z věty 3.4.1 spočítáme

$$\frac{n!}{n^n} \leq \left(\frac{n+1}{n}\right)^n 2^{-n} \leq e\, 2^{-n},$$

hledaná pravděpodobnost tedy exponenciálně klesá. Z přesnějších odhadů dokázaných níže se pak dostane, že uvedená pravděpodobnost se chová přibližně jako funkce e^{-n}.



Obrázek 3.1: Funkce $y = 1 + x$ a $y = e^x$ v okolí počátku.

Teď jinými postupy odhad z věty 3.4.1 vylepšíme. V dokonalejším odhadu bude vystupovat *Eulerovo číslo* $e = 2.718281828\ldots$, základ přirozených logaritmů. O této pozoruhodné konstantě se čtenář více dozví v matematické analýze. Zde budeme potřebovat následující užitečný

3.4.3 Fakt. *Pro každé reálné číslo x platí*

$$1 + x \leq e^x$$

(viz obrázek 3.1).

S jeho pomocí dokážeme:

3.4.4 Věta. *Pro každé $n \geq 1$,*

$$e\left(\frac{n}{e}\right)^n \leq n! \leq en\left(\frac{n}{e}\right)^n.$$

První důkaz (matematickou indukcí). Ukážeme pouze horní odhad $n! \leq en(n/e)^n$, dolní odhad ponecháváme jako cvičení 8. Pro $n = 1$ je pravá strana nerovnosti rovna 1, tvrzení tedy platí. Předpokládejme, že jsme je již dokázali pro $n-1$, a odvodíme je pro n. Máme

$$n! = n(n-1)! \leq ne(n-1)\left(\frac{n-1}{e}\right)^{n-1}$$

podle indukčního předpokladu. Pravou stranu dále upravíme na tvar

$$\left[en\left(\frac{n}{e}\right)^n\right] \times \left(\frac{n-1}{n}\right)^n e.$$

V hranaté závorce je výraz, kterým bychom potřebovali shora omezit $n!$, abychom dostali dokazovanou nerovnost pro n. Stačí tedy ukázat, že zbývající část výrazu nepřevyšuje 1. Úpravou a použitím faktu 3.4.3 pro $x = -\frac{1}{n}$ dostáváme

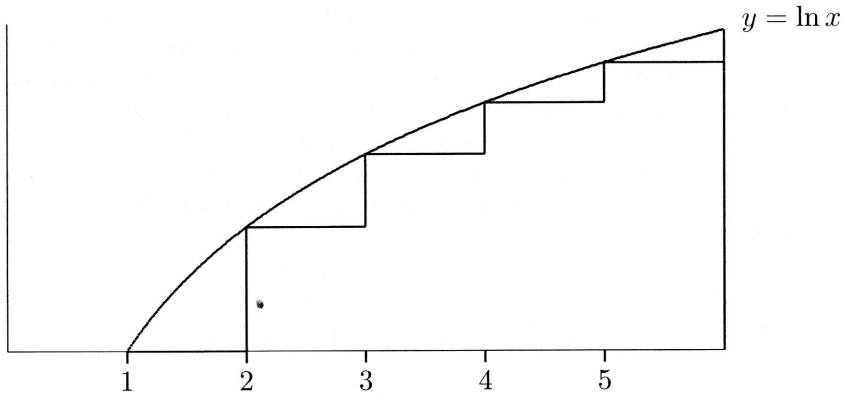
$$e\left(\frac{n-1}{n}\right)^n = e\left(1-\frac{1}{n}\right)^n \leq e\left(e^{-1/n}\right)^n = e \times e^{-1} = 1.$$

□

Ještě poznamenejme, že fakt 3.4.3 je *jediná* vlastnost čísla e, kterou jsme v důkazu použili – například numerická hodnota e se tam vůbec neobjevila. Fakt 3.4.3 totiž číslo e charakterizuje: pokud pro nějaké reálné číslo a platí $1 + x \leq a^x$ pro všechna $x \in \mathbf{R}$, potom už $a = e$. Existence čísla e s touto vlastností se ovšem musí dokázat prostředky matematické analýzy.

Druhý důkaz věty 3.4.4 (pomocí integrálu). Zase uděláme jenom horní odhad. Vyjdeme z definice faktoriálu $n! = 1 \times 2 \times \cdots \times n$ a obě strany zlogaritmujeme. Máme tedy

$$\ln n! = \ln 1 + \ln 2 + \cdots + \ln n$$



Obrázek 3.2: Odhad plochy pod stupňovitou funkcí pomocí integrálu

(funkce ln je logaritmus o základu e). Výraz na pravé straně si můžeme představit jako plochu pod grafem stupňovité funkce na intervalu $[1, n+1]$, jejíž hodnota na intervalu $[i, i+1)$ je rovna $\ln i$, viz obr. 3.2. Uvedená stupňovitá funkce je v každém bodě $x \in [1, n+1)$ nejvýš rovna $\ln x$, čili plocha pod jejím grafem nepřevyšuje plochu pod grafem funkce $\ln x$ na tomto intervalu. Odtud

$$\ln n! \leq \int_1^{n+1} \ln x \, dx = (n+1)\ln(n+1) - n,$$

jak se spočte jako jednoduché cvičení na integrování. Tento odhad můžeme dále upravit

$$n! \leq e^{(n+1)\ln(n+1)-n} = \frac{(n+1)^{n+1}}{e^n}.$$

To ještě není ten tvar, který chceme. Ale, můžeme použít tento vzorec pro $n-1$, a tím už vyjde tvar, uvedený ve větě:

$$n! = n(n-1)! \leq n\frac{n^n}{e^{n-1}} = en\left(\frac{n}{e}\right)^n.$$

□

Zvídavý čtenář si může rozmyslet, kde se číslo e vlastně vezme v právě uvedeném druhém důkazu. Zdánlivě jsme ho tam vpašovali uměle, protože jsme na začátku vzali přirozený logaritmus $n!$. Mohli jsme ale použít logaritmus o libovolném jiném základu a a e by v konečném odhadu vyšlo stejně, jenom s trochu složitějším počítáním.

Pro zajímavost (a pro vzbuzení čtenářovy zvědavosti?) zmiňme ještě přesnější odhad pro $n!$, známý pod jménem *Stirlingova formule*: Definujeme-li funkci

$$f(n) = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

(kde $\pi = 3.1415926535\ldots$ je Ludolfovo číslo), platí $f(n) \sim n!$, neboli

$$\lim_{n\to\infty} \frac{f(n)}{n!} = 1,$$

to znamená, že odhadneme-li číslo $n!$ hodnotou $f(n)$, pak relativní chyba tohoto odhadu se blíží 0 pro n rostoucí do nekonečna; např. pro $n = 8$ je chyba okolo 1%. Všimněme si, že Stirlingova formule je zhruba „uprostřed“ mezi odhady z věty 3.4.4 (viz též cvičení 9).

Cvičení

1. Rozmyslete si, co říkají následující zápisy, a rozhodněte, zda jsou pravdivé.
   (a) $n^2 = O(n^2 \ln n)$
   (b) $n^2 = o(n^2 \ln n)$
   (c) $n^2 + 5n \ln n = n^2(1 + o(1)) \sim n^2$
   (d) $n^2 + 5n \ln n = n^2 + O(n)$
   (e) $n! \sim ((n+1)/2)^n$
   (f) $\ln(n!) = \Omega(n \ln n)$
   (g) $\sum_{i=1}^{n} i^8 = \Theta(n^9)$
   (h) $\sum_{i=1}^{n} \sqrt{i} = \Theta(n^{3/2})$.

2. Jaký je význam zápisů: $C = O(1)$, $c = \Omega(1)$, $f(n) = n^{O(1)}$? Jak je krátce vyjádřit bez použití symbolu $O(.)$?

3. Srovnejte následující funkce podle rychlosti růstu, a zapište vztahy mezi nimi pomocí značení, zavedeného v této části: $n \ln n$, $(\ln \ln n)^{\ln n}$, $(\ln n)^{\ln \ln n}$, $ne^{\sqrt{\ln n}}$, $(\ln n)^{\ln n}$, $n2^{\ln \ln n}$, $n^{1+1/(\ln \ln n)}$, $n^{1+1/\ln n}$, n^2.

4.* Dokažte fakt 3.4.3.

5. (a) Vyšetřete, pro které dvojice reálných čísel (a, b), $a, b > 0$, platí $\sqrt{ab} = (a+b)/2$.

   (b) *Harmonický průměr* kladných čísel a, b se definuje výrazem $2ab/(a+b)$. Zjistěte, v jakém vztahu (nerovnosti) je harmonický průměr vzhledem k aritmetickému a geometrickému.

6. Nechť $x_1, x_2, \ldots, x_n$ jsou kladná reálná čísla. Jejich *aritmetický průměr* je $(x_1 + x_2 + \cdots + x_n)/n$, a jejich *geometrický průměr* se definuje jako $\sqrt[n]{x_1 x_2 \cdots x_n}$. Nechť $AG(n)$ značí tvrzení „pro každou n-tici kladných reálných čísel $x_1, x_2, \ldots, x_n$ je geometrický průměr nejvýš roven aritmetickému“. Dokažte platnost $AG(n)$ pro každé n následující (podivnou) indukcí:

   (a) Dokažte že z $AG(n)$ plyne $AG(2n)$, pro libovolné n.

   (b)* Dokažte že z $AG(n)$ plyne $AG(n-1)$, pro libovolné $n > 1$.

   (c) Vysvětlete, proč z (a) a (b) plyne platnost $AG(n)$ pro všechna n.

7.* Definujme posloupnosti $\{a_n\}_{n=0}^{\infty}$ a $\{b_n\}_{n=0}^{\infty}$ takto: $a_0 = 2$, $b_0 = 4$, $a_{n+1} = \sqrt{a_n b_n}$, $b_{n+1} = 2a_{n+1}b_n/(a_{n+1} + b_n)$. Dokažte, že obě posloupnosti konvergují k číslu π (návod: najděte souvislost s pravidelnými mnohoúhelníky opsanými a vepsanými jednotkové kružnici). *Poznámka:* Tato metoda (Archimédova) výpočtu π není příliš efektivní. Mnohem rychlejší algoritmus je např. tento: $x_1 = 2^{-3/4} + 2^{-5/4}$, $y_1 = \sqrt[4]{2}$, $\pi_0 = 2 + \sqrt{2}$, $\pi_n = \pi_{n-1}(x_n + 1)/(y_n + 1)$, $y_{n+1} = (y_n\sqrt{x_n} + 1/\sqrt{x_n})/(y_n + 1)$, $x_{n+1} = (\sqrt{x_n} + 1/\sqrt{x_n})/2$. Tento i další algoritmy a pozoruhodnou související teorii lze najít např. v [6].

8. Dokažte dolní odhad $n! \geq e(n/e)^n$ ve větě 3.4.4

   (a) indukcí (šikovně využijte faktu 3.4.3),

   (b) pomocí integrálu.

9.* Dokažte následující horní odhad (který je již velmi blízký Stirlingově formuli): $n! \leq e\sqrt{n}\,(n/e)^n$. Vyjděte z důkazu věty 3.4.4 pomocí integrálu, ale od plochy pod křivkou $y = \ln x$ odečtěte ještě plochu vhodných trojúhelníčků.

10. Dokažte *Bernoulliho nerovnost*: Pro každé přirozené n a pro každé reálné $x \geq -1$ platí $(1+x)^n \geq 1 + nx$.

11. Dokažte, že pro $n = 1, 2, \ldots$,

$$2\sqrt{n+1} - 2 < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \leq 2\sqrt{n} - 1.$$

12. V analýze různých algoritmů se často objevuje součet

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{i=1}^{n} \frac{1}{i}$$

(tzv. *harmonické číslo*).

(a) Ukažte, že pro každé přirozené m, $1 + \frac{m}{2} \leq H_n < m + 1$, kde $n = 2^m$.

(b) Dokažte pomocí integrálu, že $\ln n < H_n < \ln n + 1$.

3.5 Odhady: binomické koeficienty

Podobně jako jsme vyšetřovali chování funkce $n!$, budeme se teď zabývat funkcí

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{1 \times 2 \times \cdots \times k} = \prod_{i=0}^{k-1} \frac{n-i}{k-i}. \tag{3.11}$$

Je hned vidět, že

$$\binom{n}{k} \leq n^k,$$

a pro mnoho použití s tímto jednoduchým odhadem vystačíme. Pro $k > n/2$ je ovšem výhodné napřed použít vztahu $\binom{n}{k} = \binom{n}{n-k}$.

Abychom odvodili dolní odhad, podíváme se na definici binomického koeficientu zapsanou jako součin zlomků, tak jako v (3.11). Pro $n \geq k > i \geq 0$ platí $(n-i)/(k-i) \geq n/k$, a proto

$$\binom{n}{k} \geq \left(\frac{n}{k}\right)^k.$$

Následující vylepšený horní odhad je podobného tvaru, a na jeho důkazu předvedeme ještě jednu další metodu.

3.5.1 Věta. *Pro každé $n \geq 1$ a pro každé k, $1 \leq k \leq n$, platí*

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Důkaz. Ukážeme ve skutečnosti silnější nerovnost

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k} \leq \left(\frac{en}{k}\right)^k.$$

Vyjdeme z binomické věty, která pro libovolné reálné číslo x tvrdí

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = (1+x)^n.$$

Předpokládejme nyní, že $0 < x < 1$. Potom vynecháním některých sčítanců na levé straně dostaneme

$$\binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{k}x^k \leq (1+x)^n,$$

a vydělením obou stran číslem x^k máme

$$\frac{1}{x^k}\binom{n}{0} + \frac{1}{x^{k-1}}\binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Každé z kombinačních čísel na levé straně je vynásobeno číslem větším nebo rovným jedné (poněvadž jsme předpokládali $x < 1$); vynecháme-li tyto koeficienty, levou stranu nezvětšíme. Vyjde

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \frac{(1+x)^n}{x^k}.$$

Číslo x z intervalu $(0, 1)$ můžeme zvolit podle potřeby, a uděláme to tak, abychom učinili pravou stranu co nejmenší. Vhodná hodnota je $x = \frac{k}{n}$. Dosazením tohoto výrazu do pravé strany máme

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{k} \leq \left(1 + \frac{k}{n}\right)^n \left(\frac{n}{k}\right)^k.$$

Konečně s využitím faktu 3.4.3 vychází

$$\left(1 + \frac{k}{n}\right)^n \leq \left(e^{k/n}\right)^n = e^k,$$

a z toho už máme tvrzení věty 3.5.1. □

Kombinační číslo $\binom{n}{\lfloor n/2 \rfloor}$. Z definice kombinačního čísla snadno plyne následující vzorec:

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}.$$

Proto pro $k \leq n/2$ máme $\binom{n}{k} > \binom{n}{k-1}$, a naopak pro $k \geq n/2$ dostaneme symetricky $\binom{n}{k} > \binom{n}{k+1}$. Tudíž pro dané n jsou mezi kombinačními čísly $\binom{n}{k}$ největší ta prostřední: pro n sudé je $\binom{n}{n/2}$ větší než všechna ostatní, pro n liché jsou dvě největší kombinační čísla, $\binom{n}{\lfloor n/2 \rfloor}$ a $\binom{n}{\lceil n/2 \rceil}$.

Chování kombinačních čísel $\binom{n}{k}$ pro dané velké n a pro k blízké $n/2$ je znázorněno na obr. 3.3(a). Graf ve skutečnosti není souvislá křivka (protože $\binom{n}{k}$ je definováno jen pro celá k), ale pro velké n je bodů tolik, že vizuálně splývají v křivku. „Výška" této křivky je právě $\binom{n}{\lfloor n/2 \rfloor}$, a „šířka" zvonovitého tvaru je přibližně $2\sqrt{n}$ (to dokazovat nebudeme); měřítka na svislé a vodorovné ose jsou tedy podstatně odlišná. Křivka takovéhoto tvaru je velmi důležitá např. v teorii pravděpodobnosti (tzv. Gaussova křivka), kde např. dává typické rozložení chyb při měření nějaké veličiny, a vzniká v mnoha nečekaných souvislostech.

Jak je kombinační číslo $\binom{n}{\lfloor n/2 \rfloor}$ velké? Jednoduchý, ale mnohdy dostatečně přesný odhad je

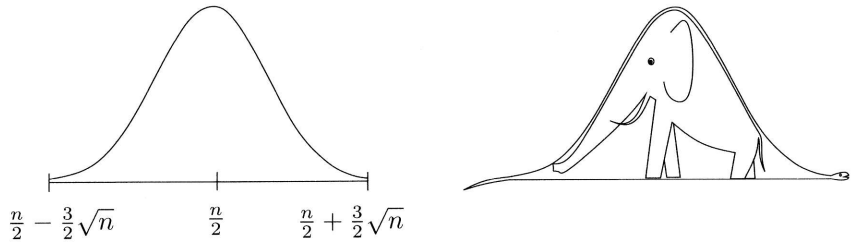
$$\frac{2^n}{n+1} \leq \binom{n}{\lfloor n/2 \rfloor} \leq 2^n.$$

Druhá nerovnost je zřejmá ze vztahu $\sum_{k=0}^{n}\binom{n}{k} = 2^n$, a první vlastně taky – $\binom{n}{\lfloor n/2 \rfloor}$ je největší mezi $n+1$ kombinačními čísly tvaru $\binom{n}{k}$, jejichž součet je 2^n.

Ukážeme podstatně přesnější odhad. Pro pohodlnější zápis budeme pracovat jen se sudými hodnotami n, tj. $n = 2m$.

3.5.2 Tvrzení. *Pro všechna $m \geq 1$ platí*

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}$$



(a) (b)

Obrázek 3.3: Znázornění relativní velikosti kombinačních čísel $\binom{n}{k}$ pro jedno velké n a k blízké $\frac{n}{2}$ (a); možná též klobouk, případně hroznýš, který sežral slona (b) – viz [27].

Důkaz. Obě nerovnosti dokážeme podobně. Uvažme číslo

$$P = \frac{1 \times 3 \times 5 \times \cdots \times (2m-1)}{2 \times 4 \times 6 \times \cdots \times 2m}$$

(v tomto kroku je zakódována skoro celá myšlenka důkazu). Protože

$$P = \frac{1 \times 3 \times 5 \times \cdots \times (2m-1)}{2 \times 4 \times 6 \times \cdots \times 2m} \cdot \frac{2 \times 4 \times \cdots \times (2m)}{2 \times 4 \times \cdots \times (2m)} = \frac{(2m)!}{2^{2m}(m!)^2},$$

dostáváme, že $P = \frac{1}{2^{2m}}\binom{2m}{m}$. Chceme tedy ukázat

$$\frac{1}{2\sqrt{m}} \leq P \leq \frac{1}{\sqrt{2m}}.$$

Pro horní odhad uvažme součin

$$\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{4^2}\right)\cdots\left(1 - \frac{1}{(2m)^2}\right),$$

který můžeme ekvivalentně přepsat na

$$\left(\frac{1 \times 3}{2^2}\right)\left(\frac{3 \times 5}{4^2}\right)\cdots\left(\frac{(2m-1)(2m+1)}{(2m)^2}\right) = (2m+1)P^2.$$

Protože hodnota součinu je zřejmě < 1, dostáváme $(2m+1)P^2 < 1$, a tedy $P \le 1/\sqrt{2m}$. Pro dolní odhad podobně uvážíme součin

$$\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\cdots\left(1-\frac{1}{(2m-1)^2}\right),$$

který přepíšeme na

$$\left(\frac{2\times 4}{3^2}\right)\left(\frac{4\times 6}{5^2}\right)\cdots\left(\frac{(2m-2)(2m)}{(2m-1)^2}\right)=\frac{1}{2(2m)P^2},$$

což dává $P \ge 1/2\sqrt{m}$. □

Poznamenejme, že aproximujeme-li $(2m)!$ a $m!$ pomocí Stirlingovy formule (kterou jsme ovšem nedokázali!), dostáváme ještě přesnější výsledek

$$\binom{2m}{m} \sim \frac{2^{2m}}{\sqrt{\pi m}}.$$

Uvažování odhadů čísel $\binom{2m}{m}$ se může zdát jako zbytečná kuriozita. Není tomu tak, a takové odhady mají zajímavé souvislosti např. s teorií čísel. Jedna z nejslavnějších matematických vět je následující tvrzení o hustotě prvočísel:

3.5.3 Věta (Prvočíselná věta). *Označme $\pi(n)$ počet prvočísel nepřevyšujících číslo n. Potom*

$$\pi(n) \sim \frac{n}{\ln n}$$

(čili $\lim_{n\to\infty} \pi(n)\ln n/n = 1$).

Je známo několik důkazů této věty, všechny jsou dost těžké (a hledání různých variací a zjednodušení pokračuje i dnes). Již v devatenáctém století ale našel Čebyšev jednoduchý důkaz takovéhoto slabšího výsledku:

$$\pi(n) = \Theta\left(\frac{n}{\ln n}\right)$$

tj. $c_1 n/\ln n \le \pi(n) \le c_2 n/\ln n$ pro jisté konstanty $c_2 \ge c_1 > 0$. Část důkazu lze založit na odhadech $2^{2m}/(2m+1) \le \binom{2m}{m} \le 2^{2m}$ (viz cvičení 3). Čebyšev dokázal rovněž tzv. *Bertrandův postulát: Pro každé $n \ge 1$ existuje prvočíslo p splňující $n < p \le 2n$.* Dnes asi nejjednodušší známý důkaz je založen (mimo jiné) právě na tvrzení 3.5.2. O těchto velmi pěkných souvislostech se čtenář může poučit např. v knize [7].

Cvičení

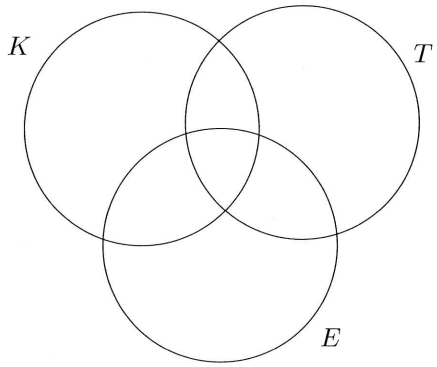
1. Dokažte odhad $\binom{n}{k} \le (en/k)^k$ indukcí podle k.
2. Srovnejte následující výrazy podle velikosti (předpokládejte, že n je velmi velké číslo):
   (a)
   $$\binom{2n}{n-1},\ \binom{2n}{n},\ \binom{2n}{10},\ n!,\ n^{\sqrt{n}},\ (\sqrt{n})^n,$$
   (b)
   $$3^n,\ \binom{2n}{n},\ \binom{2n}{2},\ \sum_{k=1}^{n} k!,\ n^n.$$
3. (a) Ukažte, že součin všech prvočísel p, $m < p \le 2m$, je nejvýš 2^{2m}.
   (b)* Pomocí (a) dokažte odhad $\pi(n) = O(n/\ln n)$, kde $\pi(n)$ je jako ve větě 3.5.3.
   (c)* Buď p prvočíslo, m, k přirozená čísla. Ukažte, že pokud p^k dělí $\binom{2m}{m}$, potom $p^k \le 2m$.
   (d) Pomocí (c) ukažte odhad $\pi(n) = \Omega(n/\ln n)$.

3.6 Princip inkluze a exkluze

Do češtiny bychom mohli název této části přeložit třeba „princip zahrnutí a vyloučení". Tím jsme tento pojem asi čtenáři ještě příliš neosvětlili, začněme tedy motivačním příkladem. Jako to již učinili jiní autoři u mnoha jiných příkladů o konečných množinách, uchýlíme se k formulaci s kluby na malém městě, a na znamení úcty k pravlasti klubů to budou kluby tenisový, kriketový a egyptologický.

3.6.1 Příklad. *Ve městě M. fungují 3 kluby. Tenisový klub má 20 členů, kriketový klub 15 členů a egyptologický klub je osmičlenný. Přitom z egyptologů jsou 2 hráči tenisu a 3 hráči kriketu, tenis a kriket zároveň provozuje 6 lidí, a jediná obzvláště agilní osoba je ve všech třech klubech. Kolik osob se celkem účastní klubového života v M.?*

Nejdřív cvičně spočítejme, kolik dohromady čítá členstvo řekněme tenisu a kriketu. Je vidět, že je třeba sečíst počet tenistů a kriketistů a odečíst osoby, které jsou v obou klubech a tedy jsme je počítali dvakrát; symbolicky zapsáno, $|T\cup K| = |T|+|K|-|T\cap K| = 20+15-6 = 29$.



Obrázek 3.4: Princip inkluze a exkluze pro 3 množiny.

Pokud čtenáře neodradí zjevná přihlouplost celého příkladu z praktického hlediska[1], najde patrně podobnými, ale komplikovanějšími úvahami odpověď pro 3 kluby, která je 33; dobré je si k tomu nakreslit obrázek (obr. 3.4).

Princip inkluze a exkluze je vztah, podle něhož lze řešit úlohy podobného typu obecně. Používá se v situaci, kdy chceme spočítat velikost sjednocení několika množin, a známe přitom velikosti všech možných průniků. Tak pro dvě množiny, K a T, jsme takový vzorec již uvedli, a pro 3 množiny K, T a E zní

$$|K \cup T \cup E| = |K| + |T| + |E| - |K \cap T| - |K \cap E| - |T \cap E| + |K \cap T \cap E|.$$

Slovně vyjádřeno, abychom dostali velikost sjednocení, sečteme napřed velikosti jednotlivých množin, pak odečteme velikosti průniků všech dvojic, a nakonec přičteme velikost průniku všech tří množin. Jak ukážeme za chvíli, takovýto návod funguje i pro obecný počet, n, konečných množin $A_1, A_2, \ldots, A_n$. Velikost jejich sjednocení, tj. $|A_1 \cup A_2 \cup \ldots \cup A_n|$, dostaneme takto: sečteme velikosti všech množin, odečteme velikosti průniků všech dvojic, přičteme velikosti průniků všech trojic, odečteme velikosti průniků čtveřic, atd.; jako poslední

[1] Což patrně indikuje jeho matematické sklony.

krok buď přičteme (pro liché n) nebo odečteme (pro sudé n) velikost průniku všech n množin. Jak to zapsat vzorcem? Jeden způsob by mohl být

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n| -$$
$$-|A_1 \cap A_2| - |A_1 \cap A_3| - \cdots - |A_1 \cap A_n| - |A_2 \cap A_3| - \cdots - |A_{n-1} \cap A_n| +$$
$$+|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \cdots$$
$$+(-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|.$$

To je velmi těžkopádné vyjádření tak jednoduchého pravidla. Trošku lepší je zápis pomocí sum:

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| +$$
$$+ \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| -$$
$$- \cdots + (-1)^{n-1}|A_1 \cap A_2 \cap \ldots \cap A_n|.$$

Vzpomeneme-li si na značení množiny všech k-prvkových podmnožin množiny X symbolem $\binom{X}{k}$ a použijeme-li i pro vícenásobné průniky a sjednocení zápis podobný sumám, můžeme ještě elegantněji zapsat totéž:

3.6.2 Věta (Princip inkluze a exkluze).
Pro každý soubor $A_1, A_2, \ldots, A_n$ konečných množin platí

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n\}}{k}} \left|\bigcap_{i \in I} A_i\right|. \tag{3.12}$$

A asi nejkratší a takřka ďábelský zápis principu inkluze a exkluze je

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|-1} \left|\bigcap_{i \in I} A_i\right|. \tag{3.13}$$

První důkaz principu inkluze a exkluze – indukcí. Indukce postupuje podle počtu množin. Pro 2 množiny vzorec, jak víme, platí. Předpokládejme jeho platnost pro libovolných $n-1$ množin. Budeme postupně upravovat:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cup A_n\right| = \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\left(\bigcup_{i=1}^{n-1} A_i\right) \cap A_n\right| =$$

(Použili jsme vztahu $|A \cup B| = |A| + |B| - |A \cap B|$ pro $A = A_1 \cup A_2 \cup \ldots \cup A_{n-1}$, $B = A_n$.)

$$= \left|\bigcup_{i=1}^{n-1} A_i\right| + |A_n| - \left|\bigcup_{i=1}^{n-1} (A_i \cap A_n)\right| =$$

(Distributivita průniku. Teď dvakrát použijeme indukční předpoklad, jednak pro $|A_1 \cup \ldots \cup A_{n-1}|$ a jednak pro $|A'_1 \cup \ldots \cup A'_{n-1}|$, kde $A'_i = A_i \cap A_n$.)

$$= \left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n-1\}}{k}} \left|\bigcap_{i \in I} A_i\right|\right) + |A_n| -$$

$$-\left(\sum_{k=1}^{n-1} (-1)^{k-1} \sum_{I \in \binom{\{1,2,\ldots,n-1\}}{k}} \left|\bigcap_{i \in I \cup \{n\}} A_i\right|\right).$$

Už jsme skoro hotovi. V první sumě sčítáme (se správnými znaménky) všechny velikosti průniků nezahrnujících množinu A_n. Ve druhé sumě se objevují právě všechny velikosti průniků obsahujících množinu A_n, a průnik $k+1$ takových množin (tj. nějakých k z množin $A_1, \ldots, A_{n-1}$ a množiny A_n) má znaménko $-(-1)^{k-1} = (-1)^k$. V druhé sumě přitom není zahrnut člen $|A_n|$, ten však je zvlášť mezi oběma sumami. Celkem tedy velikost průniku libovolné k-tice množin z $A_1, \ldots, A_n$ se ve výrazu objevuje právě jednou, a se znaménkem $(-1)^{k-1}$, což souhlasí s (3.12). Tím je důkaz indukcí ukončen (bez rozumného zápisu bychom se v tomto důkaze snadno beznadějně zapletli). □

Druhý důkaz principu inkluze a exkluze – počítáním. Uvažme libovolný prvek $x \in A_1 \cup \ldots \cup A_n$. K velikosti sjednocení na levé straně vzorce (3.12) přispívá x právě 1. Podívejme se, kolik přispívá do jednotlivých průniků na straně pravé. Předpokládejme, že x je obsažen právě v j z množin $A_1, \ldots, A_n$, $1 \leq j \leq n$; můžeme množiny přejmenovat tak, aby x byl obsažen právě v $A_1, \ldots, A_j$. Prvek x se tedy objevuje v průniku každé k-tice množin z $A_1, \ldots, A_j$ (a v žádných jiných průnicích). Protože existuje právě $\binom{j}{k}$ k-prvkových podmnožin j-prvkové množiny, bude se x objevovat v $\binom{j}{k}$ průnicích k-tic. Velikosti k-tic jsou přitom započteny se znaménkem $(-1)^{k-1}$, tudíž x na pravé straně přispívá veličinou

$$j - \binom{j}{2} + \binom{j}{3} - \cdots + (-1)^{j-1}\binom{j}{j}.$$

Podle vzorce (3.8) je toto rovno 1. Příspěvek každého prvku k oběma stranám (3.12) je tedy 1, a tím je tento vzorec dokázán. □

A ještě jeden, velmi krátký důkaz. Když se na věc vhodně pohlíží, je princip inkluze a exkluze důsledkem takovéhoto vzorečku pro roznásobení součinu:

$$(1+x_1)(1+x_2)\cdots(1+x_n) = \sum_{I \subseteq \{1,2,\ldots,n\}} \left(\prod_{i \in I} x_i\right). \tag{3.14}$$

Rozvažte, co ten vzoreček říká (rozepište to pro $n = 1, 2, 3$, řekněme) a proč platí.

Abychom dokázali princip inkluze a exkluze, označme $A = A_1 \cup A_2 \cup \ldots \cup A_n$, a nechť $f_i : A \to \{0, 1\}$ je charakteristická funkce množiny A_i, to znamená $f_i(a) = 1$ pro $a \in A_i$ a $f_i(a) = 0$ jinak. Pro každé $a \in A$ platí $\prod_{i=1}^{n}(1 - f_i(a)) = 0$ (ne?), a použitím (3.14) s $x_i = -f_i(a)$ dostaneme

$$\sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \prod_{i \in I} f_i(a) = 0.$$

Sečtením těchto rovností pro všechna $a \in A$, a potom záměnou pořadí sumace, se dopracujeme k

$$0 = \sum_{a \in A} \left(\sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \prod_{i \in I} f_i(a) \right) =$$

$$= \sum_{I\subseteq\{1,2,\dots,n\}} (-1)^{|I|}\Big(\sum_{a\in A}\prod_{i\in I} f_i(a)\Big). \tag{3.15}$$

Teď už si stačí uvědomit, že $\prod_{i\in I} f_i(a)$ je charakteristická funkce množiny $\bigcap_{i\in I} A_i$, takže $\sum_{a\in A}\prod_{i\in I} f_i(a) = \big|\bigcap_{i\in I} A_i\big|$. Speciálně pro $I=\emptyset$ je $\prod_{i\in\emptyset} f_i(a)$ prázdný součin, jenž podle definice má hodnotu 1, takže $\sum_{a\in A}\prod_{i\in\emptyset} f_i(a) = \sum_{a\in A} 1 = |A|$. Proto (3.15) znamená

$$|A| + \sum_{\emptyset\neq I\subseteq\{1,2,\dots,n\}} (-1)^{|I|}\left|\bigcap_{i\in I} A_i\right| = 0,$$

což je přesně princip inkluze a exkluze. Znalec algebry tedy může shlížet na princip inkluze a exkluze s jistým pohrdáním – trivialita, řekl by. □

Bonferroniho nerovnosti. Někdy se můžeme octnout v situaci, kdy známe velikosti všech průniků až do m-násobných, ale neznáme velikosti průniků většího počtu množin než m. Pak ovšem nemůžeme velikost sjednocení spočítat přesně. Takzvané *Bonferroniho nerovnosti* říkají, že vynecháme-li na pravé straně principu inkluze a exkluze (3.12) členy od $(m+1)$-ního počínaje, potom *chyba*, jíž se tím dopustíme při výpočtu velikosti sjednocení, *bude mít stejné znaménko jako první vynechaný člen.* Zapsáno formulí, pro každé $q = 1, 2, \dots$ a libovolné konečné množiny $A_1, \dots, A_n$ platí

$$\sum_{k=1}^{2q}(-1)^{k-1}\sum_{I\in\binom{\{1,2,\dots,n\}}{k}}\left|\bigcap_{i\in I} A_i\right| \le \left|\bigcup_{i=1}^{n} A_i\right| \le$$

$$\le \sum_{k=1}^{2q-1}(-1)^{k-1}\sum_{I\in\binom{\{1,2,\dots,n\}}{k}}\left|\bigcap_{i\in I} A_i\right|. \tag{3.16}$$

To třeba znamená, že nevíme-li v příkladu 3.6.1, kolik horlivců je ve všech třech klubech zároveň, můžeme odhadnout, že celkový počet členů všech tří klubů dohromady je nejméně 32. Důkaz nerovností (3.16) zde neuvádíme.

Cvičení

1. Rozvažte podrobně, proč formule (3.12) a (3.13) vyjadřují totéž.

2.* Dokažte Bonferroniho nerovnosti (3.16). Nevíte-li si rady s obecným případem, zkuste aspoň případ $q = 1$ a $q = 2$.

3. (Eratosthenovo síto) Kolik čísel zbude z 1,2,...,1000 po vyškrtání všech násobků čísel 2,3,5 a 7?

4. Spočítejte počet přirozených čísel $n < 100$, která nejsou dělitelná druhou mocninou žádného přirozeného čísla (většího než 1).

5. Kolik existuje pořadí písmen A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P, z nichž vypuštěním některých písmen nelze dostat ani jedno ze slov PONK, DOBA, COP? Co když zakážeme ještě OPICE?

6. Kolika způsoby lze seřadit do fronty 5 Čechů, 4 Maďary a 3 Rusy tak, aby všichni příslušníci žádného národa netvořili jeden souvislý blok?

3.7 Šatnářka a ti druzí

3.7.1 Úloha. (Problém šatnářky) *Ctihodní pánové v počtu n přijdou na shromáždění, všichni v kloboucích, a odloží si své klobouky do šatny. Při odchodu šatnářka, možná ten den velmi roztržitá, možná dokonce z mizerného osvětlení osleplá, vydá každému z pánů náhodně jeden z klobouků. Jaká je pravděpodobnost, že žádný pán nedostane od šatnářky zpět svůj klobouk?*

Tento problém je formulován jako hříčka, ale matematicky je pozoruhodný a svého času zaměstnával matematické génie té doby. Nejprve ho přeformulujeme pomocí permutací. Očíslujeme-li pány (s prominutím) $1, 2, \dots, n$, a jejich klobouky taktéž, potom činnost šatnářky vede k náhodné permutaci π množiny $\{1, 2, \dots, n\}$, kdy $\pi(i)$ je číslo klobouku navráceného i-tému pánovi. Otázka zní, s jakou pravděpodobností platí $\pi(i) \neq i$ pro všechna $i \in \{1, 2, \dots, n\}$. Nazvěme index i splňující $\pi(i) = i$ *pevným bodem* permutace π. Ptáme se tedy, jaká je pravděpodobnost, že náhodně zvolená permutace nemá žádný pevný bod. Každá z $n!$ možných permutací je, podle popisu práce šatnářky, stejně pravděpodobná, takže označíme-li $š(n)$ počet permutací bez pevného bodu na n-prvkové množině, bude zkoumaná pravděpodobnost rovna $š(n)/n!$.

Pomocí principu inkluze a exkluze se dá odvodit vzorec pro š(n). Budeme hledat počet „špatných" permutací, tj. permutací aspoň s jedním pevným bodem. Nechť S_n (tradičně) značí množinu všech permutací množiny $\{1, 2, \ldots, n\}$, a pro $i = 1, 2, \ldots, n$ definujme

$$A_i = \{\pi \in S_n;\ \pi(i) = i\}.$$

Špatné permutace jsou právě sjednocení všech A_i.

Zde doporučujeme čtenáři, aby si řádně uvědomil definici množin A_i (jejich prvky jsou permutace, nikoli čísla!) – ta bývá často zdrojem nedorozumění.

Abychom mohli aplikovat princip inkluze a exkluze, musíme vyjádřit velikosti k-násobných průniků množin A_i. Je snadno vidět, že $|A_i| = (n-1)!$ ($\pi(i)$ je fixováno, na zbývajících $n-1$ prvcích volíme libovolnou permutaci). Jaké permutace např. jsou v $A_1 \cap A_2$? Právě ty, které mají 1 a 2 jako pevné body (a zbývající prvky zpermutovány libovolně), takových je $(n-2)!$. Obecně pro libovolná $i_1 < i_2 < \cdots < i_k$ máme $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (n-k)!$, a proto dosazením do principu inkluze a exkluze vyjde

$$|A_1 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^{n} (-1)^{k-1} \frac{n!}{k!}.$$

Připomeňme, že to jsme spočítali permutace s aspoň jedním pevným bodem, tedy

$$\text{š}(n) = n! - |A_1 \cup \ldots \cup A_n| = n! - \frac{n!}{1!} + \frac{n!}{2!} - \cdots + (-1)^n \frac{n!}{n!},$$

což můžeme ještě přepsat na tvar

$$\text{š}(n) = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + (-1)^n \frac{1}{n!}\right). \tag{3.17}$$

Jak se vyučuje v kursu matematické analýzy, konverguje součet řady v závorce pro rostoucí n k e^{-1} (kde e je Eulerovo číslo), a to velice rychle. Proto máme přibližný vztah š$(n) \approx n!/e$, a pravděpodobnost v problému šatnářky tedy konverguje ke konstantě e^{-1}.

Eulerova funkce φ. V teorii čísel hraje důležitou roli funkce, označovaná zpravidla φ a pojmenovaná po Leonhardu Eulerovi. Pro přirozené číslo n definujeme hodnotu $\varphi(n)$ jako počet přirozených čísel $m \leq n$ nesoudělných s n; formálně tedy

$$\varphi(n) = |\{m \in \{1, 2, \ldots, n\};\ (n, m) = 1\}|$$

(připomeňme, že (n, m) značí největší společný dělitel čísel m a n). Jako příklad na použití principu inkluze a exkluze najdeme vzorec, který umožňuje efektivně spočítat hodnotu $\varphi(n)$ ze znalosti rozkladu čísla n na prvočinitele.

Nejjednodušší je případ, kdy $n = p$ je prvočíslo. Potom každé $m < p$ je s p nesoudělné, a tedy $\varphi(p) = p - 1$.

Další stupínek k řešení je případ, kdy $n = p^\alpha$ ($\alpha \in \mathbf{N}$) je mocnina prvočísla. Potom čísla soudělná s p^α jsou právě násobky p, tj. $p, 2p, 3p, \ldots, p^{\alpha-1}$, a takových násobků je $p^{\alpha-1}$ (obecně, pokud d je libovolný dělitel nějakého čísla n, potom násobků d nepřevyšujících n je právě n/d). Čísel nesoudělných s p^α tedy zbývá

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p).$$

Obecné n můžeme zapsat ve tvaru

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

kde $p_1, \ldots, p_r$ jsou navzájem různá prvočísla a $\alpha_i \in \mathbf{N}$. „Špatná" $m \leq n$, tj. taková, která se nepočítají do $\varphi(n)$, jsou právě násobky některého z prvočísel p_i. Označme $A_i = \{m \in \{1, 2, \ldots, n\};\ p_i | m\}$ množinu násobků p_i. Máme tedy $\varphi(n) = n - |A_1 \cup A_2 \cup \ldots \cup A_r|$. Princip inkluze a exkluze velí, abychom zjistili velikosti průniků množin A_i. Tak např. průnik $A_1 \cap A_2$ obsahuje čísla dělitelná jak p_1, tak p_2, čili právě násobky $p_1 p_2$, a proto $|A_1 \cap A_2| = n/(p_1 p_2)$. Obecně máme stejnou úvahou

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}.$$

Podívejme se nejprve na konkrétní případy $r = 2$ a $r = 3$. Pro $n = p_1^{\alpha_1} p_2^{\alpha_2}$ máme

$$\varphi(n) = n - |A_1 \cup A_2| = n - |A_1| - |A_2| + |A_1 \cap A_2| =$$

$$n - \frac{n}{p_1} - \frac{n}{p_2} + \frac{n}{p_1 p_2} == n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right).$$

Podobně pro $n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ vychází

$$\varphi(n) = n - \frac{n}{p_1} - \frac{n}{p_2} - \frac{n}{p_3} + \frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \frac{n}{p_2 p_3} - \frac{n}{p_1 p_2 p_3} =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right).$$

To vzbuzuje podezření na obecný vzorec:

3.7.2 Věta. *Pro $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ platí*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right). \tag{3.18}$$

Dokončení důkazu: Pro obecné r nám princip inkluze a exkluze (s výhodou použijeme tvar (3.13)) dává vyjádření

$$\varphi(n) = n - \sum_{\emptyset \neq I \subseteq \{1,2,\ldots,r\}} (-1)^{|I|-1} \frac{n}{\prod_{i\in I} p_i} = n \cdot \sum_{I \subseteq \{1,2,\ldots,r\}} \frac{(-1)^{|I|}}{\prod_{i\in I} p_i}.$$

Tvrdíme, že tato hrozivě vypadající formule je rovna pravé straně (3.18). Roznásobujeme-li totiž všechny závorky na pravé straně (3.18), dostaneme 2^r součinů, a v každém takovém součinu bereme z každé závorky jeden člen – buď 1 nebo $-1/p_i$. Označíme-li pro takový součin písmenem I množinu indexů i takových, že jsme z i-té závorky použili člen $-1/p_i$, můžeme uvažovaný součin napsat ve tvaru

$$\frac{(-1)^{|I|}}{\prod_{i\in I} p_i},$$

tedy po roznásobení pravé strany vzorce (3.18) vyjde stejná formule jako ta, již jsme odvodili pomocí inkluze a exkluze. □

Cvičení

1. Dokažte vztah

$$\check{s}(n) = n! - n\check{s}(n-1) - \binom{n}{2}\check{s}(n-2) - \cdots - \binom{n}{n-1}\check{s}(1) - 1.$$

2. (a)* Dokažte rekurentní vztah $\check{s}(n) = (n-1)[\check{s}(n-1) + \check{s}(n-2)]$. Dokažte s jeho pomocí vzorec (3.17).

   (b)* Vypočítejte vzorec pro $\check{s}(n)$ přímo ze vztahu odvozeného v (a). Použijte pomocnou posloupnost danou vztahem $a_n = \check{s}(n) - n\check{s}(n-1)$.

3. Na plese je n manželských párů. Kolika způsoby lze utvořit n tanečních párů, jestliže žádná manželská dvojice netancuje spolu?

4. Určete počet permutací s právě jedním pevným bodem, resp. * s právě k pevnými body.

5. Kolik existuje permutací čísel 1,2,...,10, v nichž se žádné sudé číslo nezobrazí na sebe?

6. Spočítejte, kolik existuje zobrazení n-prvkové množiny *na* m-prvkovou množinu (tj. každý prvek musí mít aspoň jeden vzor)

   (a) pro $m = 2$

   (b) pro $m = 3$

   (c)* napište vzorec pro obecné m; zkontrolujte výsledek např. pro $m = n = 10$ (co musí vyjít?).

   (d)* Ukažte, nejlépe bez použití výsledku části (c), že počet zobrazení na m-prvkovou množinu je dělitelný číslem $m!$.

7. (a)* Kolika způsoby lze rozdělit n lidí do k skupin, tj. kolik existuje ekvivalencí na n-prvkové množině s právě k třídami? Zkuste řešit nejprve pro $k = 2, 3$ a $k = n-1, n-2$.

   (b) Kolik je celkem ekvivalencí na n-prvkové množině?

   (c)* Označíme-li výsledek (b) jako B_n (*n-té Bellovo číslo*) , dokažte následující (překvapivý) vzorec

$$B_n = \frac{1}{e}\sum_{i=0}^{\infty} \frac{i^n}{i!}.$$

8.* Dokažte vzorec (3.18) pro Eulerovu funkci jiným způsobem. Předpokládejte, že platí pro $n = p^\alpha$ (mocninu jediného prvočísla). Dokažte následující *pomocné tvrzení:* Pokud m, n jsou nesoudělná, potom $\varphi(mn) = \varphi(m)\varphi(n)$.

9.* Pro libovolné přirozené n, dokažte vztah $\sum_{d|n} \varphi(d) = n$ (suma je přes všechny přirozené dělitele d čísla n).

10. (a) Kolik je všech dělitelů čísla $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$?

    (b) Ukažte, že *součet* všech dělitelů takového čísla n je roven

$$\prod_{i=1}^{r} \frac{p^{\alpha_i+1} - 1}{p_i - 1}.$$

    (c)** Nazvěme číslo n *dokonalé*, pokud je rovno součtu svých dělitelů (kromě sebe sama), tak např. $6 = 1 + 2 + 3$ je dokonalé. Dokažte, že každé sudé dokonalé číslo má tvar $2^q(2^{q+1}-1)$, kde $2^{q+1}-1$ je prvočíslo. *Poznámka:* žádná lichá dokonalá čísla známa nejsou, ale nikdo neumí dokázat, že by neexistovala.

11. (a)* Pro dané číslo N určete pravděpodobnost, že zvolíme-li náhodně 2 čísla $m, n \in \{1, 2, \ldots, N\}$, budou nesoudělná.

    (b)* Ukažte, že limita pravděpodobnosti v (a) pro $N \to \infty$ je rovna nekonečnému součinu $\prod_p (1 - 1/p^2)$, kde p probíhá všechna prvočísla. *Poznámka:* Hodnota tohoto součinu je $6/\pi^2$.

12. (a) Určete počet grafů na dané n-prvkové množině V bez izolovaných vrcholů. (Definici grafu viz část 4.1.)

    (b)* Určete počet grafů na V s aspoň 2 izolovanými vrcholy, resp. s právě 2 izolovanými vrcholy.

13.* Kolika způsoby lze rozsadit n manželských párů kolem kulatého stolu s $2n$ židlemi tak, aby manželé nikdy neseděli vedle sebe?

4

Grafy: úvod

4.1 Pojem grafu; isomorfismus

Mnoho situací v matematice, v informatice i v rozličných prakticky motivovaných úlohách lze vystihnout pomocí schématu sestávajícího hlavně ze dvou věcí:

- (konečné) množiny bodů
- a spojnic mezi některými dvojicemi bodů.

Body mohou reprezentovat třeba účastníky nějakého večírku a spojnice ty dvojice účastníků, kteří se navzájem znají. Nebo body mohou odpovídat křižovatkám ve městě a spojnice ulicím mezi nimi. Rovněž elektrotechnická schémata mají často podobný charakter. Body v takovém typu schémat je zvykem nazývat *vrcholy* (nebo též *uzly*) a příslušné spojnice *hrany* (o původu tohoto názvosloví viz část 6.6).

Matematickou abstrakcí podobných schémat je pojem grafu. Čtenář se s ním asi již setkal. Je to jeden ze základních pojmů diskrétní matematiky. To uvidíme i dále v našem textu.

4.1.1 Definice. *Graf*[1] *G je uspořádaná dvojice (V, E), kde V je nějaká neprázdná množina a E je množina dvoubodových podmnožin*

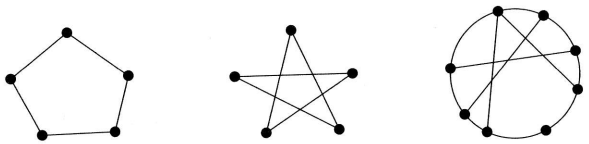
[1] To, čemu zde říkáme prostě graf, se někdy obšírněji nazývá *obyčejný neorientovaný graf*, aby se to odlišilo od dalších příbuzných pojmů – ty zmíníme později.

množiny V. Prvky množiny V se jmenují vrcholy *grafu G a prvky množiny E* hrany[2] *grafu G.*

V našem textu budeme uvažovat grafy s konečnou množinou vrcholů (v několika málo případech, kdy pojednáváme i o nekonečných grafech, to zvlášť zdůrazníme).

Chceme-li vyznačit, že graf G má množinu vrcholů V a množinu hran E, píšeme $G = (V, E)$. Mluvíme-li o nějakém známém grafu G a chceme-li odkázat na jeho množinu vrcholů, značíme ji $V(G)$; podobně množinu hran grafu G zapisujeme $E(G)$. Užitečné je také označení $\binom{V}{2}$ pro množinu všech dvouprvkových podmnožin množiny V (o motivaci tohoto značení viz definici 3.3.1). Můžeme pak krátce říci, že graf je dvojice (V, E), kde $E \subseteq \binom{V}{2}$.

Grafy se znázorňují kreslením do roviny. Vrcholům grafu se přiřadí body roviny (vyznačené zpravidla puntíky) a hrany se vyjádří spojením příslušných dvojic bodů rovnými nebo všelijak zakřivenými čarami. Spojnice se smějí případně křižit, ale nesmějí procházet jinými vrcholy. Vzniknou tak například takovéto obrázky:



Sám název graf pochází snad od možnosti takového znázornění.

Obrázek grafu má však pomocnou úlohu (graf může být koneckonců zadán i mnoha jinými způsoby a např. v paměti počítače se samozřejmě obrázkem nereprezentuje) a jeden graf lze nakreslit mnoha různými způsoby. Tak např. první dva z právě uvedených obrázků znázorňují týž graf s vrcholy $\{1, 2, 3, 4, 5\}$ a hranami $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$, $\{4, 5\}$, $\{5, 1\}$.

Pro přehlednost znázornění je dobré, aby se spojnice vrcholů odpovídající hranám co nejméně „křížily“. V některých schématech elektrických obvodů i v řadě jiných aplikací je dokonce křížení zcela nepřípustné. To vede ke studiu důležité třídy tzv. rovinných grafů, viz kapitolu 6.

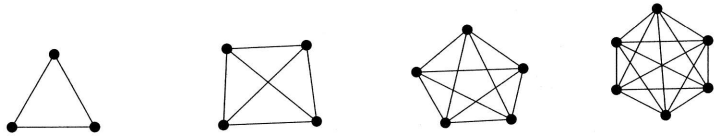
[2] Písmena V a E pocházejí z anglických termínů pro vrchol a hranu – *vertex* a *edge*.

Kreslení grafů je důležitou pomůckou při studiu grafů. Kreslete si obrázky, kdykoliv je to možné. Mnoho pojmů má „obrázkovou“ motivaci a tedy kreslení pojem ozřejmí. Na druhé straně je třeba zdůraznit, že pojem grafu (a jeho obrázku) je zde užíván v jiném smyslu než „graf funkce“.

Důležité grafy. Zavedeme několik typů konkrétních grafů, které se v teorii grafů vyskytují velmi často a pro něž se ujalo standardní názvosloví a označení.

Úplný graf K_n (kde $n \geq 1$):

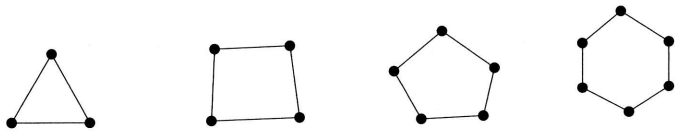
$$V = \{1, 2, \ldots, n\}, \quad E = \binom{V}{2}.$$



K_3 K_4 K_5 K_6

Kružnice C_n (kde $n \geq 3$):

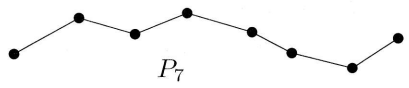
$$V = \{1, 2, \ldots, n\}, \quad E = \{\{i, i+1\};\ i = 1, \ldots, n-1\} \cup \{\{1, n\}\}.$$



C_3 C_4 C_5 C_6

Cesta P_n (kde $n \geq 0$):

$$V = \{0, 1, \ldots, n\}, \quad E = \{\{i-1, i\};\ i = 1, \ldots, n\}.$$



P_7

Úplný bipartitní graf $K_{n,m}$ (kde $n, m \geq 1$):

$$V = \{u_1, \ldots, u_n\} \cup \{v_1, \ldots, v_m\},$$

$$E = \{\{u_i, v_j\};\ i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, m\}.$$



$K_{1,1}$ $K_{1,2}$ $K_{1,3}$ $K_{2,3}$ $K_{3,3}$

Tady je asi na místě malé vysvětlení. Slovo „bipartitní" bychom mohli přeložit jako „dvoučásťový". Obecně, graf G se nazývá *bipartitní*, pokud množinu $V(G)$ můžeme rozdělit na dvě disjunktní podmnožiny V_1 a V_2 takové, že každá hrana z $E(G)$ spojuje vrchol z V_1 s vrcholem z V_2; v symbolech $E(G) \subseteq \{\{v, v'\};\ v \in V_1, v' \in V_2\}$.

Isomorfismus grafů. Dva grafy G a G' pokládáme za stejné, jestliže mají totožné množiny vrcholů a hran; tedy $G = G'$ znamená $V(G) = V(G')$ a $E(G) = E(G')$. Mnoho grafů se však liší „pouze" označením svých vrcholů a hran. To vystihuje pojem isomorfismu.

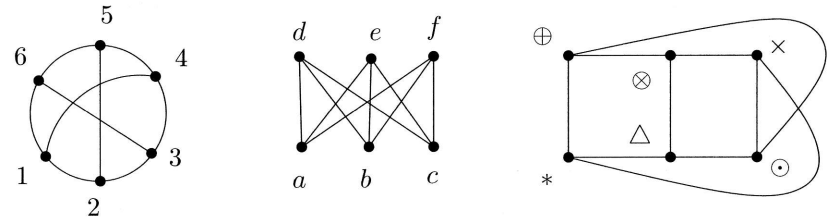
4.1.2 Definice. *Dva grafy* $G = (V, E)$ *a* $G' = (V', E')$ *nazveme* isomorfní, *jestliže existuje vzájemně jednoznačné zobrazení* $f : V \hookrightarrow\!\!\!\rightarrow V'$ *tak, že platí*

$$\{x, y\} \in E \quad \textit{právě když} \quad \{f(x), f(y)\} \in E'.$$

Zobrazení f *nazýváme* isomorfismus *grafů* G *a* G'. *Fakt, že grafy* G *a* G' *jsou isomorfní, vyznačujeme zápisem* $G \cong G'$.

Isomorfismus je tedy vlastně „přejmenování vrcholů" grafu (dejte na definici isomorfismu pozor, je důležitá, ale často se plete!). Relace $\cong$ („býti isomorfní") je ekvivalence – viz cvičení 3.

4.1.3 Úloha. *Následující 3 obrázky znázorňují isomorfní grafy. Najděte příslušné isomorfismy.*



Řešení. Všechny tři grafy jsou isomorfní $K_{3,3}$. Isomorfismus (a)→ (b): například $1 \mapsto a$, $2 \mapsto d$, $3 \mapsto b$, $4 \mapsto e$, $5 \mapsto c$, $6 \mapsto f$ (existuje víc možností!). Ostatní přenecháváme čtenáři.

Pro malé obrázky není zpravidla těžké rozhodnout, jestli odpovídají isomorfním grafům nebo ne (i když předchozí úloha naznačuje, že obrázky téhož grafu nemusí zdaleka vypadat na pohled stejně). Nicméně úloha rozhodnout, zda dané dva grafy jsou isomorfní, je obecně obtížná, a není pro ni znám žádný efektivní algoritmus (tj. fungující efektivně ve všech případech). Dokonce se soudí, že ani žádný efektivní algoritmus neexistuje.

Počet neisomorfních grafů. Na dané n-prvkové množině V je právě $2^{\binom{n}{2}}$ různých grafů (neb tolika způsoby můžeme zvolit množinu E jako podmnožinu množiny $\binom{V}{2}$, a posledně jmenovaná má $\binom{n}{2}$ prvků – viz část 3.1). Grafů, které jsou navzájem neisomorfní, je podstatně méně. Tak např. pro $V = \{1, 2, 3\}$ dostáváme následujících $8 = 2^{\binom{3}{2}}$ grafů



Z těchto 8 možností jen 4 jsou neisomorfní:



Kolik je navzájem neisomorfních grafů na n vrcholech pro obecné n? Určit to přesně je poměrně těžké; jednoduchou úvahou můžeme ale dostat aspoň dobré odhady. Navzájem neisomorfních grafů určitě není více než všech grafů na dané konkrétní n-prvkové množině, tj. $2^{\binom{n}{2}}$. Na druhé straně, uvažme jeden graf G na množině $V = \{1, 2, \ldots, n\}$. Kolik

různých grafů G' na této množině je s grafem G isomorfních? Podle definice, je-li G' takový isomorfní graf, musí existovat bijekce $f : V \hookrightarrow\!\!\!\rightarrow V$, které je isomorfismem G a G'. Všech bijekcí $f : V \hookrightarrow\!\!\!\rightarrow V$ je ale $n!$ (viz část 3.2), tedy G je isomorfní s nejvýš $n!$ grafy na množině V, a proto existuje minimálně

$$\frac{2^{\binom{n}{2}}}{n!}$$

navzájem neisomorfních grafů na n vrcholech.

Tvrdíme, že tato funkce neroste o mnoho pomaleji než $2^{\binom{n}{2}}$. Abychom to nahlédli, zlogaritmujeme obě funkce a poněkud upravíme (přitom použijeme zřejmý odhad $n! \leq n^n$):

$$\log_2 \left[2^{\binom{n}{2}}\right] = \binom{n}{2} = \frac{n^2}{2}\left(1 - \frac{1}{n}\right),$$

$$\log_2 \frac{2^{\binom{n}{2}}}{n!} = \binom{n}{2} - \log_2 n! \geq n^2/2 - n/2 - n \log_2 n =$$

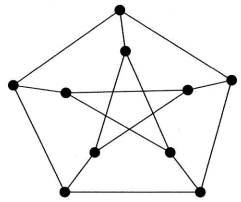
$$= \frac{n^2}{2}\left(1 - \frac{1}{n} - \frac{2\log_2 n}{n}\right).$$

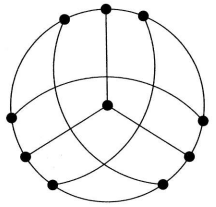
Vidíme, že pro velká n se logaritmy obou funkcí chovají „asi jako“ funkce $n^2/2$: relativní chyba, které bychom se dopustili jejich nahrazením funkcí $n^2/2$, jde v obou případech k nule pro $n \to \infty$. (Více o odhadech funkcí viz část 3.4.) Speciálně, pro dostatečně velké n je mnohem více než např. 2^n navzájem neisomorfních grafů.

Právě uvedená úvaha je pozoruhodná tím, že jsme pouze ukázali existenci velkého množství neisomorfních grafů, ale žádné takové grafy jsme nesestrojili (o podobných úvahách budeme mluvit systematičtěji v kapitole 10). Sestrojit (tj. explicitně popsat) mnoho neisomorfních grafů není jen tak – viz cvičení 7.

Cvičení

1. Nalezněte isomorfismus mezi grafy





2. Které z následujících výroků o grafech G a H jsou správné? Zdůvodněte.

   (i) G a H jsou isomorfní, právě když pro každé zobrazení $f: V(G) \to V(H)$ platí pro každé dva vrcholy $u, v \in V(G)$ následující ekvivalence: $\{u, v\} \in E(G) \Leftrightarrow \{f(u), f(v)\} \in E(H)$.

   (ii) G a H jsou isomorfní, právě když existuje bijekce $f: E(G) \to E(H)$.

   (iii) Jestliže existuje bijekce $f: V(G) \to V(H)$ taková, že každý vrchol $u \in V(G)$ má stejný stupeň jako $f(u)$, pak jsou G a H isomorfní.

   (iv) Jestliže jsou G a H isomorfní, pak existuje bijekce $f: V(G) \to V(H)$ taková, že každý vrchol $u \in V(G)$ má stejný stupeň jako $f(u)$.

   (v) Jestliže jsou G a H isomorfní, pak existuje bijekce $f: E(G) \to E(H)$.

   (vi) G a H jsou isomorfní, právě když existuje zobrazení $f: V(G) \to V(H)$ takové, že pro každé dva vrcholy $u, v \in V(G)$ platí ekvivalence $\{u, v\} \in E(G) \Leftrightarrow \{f(u), f(v)\} \in E(H)$.

   (vii) Každý graf s n vrcholy je isomorfní nějakému grafu na množině vrcholů $\{1, 2, \ldots, n\}$.

   (viii) Každý graf s $n \geq 1$ vrcholy je isomorfní nekonečně mnoha grafům.

3. Buď $\mathcal{G}$ nějaká množina grafů. Dokažte, že relace „býti isomorfní“ je ekvivalence na $\mathcal{G}$.

4. *Automorfismus* grafu $G = (V, E)$ je každý isomorfismus G s G, tj. bijekce $f : V \hookrightarrow\!\!\!\rightarrow V$ taková, že $\{u, v\} \in E$, právě když $\{f(u), f(v)\} \in E$. Graf se nazývá *asymetrický* (někdy též *strnulý*), je-li jeho jediný automorfismus identické zobrazení (každý vrchol se zobrazí sám na sebe).

   (a) Najděte příklad asymetrického grafu (s aspoň 2 vrcholy).

   (b) Ukažte, že neexistuje žádný asymetrický graf G s $1 < |V(G)| \leq 5$.

5. Dokažte, že graf G s n vrcholy je asymetrický (viz cvičení 4), právě když na množině $V(G)$ existuje $n!$ různých grafů isomorfních G.

6. Graf $G = (V, E)$ se nazývá *vrcholově transitivní*, pokud pro libovolné dva vrcholy $v, v' \in V$ existuje automorfismus $f : V \hookrightarrow\!\!\!\rightarrow V$ grafu G (viz cvičení 4) takový, že $f(v) = v'$. Podobně G je *hranově transitivní*, pokud pro libovolné dvě hrany $e, e' \in E$ existuje automorfismus $f : V \hookrightarrow\!\!\!\rightarrow V$ takový, že $f(e) = e'$ (označíme-li $e = \{u, v\}$, potom zápis $f(e)$ značí množinu $\{f(u), f(v)\}$).

   (a) Rozhodněte, zda každý vrcholově transitivní graf je také hranově transitivní.

   (b) Najděte příklad grafu, který je hranově transitivní a není vrcholově transitivní.

   (c)* Dokažte, že graf jako v (b) je nutně bipartitní.

7. Sestrojte co nejvíce navzájem neisomorfních grafů na množině $\{1, 2, \ldots, n\}$ (předpokládejte, že n je hodně velké číslo). Podaří se vám jich sestrojit více než n^2? Aspoň $2^{n/10}$, nebo ještě podstatně více?

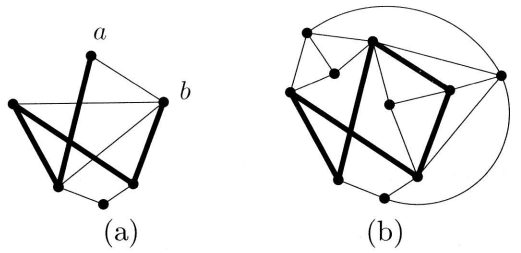
4.2 Podgrafy, souvislost, metrika, matice sousednosti

4.2.1 Definice. *Řekněme, že graf H je* podgrafem *grafu G, jestliže* $V(H) \subseteq V(G)$ a $E(H) \subseteq E(G)$.

Řekneme, že graf H je indukovaným podgrafem *grafu G, jestliže* $V(H) \subseteq V(G)$ a $E(H) = E(G) \cap \binom{V(H)}{2}$.

Tuto definici můžeme jinak vyjádřit takto: indukovaný podgraf grafu G vznikne vymazáním některých vrcholů G a všech hran vymazané vrcholy obsahujících. Pro podgraf můžeme ještě navíc vymazat některé další hrany, i když nevymažeme žádný z jejich koncových vrcholů. Na obr. 4.1(a) je nakreslen graf, a v něm je silně vytažen podgraf isomorfní cestě P_4. Tento podgraf není indukovaný (kvůli hraně $\{a, b\}$). Obrázek 4.1(b) ukazuje indukovaný podgraf (isomorfní kružnici C_5); ten je ovšem zároveň podgrafem.

Cesty a kružnice. Podgraf grafu G isomorfní nějaké cestě P_t se nazývá *cesta v grafu G* (viz obr. 4.1(a)). Cestu v grafu G můžeme též



Obrázek 4.1: Příklad podgrafu (a), indukovaného podgrafu (b).

chápat jako posloupnost

$$(v_0, e_1, v_1, \ldots, e_t, v_t),$$

kde $v_0, v_1, \ldots, v_t$ jsou navzájem různé vrcholy grafu G, a pro každé $i = 1, 2, \ldots, t$ je $e_i = \{v_{i-1}, v_i\} \in E(G)$. Obšírněji se cesta ($v_0$, e_1, v_1,..., e_t, v_t) nazývá *cesta z v_0 do v_t délky t*. Poznamenejme, že připouštíme $t = 0$, tj. cestu délky 0.

Podobně podgraf grafu G isomorfní nějaké kružnici C_t ($t \geq 3$) se nazývá *kružnice v grafu G* (viz obr. 4.1(b)). Kružnici v grafu G můžeme též chápat jako posloupnost

$$(v_0, e_1, v_1, e_2, \ldots, e_{t-1}, v_{t-1}, e_t, v_0)$$

(počáteční a koncový vrchol jsou tedy shodné), kde $v_0, v_1, \ldots, v_{t-1}$ jsou navzájem různé vrcholy grafu G, a $e_i = \{v_{i-1}, v_i\} \in E(G)$ pro $i = 1, 2, \ldots, t-1$, a také $e_t = \{v_{t-1}, v_0\} \in E(G)$. Číslo t je délka kružnice.

Souvislost, komponenty. Řekněme, že graf G je *souvislý*, jestliže pro každé dva jeho vrcholy x a y v něm existuje cesta z x do y.

Pojem souvislosti lze definovat také jinak. Nejdříve definujme relaci $\sim$ na množině $V(G)$ vztahem $x \sim y$ právě když v grafu G existuje cesta z x do y.

4.2.2 Tvrzení. *Relace $\sim$ je ekvivalence.*

Důkaz. Ověříme axiomy ekvivalence:

(a) $x \sim x$,

(b) $x \sim y \Rightarrow y \sim x$,

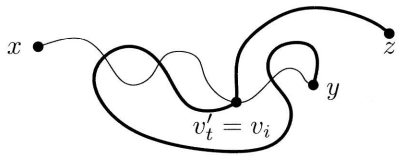
(c) $x \sim y$ a $y \sim z \Rightarrow x \sim z$.

Přitom (a) a (b) plynou bezprostředně z definice relace $\sim$ a zbývá dokázat (c).

Nechť tedy posloupnost $(x = v_0, e_1, v_1, \ldots, e_r, v_r = y)$ je cesta z x do y a posloupnost $(y = v'_0, e'_1, v'_1, \ldots, e'_s, v'_s = z)$ je cesta z y do z. Nechť t je maximální index, pro nějž $v'_t \in \{v_0, \ldots, v_r\}$ (to je korektní definice, protože přinejmenším $v'_0 \in \{v_0, \ldots, v_r\}$). Nechť $v'_t = v_i$. Potom však posloupnost

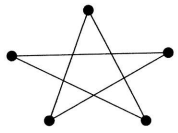
$$(x = v_0, e_1, v_1, \ldots, e_i, v_i = v'_t, e'_{t+1}, v'_{t+1}, \ldots, e'_s, v'_s = z)$$

je hledaná cesta z x do z, viz obrázek:

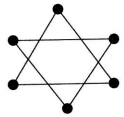


□

Nechť $V = V_1 \dot\cup V_2 \dot\cup \ldots \dot\cup V_k$ je rozklad množiny V na třídy ekvivalence $\sim$. Zřejmě graf G je souvislý, právě když $k = 1$. Množiny V_i se nazývají *komponenty* grafu G. Graf G je tedy sjednocením svých komponent. Na obr. (a) je příklad souvislého grafu,



(a)



(b)

zatímco na obrázku (b) je příklad grafu nesouvislého.

Rozhodnout, zda graf G je souvislý, popřípadě najít všechny jeho komponenty není obtížné. Příslušné algoritmy zde nebudeme popisovat; lze je najít v mnoha učebnicích informatiky (zpravidla jako algoritmy na prohledávání grafu, např. prohledávání do hloubky).

Vzdálenost v grafu. Nechť $G = (V, E)$ je souvislý graf. Pro vrcholy v, v' definujme číslo $d_G(v, v')$ jako délku nejkratší cesty z v do v' v grafu G. Číslo $d_G(v, v')$ se nazývá *vzdálenost vrcholů* v a v' v grafu G.

Funkce $d_G : V \times V \to \mathbf{R}$, kterou nazýváme *metrika grafu* G, má následující vlastnosti

1. $d_G(v, v') \geq 0$, a $d_G(v, v') = 0$ právě když $v = v'$;
2. (symetrie) $d_G(v, v') = d_G(v', v)$ pro každou dvojici vrcholů v, v';
3. (trojúhelníková nerovnost) $d_G(v, v'') \leq d_G(v, v') + d_G(v', v'')$ pro každou trojici v, v', v'' vrcholů z V.

Platnost těchto vztahů plyne bezprostředně z definice čísla $d_G(v, v')$. Každému zobrazení $V \times V$ do $\mathbf{R}$ s vlastnostmi 1–3 se říká *metrika* na množině V. Výše definovaná funkce d_G má navíc ještě následující speciální vlastnosti:

4. $d_G(v, v')$ je nezáporné celé číslo pro každou dvojici v, v';
5. jestliže $d_G(v, v'') > 1$, potom existuje v', $v \neq v' \neq v''$ tak, že $d_G(v, v') + d_G(v', v'') = d_G(v, v'')$.

Podmínku 5 bychom mohli nazvat „obrácení trojúhelníkové nerovnosti“. Podmínky 1–5 již charakterizují funkce odpovídající metrice nějakého grafu G s množinou vrcholů V (viz cvičení 5).

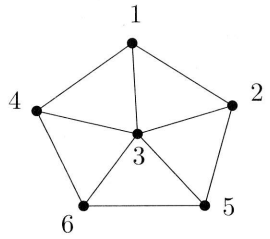
Reprezentace grafů. Kromě geometrických prostředků (kreslení grafů) se při studiu grafů používá i matic a jiných algebraických prostředků. To je důležité např. jestliže chceme zadat graf počítači. Grafy se reprezentují mnoha rozličnými způsoby. Snad nejběžnější a v jistém smyslu základní je pojem matice sousednosti grafu:

4.2.3 Definice. *Nechť $G = (V, E)$ je graf s n vrcholy. Označme vrcholy $v_1, \ldots, v_n$ (v nějakém libovolném pořadí).* Matice sousednosti *grafu G je čtvercová matice $A_G = (a_{ij})_{i,j=1}^n$ definovaná předpisem*

$$a_{ij} = \begin{cases} 1 & \text{pro } \{v_i, v_j\} \in E \\ 0 & \text{jinak.} \end{cases}$$

Tedy matice sousednosti A_G je vždy symetrická čtvercová matice, jejímiž prvky jsou 0 nebo 1, přičemž na hlavní diagonále jsou 0. Každá matice s uvedenými vlastnostmi je maticí sousednosti vhodného grafu.

Příklad. Pro graf G



je matice sousednosti

$$A_G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Poznamenejme ještě, že matice sousednosti zjevně závisí na zvoleném očíslování vrcholů grafu!

Mezi násobením matice sousednosti a metrikou grafu je jednoduchá souvislost. Nejdříve definujeme pojem sledu v grafu (podobný pojmu cesty):

Nechť $G = (V, E)$ je graf. Posloupnost $(v_0, e_1, v_1, e_2, \ldots, e_n, v_n)$ se nazývá *sled* v grafu G (obšírněji *sled délky n z v_0 do v_n*), jestliže platí $e_i = \{v_{i-1}, v_i\} \in E$ pro $i = 1, \ldots, n$. Narozdíl od cesty se ve sledu mohou některé vrcholy i hrany opakovat; sled si můžeme představovat jako záznam trasy bloudícího poutníka.

Pišme $v \sim_1 v'$, jestliže existuje sled z v do v'. Z definice sledu plyne, že $\sim_1$ je ekvivalence na množině V. Ve skutečnosti tato ekvivalence splývá ekvivalencí $\sim$ definovanou výše pomocí existence cesty. Plyne to z následujícího:

4.2.4 Lemma. *V grafu G existuje cesta z x do y právě když v G existuje sled z x do y.*

Důkaz. Zřejmě každá cesta tvoří sled. Na druhé straně sled z x do y, který má nejmenší možnou délku, je již nutně cesta. □

4.2.5 Tvrzení. *Nechť $G = (V, E)$ je graf, $V = \{v_1, \ldots, v_n\}$, a nechť $A = A_G$ je jeho matice sousednosti. Označme A^k k-tou mocninu matice sousednosti (při běžném násobení matic, tj. označíme-li $B = A^2$, platí $b_{ij} = \sum_{k=1}^{n} a_{ik}a_{kj}$). Nechť $a_{ij}^{(k)}$ označuje prvek matice A^k v pozici (i, j). Pak $a_{ij}^{(k)}$ je počet sledů délky k z vrcholu v_i do vrcholu v_j v grafu G.*

Důkaz. Je jednoduchý leč poučný. Pracujeme indukcí podle k. Sled délky 1 mezi dvěma vrcholy znamená přesně že tyto vrcholy jsou spojeny hranou, takže pro $k = 1$ tvrzení je jenom jinak řečená definice matice sousednosti.

Teď předpokládejme, že $k > 1$, a že v_i, v_j jsou nějaké vrcholy (dovolujeme i $v_i = v_j$). Každý sled délky k z v_i do v_j začíná nějakou hranou jdoucí z v_i do nějakého v_ℓ, a zbytek je sled délky $k-1$ z v_ℓ do v_j. Podle indukčního předpokladu je počet sledů délky $k-1$ z v_ℓ do v_j roven $a_{\ell j}^{(k-1)}$. Tím pádem je počet sledů délky k z v_i do v_j

$$\sum_{\{v_i, v_\ell\} \in E(G)} a_{\ell j}^{(k-1)} = \sum_{\ell=1}^{n} a_{i\ell} a_{\ell j}^{(k-1)}.$$

Tohle ale je, podle definice násobení matic, přesně prvek v pozici (i, j) v součinu matic A a A^{k-1}, neboli $a_{ij}^{(k)}$. □

4.2.6 Důsledek. *Pro vzdálenost vrcholů platí*

$$d_G(v_i, v_j) = \min\{k;\, a_{ij}^{(k)} \neq 0\}.$$

Poznamenejme ještě, že matice sousednosti není vždy nejvhodnější způsob reprezentace grafu v paměti počítače. Obzvlášť když má graf málo hran (podstatně méně než $\binom{n}{2}$), bývá výhodnější např. pro každý vrchol zadat seznam jeho sousedů. Pro urychlení některých složitějších algoritmů se používají ještě další, složitější reprezentace.

Cvičení

1.* Kolik nejvíce hran může mít graf s n vrcholy a k komponentami?

2. Zkuste navrhnout algoritmus, který pro zadaný graf G rozhodne, zda je souvislý, a pro nesouvislý graf najde rozklad množiny $V(G)$ na komponenty. (Lze navrhnout algoritmus, který pro graf s n vrcholy a m hranami potřebuje $O(n+m)$ kroků.)

3.* Dokažte, že graf je bipartitní, právě když neobsahuje žádnou kružnici liché délky.

4. (a)* Popište, jak vypadají grafy, neobsahující žádnou cestu délky 3.
   (b)* Popište, jak vypadají grafy, neobsahující žádnou cestu délky 4.

5. Dokažte, že splňuje-li funkce $d : V \times V \to \{0, 1, 2, \ldots\}$ podmínky 1–5, potom existuje graf $G = (V, E)$ tak, že $d_G(v, v') = d(v, v')$ pro každou dvojici prvků množiny V.

6. Definujte průměr a poloměr grafu (v analogii s intuitivním významem těchto pojmů).

7. (a) Najděte souvislý graf na n vrcholech, pro nějž každá mocnina matice sousednosti obsahuje nulové členy.
   (b) Buď G graf na n vrcholech, $A = A_G$ jeho matice sousednosti, a I_n jednotková matice typu $n \times n$ (mající jedničky na diagonále a nuly všude jinde). Dokažte, že G je souvislý právě když $(I_n + A)^{n-1}$ nemá žádné nulové členy.
   (c) Kde má matice $(I_n + A)^{n-1}$ nulové členy, je-li G nesouvislý?

8. Dokažte, že grafy G a G' jsou isomorfní právě když existuje permutační matice P tak, že
$$A_{G'} = P A_G P^T.$$
   Zde A_G je matice sousednosti G a P^T označuje matici transponovanou k matici P. Matice P se nazývá *permutační*, jestliže její prvky jsou 0 a 1 a v každém řádku a sloupci je právě jediná 1.

4.3 Hledání nejkratší cesty

Jednou ze základních algoritmických úloh v teorii grafů je najít nejkratší cestu mezi dvěma danými vrcholy v daném grafu. Takový požadavek vzniká v mnoha praktických aplikacích (třeba při hledání nejkratšího dopravního spojení, vlakem nebo po silnici apod.). Dosud

objevené algoritmy řešící tuto úlohu většinou počítají mnohem více, než se přímo požaduje – zpravidla naleznou nejkratší cesty z výchozího vrcholu do všech (nebo mnoha) vrcholů. Jedna z nejjednodušších a nejdůležitějších takových metod je tzv. *Dijkstrův algoritmus* (čte se, jakožto holandské jméno, „Dajkstrův“).

Dijkstrův algoritmus předvedeme v situaci, kdy daný graf G má hrany ohodnocené kladnými reálnými čísly, to znamená, že spolu s každou hranou $e \in E(G)$ je dáno kladné reálné číslo $w(e)$, nebo jinak řečeno, je dána funkce $w : E(G) \to (0, \infty)$. Ohodnocení $w(e)$ hrany e si můžeme představovat jako její délku, nebo cenu, kterou musíme zaplatit za její projití, apod. Délka nějaké cesty v takto ohodnoceném grafu G je rovna součtu délek jejích hran, a vzdálenost $d_{G,w}(u, v)$ dvou vrcholů $u, v \in V(G)$ je pak rovna nejmenší z délek všech cest, spojujících u a v. „Obyčejná“ grafová vzdálenost d_G (definovaná v části 4.2) se dostane jako speciální případ, totiž je-li $w(e) = 1$ pro každou hranu e.

Vstupem Dijkstrova algoritmu je graf $G = (V, E)$, ohodnocení hran $w : E \to (0, \infty)$ a počáteční vrchol s („start“). Algoritmus pro každý vrchol $v \in V(G)$ vypočítá číslo $d_{G,w}(s, v)$, tj. vzdálenost z s do v. Pro každý vrchol $v \in V$ se zavede jedna číselná proměnná $d(v)$. To je číslo, udávající momentální „odhad“ na hledanou hodnotu $d_{G,w}(s, v)$. V každém kroku se pro některé vrcholy v momentální hodnota $d(v)$ prohlásí za definitivní (tj. je to skutečná vzdálenost v od s), pro ostatní vrcholy se $d(v)$ přepočítává. Proměnná A je množina „aktivních“ vrcholů, což jsou vrcholy, pro něž $d(v)$ dosud nebylo prohlášeno za definitivní. Na začátku volíme $A = V$ a

$$d(v) = \begin{cases} 0 & \text{pro } v = s \\ \infty & \text{pro } v \neq s, \end{cases}$$

což odpovídá tomu, že na začátku známe cestu délky nula z s do s, ale zbytek grafu jsme ještě neprozkoumali.

V obecném kroku algoritmu utvoříme nejdříve množinu N vrcholů, pro něž je $d(v)$ nejmenší možné mezi všemi vrcholy $v \in A$ (množina N bude mít často jen jediný vrchol, aspoň pokud jsou ohodnocení hran např. náhodně vybraná čísla). Všechny vrcholy z N vyjmeme z A a přepočítáme hodnoty $d(x)$ pro jejich sousedy: Pro kaž-

dou hranu $\{v, y\} \in E$, kde $v \in N$ a $y \in A$, porovnáme hodnoty $d(y)$ a $d(v) + w(\{v, y\})$. Je-li $d(v) + w(\{v, y\}) < d(y)$, znamená to, že přes vrchol v vede do y cesta kratší, než jsme zatím znali. Změníme proto hodnotu $d(y)$ na $d(v) + w(\{v, y\})$. Po takovémto přepočítání přejdeme k dalšímu kroku algoritmu. Algoritmus končí, platí-li $d(x) = \infty$ pro všechna $x \in A$. V takovém případě je buď $A = \emptyset$ (je-li G souvislý), anebo A obsahuje pouze vrcholy nedosažitelné cestou z vrcholu s.

Uvedeme ještě formální popis algoritmu:

4.3.1 Algoritmus (Dijkstrův algoritmus).
Vstup: graf $G = (V, E)$, ohodnocení hran $w(e)$, $e \in E$, startovní vrchol s.
Proměnné: čísla $d(v)$, $v \in V$, číslo δ, množiny $A, N \subseteq V$.
Výstup: po skončení algoritmu udává $d(v)$ vzdálenost v od s, pro každé $v \in V$.

Krok 1. (Inicializace)
$d(s) := 0$; $d(x) := \infty$ pro $x \in V \setminus \{s\}$; $A := V$.

Krok 2. (Test ukončení)
Jestliže pro všechna $x \in A$ platí $d(x) = \infty$, algoritmus končí, jinak se pokračuje krokem 3.

Krok 3. (Volba množiny N)
$\delta := \min\{d(y);\ y \in A\}$
$N := \{v \in A;\ d(v) = \delta\}$
$A := A \setminus N$

Krok 4. (Aktualizace $d(y)$ pro sousedy N)
Pro každou hranu $e = \{v, y\}$, kde $v \in N$ a $y \in A$, proveď příkaz
$d(y) := \min(d(y), d(v) + w(e))$.
Po vyčerpání všech takových hran e pokračuj krokem 2.

Poznámka. Při praktickém programování nahradíme symbol ∞ v inicializaci algoritmu nějakou velkou hodnotou, o které máme zaručeno, že bude větší než délka nejdelší cesty v G, např. $M = 1 + \sum_{e \in E} w(e)$.

Důkaz správnosti algoritmu. Nejprve nahlédneme (indukcí podle počtu opakování kroků 2–4 algoritmu), že v každém okamžiku činnosti algoritmu (a tedy i po jeho skončení) platí pro každý vrchol $v \in V$ nerovnost

$$d(v) \geq d_{G,w}(s, v).$$

To je zajisté pravda na začátku, kdy $0 = d_{G,w}(s, s)$ a $\infty \geq d_{G,w}(s, v)$ pro každé $v \in V$. V okamžiku změny hodnoty $d(y)$ pro nějaké $y \in V$ v kroku 4 ke změně dochází, protože existuje $v \in N$ takové, že $d(v) + w(\{v, y\}) < d(y)$. Pro v však podle indukčního předpokladu platí $d(v) \geq d_{G,w}(s, v)$. Přidáním hrany $\{v, y\}$ za nejkratší cestu z s do v (která má délku $d_{G,w}(s, v)$) získáme cestu z s do y délky $d_{G,w}(s, v) + w(\{v, y\})$, a proto

$$d_{G,w}(s, y) \leq d_{G,w}(s, v) + w(\{v, y\}) \leq d(v) + w(\{v, y\}) = d(y),$$

kde $d(y)$ je hodnota po provedení změny.

Nyní ukážeme, že po skončení činnosti algoritmu bude $d(v) \leq d_{G,w}(s, v)$ pro všechna $v \in V$. Ukážeme dokonce silnější tvrzení: *Jsou-li* $0 = d_1 < d_2 < \ldots < d_k < \infty$ *všechny různé konečné vzdálenosti vrcholů grafu od vrcholu* s, *a označíme-li*

$$M_i = \{v \in V;\ d_{G,w}(s, v) = d_i\}$$

pro $i = 1, 2, \ldots, k$, *pak krok 3 algoritmu se provede přesně* k*-krát, a pro každé* i *po* i*-tém vykonání kroku 3 platí* $N = M_i$, $\delta = d_i$ *a* $V \setminus A = \bigcup_{j=1}^{i} M_j$.

Toto tvrzení dokážeme indukcí podle i. Pro lepší orientaci v algoritmu přidáme ke jménům proměnných horní index $^{(i)}$ značící hodnotu po i-tém vykonání kroku 2. Pro $i = 1$ tvrzení triviálně platí.

Vezměme nějaké $i > 1$ a $y \in M_i$ a předpokládejme, že tvrzení platí pro každé $j < i$. Jestliže $d_{G_w}(s, y) = d_i < \infty$, pak existuje cesta $(s = v_0, e_1, v_1, \ldots, v_t, e_{t+1}, v_{t+1} = y)$ z s do y délky d_i. Potom $d_{G,w}(s, v_t) \leq d_i - w(\{v_t, y\}) < d_i$, takže $v_t \in M_j$ pro nějaké $j < i$. Podle indukčního předpokladu je $v_t \in N^{(j)}$ a $d^{(j)}(v_t) = d_{G,w}(s, v_t)$. Proto $d^{(j+1)}(y) = d_{G,w}(s, v_t) + w(\{v_t, y\}) = d_{G,w}(s, y) = d_i$ a tím spíše $d^{(i)}(y) = d_i$.

Podle indukčního předpokladu je $d^{(i)}(v) = d_{G,w}(s,v) < d_i$ pro každé $v \in \bigcup_{j=1}^{i-1} M_j = V \setminus A^{(i-1)}$, a podle výše ukázaného je $d^{(i)}(v) \geq d_{G,w}(s,v) > d_i$ pro každé $v \in \bigcup_{i<j\leq k} M_j$. Proto $\delta^{(i)} = d_i$ a $N^{(i)} = M_i$. □

Poznamenejme, že algoritmus můžeme (prakticky beze změny) použít i pro tzv. orientované grafy (ty budou definovány v části 4.6), kde některé hrany se smějí procházet jenom jedním směrem.

Požadavek, že ohodnocení všech hran je kladné, je velmi podstatný. Pro úlohu nalezení nejkratší cesty v grafu, kde některé hrany mohou být ohodnoceny i záporně (za jejich projití dostaneme „prémii"), není známý žádný efektivní algoritmus, a nejspíše ani žádný neexistuje.

Zajímá-li nás pouze nejkratší cesta z vrcholu s do nějakého zadaného vrcholu c (cíl), můžeme použít Dijkstrův algoritmus, ale ukončit jej, jakmile vrchol c opustí množinu A (tj. jeho vzdálenost se stane definitivní). Přitom však algoritmus stále může prohledávat mnoho vrcholů, z pohledu „zdravého rozumu", zbytečně (hledáme-li nejkratší silniční spojení z Brna do Ostravy, očekáváme, že k tomu není potřeba zjistit nejkratší cestu z Brna do Karlových Varů). K urychlení takového počítání byla vyvinuta zajímavá modifikace Dijkstrova algoritmu, tzv. *Dijkstrův algoritmus s heuristikou.* Slovo heuristika zde znamená (zhruba) něco, o čem si myslíme, že nám to v řešení úlohy pomůže, co „vypadá rozumně", ale zpravidla to neumíme dokázat. Konkrétně, v našem případě pro daný graf G, ohodnocení hran w a cílový vrchol c budeme *heuristikou* rozumět funkci $h : V(G) \to [0,\infty)$, splňující $h(c) = 0$ a následující podmínku:

$$\text{Pro každou hranu } e = \{u,v\} \in E \text{ platí}$$
$$|h(u) - h(v)| \leq w(e).$$

Hodnota $h(v)$ je nějaký dolní odhad vzdálenosti v od c. V problémech dopravního spojení může být $h(v)$ například vzdálenost mezi v a c vzdušnou čarou. Máme-li nějakou takovou funkci h, můžeme Dijkstrův algoritmus modifikovat takto: v kroku 2 položíme $\delta := \min\{h(x) + d(x);\ x \in A\}$, a $N := \{v \in A;\ h(v) + d(v) = \delta\}$. Tento algoritmus zase správně najde vzdálenosti všech vrcholů od s, ale je-li h „kvalitní" (je to dobrý dolní odhad pro vzdálenosti od c), dá se čekat, že algoritmus najde definitivní vzdálenost do c rychleji než Dijkstrův algoritmus samotný. Důkaz správnosti ponecháváme jako cvičení 6.

Cvičení

1. Podle algoritmu napište program ve vašem oblíbeném programovacím jazyce.

2.* Navrhněte podrobně implementaci (způsob naprogramování) Dijkstrova algoritmu tak, aby pracoval vždy v čase $O(n \log n + m)$, kde $n = |V(G)|$, $m = |E(G)|$.

3. Ve kterém místě selže uvedený důkaz správnosti Dijkstrova algoritmu, připustíme-li i záporná ohodnocení hran?

4.* Upravte algoritmus tak, aby nejen našel vzdálenosti $d_{G,w}(s,v)$, ale aby pro každé v též nalezl nějakou nejkratší cestu z s do v.

5. Uvažte následující algoritmus pro graf $G = (V,E)$ a počáteční vrchol s (algoritmus známý pod jménem *prohledávání do šířky*): Položíme $V_0 = \{s\}$, a bylo-li V_i již definováno, položíme

$$V_{i+1} = \{v \in V \setminus (V_0 \cup V_1 \cup \ldots \cup V_i);\ \text{existuje } u \in V_i,\ \{u,v\} \in E\}.$$

   (a) Formulujte přesně podmínku ukončení algoritmu (tak, aby fungoval i pro nesouvislý graf).

   (b) Dokažte, že množina V_i jsou vrcholy v, pro něž $d_G(s,v) = i$.

   (c) Navrhněte implementaci (způsob naprogramování) algoritmu, který vyžaduje nejvýš $O(n+m)$ kroků, kde $n = |V|$, $m = |E|$.

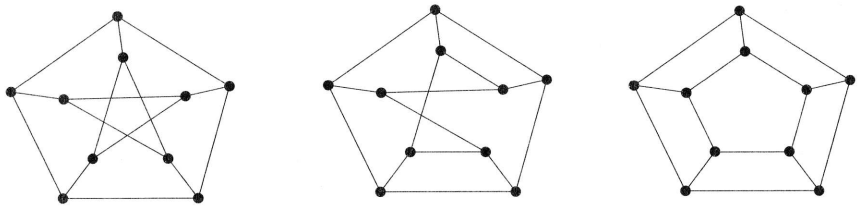
6.* Dokažte správnost Dijkstrova algoritmu s heuristikou, popsaného v závěru této části.

4.4 Skóre grafu

Nechť G je graf, v jeho vrchol. Symbolem $\deg_G(v)$ označme počet hran grafu G obsahujících vrchol v. Číslo $\deg_G(v)$ nazveme *stupněm* vrcholu v v grafu G.

Označme vrcholy grafu G $v_1, v_2, \ldots, v_n$ (v nějakém libovolně zvoleném pořadí). Posloupnost

$$(\deg_G(v_1), \deg_G(v_2), \ldots, \deg_G(v_n))$$



Obrázek 4.2: Tři grafy se skóre $(3,3,3,3,3,3,3,3,3,3)$.

nazýváme *posloupnost stupňů* grafu G, nebo *skóre* grafu G. Dvě skóre přitom považujeme za stejná, pokud jedno můžeme dostat z druhého přerovnáním čísel (to znamená, že skóre nezávisí na zvoleném pořadí vrcholů).

Je snadno vidět, že dva isomorfní grafy mají stejná skóre (v právě zavedeném smyslu); tudíž dva grafy s různým skóre jsou nutně neisomorfní. Na druhé straně, grafy se stejným skóre ještě isomorfní být nemusí. Tak například následující dva grafy



mají oba skóre $(2,2,2,2,2,2)$, a přitom jsou zjevně neisomorfní – jeden je totiž souvislý, zatímco druhý není. Všechny tři grafy na obr. 4.2 mají skóre $(3,3,3,3,3,3,3,3,3,3)$ a přitom žádné dva nejsou isomorfní (přesvědčit se o tom je trochu těžší, viz cvičení 1). Přesto skóre představuje důležitou a snadno zjistitelnou charakteristiku grafu.

Budeme nyní hledat vlastnosti, které musí posloupnost čísel mít, aby byla skórem nějakého grafu. Jedna taková významná vlastnost je následující:

4.4.1 Tvrzení (Princip sudosti). *Pro každý graf $G = (V, E)$ platí*

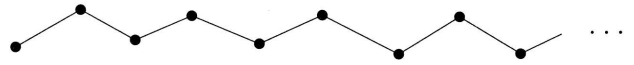
$$\sum_{v \in V} \deg_G(v) = 2|E|.$$

Důkaz. Stupeň vrcholu v udává počet hran G obsahujících v. Přitom každá hrana obsahuje dva vrcholy; sečteme-li tedy všechny stupně, dostaneme dvojnásobek počtu hran. □

4.4.2 Důsledek. *Počet vrcholů lichého stupně je sudé číslo pro každý graf.*

(Neboli počet účastníků večírku, kteří si potřásli rukou s lichým počtem jiných účastníků, je sudé číslo – pro každý konečný večírek.)

Poznamenejme, že pro nekonečné večírky věta neplatí: následující graf (jednostranně nekonečná cesta) má jen jediný vrchol lichého stupně.



Důsledek 4.4.2 (ani některé další snadné podmínky) na charakterizaci skóre grafu nestačí. Charakteristika skóre není zrovna jednoduchá a souvisí s problematikou tzv. toků v sítích, jež přesahuje rámec tohoto textu. Ukážeme zde však jednoduchý postup, jak o dané posloupnosti rozhodnout, zda je to skóre nějakého vhodného grafu. Základem je následující:

4.4.3 Věta (Věta o skóre). *Nechť $D = (d_1, d_2, \ldots, d_n)$ je posloupnost přirozených čísel. Předpokládejme, že $d_1 \leq d_2 \leq \ldots \leq d_n$, a označme symbolem D' posloupnost $(d'_1, \ldots, d'_{n-1})$, kde*

$$d'_i = \begin{cases} d_i & \text{pro } i < n - d_n \\ d_i - 1 & \text{pro } i \geq n - d_n. \end{cases}$$

Potom D je skóre grafu právě když D' je skóre grafu.

Důkaz. Jedním směrem je tvrzení snadné. Předpokládejme, že D' je skóre grafu $G' = (V', E')$, kde $V' = \{v_1, \ldots, v_{n-1}\}$ a $\deg_G(v_i) = d'_i$.

Zvolme nový vrchol v_n, různý od $v_1, \ldots, v_{n-1}$, a definujme nový graf $G = (V, E)$, kde

$$V = V' \cup \{v_n\}$$
$$E = E' \cup \{\{v_i, v_n\};\ i = n - d_n, n - d_n + 1, \ldots, n - 1\}$$

(méně formálně řečeno, nový vrchol v_n připojíme k posledním d_n vrcholům grafu G'). Zřejmě skóre grafu G je právě D.

Těžší je dokázat opačnou implikaci. Předpokládejme tedy, že D je skóre nějakého grafu. Uvažme množinu $\mathcal{G}$ všech grafů na množině vrcholů $\{v_1, \ldots, v_n\}$, v nichž je stupeň každého v_i roven d_i (tj. mají skóre D). Dokážeme následující

> *Pomocné tvrzení:* V množině $\mathcal{G}$ existuje graf G_0, v němž je vrchol v_n spojen právě s vrcholy $v_{n-d_n}, v_{n-d_n+1}, \ldots, v_{n-1}$ (neboli s posledními d_n vrcholy).

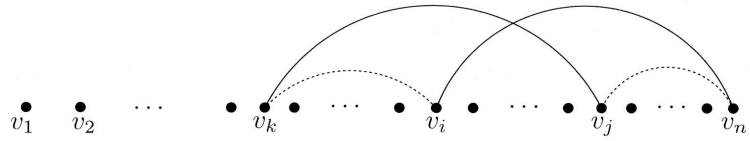
Budeme-li mít graf G_0 jako v pomocném tvrzení, je už jasné, že graf $G' = (\{v_1, \ldots, v_{n-1}\}, E')$, kde $E' = \{e \in E(G_0);\ v_n \notin e\}$, má skóre D', a tím bude věta o skóre dokázána. Zbývá dokázat pomocné tvrzení.

Pokud $d_n = n-1$, tj. pokud vrchol v_n je spojen s každým z vrcholů $v_1, \ldots, v_{n-1}$, vyhovuje pomocnému tvrzení kterýkoli graf z $\mathcal{G}$ a jsme hotovi. Jinak, tj. pokud v_n není spojen se všemi ostatními vrcholy, definujme pro každý graf $G \in \mathcal{G}$ číslo $j(G)$, což bude největší index $j \in \{1, 2, \ldots, n-1\}$ takový, že $\{v_j, v_n\} \notin E(G)$. Buď G_0 graf, pro nějž je $j(G)$ nejmenší možné; dokážeme, že $j(G_0) = n - d_n - 1$, z čehož je už patrné, že G_0 vyhovuje pomocnému tvrzení.

Předpokládejme tedy pro spor, že $j = j(G_0) > n - d_n - 1$. Vrchol v_n musí být spojen s d_n vrcholy, a z nich nejvýš $d_n - 1$ může následovat po vrcholu v_j. Proto existuje nějaké $i < j$ takové, že v_i je spojen s vrcholem v_n. Máme tedy $\{v_j, v_n\} \notin E(G_0)$, $\{v_i, v_n\} \in E(G_0)$. Vzhledem k tomu, že $\deg_{G_0}(v_i) \leq \deg_{G_0}(v_j)$, existuje nějaký vrchol v_k, který je spojený hranou s v_j, ale nikoli s v_i. V této situaci uvážíme nový graf $G' = (V(G_0), E')$, kde

$$E' = (E(G_0) \setminus \{\{v_i, v_n\}, \{v_j, v_k\}\}) \cup \{\{v_j, v_n\}, \{v_i, v_k\}\}.$$

Viz obrázek:



Je snadno vidět, že graf G' má rovněž skóre D, a přitom $j(G') \leq j(G_0) - 1$, což je spor s volbou grafu G_0. Tím je dokázáno pomocné tvrzení, a tudíž i věta 4.4.3. □

Z věty 4.4.3 lze odvodit algoritmus, který umožňuje rychle rozhodnout, jestli je daná konečná posloupnost skórem nějakého grafu.

4.4.4 Úloha. *Rozhodněte, zda posloupnost* (1, *1, 1, 2, 2, 3, 4, 5,* 5) *je skóre grafu.*

Řešení. Danou posloupnost redukujeme opakovaným použitím věty 4.4.3. Dostáváme tak posloupnosti

(1, 1, 1, 1, 1, 2, 3, 4)
(1, 1, 1, 0, 0, 1, 2), po přerovnání (0, 0, 1, 1, 1, 1, 2)
(0, 0, 1, 1, 0, 0), po přerovnání (0, 0, 0, 0, 1, 1)
(0, 0, 0, 0, 0).

Protože poslední posloupnost je skóre grafu (grafu s 5 vrcholy a žádnou hranou), dostáváme, že i posloupnost (1, 1, 1, 2, 2, 3, 4, 5, 5) je skóre grafu. Sestrojte sami příklad takového grafu!

Cvičení

1. Dokažte, že tři grafy na druhém obrázku této sekce jsou navzájem neisomorfní.

2. Sestrojte příklad posloupnosti délky n, jejíž každý člen je některé z čísel $1, \ldots, n-1$ a která má sudý počet lichých členů, a přesto není skórem žádného grafu.

3. Najděte nejmenší možný příklad (s co nejméně vrcholy) dvou souvislých neisomorfních grafů se stejným skórem.

4. Nakreslete všechny navzájem neisomorfní grafy se skórem (6, 3, 3, 3, 3, 3, 3) (ukažte, že jste žádný nevynechali!).

5. Uveďte co nejmenší příklad grafu s 6 vrcholy stupně 3, ostatními vrcholy stupně ≤ 2, a s 12 hranami.

6. Buď G graf s 9 vrcholy, každý stupně 5 nebo 6. Dokažte, že má aspoň 5 vrcholů stupně 6 nebo aspoň 6 vrcholů stupně 5.

7. (a) Rozhodněte, zda existuje graf se skórem tvořeným $n \geq 2$ navzájem různými čísly.

   (b)* Pro která n existuje graf na n vrcholech, jehož skóre má všechna čísla navzájem různá až na 2?

8.* Nechť G je graf s maximálním stupněm 3. Dokažte, že jeho vrcholy lze obarvit dvěma barvami tak, že nevznikne jednobarevná cesta se 3 vrcholy.

9.** Nechť G je graf, jehož všechny vrcholy mají stupeň aspoň 3. Dokažte, že potom G obsahuje kružnici, která není indukovaným podgrafem (tj., má „diagonálu").

10. Graf G se nazývá *k-regulární* (česky k-pravidelný), jsou-li stupně všech jeho vrcholů přesně k. Určete všechny dvojice (k, n) takové, že existuje k-regulární graf na n vrcholech.

11. Nakreslete všechny 3-regulární grafy na 6 vrcholech.

12. Najděte 3-regulární asymetrický graf (viz cvičení 4 v části 4.1).

13.* Nechť G je souvislý graf, v němž mají každé dva různé vrcholy u, v buď 0 nebo 5 společných sousedů. Dokažte, že G je k-regulární (pro nějaké k).

14.** Dokažte, že v každém grafu se sudým počtem vrcholů existují dva vrcholy, které mají sudý počet společných sousedů.

15. Nechť G je graf s n vrcholy, jehož každý vrchol má stupeň větší než $\frac{n}{2}$.

   (a) Dokažte, že G obsahuje aspoň 1 trojúhelník (cyklus délky 3).

   (b)* Dokažte, že existuje hrana $\{x, y\}$ obsažená aspoň v $n/6$ trojúhelnících (tj. existuje aspoň $n/6$ vrcholů spojených jak s x tak s y). Použijte principu inkluze a exkluze.

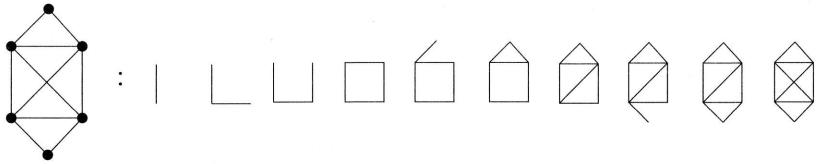
4.5 Jednotažky – eulerovské grafy

Jednou ze základních (a nejstarších) úloh týkající se grafů je následující otázka:

> *Nakreslete daný graf $G = (V, E)$ jedním uzavřeným tahem, bez zvednutí tužky z papíru (přičemž žádná hrana se neobtahuje dvakrát).*

Matematicky lze úlohu formalizovat takto: Najděte uzavřený sled $(v_0, e_1, v_1, \ldots, e_{m-1}, v_{m-1}, e_m, v_0)$, v němž se každá hrana vyskytuje právě jednou a každý vrchol aspoň jednou. Takový sled budeme nazývat *uzavřeným eulerovským tahem*. Graf je eulerovský právě když má aspoň jeden uzavřený eulerovský tah.

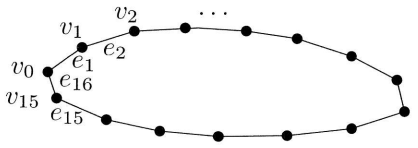
Následující obrázek ukazuje příklad kreslení grafu jedním tahem:



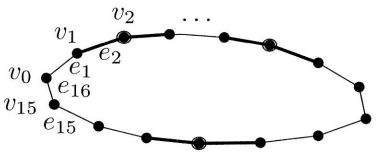
Podáme nyní charakteristiku eulerovských grafů. Pro stručnost definujeme *tah* v grafu G jako sled, v němž se žádná hrana neopakuje (vrcholy se opakovat mohou).

4.5.1 Věta (Charakterizace eulerovských grafů). *Graf G je eulerovský právě když je souvislý a každý vrchol G má sudý stupeň.*

První důkaz. Uvedená podmínka je nutná. Eulerovský graf musí zjevně být souvislý. Stupně vrcholů jsou sudé, protože kdykoli eulerovský tah vstoupí do vrcholu, musí jej také zase opustit. Řekněme to přesněji. Nakresleme si nějaký eulerovský tah schématicky jako kružnici:



V tomto obrázku jsou všechny hrany $e_1, e_2, \ldots$ navzájem různé, ale některé z puntíků $v_0, v_1, \ldots$ mohou ve skutečnosti označovat týž vrchol. Podívejme se na nějaký vrchol $v \in V$, a vyznačme všechny jeho výskyty na předchozím obrázku. Například:



Stupeň v je roven počtu hran zasahujících do vyznačených puntíků na tomto obrázku. Každý vyznačený puntík přispěje dvěma hranami, a žádná hrana nemá oba konce vyznačené (protože vyznačené puntíky odpovídají všechny stejnému vrcholu zatímco hrana má dva různé konce). Proto $\deg_G(v)$ je sudé pro každý vrchol v.

Naopak, nechť souvislý graf G má všechny vrcholy sudého stupně. Uvažme v G tah $T = (v_0, e_1, v_1, \ldots, e_m, v_m)$, který má maximální možnou délku, m.

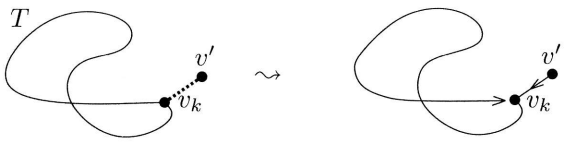
Nejdříve dokážeme, že $v_0 = v_m$. Kdyby ne, potom do vrcholu v_0 zasahuje lichý počet hran tahu T. Protože ale $\deg_G(v_0)$ je sudý, existuje nějaká hrana $e \in E$, která není v T obsažena, a o tuto hranu bychom mohli tah prodloužit – spor.

Předpokládejme tedy $v_0 = v_m$ a dokazujme $\{e_1, e, \ldots, e_m\} = E$. Definujme pomocný graf $G' = (V', E')$, kde V' je množina všech vrcholů tahu T a E' je množina všech jeho hran.

Nejdříve předpokládejme $V' \neq V$. Díky souvislosti grafu G existuje hrana tvaru $e = \{v_k, v'\} \in E$, kde $v_k \in V'$ a $v' \notin V'$. V tomto případě tah

$$(v', e, v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, e_m, v_0, e_1, v_1, \ldots, e_k, v_k)$$

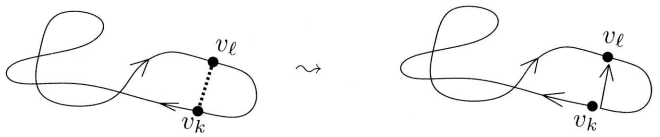
má délku $m+1$ a vede tedy ke sporu, viz obrázek:



Jestliže $V' = V$ a $E' \neq E$, uvažme hranu $e = \{v_k, v_\ell\} \in E \setminus E'$. Podobně jako v předchozím případě vede tah

$$(v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, e_m, v_0, e_1, v_1, \ldots, e_k, v_k, e, v_\ell)$$

ke sporu:



□

Druhý důkaz. Budeme dokazovat jen to, že každý souvislý graf se všemi stupni sudými má eulerovský tah (obrácená implikace je snadná a stačí nám pro ni jeden důkaz). Prvním krokem je

4.5.2 Lemma. *Má-li graf $G = (V, E)$ všechny stupně sudé, potom množinu hran E lze rozložit na disjunktní podmnožiny $E_1, E_2, \ldots, E_k$ takové, že každá E_i je množinou hran kružnice.*

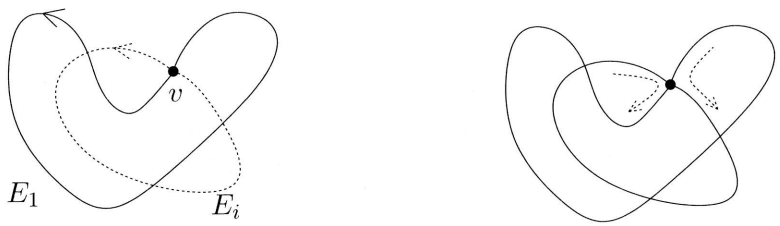
Důkaz lemmatu. Postupujeme indukcí podle $|E|$, pro $E = \emptyset$ lemma platí. V indukčním kroku stačí ukázat, že G obsahuje aspoň jednu kružnici. Označíme-li totiž její množinu hran E_1, potom graf $(V, E \setminus E_1)$ má opět všechny stupně sudé, a podle indukčního předpokladu lze jeho množinu hran rozložit na kružnice.

Hledejme tedy kružnici v G za předpokladu $E \neq \emptyset$. Budeme konstruovat cestu v G. Zvolíme libovolný vrchol v_0, z něhož vychází aspoň jedna hrana $e_1 = \{v_0, v_1\}$, a vezmeme (v_0, e_1, v_1) jako počáteční cestu. Když už jsme zkonstruovali cestu $(v_0, e_1, \ldots, v_{i-1}, e_i, v_i)$, podíváme se, jestli v_i sousedí s některým z vrcholů v_j, $0 \leq j \leq i-2$. Pokud ano, hrana $\{v_i, v_j\}$ spolu s úsekem vybudované cesty mezi v_j a v_i tvoří hledanou kružnici. Pokud v_i nesousedí s žádným v_j, $0 \leq j \leq i-2$, potom můžeme cestu prodloužit o další hranu $e_{i+1} = \{v_i, v_{i+1}\}$, poněvadž v_{i-1} není jediným sousedem vrcholu v_i (jinak by v_i měl stupeň 1, což není sudé číslo).

V konečném grafu nemůže cesta pokračovat do nekonečna, takže popsaný postup dříve či později najde kružnici. □

Dokončíme teď druhý důkaz věty 4.5.1. Máme dán souvislý graf $G = (V, E)$ se sudými stupni. Rozložíme E na disjunktní množiny $E_1, E_2, \ldots, E_k$ hran kružnic jako v právě dokázaném lemmatu. Nyní tyto kružnice postupně propojíme do eulerovského tahu. Přesněji, dokážeme toto: *Buď $G = (V, E)$ souvislý graf, a nechť E je disjunktním sjednocením množin $E_1, E_2, \ldots, E_\ell$, $\ell > 1$, kde každou E_i lze projít jedním uzavřeným tahem. Potom existuje index $i \neq 1$ takový, že také $E_1 \cup E_i$ lze projít jedním uzavřeným tahem.*

Opakovaným použitím tohoto tvrzení se dá z počátečních k kružnic vyrobit eulerovský tah. Abychom to tvrzení dokázali, označme V_i množinu všech vrcholů, které jsou obsaženy v aspoň jedné hraně z E_i. Stačí nahlédnout, že existuje $i \neq 1$ tak, že $V_1 \cap V_i \neq \emptyset$ (pak můžeme uzavřené tahy E_1 a E_i za společný vrchol slepit do jediného uzavřeného tahu, viz obrázek).



Předpokládejme tedy opak: $V_1 \cap (V_2 \cup V_3 \cup \cdots \cup V_k) = \emptyset$. To ale znamená, že mezi V_1 a $V_2 \cup V_3 \cup \cdots \cup V_k$ nejde žádná hrana (připomeňme, že každá hrana patří do nějakého E_i), a G tedy není souvislý – spor. □

Poznámka o hamiltonovských kružnicích. *Hamiltonovská kružnice* v grafu G je kružnice obsahující všechny vrcholy G. Tento pojem je na první pohled podobný uzavřenému eulerovskému tahu: hamiltonovská kružnice má procházet bez opakování všechny vrcholy, a uzavřený eulerovský tah všechny hrany. Přesto je matematická a algoritmická obtížnost obou pojmů úplně rozdílná. Zatímco uzavřené eulerovské tahy jsou snadno zvládnutelné, problém existence hamiltonovské kružnice je matematicky i algoritmicky obtížný a žádnou jednoduchou charakterizaci grafů s hamiltonovskou kružnicí nelze čekat. Některé úvahy o hamiltonovských kružnicích si může čtenář zkusit ve cvičení 5.

Poznámka o násobných hranách. Zatím jsme definovali hrany grafu jako dvoubodové množiny vrcholů (a této definice se budeme zpravidla držet i nadále). To mimo jiné znamená, že dva dané vrcholy mohou být spojeny nejvýš jednou hranou. V některých aplikacích je však přirozené připustit, aby dva vrcholy mohly být spojeny i několika (různými) hranami; dostáváme tak *grafy s násobnými hranami* (zvané též *multigrafy*). Matematicky lze tento pojem vystihnout několika různými (a různě šikovnými) způsoby.

Mohli bychom například každé dvojici vrcholů $\{u, v\}$ přiřadit nezáporné celé číslo $m(u, v)$, *násobnost* hrany $\{u, v\}$. Přitom $m(u, v) = 0$ by znamenalo, že hrana v grafu není přítomna, $m(u, v) = 1$ by znamenalo „obyčejnou“ (jednoduchou) hranu, a $m(u, v) > 1$ by znamenalo, že graf obsahuje $m(u, v)$ „kopií“ hrany $\{u, v\}$. Multigraf by pak byl uspořádaná dvojice (V, m), kde $m : \binom{V}{2} \to \{0, 1, \ldots\}$.

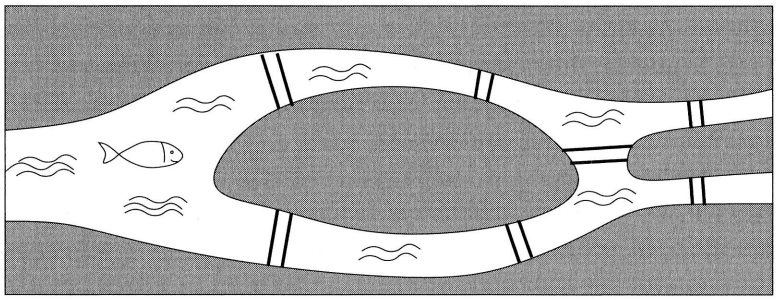
Jiný používaný způsob, z jistého hlediska elegantnější, je prohlásit hrany za „abstraktní“ objekty, tj. vzít E jako nějakou konečnou množinu disjunktní s množinou vrcholů V, a potom pro každou hranu určit dvojici vrcholů, které jsou jejími „konci“ (a jedna dvojice vrcholů se může vyskytnout pro více hran). Formálně, graf s násobnými hranami by byl trojice (V, E, ε), kde V a E jsou disjunktní množiny a $\varepsilon : E \to \binom{V}{2}$ je zobrazení, určující konce hran.

Někdy je také výhodné v grafu připouštět *smyčky*, tj. hrany začínající a končící v témže vrcholu. Formálně je opět možné smyčky zavést řadou způsobů. Nejjednodušeji můžeme smyčku u vrcholu v v množině hran E reprezentovat jako jednoprvkovou množinu $\{v\}$ (zatímco ostatní hrany jsou dvouprvkové). Při zavedení násobných hran pomocí zobrazení ε by se smyčky zavedly tím, že ε bude zobrazení do množiny $\binom{V}{2} \cup V$, a smyčka e se zobrazí na svůj (jediný) koncový vrchol. O ještě další modifikaci pojmu grafu (orientované grafy) budeme mluvit v části 4.6.

U většiny jednodušších aplikací není způsob formálního zavedení grafů s násobnými hranami příliš důležitý, pokud ovšem zvolíme jeden způsob a nadále se jej konzistentně držíme, a pokud to není způsob zbytečně neohrabaný.

Cvičení

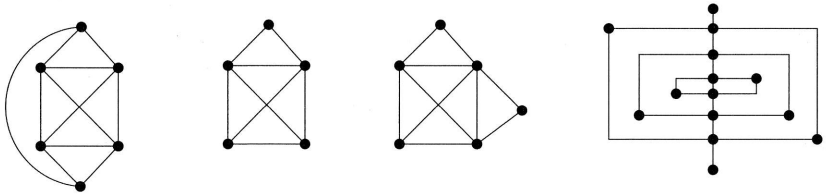
1. Na následujícím plánku města je schématicky znázorněno 7 mostů.



(a) Rozhodněte, zda je možno vyjít z určitého místa, projít všechny mosty, každý z nich však pouze jedenkrát, a vrátit se do výchozího místa. Je možno projít tímto způsobem všechny mosty, aniž bychom požadovali návrat do výchozího místa?
(Toto je historická motivace pojmu eulerovských grafů: plánek odpovídá části města Královce, Königsbergu, či Kaliningradu – jak různě se ve své pohnuté historii nazývalo – a tuto úlohu řešil Euler roku 1736.)

(b) Kolik mostů by bylo třeba přistavět (a kde), aby úloha měla kladné řešení?

2. Nakreslete jedním tahem následující grafy



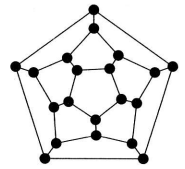
3. Charakterizujte grafy, které lze nakreslit jedním tahem, jenž nemusí být nutně uzavřený.

4. (a) Na základě prvního důkazu věty 4.5.1 formulujte algoritmus pro nalezení uzavřeného eulerovského tahu.

(b) Podobně pro druhý důkaz. *Pro který z algoritmů se vám podaří ukázat lepší časovou složitost?

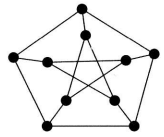
5. (Hamiltonovské kružnice)

(a) Najděte hamiltonovskou kružnici grafu



(to je abstraktní verze hlavolamu, vynalezeného významným matematikem sirem Hamiltonem). Které další z grafů na obr. 6.1 (str. 216) mají hamiltonovskou kružnici?

(b) Pokuste se ukázat, že Petersenův graf

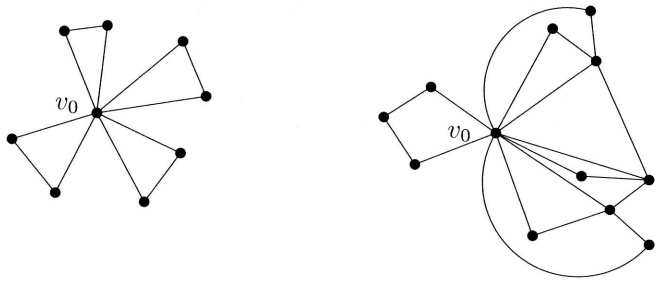


hamiltonovskou kružnici nemá.

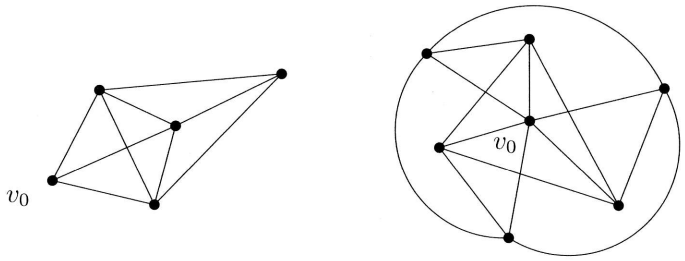
(c) Najděte dva grafy s týmž skóre, z nichž jeden má hamiltonovskou kružnici a druhý ne.

6. Řekněme, že graf $G = (V, E)$ je *náhodně eulerovský* z vrcholu v_0 jestliže každý maximální tah z vrcholu v_0 představuje již nakreslení grafu G jedním tahem (ekvivalentně: jestliže libovolný tah počínající ve vrcholu v_0, který již nelze prodloužit, představuje nakreslení grafu G jedním tahem).

(a) Dokažte, že následující grafy jsou náhodně eulerovské:



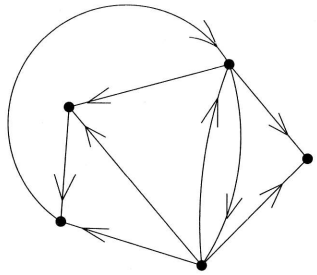
(b) Dokažte, že následující grafy nejsou náhodně eulerovské:

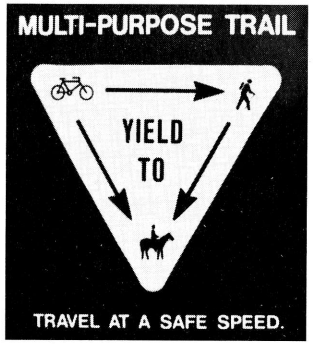


(c)* Dokažte následující charakteristiku náhodně eulerovských grafů: Souvislý graf $G = (V, E)$, jehož všechny vrcholy mají sudý stupeň, je náhodně eulerovský z vrcholu v_0, právě když graf $(V \setminus \{v_0\}, \{e \in E; v_0 \notin e\})$ neobsahuje kružnici (tj., každá komponenta tohoto grafu je strom; takové grafy se také nazývají *lesy*).

4.6 Eulerovské orientované grafy

Všechny grafy, které jsme dosud uvažovali, byly „neorientované" – jejich hrany byly neuspořádané dvojice. Čtenář se však zajisté setkal se schématy zahrnujícími jednosměrné ulice a schématy podobnými těm na obrázku:





4.6.1 Definice. Orientovaný graf G *je dvojice* (V, E) *kde* E *je podmnožina kartézského součinu* $V \times V$. *Prvky* E *nazýváme* šipky *(nebo* orientované hrany*). Tedy šipka* e *má tvar* (x, y). *Říkáme, že tato šipka* vychází *z* x *a* končí *v* y.

Mnoho úloh a pojmů, které se v tomto textu vyšetřují, je možno snadno modifikovat pro orientované grafy. Často však tato obecnější tvrzení jsou snadným zobecněním a přitom značení a postup by se zkomplikovaly. Proto jsme se rozhodli uvažovat ve většině textu pouze neorientované grafy. Učiňme na tomto místě výjimku a zaveďme eulerovské orientované grafy a popišme jednu jejich aplikaci.

Pozorný čtenář si možná všiml, že orientovaný graf $G = (V, E)$ je vlastně totéž co relace na množině V. Přesto se zavádějí oba tyto pojmy, protože orientované grafy se vyšetřují v jiných souvislostech než relace.

Nyní je přirozené definovat *orientovaný tah* jako posloupnost

$$(v_0, e_1, v_1, e_2, \ldots, e_m, v_m)$$

pro niž platí, že $e_i = (v_{i-1}, v_i) \in E$ pro každé $i = 1, 2, \ldots, m$ a navíc $e_i \neq e_j$ kdykoliv $i \neq j$. (Podobně definujeme pojmy orientovaný sled, orientovaná cesta, orientovaná kružnice – orientované kružnice je zvykem nazývat *cykly*.)

Řekněme, že orientovaný graf (V, E) je *eulerovský*, jestliže v něm existuje uzavřený orientovaný tah, který obsahuje každou hranu právě jednou a každý vrchol aspoň jednou.

Orientované eulerovské grafy lze opět charakterizovat velmi dobře. Před příslušnou větou je však třeba zavést ještě několik pojmů.

Pro daný vrchol v v orientovaném grafu $G = (V, E)$ označme $\deg^+_G(v)$ počet šipek G, které končí ve v. Podobně $\deg^-_G(v)$ označuje počet šipek G, které začínají ve v. Číslo $\deg^+_G(v)$ se nazývá *vstupní stupeň vrcholu* v a $\deg^-_G(v)$ se nazývá *výstupní stupeň* vrcholu v. Orientovaný graf $G = (V, E)$ nazýváme *vyvážený*, jestliže pro každý vrchol $v \in V$ platí $\deg^+_G(v) = \deg^-_G(v)$.

Každému orientovanému grafu $G = (V, E)$ lze přiřadit neorientovaný graf $\operatorname{sym}(G) = (V, \bar{E})$, kde

$$\bar{E} = \{\{x, y\};\ (x, y) \in E \text{ nebo } (y, x) \in E\}.$$

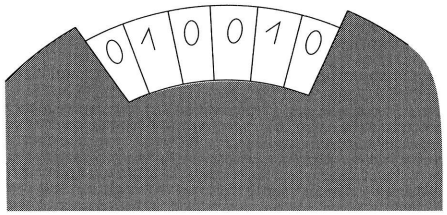
Graf $\operatorname{sym}(G)$ se nazývá *symetrizace* grafu G.

Platí následující charakteristika eulerovských grafů:

4.6.2 Tvrzení. *Orientovaný graf je eulerovský právě když je vyvážený a jeho symetrizace je souvislý graf*[3].

Důkaz tohoto tvrzení je velice podobný důkazu věty 4.5.1, a proto jej ponecháváme jako cvičení.

Aplikace. Představme si, že máme na obvod kotouče rozmístit čísla 0 a 1 takovým způsobem, že v každé poloze kotouče zjistíme tuto polohu jednoznačně z k po sobě jdoucích cifer, které pozorujeme na určitém místě. Při daném k bychom chtěli navrhnout co největší kotouč.



[3]Orientovaný graf se souvislou symetrizací se nazývá *slabě souvislý*. Naproti tomu v *silně souvislém* orientovaném grafu lze každé dva vrcholy spojit orientovanou cestou (v obou směrech).

Jiná formulace problému je následující:

> *Nalezněte co nejdelší cyklické uspořádání čísel 0 a 1, tak, aby žádné dvě k-tice po sobě jdoucích cifer nebyly stejné (zde cyklickým uspořádáním myslíme rozestavení čísel na obvodu kruhu).*

Pro dané k označme délku nejdelšího možného cyklického uspořádání symbolem $u(k)$. Dokážeme následující překvapivé

4.6.3 Tvrzení. *Pro každé $k \geq 1$ platí $u(k) = 2^k$.*

Důkaz. Protože různých posloupností čísel 0 a 1 délky k je 2^k, délka uspořádání nemůže být větší než 2^k. Zbývá sestrojit cyklické uspořádání délky 2^k s požadovanou vlastností.

Definujeme orientovaný graf $G = (V, E)$ následovně:

- V je množina všech posloupností 0 a 1 délky $k - 1$ (tedy $|V| = 2^{k-1}$).
- Množina šipek je tvořena množinou všech dvojic tvaru

$$((a_1, \ldots, a_{k-1}), (a_2, \ldots, a_k)).$$

Šipky tedy odpovídají posloupnostem tvaru

$$(a_1, \ldots, a_k),$$

a proto $|E| = 2^k$.

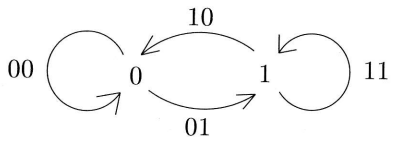
Pro zkrácení budeme rovněž šipku $((a_1, \ldots, a_{k-1}), (a_2, \ldots, a_k))$ označovat symbolem $(a_1, \ldots, a_k)$. Nemůže dojít k mýlce.

Zřejmě $\deg^-_G(v) = \deg^+_G(v) = 2$ pro každý vrchol $v \in V$. Graf $\operatorname{sym}(G)$ je rovněž souvislý, neb postupným vynecháváním posledních členů posloupnosti a přidáváním 0 na prvé místo lze každou posloupnost převést na posloupnost $(0, 0, \ldots, 0)$. Tedy G je eulerovský graf.

Položme $|E| = 2^k = K$, a nechť $(e^1, \ldots, e^K)$ je posloupnost hran v nějakém eulerovském tahu v G. Každá hrana e^i je tvaru

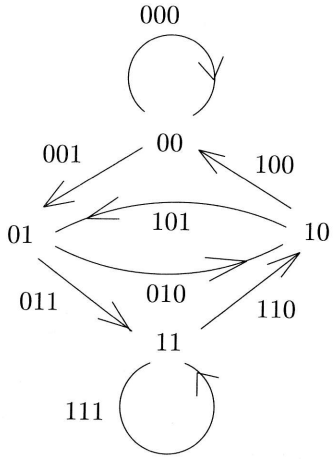
$e^i = (a_1^i, \ldots, a_k^i)$. Požadované cyklické uspořádání K číslic 0 a 1 definujeme jako $(a_1^1, a_1^2, \ldots, a_1^K)$ (tj., vzali jsme první prvek z každé posloupnosti e^i). Vzhledem k volbě vrcholů a hran se každá posloupnost délky k vyskytuje v cyklickém uspořádání $(a_1^1, a_1^2, \ldots, a_1^K)$, a to právě jednou. To dokazuje, že $u(k) = 2^k$. □

Eulerovské orientované grafy, sestrojené v tomto důkaze, se nazývají *De Bruijnovy grafy*. Pro $k = 2$ dostaneme takovouto situaci



tah: 00,01,11,10
cyklická posloupnost: 0011

a pro $k = 3$ tuto:



tah: 000,001,011,111,110,101,010,100
cyklická posloupnost: 00011101.

Cvičení

1. Dokažte tvrzení 4.6.2.
2. Navrhněte algoritmus pro nakreslení orientovaného grafu jedním tahem.
3. Kdy lze nakreslit orientovaný graf jedním tahem, který nemusí být nutně uzavřený?
4. Je-li $G = (V, E)$ graf, *orientace* G je každý orientovaný graf $G' = (V, E')$, který vznikne nahrazením každé hrany $\{u, v\} \in E$ buď šipkou (u, v), nebo šipkou (v, u).

   (a) Dokažte, že má-li graf G všechny stupně sudé, potom existuje jeho vyvážená orientace.

   (b) Dokažte, že vyvážený orientovaný graf je slabě souvislý, právě když je silně souvislý.
5.* Buď $G = (V, E)$ orientovaný graf, $w : E \to \mathbf{R}$ nějaké ohodnocení hran reálnými čísly. Funkci $p : V \to \mathbf{R}$ nazveme *potenciálem* pro w, pokud pro každou šipku $e = (u, v)$ platí $w(e) = p(v) - p(u)$. Dokažte, že potenciál pro w existuje právě když součet hodnot w přes hrany každého orientovaného cyklu v G je 0.
6.* Dokažte, že následující 2 podmínky pro silně souvislý orientovaný graf G jsou ekvivalentní:

   (i) G obsahuje orientovaný cyklus sudé délky.

   (ii) Vrcholy G lze obarvit dvěma barvami tak, že z každého vrcholu vychází šipka do vrcholu opačné barvy.

4.7 2-souvislost

Graf G nazveme *vrcholově k-souvislý*, má-li aspoň $k + 1$ vrcholů, a odebráním libovolných nejvýše $k - 1$ vrcholů vždy dostaneme souvislý graf. Graf G nazveme *hranově k-souvislý*, pokud po odebrání libovolných nejvýš $k - 1$ hran zůstane souvislý.

Je-li nějaký graf schématem např. spojů městské dopravy, železniční sítě, elektrického rozvodu a podobně, dává jeho vyšší souvislost naději na rozumné fungování příslušné sítě i za krizových podmínek, kdy jedna nebo několik křižovatek či spojnic selže. Pojem k-souvislosti je v teorii grafů teoreticky i prakticky velmi důležitý a souvisí s problematikou tzv.

toků v sítích, jíž se v tomto textu zabývat nebudeme. Zde se omezíme na vrcholovou 2-souvislost, již budeme potřebovat v kapitole o rovinných grafech a která nám rovněž poslouží pro ilustraci některých důkazových postupů a konstrukcí.

Vrcholové 2-souvislosti budeme říkat krátce 2-souvislost. Zopakujme tedy ještě pro jistotu definici:

4.7.1 Definice (2-souvislost). *Graf G nazveme* 2-souvislým, *má-li aspoň 3 vrcholy, a vynecháním jeho libovolného vrcholu vznikne souvislý graf.*

Je snadné nahlédnout, že každý 2-souvislý graf je také souvislý (tady se ovšem potřebuje předpoklad, že 2-souvislý graf má aspoň 3 vrcholy – doporučujeme čtenáři rozvážit si to). V tomto článku uvedeme alternativní popisy 2-souvislých grafů. Než začneme, zavedeme označení pro několik grafových operací, které zjednoduší zápis a budou se hodit i v budoucnu.

4.7.2 Definice (Některé grafové operace). *Nechť $G = (V, E)$ je graf. Definujeme*

- *(odebrání hrany)*

$$G - e = (V, E \setminus \{e\}),$$

kde $e \in E$ je hrana grafu G,

- *(přidání nové hrany)*

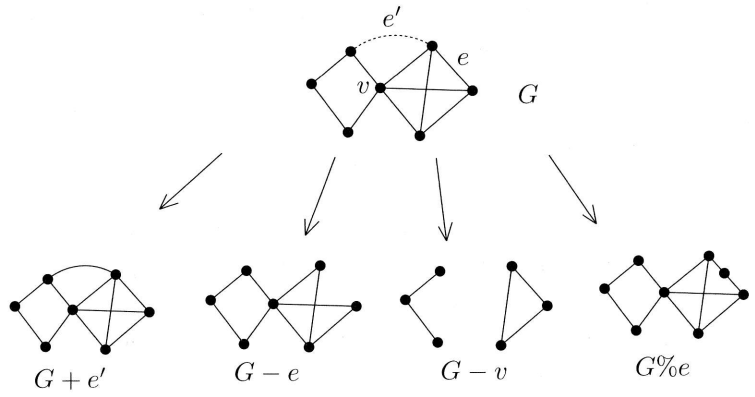
$$G + e' = (V, E \cup \{e'\}),$$

kde $e' \in \binom{V}{2} \setminus E$ je dvojice vrcholů, která není hranou,

- *(odebrání vrcholu)*

$$G - v = (V \setminus \{v\}, \{e \in E;\ v \notin e\}),$$

kde $v \in V$ (odebereme vrchol v a všechny hrany do něj zasahující),



Obrázek 4.3: Příklady grafových operací.

- *(dělení hrany)*

$$G\%e = \Big(V \cup \{z\}, (E \setminus \{\{x, y\}\}) \cup \{\{x, z\}, \{z, y\}\}\Big),$$

kde $\{x, y\} \in E$ je hrana, a $z \notin V$ je nový vrchol (na hranu $\{x, y\}$ „přikreslíme“ nový vrchol z).

Řekneme, že graf G' je dělení *grafu G, pokud G' je isomorfní grafu vytvořenému z grafu G postupným opakováním operace dělení hrany.*

Příklady právě zavedených operací jsou na obr. 4.3.

Vraťme se nyní ke 2-souvislosti. První význačná ekvivalentní charakterizace je následující:

4.7.3 Věta. *Graf G je 2-souvislý, právě když pro každé dva jeho vrcholy existuje kružnice v grafu G, která je obsahuje (tj., G je 2-souvislý, právě když každé dva vrcholy leží na společné kružnici).*

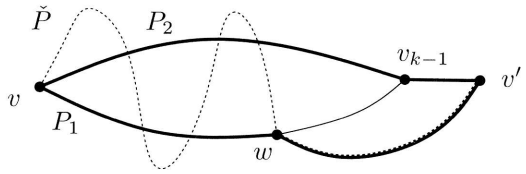
Důkaz. Uvedená podmínka je zřejmě postačující, neboť leží-li dva vrcholy v, v' na společné kružnici, potom mezi nimi existují dvě cesty,

které nemají žádné společné vrcholy mimo koncové, a tedy odebráním jednoho vrcholu se v a v' nemohou nikdy octnout v různých komponentách.

Dokážeme nyní obrácenou implikaci. Existenci společné kružnice pro vrcholy v, v' ukážeme indukcí podle $d_G(v, v')$, vzdálenosti vrcholů v a v'.

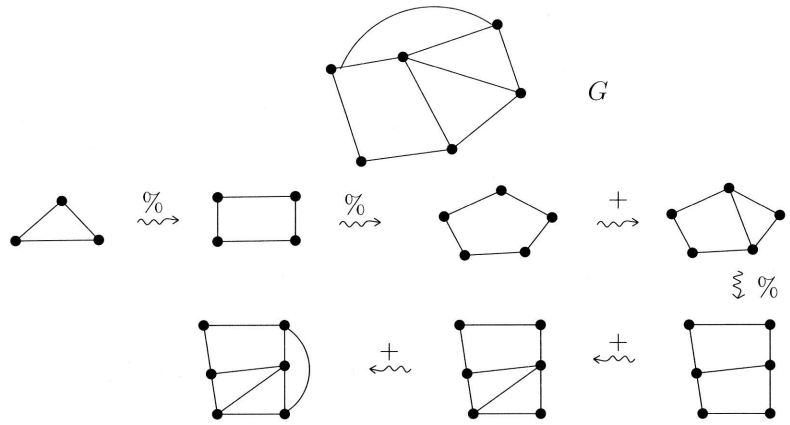
Nejdříve nechť $d_G(v, v') = 1$, to znamená, že $\{v, v'\} = e \in E(G)$. Díky 2-souvislosti G je graf $G - e$ také souvislý (kdyby byl $G - e$ nesouvislý, byl by aspoň jeden z grafů $G - v$, $G - v'$ také nesouvislý). Proto existuje v grafu $G - e$ cesta z v do v', a ta spolu s hranou e tvoří kružnici obsahující v i v'.

Předpokládejme nyní pro nějaké $k \geq 2$, že každá dvojice vrcholů ve vzdálenosti menší než k leží na společné kružnici, a uvažme dva vrcholy $v, v' \in V$ ve vzdálenosti k. Nechť $P = (v = v_0, e_1, v_1, \ldots, e_k, v_k = v')$ je cesta nejkratší délky z v do v'. Poněvadž $d_G(v, v_{k-1}) = k - 1$, existuje kružnice obsahující v i v_{k-1}. Tato kružnice je tvořena dvěma cestami, P_1 a P_2, z v do v_{k-1}. Uvažme nyní graf $G - v_{k-1}$. Ten je souvislý, a tedy v něm existuje cesta $\check{P}$ z vrcholu v do vrcholu v'. Tato cesta tedy neobsahuje vrchol v_{k-1}. Uvažme poslední vrchol na cestě $\check{P}$ (směrem od vrcholu v) náležející některé z cest P_1, P_2, a označme jej w, viz obrázek:



Předpokládejme (bez újmy na obecnosti), že w je vrcholem cesty P_1. Potom hledaná kružnice obsahující vrcholy v a v' bude tvořena cestou P_2, úsekem cesty P_1 mezi v a w, a úsekem cesty $\check{P}$ mezi w a v' (na obrázku vyznačena silně). □

4.7.4 Tvrzení. *Graf G je 2-souvislý, právě když libovolné jeho dělení je 2-souvislé.*



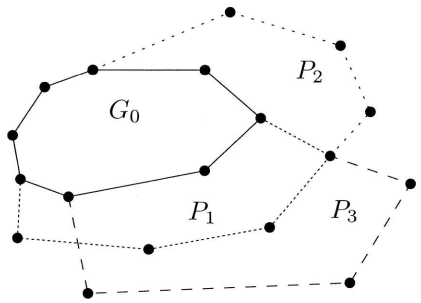
Obrázek 4.4: Příklad syntézy 2-souvislého grafu.

Důkaz. Stačí dokázat, že G je 2-souvislý, právě když $G\%e$ je 2-souvislý (pro libovolnou hranu $e \in E(G)$). Je-li $v \in V(G)$ libovolný vrchol grafu G, je snadno vidět, že $G - v$ je souvislý právě když $(G\%e) - v$ je souvislý. Dále využijeme jednoduchého pozorování, zmíněného v předchozím důkazu: (vrcholově) 2-souvislý graf zůstane souvislý i po odebrání libovolné hrany. Přitom je-li z nově přidaný vrchol v grafu $G\%e$, je $(G\%e) - z$ souvislý právě když $G - e$ je souvislý. Proto je 2-souvislost G a $G\%e$ ekvivalentní. □

Následující charakterizace 2-souvislých grafů je obzvlášť výhodná pro důkazy. Ukážeme totiž, jak lze 2-souvislé grafy konstruovat z grafů jednodušších.

4.7.5 Věta (Syntéza 2-souvislých grafů). *Graf G je 2-souvislý, právě když jej lze vytvořit z trojúhelníku (tj. z K_3) posloupností dělení hran a přidávání hran (viz obr. 4.4).*

Důkaz. Každý graf, který lze vytvořit z K_3 uvedenými operacemi, je zřejmě 2-souvislý. Chceme tedy ukázat, že můžeme vyrobit libovolný 2-souvislý graf.



Obrázek 4.5: Konstrukce 2-souvislého grafu přilepováním uší.

Budeme ve skutečnosti dokazovat možnost trochu jiného vytvoření. Začneme s nějakou kružnicí G_0, a byl-li již vytvořen graf G_{i-1}, graf G_i vznikne přidáním nějaké cesty P_i spojující dva vrcholy grafu G_{i-1}; přitom cesta P_i má s G_{i-1} společné pouze své koncové vrcholy (tedy žádné hrany ani žádné vnitřní vrcholy). Ke grafu tedy postupně „přilepujeme uši", viz obr 4.5.

Protože přidávání cesty lze zaměnit přidáním hrany a jejím opakovaným dělením[4], stačí zřejmě ukázat, že každý 2-souvislý graf G můžeme dostat opakovaným přidáváním uší.

Zvolme kružnici G_0 v grafu G libovolně. Předpokládejme, že jsme již definovali grafy $G_j = (E_j, V_j)$ pro $j \leq i$ s vlastnostmi jako výše. Pokud $G_i = G$, jsme hotovi; předpokládejme tedy, že $E_i \neq E(G)$. Protože G je souvislý, existuje hrana $e \in E(G) \setminus E_i$ taková, že $e \cap V_i \neq \emptyset$. Jestliže dokonce oba vrcholy hrany e náleží V_i, položme $G_{i+1} = G_i + e$.

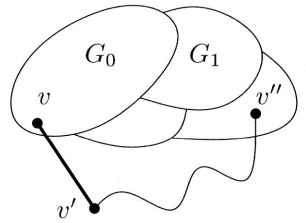
V opačném případě nechť $e = \{v, v'\}$, kde $v \in V_i$, $v' \notin V_i$. Uvažme nyní graf $G - v$. Ten je souvislý (neb G je 2-souvislý), takže existuje cesta P spojující vrchol v' s nějakým vrcholem $v'' \in V_i$, přičemž v'' je jediný vrchol cesty P náležející V_i (pro to stačí vzít např. nejkratší

[4]Musí se dát malinko pozor: jsou-li $v, v' \in V(G_{i-1})$ již spojeny hranou a spojujeme-li je novou cestou, nemůžeme začít přidáním hrany $\{v, v'\}$ (aspoň nepřipouštíme-li násobné hrany). Musíme nejdříve hranu $\{v, v'\}$ podrozdělit, potom znova přidat hranu $\{v, v'\}$ a pak případně pokračovat v prodlužování cesty dělením.

cestu mezi v' a V_i v grafu $G - v$). Pak můžeme definovat graf G_{i+1} přidáním hrany e a cesty P ke grafu G_i, tj.

$$V_{i+1} = V_i \cup V(P), \quad E_{i+1} = E_i \cup \{e\} \cup E(P).$$

Viz obrázek:



□

Cvičení

1. Dokažte, že pro každé dvě hrany 2-souvislého grafu existuje kružnice, která je obsahuje.

2. Buď G *kritický 2-souvislý graf*, to znamená, že G je 2-souvislý, ale žádný z grafů tvaru $G - e$ pro $e \in E(G)$ není 2-souvislý.

   (a) Dokažte, že aspoň jeden vrchol G má stupeň 2.

   (b) Pro každé n uveďte příklad kritického 2-souvislého grafu s vrcholem stupně aspoň n.

   (c)* Pro každé n uveďte příklad kritického 2-souvislého grafu s vrcholem stupně aspoň n, jenž je od všech vrcholů stupně 2 vzdálen aspoň n.

3. (a)* Je pravda, že libovolný kritický 2-souvislý graf (viz cvičení 2) lze dostat z nějaké kružnice postupným přilepováním „uší" (cest připojených za koncové vrcholy) délky aspoň 2?

   (b)* Je pravda, že libovolný kritický 2-souvislý graf lze dostat z nějaké kružnice postupným přilepováním „uší" tak, aby všechny mezistupně (po přilepení několika prvních uší) byly kritické 2-souvislé grafy?

4.* Dokažte, že každý 2-souvislý graf má silně souvislou orientaci (pojmy viz část 4.6).

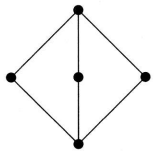
4.8 Grafy bez trojúhelníků: extremální úloha poprvé

Nechť graf G má n vrcholů. Co můžeme tvrdit o jeho počtu hran? To je snadná otázka a odpověď již známe: počet hran může být libovolné přirozené číslo mezi 0 a $\binom{n}{2}$. Maximální („extremální") počet hran grafu s n vrcholy je tedy $\binom{n}{2}$ a jediný graf s tímto počtem hran je isomorfní úplnému grafu K_n.

V tomto článku vyřešíme složitější, opravdovou extremální úlohu. Kolik hran může mít graf G s n vrcholy, jestliže víme, že neobsahuje trojúhelník (tedy podgraf isomorfní grafu K_3)? Opět nás zajímá maximální počet hran takového grafu. Označme toto číslo $T(n)$.

Zřejmě $T(1) = 0$, $T(2) = 1$ a $T(3) = 2$. Snadno se rovněž přesvědčíme, že $T(4) = 4$: Pro platnost nerovnosti $T(4) \geq 4$ stačí uvážit kružnici C_4 délky 4. Nerovnost $T(4) < 5$ dokážeme například tak, že graf se 4 vrcholy a 5 hranami je až na isomorfismus jednoznačně určen a obsahuje trojúhelník.

Kolik je $T(5)$? Kružnice C_5 délky 5 ukazuje, že $T(5) \geq 5$. Tento graf se zdá být nejlepší možný, protože libovolným přidáním hrany již vytvoříme trojúhelník. Ale zdání klame. Ve skutečnosti $T(5) \geq 6$, jak ukazuje graf na obrázku.



Jak uvidíme, tento graf již nejlepší možný opravdu je. V následující větě ukážeme, že platí $T(5) = 6$, a číslo $T(n)$ určíme dokonce pro každé n.

4.8.1 Věta. *Pro každé přirozené číslo n platí $T(n) = \lfloor \frac{n^2}{4} \rfloor$.*

Připomeňme, že symbol $\lfloor x \rfloor$ (pro reálné číslo x) označuje největší celé číslo nepřevyšující x.

Důkaz. Nejprve ukážeme platnost (podstatně snadnější) nerovnosti $T(n) \geq \lfloor \frac{n^2}{4} \rfloor$. Na to stačí najít vhodné grafy bez trojúhelníků. V tomto případě je výhodné postupovat poněkud obecněji. Nechť X a Y jsou disjunktní množiny. Označme $K_{X,Y}$ graf s množinou vrcholů $X \cup Y$ a s množinou hran $\{\{x, y\}; x \in X, y \in Y\}$. Graf $K_{X,Y}$ se nazývá úplný bipartitní a pro $|X| = a$, $|X| = b$ je $K_{X,Y}$ isomorfní grafu $K_{a,b}$, který jsme zavedli v části 4.1. Úplný bipartitní graf neobsahuje trojúhelník (neboť hrany jsou pouze „mezi" množinami X a Y). Stejně snadné je nahlédnout, že graf $K_{a,b}$ má $a \cdot b$ hran. Všimněme si, že graf na předchozím obrázku, dosvědčující $T(5) \geq 6$, je isomorfní grafu $K_{2,3}$.

Pro náš důkaz tedy stačí najít hodnoty a, b tak, aby platilo $a+b = n$ a $a \cdot b = \lfloor \frac{n^2}{4} \rfloor$. Ověříme, že vyhovují hodnoty $a = \lfloor \frac{n}{2} \rfloor$ a $b = n - a$. Rozlišíme dva případy: n liché a n sudé. Nejdřív nechť je n liché, tj. $n = 2k + 1$. V tomto případě $a = k$, $b = k + 1$ a $ab = k^2 + k$. Na druhé straně $\lfloor \frac{n^2}{4} \rfloor = \lfloor \frac{(2k+1)^2}{4} \rfloor = \lfloor k^2 + k + \frac{1}{4} \rfloor = k^2 + k = ab$. Druhý, snazší případ $n = 2k$ přenecháváme čtenáři. Ukázali jsme tedy platnost nerovnosti $T(n) \geq \lfloor \frac{n^2}{4} \rfloor$.

Nyní ukážeme těžší nerovnost $T(n) \leq \lfloor \frac{n^2}{4} \rfloor$. Protože $T(n)$ je celé číslo, stačí dokázat $T(n) \leq \frac{n^2}{4}$. Toto tvrzení ukážeme (trochu neobvyklou) indukcí dle n. Víme již, že tvrzení platí pro $n \leq 4$. V indukčním kroku dokážeme platnost implikace:

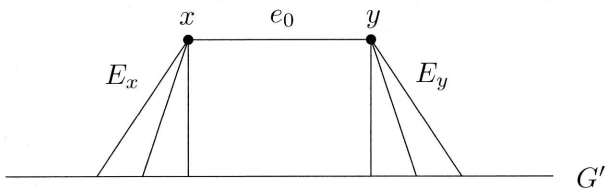
$$T(n) \leq \frac{n^2}{4} \quad \Rightarrow \quad T(n+2) \leq \frac{(n+2)^2}{4}.$$

Nechť tedy $G = (V, E)$ je libovolný graf s $n + 2$ vrcholy, který neobsahuje trojúhelník. Naším cílem je ukázat, že $|E| \leq \frac{(n+2)^2}{4}$. Zvolme libovolnou hranu $e_0 = \{x, y\} \in E$, položme $V' = V \setminus \{x, y\}$ a nechť $G' = (V', E')$ je podgraf G určený množinou V'. Graf G' neobsahuje trojúhelníky, a tedy podle indukčního předpokladu $|E'| \leq \frac{n^2}{4}$.

Označme E_x množinu hran grafu G incidentních s vrcholem x – formálně $E_x = \{e \in E; x \in e \in E, e \neq e_0\}$ – a množinu E_y definujeme obdobně pro y. Platí tedy

$$E = E' \cup (E_x \cup E_y) \cup \{e_0\} \quad \text{a} \quad |E| = |E'| + |E_x \cup E_y| + 1.$$

Klíčovým bodem důkazu je vztah $|E_x \cup E_y| \leq n$, což plyne z faktu, že žádná hrana z E_x nemá společný vrchol s žádnou hranou z E_y.



Celkem tedy dostáváme $|E| \leq \frac{n^2}{4} + n + 1 = \frac{(n+2)^2}{4}$. □

Z uvedeného důkazu můžeme vytěžit ještě více. Zavedeme následující pojem: Řekneme, že graf $G = (V, E)$ s n vrcholy je *extremální*, jestliže neobsahuje trojúhelník a má $\lfloor \frac{n^2}{4} \rfloor$ hran. Víme již, že $K_{\lfloor n/2 \rfloor, n-\lfloor n/2 \rfloor}$ je extremální.

4.8.2 Věta. *Pro každé n je každý extremální graf isomorfní grafu $K_{a,b}$, kde $a = \lfloor \frac{n}{2} \rfloor$, $b = n - \lfloor \frac{n}{2} \rfloor$.*

Úplný bipartitní graf je tedy jediný extremální graf. To je pozoruhodná skutečnost, které se stala základem celé teorie – *extremální teorie*. Další příklady uvádíme v části 7.3. Rovněž Spernerovu větu, viz část 7.2, lze považovat za výsledek extremální teorie.

Důkaz věty 4.8.2. Postupujeme podobně jako v důkazu věty 4.8.1, a protože důkaz vlastně opisujeme, zdůrazníme jen odlišnosti. Naše tvrzení opět platí pro $n = 1, 2, 3$, protože na těchto množinách můžeme uvážit všechny extremální grafy. V indukčním kroku předpokládáme jednoznačnost extremálních grafů s n vrcholy. Naším cílem je dokázat jednoznačnost extremálních grafů s $n + 2$ vrcholy.

Nechť tedy $G = (V, E)$ je extremální graf s $n+2$ vrcholy a $\lfloor \frac{(n+2)^2}{4} \rfloor$ hranami, který neobsahuje trojúhelník. Zvolme libovolnou hranu $e_0 = \{x, y\}$ a uvažme graf $G' = (V', E')$, kde $V' = V \setminus \{x, y\}$ a $E' = E \cap \binom{V'}{2}$. Protože $|E| = \lfloor \frac{n^2}{4} \rfloor + n + 1$ a protože $|E'| \leq \lfloor \frac{n^2}{4} \rfloor$ a $|E_x \cup E_y| \leq n$ (vše podle důkazu 4.8.1), dostáváme, že musí platit dokonce $|E'| = \lfloor \frac{n^2}{4} \rfloor$. Tedy graf G' je extremální a je isomorfní grafu $K_{a,b}$, kde $a = \lfloor \frac{n}{2} \rfloor$ a $b = n - a$. Tedy máme $G' = K_{X,Y}$ pro vhodný rozklad množiny V' na dvě části X a Y, $|X| = a$, $|Y| = b$. Všimneme si, že x nemůže být zároveň spojeno s vrcholem z X a s vrcholem z Y, a podobně pro y. Protože však musí platit rovněž $|E_x| + |E_y| = n$, dostáváme, že nastane jedna z následujících možností: buď je vrchol x spojen hranou s každým vrcholem množiny X a vrchol y je spojen hranou s každým vrcholem množiny Y, nebo vrchol x je spojen hranou s každým vrcholem množiny Y a vrchol y je spojen hranou s každým vrcholem množiny X. Obě možnosti, jakkoliv vypadají na první pohled různě, dávají isomorfní graf. □

Na závěr tohoto odstavce uveďme stručně jiný důkaz věty 4.8.1. Vlastně dokážeme trochu jinou větu.

4.8.3 Věta. *Nechť $G = (V, E)$ je graf bez trojúhelníků. Potom existuje rozklad množiny V na dvě podmnožiny X a Y takový, že pro každý vrchol $x \in V$ platí $d_G(x) \leq d_{K_{X,Y}}(x)$.*

Napřed si uvědomíme, jak z věty 4.8.3 plyne věta 4.8.1. Je to snadné. Z nerovnosti ve větě 4.8.3 dostáváme, že počet hran G je menší nebo roven počtu hran grafu $K_{X,Y}$, a stačí tedy ověřit, že maximální možný počet hran grafu $K_{a,b}$ pro $a + b = n$ je roven $\lfloor \frac{n^2}{4} \rfloor$ – viz cvičení 1.

Důkaz věty 4.8.3. Nechť $G = (V, E)$ je graf bez trojúhelníků. Zvolme vrchol x_0, jehož stupeň v G je maximální. Položme $Y = \{y; \{x_0, y\} \in E\}$ a $X = V \setminus Y$. Zřejmě $x_0 \in X$ a pro libovolné $x \in X$ máme $d_{K_{X,Y}}(x) = |Y| = d_G(x_0) \geq d_G(x)$, takže nerovnost z věty platí pro všechna $x \in X$. Dále si všimneme, že žádné dva vrcholy z Y nejsou spojeny hranou, protože všechny vrcholy z Y jsou sousedy vrcholu x_0 a G neobsahuje trojúhelníky. Tedy všichni sousedé každého $y \in Y$ leží v X a máme $d_G(y) \leq |X| \leq d_{K_{X,Y}}(y)$.

□

Cvičení

1. Určete, kdy výraz $a \cdot b$ nabývá maximální hodnoty pro přirozené čísla a, b splňující $a + b = n$.

2. Určete, kdy součin $a_1 \cdot a_2 \cdot \ldots \cdot a_k$ nabývá maximální hodnoty pro přirozené čísla $a_1, a_2 \ldots, a_k$ splňující $\sum_{i=1}^{k} a_i = n$ (k a n jsou přirozená čísla).

3.* Formulujte analogii tvrzení 4.8.1 pro grafy neobsahující K_4. Jaké jsou možné extremální grafy?

4. Úplný *k-partitní* graf $K(V_1, V_2, \ldots, V_k)$ na množině V je určen rozkladem $V_1, \ldots, V_k$ množiny V a jeho hrany jsou ty dvojice, které nejsou obsaženy v žádné z tříd rozkladu. Formálně $K(V_1, \ldots, V_k) = (V, E)$, kde $\{x, y\} \in E$ právě když $x \neq y$ a $|\{x, y\} \cap V_i| \leq 1$ pro každé $i = 1, \ldots, k$. Dokažte (použitím cvičení 2), že maximální počet hran úplného k-partitního grafu odpovídá rozkladu na skoro stejné velké části, tj. na části, jejichž velikosti se liší nejvíce o 1 (o rozkladech obecně viz část 1.6). Kolik má takový graf $K(V_1, \ldots, V_k)$ hran?

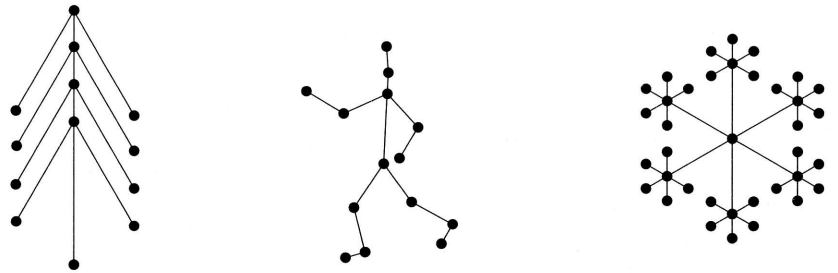
5.* Použitím cvičení 2 ukažte, že pro každé $k \geq 1$ a pro každý graf $G = (V, E)$ neobsahující úplný graf K_{k+1} existuje rozklad $V_1, \ldots, V_k$ množiny V tak, že stupeň libovolného vrcholu x v G je menší nebo roven stupni vrcholu x v $K(V_1, \ldots, V_k)$ (což je analogie věty 4.8.3). Dostanete tak analogii věty 4.8.1 pro každý úplný graf, což je slavná Turánova věta.

5

Stromy

5.1 Definice a charakteristika stromů

Strom je jeden z nejpřirozenějších útvarů jak v přírodě, tak v matematice. Stromy v přírodě jsou košaté, rozmanité a nesmírně složité. Stromy v teorii grafů jsou téměř nejjednodušší ze všech grafů, ale přesto jejich studium tvoří bohatou a zajímavou oblast. V teorii grafů se stromem rozumí konečný graf, který vypadá podobně jako na následujících obrázcích:



Jak tento pojem vystihnout? Pokuste se o to sami dřív, než budete pokračovat ve čtení.

Z hlediska teorie grafů lze pojem stromu definovat mnoha rozdílnými způsoby. Uvidíme to za okamžik, kdy podáme dokonce pět na-

prosto rozdílných charakteristik. Snad nejběžnější je však následující definice:

5.1.1 Definice. Strom *je souvislý graf neobsahující kružnici.*

Z mnoha hledisek je tato definice trochu nešikovná. Například není jasné, jak jednoduše zkontrolovat, že daný graf je strom. Souvislost lze ověřit snadno, s neexistencí kružnic je to však horší. Proto jsou důležité alternativní popisy stromů, které budou následovat. Začneme téměř zřejmým pozorováním:

5.1.2 Lemma (O koncovém vrcholu). *Každý strom s alespoň dvěma vrcholy obsahuje alespoň dva vrcholy stupně* 1. *Vrchol stupně* 1 *se nazývá* koncový vrchol *nebo* list.

Důkaz. Nechť $P = (v_0, e_1, v_1, \ldots, e_t, v_t)$ je cesta maximální možné délky ve stromu $T = (V, E)$ (strom se v teorii grafů zpravidla označuje písmenem T). Zřejmě délka cesty P je aspoň 1. Tvrdíme, že jak v_0, tak v_t jsou koncové vrcholy T. To můžeme nahlédnout sporem: Není-li např. v_0 koncový vrchol, pak existuje ještě jiná hrana $e \neq e_1$ obsahující vrchol v_0; označme $e = \{v_0, v\}$. Potom buď je v některým z vrcholů cesty P, tj. $v = v_i$, $i \geq 2$ (v tom případě e spolu s úsekem cesty P od v_0 do v_i tvoří kružnici), anebo $v \notin \{v_0, \ldots, v_t\}$ – tehdy bychom mohli cestu P prodloužit o hranu e. V obou případech dostaneme spor. □

Poznamenejme, že lemma o koncovém vrcholu neplatí pro nekonečné stromy (právě předvedený důkaz selže pro nekonečné stromy na tom, že nejdelší cesta nemusí existovat): například jednostranně nekonečná cesta má jen jeden koncový vrchol



a oboustranně nekonečná cesta nemá dokonce žádný:



My však uvažujeme jen konečné grafy.

Výstavba stromů. Připomeňme značení ze sekce 4.7: je-li G graf a v jeho vrchol, potom $G - v$ označuje graf, který vznikne z G vynecháním v a všech hran, které vrchol v obsahují. V případě, že v je koncový vrchol stromu T, vznikne $T - v$ odebráním v a jediné hrany jej obsahující.

5.1.3 Tvrzení (Postupná výstavba stromů). *Pro daný graf G a jeho koncový vrchol v jsou následující dvě tvrzení ekvivalentní:*

(i) G je strom.

(ii) $G - v$ je strom.

Důkaz je velmi snadný. Dokážeme nejprve implikaci $(i) \Rightarrow (ii)$. Graf G je tedy strom, a chceme dokázat, že i $G - v$ je strom. Jsou-li x, y dva vrcholy grafu G různé od v, uvažme (nějakou) cestu z x do y. Tato cesta nemůže obsahovat vrchol stupně 1 mimo x a y, a tedy neobsahuje v. Proto je celá obsažena také v $G - v$, čili $G - v$ je souvislý. Protože G neobsahuje kružnici, očividně ani $G - v$ neobsahuje kružnici, a je to tudíž strom.

Zbývá dokázat implikaci $(ii) \Rightarrow (i)$. Nechť $G - v$ je strom. Přidáním koncového vrcholu v nemůžeme zjevně vytvořit kružnici. Zbývá nahlédnout souvislost G, ale ta je též zřejmá: mezi libovolnými dvěma vrcholy různými od v vedla cesta už v grafu $G - v$, a cesta z nějakého vrcholu x do vrcholu v se dostane prodloužením cesty spojující x s v' o hranu $\{v', v\}$, kde v' je (jediný) soused vrcholu v v grafu G. □

Toto tvrzení umožňuje postupně převádět daný strom na menší a menší stromy. Ukazuje, že graf G je strom právě když ho lze převést na jeden vrchol postupným odebíráním koncových vrcholů. Přitom v každém kroku můžeme odebrat libovolný koncový vrchol.

Následující věta shrnuje základní poznatky o stromech. Větu formulujeme jako ekvivalenci 5 tvrzení. Jedno z nich např. ukazuje, že strom se mezi souvislými grafy pozná podle počtu vrcholů a hran.

5.1.4 Věta (Charakterizace stromů). *Pro graf $G = (V, E)$ jsou následující podmínky ekvivalentní:*

(i) *G je strom.*

(ii) *(jednoznačnost cesty)*
Pro každé dva vrcholy $x, y \in V$ existuje právě jediná cesta z x do y.

(iii) *(minimální souvislost)*
Graf G je souvislý, a vynecháním libovolné hrany vznikne nesouvislý graf.

(iv) *(maximální graf bez kružnic)*
Graf G neobsahuje kružnici, a každý graf vzniklý z G přidáním hrany (tj. graf tvaru $G+e$, kde $e \in \binom{V}{2} \setminus E$) již kružnici obsahuje.

(v) *(Eulerův vzorec)*
G je souvislý a $|V| = |E| + 1$.

Toto je pozoruhodná věta, která vlastně popisuje pojem stromu pomocí čtyř dalších způsobů, které jsme se pokusili pojmenovat v záhlaví jednotlivých bodů. Tyto popisy jsou velmi různorodé a zakládají širokou použitelnost pojmu strom.

Důkaz. Důkaz je poměrně snadný, jde jen o to jej vhodně zorganizovat. Dokážeme, že každé z tvrzení (ii)–(v) je ekvivalentní (i) (tím je ovšem dokázána i ekvivalence všech tvrzení navzájem). Důkazy povedeme většinou indukcí podle počtu vrcholů grafu G (přitom pro jediný graf s jedním vrcholem všechna tvrzení platí), a budeme využívat postupné výstavby stromu odebíráním koncového vrcholu.

Nejdříve nahlédneme, že z (i) plyne (ii)–(v). Buď tedy G strom na aspoň 2 vrcholech, v jeho koncový vrchol, v' jediný soused vrcholu v, a nechť pro graf $G - v$ už platí (ii)–(v). Platnost (ii), (iii) a (v) pro G je pak téměř zřejmá (přenecháváme detailní rozmyšlení čtenáři). Co se týče (iv), nepotřebujeme ani indukci: poněvadž G je souvislý, mezi libovolnými dvěma vrcholy $x, y \in V(G)$ vede cesta, a pokud $\{x, y\} \notin E(G)$, potom hrana $\{x, y\}$ spolu se zmíněnou cestou tvoří kružnici.

Teď budeme dokazovat, že z každé z podmínek (ii)–(v) plyne (i). U (ii), (iii) již předpokládáme souvislost, a dále graf G splňující (ii)

nebo (iii) nemůže obsahovat kružnici, protože kružnice sama již (ii) ani (iii) nesplňuje. Tím už jsme dokázali ekvivalenci (i)–(iii).

Pro platnost implikace (iv)⇒(i) stačí ověřit, že G je souvislý. Na to se použije argument, jímž jsme dokazovali (i)⇒(iv), obrácený naruby: Jsou-li $x, y \in V(G)$ dva vrcholy, pak buď jsou přímo spojeny hranou, nebo graf $G+\{x, y\}$ obsahuje kružnici, a z té po odebrání hrany $\{x, y\}$ vznikne cesta z x do y v G.

Trochu těžší je důkaz poslední zbývající implikace (v)⇒(i). Postupuje se opět indukcí podle počtu vrcholů. Mějme tedy souvislý graf G na aspoň dvou vrcholech splňující $|V| = |E| + 1$. Potřebujeme ukázat, že v G existuje koncový vrchol, což se udělá počítáním stupňů.

Součet stupňů všech vrcholů je dvojnásobek počtu hran, tj. $2|V| - 2$. Kdyby všechny vrcholy měly stupně 2 a více, byl by součet stupňů aspoň $2|V|$, tudíž nějaký vrchol v má stupeň nejvýš 1. Stupeň 0 ale mít nemůže, poněvadž by G nebyl souvislý, takže má stupně právě 1. Tak jsme našli koncový vrchol. Graf $G' = G - v$ je opět souvislý a splňuje $|V(G')| = |E(G')| + 1$, je to tedy podle indukčního předpokladu strom, a tudíž i G je strom. □

Cvičení

1. Nakreslete všechny stromy na množině $\{1, 2, 3, 4\}$, a všechny navzájem neisomorfní stromy na 6 vrcholech.

2. Dokažte, že graf $G = (V, E)$, který nemá kružnice a pro nějž $|V| = |E| + 1$, je strom.

3. Dokažte, že graf na n vrcholech s c komponentami má aspoň $n - c$ hran.

4. Nechť strom G obsahuje vrchol stupně k. Ukažte, že G obsahuje alespoň k vrcholů stupně 1.

5.* Nechť T je strom s n vrcholy, $n \geq 2$. Pro kladné celé číslo i označme p_i počet vrcholů T, které mají stupeň i. Dokažte, že

$$p_1 - p_3 - 2p_4 - \ldots - (n-3)p_{n-1} = 2.$$

(To dává jiný důkaz lemmatu o koncovém vrcholu.)

6.* Dokažte, že následující dvě podmínky pro posloupnost $(d_1, \ldots, d_n)$ kladných přirozených čísel jsou navzájem ekvivalentní:

(i) Existuje strom T se skórem $(d_1, \ldots, d_n)$.

(ii) Platí $\sum_{i=1}^{n} d_i = 2n - 2$.

5.2 Isomorfismus stromů

Jak jsme se zmínili v části 4.1, není znám žádný rychlý algoritmus, který by pro dva dané grafy rozhodl, zda jsou isomorfní nebo ne. Pro některé speciální třídy grafů však rychlé algoritmy existují. Jedna z takových (jednoduchých) tříd jsou stromy. Ostatně velmi mnoho – asi dokonce většina – algoritmických úloh, které jsou pro obecné grafy obtížné, se dá pro stromy vyřešit poměrně snadno.

V tomto odstavci předvedeme rychlý a snadný postup, který pro dva stromy T a T' rozhodne, zda T a T' jsou isomorfní či nikoliv. Každému stromu T na n vrcholech přiřadíme posloupnost nul a jedniček délky $2n$, zvanou *kód* stromu T, a to tak, že isomorfním stromům se přiřadí týž kód, zatímco neisomorfní stromy budou mít různé kódy. Tím bude isomorfismus stromů převeden na prosté porovnání posloupností.

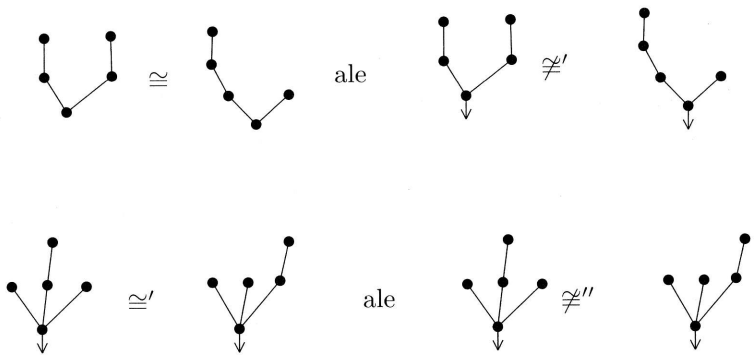
Následuje řada speciálních pojmů, každý se zvláštním názvem. To je běžné v hraničních oblastech teorie grafů a informatiky, kde mnoho pojmů vzešlo z praxe a kde je terminologie velmi různorodá.

Kořenový strom je dvojice (T, r), kde $r \in V(T)$ je jeden zvolený vrchol T, zvaný *kořen*. Je-li $\{x, y\} \in E(T)$ hrana, a leží-li x na (jediné) cestě z y do kořene, říkáme, že x je *otec* y a y je *syn* x.

Pěstovaný strom je nějaký kořenový strom (T, r), plus jeho pevně zvolené rovinné nakreslení. Přitom kořen se vyznačí šipkou směřující dolů.

Komu se tato definice nelíbí, nechť si uvědomí, že rovinné nakreslení je plně popsáno[1] pořadím synů každého vrcholu. Pěstovaný strom je tedy kořenový strom, kde pro každý vrchol v je dáno pořadí jeho synů. Můžeme proto pěstovaný strom zapisovat jako trojici (T, r, ν), kde ν je soubor lineárních uspořádání, jedno lineární uspořádání pro množinu synů každého vrcholu.

[1] Až na vhodnou spojitou deformaci roviny.



Obrázek 5.1: Isomorfismy stromů.

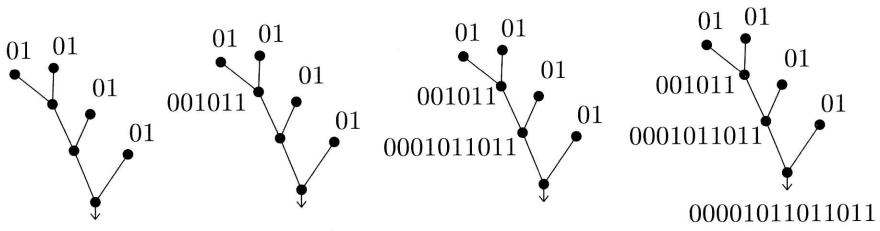
Tyto definice se zavádějí proto, že pro každý pojem se definuje isomorfismus trochu jinak. Připomeňme, že zobrazení $f : V(T) \to V(T')$ je isomorfismus stromů T a T', jestliže f je vzájemně jednoznačné zobrazení (tj. prosté a na) splňující $\{x, y\} \in E(T)$, právě když $\{f(x), f(y)\} \in E(T')$. Existenci takového isomorfismu zapisujeme $T \cong T'$. *Isomorfismus kořenových stromů* (T, r) a (T', r') je takový isomorfismus f stromů T a T', pro nějž navíc $f(r) = r'$. Značíme to $(T, r) \cong' (T', r')$. *Isomorfismus pěstovaných stromů* je takový isomorfismus příslušných kořenových stromů, který zachovává uspořádání synů každého vrcholu. Budeme jej značit $(T, r, \nu) \cong'' (T', r', \nu')$.

Definice $\cong$, $\cong'$ a $\cong''$ se postupně zesilují. To je nejlépe si uvědomit na malém případě na obr. 5.1.

Definice pěstovaného stromu (a jeho isomorfismus) je nejvíce omezující, a proto je kódování těchto stromů nejsnazší. Následující metoda přiřadí jistý kód každému vrcholu pěstovaného stromu; kód celého stromu bude pak totožný s kódem kořene.

K1. Koncovým vrcholům (různým od kořene) přiřadíme 01.

K2. Buď v nějaký vrchol, $v_1, \ldots, v_t$ jeho synové v pořadí zleva doprava. Má-li syn v_i kód A_i, potom vrcholu v přiřadíme kód $0A_1A_2 \ldots A_t1$.



Obrázek 5.2: Kódování pěstovaného stromu.

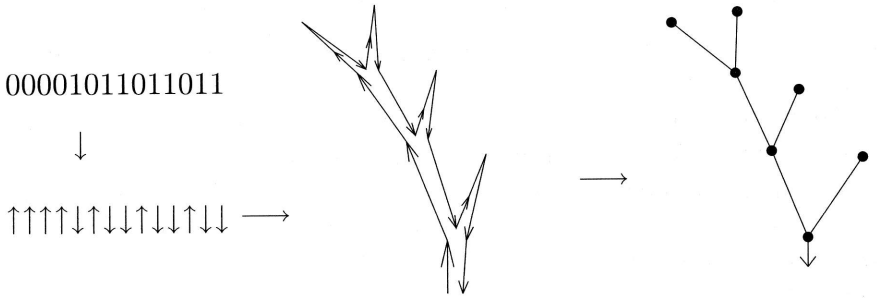
Proces postupného vytváření kódu je znázorněn na obr. 5.2. Zřejmě jsme isomorfním pěstovaným stromům přiřadili stejný kód, neboť jsme při konstrukci kódu použili jen vlastností, které se zachovávají isomorfismem pěstovaných stromů.

Ukážeme teď, jak ze znalosti kódu jednoznačně rekonstruovat výchozí pěstovaný strom (tím ukážeme, že neisomorfním pěstovaným stromům je přiřazen různý kód). Budeme postupovat indukcí podle délky kódové posloupnosti.

Nejkratší možný kód 01 odpovídá jedinému pěstovanému stromu s jedním vrcholem. V indukčním kroku nechť je dán kód k délky $2(n+1)$. Tento kód je tvaru $0\,A\,1$, přičemž $A = A_1 A_2 \ldots A_t$ je zřetězení kódů několika pěstovaných stromů. Část A_1 identifikujeme jako nejkratší počáteční úsek posloupnosti A, který obsahuje stejný počet nul a jedniček. Podobně A_2 je nejkratší následující úsek posloupnosti obsahující stejně nul a jedniček, atd. Podle indukčního předpokladu každému A_i odpovídá právě jediný pěstovaný strom. Pěstovaný strom kódovaný kódem k bude mít jeden kořen r, a k němu budou v pořadí $r_1, \ldots, r_t$ připojeny hranou kořeny stromů kódovaných A_1, A_2, ... Tedy kód určuje jednoznačně pěstovaný strom.

Dekódování metodou šipek. Ukážeme názorný – obrázkový – postup, jak pěstovaný strom z daného kódu zrekonstruovat.

V daném kódu nahradíme 0 šipkou "↑" a 1 šipkou "↓" a kreslíme graf podle pravidla, že šipka "↑" nikdy nevede po jiné šipce, zatímco šipka "↓" vždy sleduje šipku v protisměru. Celý postup je patrný z obrázku 5.3.



Obrázek 5.3: Dekódování metodou šipek.

(Přitom se nakreslí i kořenová šipka; jednobodový strom má kód 01.)

Věnovali jsme isomorfismu pěstovaných stromů pozornost proto, že isomorfismus jak kořenových tak obecných stromů se již snadno převede na tento případ.

Vyšetřeme nejprve kořenové stromy. Je-li (T, r) kořenový strom, budujeme jeho kód podobně jako pro pěstovaný strom, až na to, že pravidlo K2 nahradíme jeho následující modifikací:

K2′ Předpokládejme, že jsme již přiřadili kód $A(w)$ každému synu w vrcholu v. Označme syny $w_1, w_2, \ldots, w_t$ tak, aby platilo $A(w_1) \leq A(w_2) \leq \cdots \leq A(w_t)$. Vrchol v pak dostane kód $0A_1A_2 \ldots A_t1$, kde $A_i = A(w_i)$.

Zde $A \leq B$ značí, že posloupnost A je menší nebo rovna posloupnosti B v nějakém pevně zvoleném lineárním uspořádání všech konečných posloupností nul a jedniček. Pro určitost můžeme např. použít tzv. *lexikografického uspořádání*, viz též sekci 2.1. Dvě (různé) posloupnosti $A = (a_1, a_2, \ldots, a_n)$ a $B = (b_1, \ldots, b_m)$ přitom porovnáváme takto:

- Je-li A počátečním úsekem B, potom $A < B$. Je-li B počátečním úsekem A, potom $B < A$.
- Jinak, buď j nejmenší index takový, že $a_j \neq b_j$. Potom pokud $a_j < b_j$, klademe $A < B$, a pokud $a_j > b_j$, klademe $A > B$.

Podobně, jako jsme se o tom přesvědčili výše pro pěstované stromy, nahlédneme, že dva kořenové stromy jsou isomorfní právě když mají stejné kódy.

Obraťme pozornost ke kódování obecného stromu – stromu bez kořene. Úlohu bychom si zjednodušili, kdybychom nalezli vrchol, který by měl úlohu kořene. Přitom takto nalezený vrchol by se měl zachovávat isomorfismem. Je důležitou skutečností, že v případě stromů lze takový význačný vrchol vždy najít. Příslušné definice mohou být užitečné i jinde, a proto je formulujme poněkud obecněji pro grafy.

Pro vrchol v grafu G označme symbolem $\mathrm{ex}_G(v)$ maximální vzdálenost vrcholu v od jiného vrcholu grafu G. Číslo $\mathrm{ex}_G(v)$ se nazývá *výstřednost* (cizím slovem *excentricita*) vrcholu v grafu G. Vrcholy s velkou výstředností si můžeme představovat "na okraji" grafu G.

Označme nyní $C(G)$ množinu všech vrcholů grafu G, jejichž výstřednost nabývá minimální hodnoty. Množina $C(G)$ se nazývá *střed*[2] (*centrum*) grafu G. Příklad kružnic (a dalších grafů) ukazuje, že střed grafu může splývat s množinou všech vrcholů. Pro stromy však platí:

5.2.1 Tvrzení. *Pro každý strom T má $C(T)$ nejvýše dva vrcholy. Je-li $C(T)$ tvořeno dvěma vrcholy x a y, potom $\{x, y\}$ tvoří hranu.*

Důkaz. Popíšeme postup, jak střed stromu najít. Nechť $T = (V, E)$ je daný strom. Jestliže T má nejvýše dva vrcholy, potom střed T splývá s množinou jeho vrcholů a tvrzení platí. V opačném případě označme $T' = (V', E')$ strom, který vznikne odstraněním všech koncových vrcholů stromu T. Explicitně

$$V' = V \setminus \{x;\ \deg_T(x) = 1\},$$
$$E' = E \setminus \{\{x, y\} \in E;\ \deg_T(x) = 1 \text{ nebo } \deg_T(y) = 1\}.$$

Máme $V(T') \neq \emptyset$. Dále, pro každý vrchol v jsou všechny vrcholy od něj nejvzdálenější nutně koncové, a tím pádem platí pro každý $v \in V'$ vztah

$$\mathrm{ex}_T(v) = \mathrm{ex}_{T'}(v) + 1.$$

[2] Výstřednost vrcholů středu se jmenuje *poloměr* grafu G.

Speciálně z toho dostaneme $C(T') = C(T)$. V případě, že T' má alespoň 3 vrcholy, opakujeme uvedenou konstrukci, v opačném případě jsme našli střed stromu T. □

Popišme nyní vytváření kódu stromu T.

- Jestliže střed stromu T tvoří jediný vrchol, v, potom mu přiřadíme kód jako kořenovému stromu (T, v).

- Jestliže střed stromu T je tvořen hranou $e = \{x_1, x_2\}$, potom uvažme graf $T - e$. Tento graf má právě dvě komponenty T_1 a T_2 (kde $x_i \in V(T_i)$). Označme kód kořenového stromu (T_1, x_1) písmenem A, a kód kořenového stromu (T_2, x_2) písmenem B. Jestliže v lexikografickém uspořádání platí $A \leq B$, kódujeme strom T kódem kořenového stromu (T, x_1), a pro $A \geq B$ kódem kořenového stromu (T, x_2).

Tím je procedura kódování ukončena.

Dekódování se provádí ve všech případech stejně jako pro pěstované stromy. Poněvadž isomorfismus zřejmě převádí střed na střed, a protože jsme již nahlédli, že kódování funguje pro zakořeněné stromy, je už snadno patrné, že dva stromy mají stejný kód právě když jsou isomorfní.

Algoritmy pro isomorfismus stromů uvedené v této části lze implementovat tak, že počet elementárních kroků je omezen lineární funkcí počtu vrcholů vstupních stromů.

Jsou známy i další třídy grafů, pro něž lze problém isomorfismu řešit. Snad nejvýznamnějším takovým příkladem je třída rovinných grafů; zde jsou ale algoritmy na isomorfismus již značně složité.

Cvičení

1. (a) Najděte nějaký *asymetrický* strom s aspoň dvěma vrcholy (tj. strom jen s jediným automorfismem, viz cvičení 4.1.4).

   (b) Jaký je nejmenší možný počet vrcholů asymetrického stromu (s nejméně 2 vrcholy)?

2. Zakořeněný strom se nazývá *binární*, jestliže každý vrchol kromě koncových má právě dva syny.

   (a) Nakreslete všechny neisomorfní binární stromy s ≤ 9 vrcholy.

   (b) Popište, jak mohou vypadat kódy binárních stromů.

3. Dokažte podrobně, že isomorfní stromy (nezakořeněné) dostanou uvedenou metodou stejný kód, a neisomorfní různé kódy.

4.* Buďte $A_1, A_2, \ldots, A_t$ posloupnosti nul a jedniček (mohou být různě dlouhé). Označme součet jejich délek n. Navrhněte algoritmus, který tyto posloupnosti lexikograficky setřídí v $O(n)$ krocích (přičemž jeden krok smí manipulovat jen s jediným členem některého A_i, nikoliv s celou posloupností 0 a 1 najednou).

5. Dokažte, že existuje nejvýš 4^n navzájem neisomorfních stromů na n vrcholech.

6. Buď $T = (V, E)$ strom, v jeho vrchol. Označme $\tau(v)$ číslo $\max(|V(T_1)|, |V(T_2)|, \ldots, |V(T_k)|)$, kde $T_1, \ldots, T_k$ jsou všechny komponenty grafu $T - v$. *Centroid* stromu T je množina všech vrcholů $v \in V$ s minimální hodnotou $\tau(v)$.

   (a)* Dokažte, že centroid každého stromu je buď jeden vrchol, nebo dva vrcholy spojené hranou.

   (b) Musí centroid vždy splývat se středem stromu?

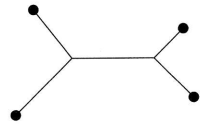
   (c) Dokažte, že je-li v vrchol centroidu, potom $\tau(v) \leq \frac{1}{2}|V(T)|$.

5.3 Problém minimální kostry

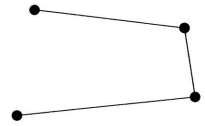
Představme si mapu jižní Moravy. Máme na ní vyznačeno 30–40 měst a vesniček. Naším úkolem bude tato města navzájem propojit (třeba elektrickým vedením) tak, aby délka spojení nebyla příliš velká. Řekněme dokonce, že bychom chtěli, aby celková délka propojení byla co nejkratší.

> Komu tento příklad připadá příliš umělý a dnes už neaktuální (což je pravda), ať si představí návrh letecké sítě nějaké společnosti. Takové úlohy se řeší dosud.

Navíc se rozhodneme, že naše síť se nebude větvit nikde mimo spojované obce, tj. nebudou v ní situace typu



takže tato 4 místa by se musela propojit takto[3]:



Tím dostáváme zadání důležité úlohy, známé pod názvem *problém minimální kostry*. Tento oddíl je věnován jejímu řešení.

Úloha vyžaduje malého obohacení pojmu graf: Budeme uvažovat grafy $G = (V, E)$ spolu s *ohodnocenými hranami*. Tím míníme, že pro každou hranu $e \in E$ je dáno číslo $w(e)$, které nazýváme *váha* hrany e – takovou situaci jsme již uvažovali v části 4.3. (Váha je zpravidla kladné číslo.) Graf spolu s ohodnocením w, kde $w : E \to \mathbf{R}$, se nazývá *síť*.

Formulujme tedy problém propojení v grafové formě:

> *Pro souvislý graf $G = (V, E)$ s nezáporným ohodnocením hran w nalezněte souvislý podgraf (V, E') takový, že výraz*
>
> $$w(E') = \sum_{e \in E'} w(e) \tag{5.1}$$
>
> *nabývá minimální hodnoty.*

Je snadno vidět, že mezi řešeními této úlohy je vždy nějaký strom (je-li ohodnocení všech hran kladné, může být dokonce řešením *jenom* strom). Například, jestliže ohodnocení w splňuje $w(e) = 1$ pro každou hranu e, úlohu řeší libovolný podgraf, jenž obsahuje všechny vrcholy a jenž je strom (a tedy má $|V| - 1$ hran). Pro takové podgrafy se zavádí zvláštní název:

[3] Vynecháme-li právě zavedené omezení, dostaneme problém *minimálního Steinerova stromu*. To je zcela jiná úloha, pro niž nejspíš neexistuje efektivní algoritmus, a která se v praxi zpravidla řeší pouze přibližně.

5.3.1 Definice. *Nechť $G = (V, E)$ je graf. Libovolný strom tvaru (V, E'), kde $E' \subseteq E$, nazveme* kostra[4] grafu G.

Je zřejmé, že kostra může existovat pouze tehdy, je-li graf G souvislý. Je snadné ukázat, že každý souvislý graf má kostru, a vyplyne to i z našich dalších úvah.

Uvažovanou úlohu můžeme určitěji formulovat takto:

5.3.2 Úloha (Problém minimální kostry). *Pro souvislý graf $G = (V, E)$ s nezáporným ohodnocením hran w nalezněte kostru $T = (V, E')$ grafu G s nejmenší možnou hodnotou $w(E')$.*

Daný graf může mít velmi mnoho koster (viz kapitolu 8) a nalézt tu nejlepší z nich se může zdát obtížné. Není tomu tak: Tento problém je algoritmicky velmi dobře zvládnutý. V tomto oddílu vysvětlíme jeden oblíbený a jednoduchý postup.

5.3.3 Algoritmus (Kruskalův čili „hladový" algoritmus).
Je dán souvislý graf $G = (V, E)$ s n vrcholy, m hranami a s ohodnocením w. Očíslujme hrany $e_1, e_2, \ldots, e_m$ tak, aby

$$w(e_1) \leq w(e_2) \leq \ldots \leq w(e_m).$$

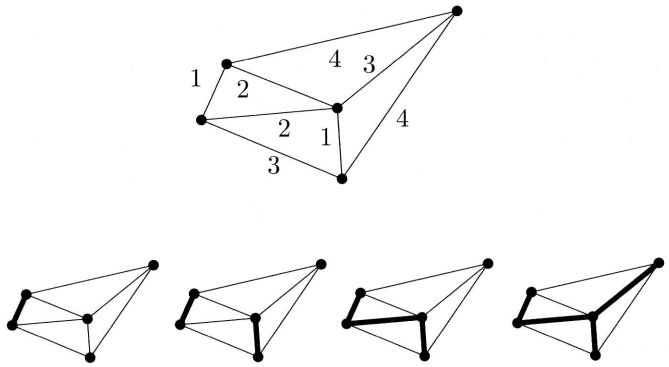
(Tento krok tedy vyžaduje setřídění vah.)

Nyní budeme postupně konstruovat množiny hran $E_0, E_1, E_2, \ldots, E_m \subseteq E$. Položme $E_0 = \emptyset$. Byla-li již nalezena množina E_{i-1}, spočítáme množinu E_i následovně:

$$E_i = \begin{cases} E_{i-1} \cup \{e_i\} & \text{neobsahuje-li graf } (V, E_{i-1} \cup \{e_i\}) \text{ kružnici} \\ E_{i-1} & \text{jinak.} \end{cases}$$

Algoritmus se zastaví po m-tém kroku. Nechť T značí graf (V, E_m).

5.3.4 Příklad. *Aplikujme hladový algoritmus na graf na obr. 5.4 s naznačeným ohodnocením hran. Ohodnocení tvoří posloupnost* 1, 1, 2, 2, 3, 3, 4, 4. *Jeden možný průběh algoritmu je na obrázku vyznačen.*



Obrázek 5.4: Hledání minimální kostry hladovým algoritmem.

5.3.5 Tvrzení (Správnost Kruskalova algoritmu).
Kruskalův algoritmus řeší problém minimální kostry. To znamená, že vždy vydá minimální kostru G vzhledem k ohodnocení w (přesněji, pokud má G více minimálních koster, T bude některá z nich).

Důkaz. Algoritmus určitě pokaždé skončí. Nejdříve ověříme, že *výsledný graf T je kostra grafu G*. Podle pravidla vytváření množin E_i neobsahuje graf T kružnici. Předpokládejme pro spor, že je je nesouvislý. Zvolme vrcholy x a y v různých komponentách grafu T. Označme C komponentu T obsahující vrchol x, a uvažme nějakou cestu $(x = x_0, e_1, x_1, e_2, \ldots, x_\ell = y)$ z x do y v grafu G. Nechť i je poslední index, pro nějž je vrchol x_i obsažen v komponentě C. Zřejmě $i < \ell$, a tedy $x_{i+1} \notin C$. Hrana $e = \{x_i, x_{i+1}\}$ tudíž nepatří do grafu T, a musela proto někdy v průběhu algoritmu tvořit spolu s již vybranými hranami kružnici. Proto i graf $T + e$ obsahuje kružnici, to ale není možné, protože e spojuje různé komponenty grafu T. To je spor ukazující, že T je opravdu kostra.

[4] Tento morbidní název je zaveden v češtině – anglicky se kostře grafu říká optimističtěji *spanning tree*.

Teď se dáme do dokazování, že T *je minimální kostra.* Uvažme libovolnou jinou kostru $\check{T}$; potřebujeme dokázat, že $w(E(T)) \leq w(E(\check{T}))$. Přeznačme hrany kostry T jako $e'_1, e'_2, \ldots, e'_{n-1}$ tak, že $w(e'_1) \leq w(e'_2) \leq \cdots \leq w(e'_{n-1})$ (každá hrana kostry T má teď dvě označení, čárkované a nečárkované). Podobně nechť $\check{e}_1, \ldots, \check{e}_{n-1}$ jsou hrany kostry $\check{T}$, uspořádané taky vzestupně podle vah.

Dokážeme, že pro $i = 1, \ldots, n-1$ platí dokonce

$$w(e'_i) \leq w(\check{e}_i). \tag{5.2}$$

Odtud samozřejmě plyne, že T je minimální kostra.

Předpokládejme tedy pro spor, že (5.2) neplatí a zvolme nejmenší i takové, že $w(e'_i) > w(\check{e}_i)$. Zřejmě $i > 1$. Uvažme množiny

$$E' = \{e'_1, \ldots, e'_{i-1}\},$$
$$\check{E} = \{\check{e}_1, \ldots, \check{e}_i\}.$$

Grafy (V, E') a $(V, \check{E})$ neobsahují kružnice a navíc $|E'| = i-1$, $|\check{E}| = i$.

K hledanému sporu stačí ukázat, že existuje hrana $e \in \check{E}$, pro niž graf $(V, E' \cup \{e\})$ nemá kružnici. Potom totiž $w(e) \leq w(\check{e}_i) < w(e'_i)$ a v tom okamžiku, kdy se v algoritmu rozhodovalo o hraně e, jsme učinili chybu, protože nebylo důvodu ji zamítnout; např. jsme ji měli vybrat místo hrany e'_i.

Stačí tedy ukázat toto: *Jsou-li* $E', \check{E} \subseteq \binom{V}{2}$ *dvě množiny hran, přičemž* $(V, \check{E})$ *neobsahuje kružnici a* $|E'| < |\check{E}|$, *potom nějaká hrana* $e \in \check{E} \setminus E'$ *spojuje vrcholy dvou různých komponent grafu* (V, E'). Nechť $V_1, \ldots, V_s$ je rozklad množiny V na komponenty grafu (V, E'). Platí $\left|E' \cap \binom{V_j}{2}\right| \geq |V_j| - 1$, a proto $|E'| \geq n - s$. Na druhé straně, ježto $\check{E}$ neobsahuje kružnice, máme $\left|\check{E} \cap \binom{V_j}{2}\right| \leq |V_j| - 1$, tudíž nanejvýš $n-s$ hran z $\check{E}$ je obsaženo v nějaké z komponent V_j. Protože ale $|\check{E}| > |E'|$, některá hrana $e \in \check{E}$ jde mezi dvěma různými komponentami. □

Pozor, právě dokončený důkaz je velmi snadné poplést (jak vědí oba autoři z vlastní zkušenosti)!

Složitost algoritmu. Tím jsme ukázali, že hladový algoritmus skutečně vždycky spočítá to, co má, tj. minimální kostru grafu G. Kdybychom ale doopravdy potřebovali nacházet minimální kostry nějakých (velkých) grafů, máme zvolit zrovna tento algoritmus a trávit čas tím, že ho budeme programovat, případně utratit své peníze za program již hotový?

Odpověď není jednoduchá a algoritmy se porovnávají na základě různých (a mnohdy navzájem protichůdných) kritérií. Je např. vhodné si všímat přehlednosti algoritmu (přehlednost vede k lepšímu pochopení a méně chybám), jeho robustnosti (jak se průběh řešení změní při malé změně dat), jeho paměťové náročnosti. Snad nejrozpracovanější mírou je však *časová složitost* algoritmu, to znamená počet operací (jako například sčítání, násobení, porovnání dvou čísel, atd.), které algoritmus potřebuje na vyřešení dané úlohy. Zpravidla se uvažuje časová složitost *v nejhorším případě*, tj. počet operací potřebných k vyřešení nejhorší možné (nejnaschválnější) úlohy při dané velikosti vstupu. Velikost vstupu by se v našem případě – počítání kostry – mohla měřit jako počet vrcholů plus počet hran grafu G. Místo „časová složitost v nejhorším případě" budeme v dalším říkat krátce „složitost", poněvadž o jiných typech složitosti hovořit nebudeme.

Složitost algoritmu lze jen velmi zřídka určit přesně. Aby byla vůbec naděje to udělat, museli bychom v první řadě přesně stanovit, co jsou povolené elementární operace, tj. v podstatě se vázat na jeden konkrétní počítač, a potom také algoritmus popsat do nejmenších detailů, včetně různých rutinních operací, tj. vycházet z konkrétního naprogramování. I kdybychom obě tyto věci udělali, určení přesné složitosti je velmi pracné i pro jednoduché algoritmy. Z těchto důvodů se v teoretické analýze algoritmů složitost odhaduje pouze asymptoticky, třeba že nějaký algoritmus má složitost $O(n^{3/2})$, jiný $O(n \log n)$, a podobně (n je přitom míra velikosti vstupu).

Při skutečném posuzování algoritmů je vhodné (a někdy nutné) takovou asymptotickou analýzu doplnit testováním algoritmu pro konkrétní data na konkrétním počítači. Dá-li totiž např. asymptotická analýza pro jeden algoritmus složitost $O(n^2)$ a pro druhý $O(n \log^4 n)$, vypadá druhý podle toho jasně lepší (funkce $n \log^4 n$ roste mnohem pomaleji než n^2). Kdyby však přesná složitost prvního algoritmu byla třeba $n^2 - 5n$ a druhého $20n(\log_2 n)^4$, projeví se převaha druhého algoritmu až od zhruba $n = 5 \times 10^6$, a taková převaha je z praktického hlediska dosti iluzorní.

Pokusme se nějak odhadnout asymptotickou složitost Kruskalova algoritmu. První část algoritmu spočívá v třídění m vah. To je velmi dobře

prostudovaná úloha, o níž se zpravidla podrobně pojednává v základních kursech programování a algoritmů. Ví se, že m reálných čísel se dá setřídit pomocí $O(m \log m)$ operací, a pokud bychom předpokládali, že váhy jsou třeba celá čísla mezi 1 a m, pak třídění je možné dokonce v čase $O(m)$. V dalším se budeme zabývat jenom zbývající částí algoritmu, kdy již máme hrany seřazeny podle vah.

Algoritmus jsme ovšem popsali na „vysoké úrovni", čímž se neníní společenská prestiž, ale to, že jsme při popisu užívali např. test, zda daná množina hran obsahuje kružnici, což ani při liberálním pojetí nelze považovat za elementární operaci. Složitost algoritmu tedy bude záviset na tom, jak efektivně umíme takovou komplikovanou operaci realizovat operacemi elementárními.

U Kruskalova algoritmu je vidět, že nemusíme uchovávat všechny množiny E_i, a všechny tedy mohou být reprezentovány jednou proměnnou, např. seznamem hran, která postupně nabývá hodnot $E_0, E_1, \ldots$. Jediná složitější otázka je, jak efektivně testovat, jestli přidání nové hrany e_i k již vybraným hranám vytvoří kružnici. Kružnice zřejmě vznikne, právě když koncové vrcholy hrany e_i náleží téže komponentě grafu (V, E_{i-1}). Takže potřebujeme řešit následující úlohu:

5.3.6 Úloha (Udržování ekvivalence).[5] *Uvažujeme množinu vrcholů $V = \{1, 2, \ldots, n\}$. Na počátku je rozdělena do jednoprvkových tříd ekvivalence, tj. žádné dva vrcholy nejsou ekvivalentní. Navrhněte algoritmus, který uchovává ve vhodné datové struktuře ekvivalenci na V (neboli rozdělení V do tříd) tak, aby mohl efektivně vykonávat operace následujících dvou typů:*

(i) (Sjednocení tříd – UNION) Učinit dané dva neekvivalentní vrcholy $i, j \in V$ ekvivalentními, tj. nahradit třídy obsahující i a j jejich sjednocením.

(ii) (Testování ekvivalence – FIND) Pro dané dva vrcholy $i, j \in V$ rozhodnout, zda jsou momentálně ekvivalentní.

Přitom každá další operace je algoritmu zadána až poté, co vykonal operaci předchozí.

Kruskalův algoritmus potřebuje nejvýš $n - 1$ operací sjednocení tříd a nejvýš m operací testování ekvivalence.

Jednoduché řešení úlohy 5.3.6 je následující: Vrcholům z množiny V přiřadíme na počátku různé značky, třeba $1, 2, \ldots, n$. Značky nyní i v budoucnosti budou splňovat podmínku, že dva vrcholy budou mít tutéž značku, právě když jsou ekvivalentní. Testování ekvivalence je pak triviální porovnání značek. Při sjednocení dvou tříd je třeba přeznačit vrcholy jedné z nich. Pokud prvky každé třídy zároveň uchováváme v seznamu, je čas potřebný na takovou operaci úměrný velikosti přeznačované třídy.

[5] V literatuře čtenář tuto úlohu najde nejspíš pod jménem *UNION-FIND problem.*

Při hrubém odhadu můžeme říci, že každá třída má vždy nejvýš n prvků, tedy jedna operace sjednocení tříd nezabere nikdy více než $O(n)$. Pro $n - 1$ operací sjednocení a m operací testování ekvivalence potom vychází odhad $O(n^2 + m)$.

Jedno nenápadné vylepšení je, že uchováváme také počty prvků tříd a přeznačujeme vždycky menší třídu. Pro takový algoritmus se dá ukázat celkový odhad $O(n \log n + m)$, viz cvičení 9.

Nejlepší známé řešení úlohy 5.3.6 potřebuje na m testů a $n - 1$ sjednocení čas nejvýš $O(n\alpha(n) + m)$ (viz např. [1]), kde $\alpha(n)$ je jistá funkce. Definici této funkce zde neuvedeme; poznamenejme jen, že $\alpha(n)$ roste sice do nekonečna pro $n \to \infty$, ale nepředstavitelně pomalu, mnohem pomaleji než např. funkce jako $\log \log n$, $\log \log \log n$, atd. Pro praktické použití je však výše naznačené řešení (s přeznačováním menší třídy) zcela dostačující.

Hladové algoritmy obecně. Kruskalův algoritmus je prototypem tzv. *hladového algoritmu*: vzhledem k platným omezením (zde „neobsahovat kružnici") vybereme v každém okamžiku tu nejlacinější hranu. Hladový algoritmus se tedy snaží vždycky „urvat co se dá", a přitom nehledí do budoucnosti.

Pro četné problémy může taková krátkozraká strategie úplně selhat. To není příliš překvapivé: Např. hladový algoritmus aplikován na šachovou hru by odpovídal strategii, kdy by hráč pokud možno bral v každém okamžiku, a to tu nejcennější figuru. A také by snadno při dodržování tak naivního postupu prohrál.

V této souvislosti je spíš překvapivé, že pro problém minimální kostry najde hladový algoritmus optimální řešení. I pro mnoho jiných úloh je hladová strategie užitečná (zejména nevíme-li nic lepšího); mnohdy dává aspoň dobré přibližné řešení. Úlohy, pro něž hladový algoritmus vždy najde optimální řešení, se studují v tzv. *teorii matroidů.*

Poznámka historická. Příklad z jižní Moravy, kterým jsme uvedli tento oddíl, si autoři nevymysleli. Ve skutečnosti to je první případ úspěšného řešení problému minimální kostry, které našel v roce 1928 Otakar

Borůvka. Značně tak předběhl dobu; mimo Československo na jeho výzkumy navázal až v roce 1956 M. Kruskal. Téma se v té době stalo velmi aktuální v rámci celkového zvýšeného zájmu o algoritmické a výpočetní metody. Od té doby jsou problému minimální kostry věnovány stovky prací. Borůvkův postup byl složitě napsán (v duchu tehdejšího stylu psaní matematických článků), jeho algoritmus není však složitý a je odlišný od Kruskalova hladového algoritmu. Výstižný popis událostí provázejících Borůvkův objev i celkové ovzduší předválečného brněnského akademického života čtenář najde v práci [5].

Cvičení

1. (a) Nechť úplný graf K_n na množině vrcholů $\{1, 2, \ldots, n\}$ má hranu $\{i, j\}$ ohodnocenou číslem $\max(i, j)$. Nalezněte minimální kostru a spočtěte její váhu.

   (b) Řešte podobný problém s ohodnocením $i + j$.

2. Podobně jako jsme definovali problém minimální kostry, definujte *problém maximální kostry*. Formulujte hladový algoritmus pro tento problém a ukažte, že najde optimální řešení.

3. Dokažte, že je-li w prosté zobrazení, je minimální kostra souvislého grafu G s ohodnocením w určena jednoznačně.

4. Dokažte, že je-li (V, E') kostra grafu $G = (V, E)$, potom graf $(V, E' \cup \{e\})$, kde e je libovolná hrana z $E \setminus E'$, obsahuje právě jedinou kružnici.

5. Dokažte, že je-li (V, E') kostra grafu $G = (V, E)$, potom pro každé $e \in E \setminus E'$ existuje $e' \in E'$ tak, že $\big(V, (E' \setminus \{e'\}) \cup \{e\}\big)$ je opět kostra grafu G. (Tato vlastnost, tzv. výměnný axiom, je klíčová pro správnost hladového algoritmu.)

6. Nechť w a w' jsou dvě ohodnocení hran grafu $G = (V, E)$. Předpokládejme $w(e_1) < w(e_2)$ právě když $w'(e_1) < w'(e_2)$, pro libovolné hrany $e_1, e_2 \in E$. Dokažte, že (V, E') je minimální kostra G pro ohodnocení w, právě když (V, E') je minimální kostra G pro ohodnocení w'. (Tedy: řešení problému minimální kostry závisí jen na uspořádání vah na hranách grafu G.)

7. Uvažme n-bodovou množinu V v rovině. Definujme ohodnocení hran úplného grafu na V: ohodnocením hrany $\{x, y\}$ bude vzdálenost bodů x a y.

   (a)* Ukažte, že maximální stupeň vrcholu v libovolné minimální kostře je nejvýš 6.

   (b)* Ukažte, že existuje minimální kostra, jejíž hrany se navzájem nekříží.

8.* Nechť V je množina n bodů ve čtverci o straně 1. Dokažte, že existuje kostra na V s celkovou délkou hran nejvýš $10\sqrt{n}$ (uvažujeme všechny kostry úplného grafu na V, a váha hrany $\{x, y\}$ je euklidovská vzdálenost bodů x a y). Konstantu 10 lze podstatně zlepšit, ale nejlepší možná hodnota není známa (jaký nejlepší odhad se podaří najít vám?).

9. Dokažte, že řešíme-li úlohu 5.3.6 popsaným algoritmem (přeznačujícím vždy menší ze sjednocovaných tříd), je celková složitost $n - 1$ operací sjednocení nejvýš $O(n \log n)$.

10. Buď $G = (V, E)$ graf, w nezáporné ohodnocení jeho hran.

    (a)* Každá množina $E' \subseteq E$ navzájem disjunktních hran se nazývá *párování* v grafu G. Označme $\nu_w(G)$ maximální možnou hodnotu $w(E')$ pro párování $E' \subseteq E$. Hladový algoritmus pro maximální párování funguje podobně jako algoritmus Kruskalův pro maximální kostru, jenže zamítá hrany protínající některou dříve vybranou hranu. Ukažte, že takový algoritmus vždy najde párování váhy nejméně $\nu_w(G)/2$.

    (b) Ukažte, že odhad v (a) nelze zlepšit, tj. že pro libovolné $\alpha > \frac{1}{2}$ existuje zadání, pro nějž hladový algoritmus najde párování váhy menší než $\alpha\, \nu_w(G)$.

11. Množinu $C \subseteq E$ v grafu $G = (V, E)$ nazveme *hranovým pokrytím*, pokud každý vrchol $v \in V$ je obsažen aspoň v jedné hraně $e \in C$. Hledejme malé hranové pokrytí hladovým algoritmem (dokud existuje hrana, pokrývající dva dosud nepokryté vrcholy, vybereme libovolnou takovou, jinak libovolnou hranu pokrývající jeden dosud nepokrytý vrchol). Ukažte, že velikost takto nalezeného hranového pokrytí je vždy

    (a) nejvýše dvojnásobek velikosti optimálního pokrytí,

    (b)** dokonce nejvýš $\frac{3}{2}$ velikosti optimálního pokrytí.

12.** Množinu $D \subseteq V$ v grafu $G = (V, E)$ nazveme *dominující*, pokud $\bigcup_{e \in E;\, e \cap D \neq \emptyset} e = V$. Hledejme malou dominující množinu hladovým algoritmem (vždy vybereme vrchol, který je spojen s největším počtem dosud nepokrytých vrcholů). Ukažte, že pro každé číslo C existuje graf takový, že $|D_H| \geq C|D_M|$, kde D_H je dominující množina

vybraná hladovým algoritmem a D_M je nejmenší dominující množina.

5.4 Jarníkův algoritmus a Borůvkův algoritmus

Název „Jarníkův algoritmus“, ani v poangličtěné podobě, anglickému nebo americkému čtenáři nejspíš mnoho neřekne, a to i když příslušný algoritmus ve skutečnosti zná – zná ho totiž pod jménem *Primův algoritmus*. Protože však Jarník bezprostředně reagoval na průkopnickou Borůvkovu práci již v roce 1930 (Primova práce je z roku 1957) a protože jeho postup je elegantní a precizní (jako veškerá Jarníkova matematická produkce), domníváme se, že je na čase vrátit algoritmu jeho pravé jméno.

5.4.1 Algoritmus (Jarníkův algoritmus). Je dán souvislý graf $G = (V, E)$ s n vrcholy, m hranami a nezáporným ohodnocením hran w.

Budeme postupně vytvářet množiny vrcholů V_0, V_1,... $\subseteq V$ a množiny hran $E_0, E_1, \ldots \subseteq E$, přičemž $E_0 = \emptyset$ a $V_0 = \{v\}$, kde v je libovolně zvolený vrchol.

Jsou-li již V_{i-1} a E_{i-1} vytvořeny, uvážíme množinu F_i všech hran $\{x_i, y_i\} \in E(G)$, kde $x_i \in V_{i-1}$ a $y_i \in V \setminus V_{i-1}$. Pokud $F_i = \emptyset$, algoritmus končí (grafem $(V_t, E_t) = T$). Jinak zvolíme hranu $e_i \in F_i$, jejíž váha je nejmenší mezi všemi hranami F_i, a položíme $V_i = V_{i-1} \cup \{y_i\}$, $E_i = E_{i-1} \cup \{e_i\}$.

5.4.2 Tvrzení (Správnost Jarníkova algoritmu). *Jarníkův algoritmus nalezne minimální kostru pro každý souvislý graf G s libovolným ohodnocením w.*

Důkaz. Graf T vypočtený Jarníkovým algoritmem je strom, protože je souvislý a má správný počet vrcholů a hran. Má-li n vrcholů, potom je to kostra.

Předpokládejme opak, nechť $V(T) \neq V$. Poněvadž G je souvislý, existuje aspoň jedna hrana spojující nějaký vrchol z množiny $V(T)$ s nějakým vrcholem mimo $V(T)$. Tudíž množina F_i v posledním kroku algoritmu nemohla být prázdná a algoritmus nemohl skončit. Tento

spor dokazuje, že algoritmus najde nějakou kostru grafu G, a zbývá ověřit její minimalitu.

Označme E' množinu hran kostry T, a nechť pořadí, v němž byly hrany E' algoritmem vybrány, je $e_1, e_2, \ldots, e_{n-1}$. Předpokládejme pro spor, že T není minimální kostra.

Buď T' nějaká minimální kostra. Symbolem $k(T')$ označme index k takový, že hrany $e_1, e_2, \ldots, e_k$ náležejí do $E(T')$, ale e_{k+1} už nikoliv. Vyberme mezi všemi minimálními kostrami takovou, pro niž je tento index k maximální, a označme ji $\check{T} = (V, \check{E})$.

Nyní uvažme ten okamžik algoritmu, kdy byla e_{k+1} vybrána do T. Nechť $T_k = (V_k, E_k)$ je strom tvořený hranami $e_1, \ldots, e_k$. Potom e_{k+1} je tvaru $\{x, y\}$, kde $x \in V(T_k)$ a $y \notin V(T_k)$. Podívejme se na graf $\check{T} + e_{k+1}$. Ten obsahuje nějakou kružnici C (neboť je souvislý a má více než $n-1$ hran), a C musí nutně obsahovat hranu e_{k+1} (viz též cvičení 5.3.4).

Kružnice C sestává z hrany $e_{k+1} = \{x, y\}$ a z cesty P z vrcholu x do y v kostře $\check{T}$. Alespoň jedna hrana cesty P má jeden vrchol v množině V_k a druhý vrchol mimo V_k. Označme e některou takovou hranu. Zřejmě $e \neq e_{k+1}$, a dále víme $e \in \check{E}$, $e_{k+1} \notin \check{E}$, viz obr. 5.5. Jak hrana e, tak hrana e_{k+1} spojují vrchol z V_k s vrcholem mimo V_k, a z pravidla výběru hran v algoritmu tedy plyne $w(e_{k+1}) \leq w(e)$.

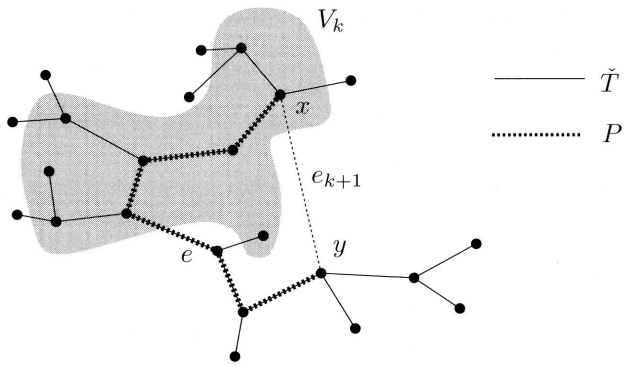
Uvažme nyní graf $T' = (\check{T} + e_{k+1}) - e$. Tento graf má $n-1$ hran, a je snadné ověřit, že je souvislý; je to tedy kostra. Přitom

$$w(E(T')) = w(\check{E}) - w(e) + w(e_{k+1}) \leq w(\check{E}),$$

čili T' je taky minimální kostra, pro niž ale $k(T') > k(\check{T})$. Vzniklý spor s volbou $\check{T}$ dokazuje tvrzení 5.4.2. □

Poznámka. Detaily právě probraného Jarníkova algoritmu se dají navrhnout tak, že pracuje v čase $O(n+m)$.

Borůvkův algoritmus. Na závěr zmiňme ještě algoritmus, který byl historicky prvním postupem pro řešení problému minimální kostry. Jak už to bývá, tento postup je složitější – jak Kruskalův, tak (zvláště) Jarníkův algoritmus jsou koncepčně jednodušší. V poslední době se však právě



Obrázek 5.5: K důkazu správnosti Jarníkova algoritmu.

Borůvkův algoritmus stal koncepčním základem nejrychlejšího známého algoritmu pro problém minimální kostry [17]. Tento algoritmus najde minimální kostru v čase $O(n+m)$, kde n je počet vrcholů a m počet hran sítě. Je poměrně složitý a používá ještě řadu dalších myšlenek (do nichž se zde ovšem pouštět nebudeme).

5.4.3 Algoritmus (Borůvkův algoritmus). Je dán graf $G = (V, E)$ s ohodnocením hran w. Předpokládáme navíc, že *různým hranám jsou přiřazena různá čísla*, tj. že funkce w je prostá. (Tento předpoklad není příliš omezující; každé ohodnocení můžeme libovolně malými změnami některých vah převést na prosté ohodnocení, a váha minimální kostry se přitom změní libovolně málo.)

Algoritmus postupně vytváří množiny hran $E_0, E_1, \ldots \subseteq E$, přičemž $E_0 = \emptyset$.

Předpokládejme, že jsme již spočítali množinu E_{i-1}, a nechť $(V_1, V_2, \ldots, V_t)$ je rozklad množiny V podle komponent souvislosti grafu (V, E_{i-1}) (přísně vzato, měl by tento rozklad mít ještě index i, protože bude v každém kroku jiný, ale pro zjednodušení zápisu index i vynecháme). Pro každou třídu V_j tohoto rozkladu vyhledáme hranu $e_j = \{x_j, y_j\}$ (kde $x_j \in V_j$, $y_j \notin V_j$), jejíž váha je minimální mezi hranami tvaru $\{x, y\}$, $x \in V_j$, $y \in V \setminus V_j$ (přitom se může stát $e_j = e_{j'}$ pro $j \neq j'$). Definujeme $E_i = E_{i-1} \cup \{e_1, \ldots, e_t\}$. Algoritmus končí, má-li graf (V, E_i) jedinou komponentu.

Algoritmus by se také mohl nazývat *bublinkový*. Graf G pokrýváme souborem „bublinek“ (kterých je jak borůvek v lese). Nacházíme mezi nimi nejkratší spojení a každé takové spojení vede k tomu, že se bublinky spojí v jednu.

Nebudeme dokazovat správnost algoritmu. Ukážeme pouze, že zkonstruovaný graf $T = (V, E')$ je skutečně strom. Podle definice je tento graf souvislý; stačí tedy ukázat, že nemá kružnici. Předpokládejme pro spor, že v nějakém kroku i kružnice vznikla. To znamená, že existují navzájem různé indexy $j(1), j(2), \ldots, j(k)$, pro něž platí

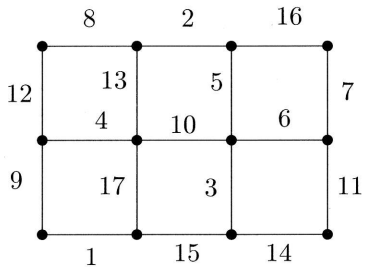
$$\begin{aligned} &x_{j(1)} \in V_{j(1)}, && y_{j(1)} \in V_{j(2)} \\ &x_{j(2)} \in V_{j(2)}, && y_{j(2)} \in V_{j(3)} \\ &\qquad\vdots \\ &x_{j(k-1)} \in V_{j(k-1)}, && y_{j(k-1)} \in V_{j(k)} \\ &x_{j(k)} \in V_{j(k)}, && y_{j(k)} \in V_{j(1)}. \end{aligned}$$

Vzhledem prostotě w a k volbě hran $e_j = \{x_j, y_j\}$ dostáváme následující nerovnosti:

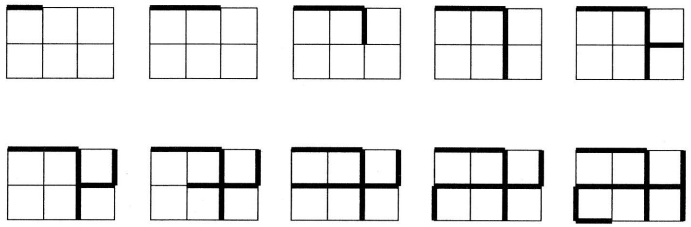
$$w(e_{j(1)}) > w(e_{j(2)}) > \cdots > w(e_{j(k)}) > w(e_{j(1)}).$$

To je však spor, a Borůvkův algoritmus tedy nalezne kostru grafu G (ve skutečnosti nalezne minimální kostru). □

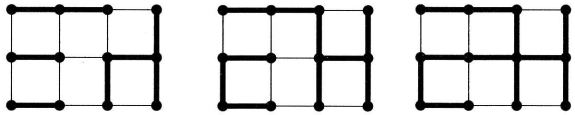
Příklad. Uvažme následující síť (ohodnocení jsou připsána k příslušným hranám):



Jarníkův algoritmus použitý na tuto síť proběhne takto (začínáme v levém horním rohu):



Kruskalův algoritmus by probíhal v 17 krocích (ale jenom v 10 z nich by přibyly hrany kostry). Borůvkův algoritmus je oproti tomu krátký:



V každém kroku však musíme vykonat více práce.

Cvičení

1.* Uvažme takovýto algoritmus pro hledání minimální kostry: Vstupem je souvislý graf $G = (V, E)$ s ohodnocením w. Položíme $E_0 = \emptyset$. Nechť E_{i-1} bylo již definováno. Zvolme libovolně některou komponentu V_i grafu (V, E_{i-1}), vyberme hranu e_i minimální váhy s jedním vrcholem ve V_i a druhým mimo V_i, a položme $E_i = E_{i-1} \cup \{e_i\}$. Dokažte, že (V, E_{n-1}) je minimální kostra (upravte důkaz správnosti Jarníkova algoritmu).

   Ověřte, že tím se naráz dokazuje správnost jak Kruskalova, tak Jarníkova algoritmu.

2.* Uvažme následující algoritmus. Vstupem je souvislý graf $G = (V, E)$ s ohodnocením hran w. Seřadíme hrany do pořadí $e_1, \ldots, e_m$ tak, aby $w(e_1) \geq \ldots \geq w(e_m)$. Položíme $E_0 = E$, a

$$E_i = \begin{cases} E_{i-1} \setminus \{e_i\} & \text{je-li } (V, E_{i-1} \setminus \{e_i\}) \text{ souvislý graf} \\ E_i & \text{jinak.} \end{cases}$$

   Dokažte, že (V, E_m) je minimální kostra G.

3.* Dokažte správnost Borůvkova algoritmu.

4. Navrhněte podrobnosti Jarníkova algoritmu tak, aby měl časovou složitost $O((m + n) \log n)$ (toto cvičení patrně vyžaduje aspoň základní znalost datových struktur).

5. (a) Ukažte, že Borůvkův algoritmus má nejvýš $O(\log n)$ fází, tj. že (V, E_i) je souvislý graf již pro nějaké $i = O(\log n)$.

   (b) Navrhněte podrobnosti Borůvkova algoritmu tak, aby měl časovou složitost $O((m + n) \log n)$.

6

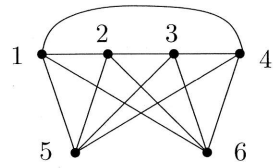
Rovinné kreslení grafů

6.1 Úvod do rovinných grafů

Grafy je výhodné kreslit. Ostatně většina grafů v tomto textu je zadána obrázkem (místo seznamu vrcholů a hran nebo nějakého jiného způsobu vhodného pro počítače). Dosud jsme však studovali vlastnosti grafu, které závisely pouze na vztahu jeho množiny vrcholů a množiny hran, a nikoli na tom, jak byl graf znázorněn. Obrázky měly funkci pouze pomocnou. V této kapitole podrobíme bližší analýze právě kreslení grafů.

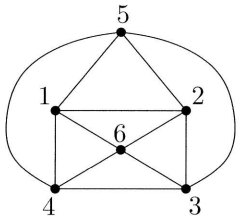
Nakreslení grafu se nazývá *rovinné*, pokud se v něm žádné hrany nekříží. *Rovinný graf* je graf, který má nějaké rovinné nakreslení.

Rovinný graf je snadné poznat, když dostaneme jeho rovinné nakreslení. Pokud ovšem máme graf nakreslený třeba takto,



je to poněkud složitější. Než otočíte stránku, schválně zkuste najít rovinné nakreslení.

Zde je tentýž graf překreslený bez křížení hran:



Rovinné nakreslení je výhodné pro znázornění grafu – při nerovinném nakreslení by se například průsečíky hran mohly plést s vrcholy. Při některých aplikacích, kdy má nakreslení grafu fyzikální význam, může být křížení hran přímo nežádoucí – třeba při návrhu jednovrstevných integrovaných obvodů. Obecně se dá říct, že rovinné grafy tvoří jednu z nejdůležitějších tříd grafů, a to jak v teorii, tak v praxi (další takovou významnou třídou jsou stromy, které jsme probírali v předchozím).

Setkání s geometrií. Pojem rovinného grafu je definován geometricky, pomocí kreslení v rovině, a tudíž teorie rovinných grafů není „čistou" diskrétní matematikou (na rozdíl od studia eulerovských grafů, stromů a řady dalších tříd grafů). Proto má trochu neobvyklé, mezioborové postavení.

Důkazy základních výsledků o rovinných grafech mají zpravidla kombinatorickou část a geometrickou část. V kombinatorické části se pracuje podobně jako v jiných odvětvích teorie grafů, například se postupuje indukcí podle počtu hran či vrcholů, počítají se stupně vrcholů a podobně.

V geometrické části se dokazují výsledky o kreslení v rovině, které se většinou zdají být zřejmé z obrázku, nicméně jejich logicky přesné důkazy jsou někdy dlouhé a složité.

V této kapitole nejdříve zavedeme přesnou definici nakreslení grafu a pojednáme o *Jordanově větě o kružnici*, což je jedno ze zmíněných zřejmě vypadajících tvrzení s nesnadným důkazem. Ukážeme, že pokud se omezíme na kreslení lomenými čarami, je Jordanova věta zvládnutelná i prostředky středoškolské geometrie. Teprve potom se pustíme do základních vět o rovinných grafech.

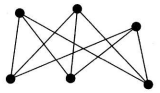
Cvičení

1. Najděte
   (a) rovinný graf, jehož všechny vrcholy mají stupeň 5,
   (b)* pro všechna přirozená čísla n souvislé grafy jako v (a) s více než n vrcholy.
2.* Buď G rovinný eulerovský graf, a mějme nějaké jeho rovinné nakreslení. Ukažte, že existuje uzavřený eulerovský tah, který v daném nakreslení nikde nekříží sama sebe (může se dotýkat ve vrcholech, ale nikdy nepřejde „na druhou stranu").

6.2 Proč a jak definovat rovinné nakreslení grafu

Nerovinný graf? Pokud chceme dokázat, že nějaký graf je rovinný, stačí předvést jedno konkrétní rovinné nakreslení. Možná ho nebude snadné najít, ale když už ho budeme mít, mělo by přesvědčit každého soudného člověka, dokonce i hodně skeptického. Jak ale někoho přesvědčit, že určitý graf rovinný *není*?

Uvažme například $K_{3,3}$, úplný bipartitní graf na $3+3$ vrcholech:



Rádi bychom dokázali, že není rovinný – to je matematická formulace problému se třemi domy a třemi studnami z oddílu 1.1.

Když budete zkoušet kreslit $K_{3,3}$ bez křížení hran, po několika pokusech to pravděpodobně vzdáte a uvěříte, že to nejde. Určitě nejste jediní – nakreslit $K_{3,3}$ bez křížení hran se zatím nepodařilo *nikomu*.

To se ale v matematice nepovažuje za důkaz. Co kdyby třeba nějaká mimozemská či nadpřirozená bytost, mnohem chytřejší než všichni lidé, uspěla tam, kde lidé selhali, a nakreslila $K_{3,3}$ bez křížení hran? Možná nějakým způsobem pro nás zcela nepředstavitelným. Také bychom měli mít na paměti, že se lidem často podaří věci, které byly dříve považovány za nemožné nebo nemyslitelné, jako postavení létajícího stroje, uběhnutí 100 m pod 10 vteřin, nošení bikin na veřejnosti nebo snížení stavů některých ryb v oceánech na desetinu. Navíc jevy zdánlivě nemožné, nebo

aspoň v rozporu s představivostí, byly odhaleny i v oblasti rovinné geometrie: například spojitá křivka procházející všemi body roviny, či spojitá reálná funkce, která není diferencovatelná v žádném bodě, nebo množina („zahrada") v rovině libovolně malé plochy, ve které lze obrátit úsečku jednotkové délky („žebřík"; během obracení se s úsečkou smí všelijak posunovat, ale musí zůstat stále uvnitř množiny).[1]

Abychom věděli jistě, že $K_{3,3}$ rovinný není, potřebujeme matematický důkaz, který nějak vezme v úvahu *všechna* možná nakreslení najednou. A hned narazíme na první citlivý bod: co přesně nakreslení grafu je?

Co je nakreslení grafu? Z mnoha již uvedených obrázků by čtenář měl mít dobrou představu, co se nakreslením grafu myslí. V části 4.1 jsme uvedli i neformální definici: vrcholům grafu se přiřadí různé body v rovině a hrany se kreslí jako rovné nebo křivé čáry spojující odpovídající dvojice bodů.

S takovou „definicí" nejspíš vystačíme při vlastním kreslení grafů, ale pokud potřebujeme doopravdy dokázat, že nějaký graf rovinný *není*, narazíme na problém: čára je pojem neformální, pro nějž jsme matematickou definici nepodali.

Pro ilustraci možných obtíží si uvědomíme, že křivá čára se určitě může vlnit jako na levém obrázku,



ale může se například vlnit nekonečněkrát, jak je naznačeno na obrázku pravém? Může vypadat třeba jako *Kochova křivka*, což je vhodně definovaná limita nekonečné posloupnosti stále složitějších lomených čar jako na obrázku?



Musíme povolený způsob kreslení hran definovat exaktně, a to na základě jiných přesných matematických pojmů.

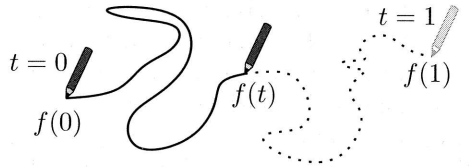
[1] Pokud by vás tyto příklady zajímaly, najdete je pomocí klíčových slov *Peanova křivka*, *nikde nediferencovatelná funkce* a *Kakeyův-Bezikovičův problém*.

V této sekci podáme dokonce dvě různé definice. Každá popisuje jiný matematický pojem, ale obě docela dobře vystihují intuitivní pojem „křivé čáry". Pro logicky přesné budování teorie rovinných grafů se tak naskýtají dvě cesty, podle toho, ze které z těchto dvou definic vyjdeme.

Kreslení oblouky: cesta přirozená, elegantní, ale trnitá. Intuitivní představu křivé čáry jako něčeho, co vznikne spojitým pohybem tužky po papíře, odráží následující pojem *oblouku*.

6.2.1 Definice. Oblouk *je podmnožina roviny tvaru* $\gamma = f([0,1]) = \{f(x);\ x \in [0,1]\}$, *kde* $f : [0,1] \to \mathbf{R}^2$ *je nějaké prosté spojité zobrazení*[2] *uzavřeného intervalu* $[0,1]$ *do roviny. Přitom body* $f(0)$ *a* $f(1)$ *se jmenují* koncové body *oblouku* γ.

Tato definice, ač může vypadat nepřístupně, má velmi blízko k pojmu kreslení. Interval $[0,1]$ si můžeme představovat jako časový úsek, v němž kreslíme čáru z bodu $f(0)$ do bodu $f(1)$. Potom $f(t)$ vyjadřuje polohu hrotu tužky v čase t. Spojitost zobrazení f znamená souvislý pohyb po papíře, a prostota vyjadřuje, že čára nikde sama sebe neprotíná.



Na základě pojmu oblouku můžeme přesně definovat i rovinné nakreslení grafu.

6.2.2 Definice. Nakreslením grafu $G = (V, E)$ *rozumíme přiřazení, které*

[2] Připomeňme, že spojitost f znamená následující: Pro všechna $x_0 \in [0,1]$ a pro všechna $\varepsilon > 0$ existuje $\delta > 0$ takové, že pro všechna $x \in [0,1]$ splňující $|x - x_0| < \delta$ je vzdálenost bodů $f(x)$ a $f(x_0)$ menší než ε. Vzdáleností se myslí obvyklá eukleidovská vzdálenost: bod o souřadnicích (x_1, y_1) má od bodu o souřadnicích (x_2, y_2) vzdálenost $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$.

- *každému vrcholu v grafu G přiřazuje bod $b(v)$ roviny*
- *a každé hraně $e = \{u, v\} \in E$ přiřazuje oblouk $\gamma(e)$ v rovině s koncovými body $b(u)$ a $b(v)$.*

Přitom předpokládáme, že

- *zobrazení b je prosté (různým vrcholům odpovídají různé body)*
- *a žádný z bodů tvaru $b(v)$ není nekoncovým bodem žádného z oblouků $\gamma(e)$ (hrany se vyhýbají vrcholům).*

Nakreslení grafu $G = (V, E)$, v němž oblouky odpovídající různým hranám mají společné nanejvýš koncové body, se nazývá rovinné nakreslení. *Graf G je* rovinný, *má-li alespoň jedno rovinné nakreslení.*

Když hovoříme o grafech a jejich nakresleních, často nerozlišujeme mezi hranou e a obloukem $\gamma(e)$, který hraně odpovídá v uvažovaném nakreslení. Mluvíme tedy někdy o hraně v nakreslení, i když samozřejmě myslíme příslušný oblouk. Nemělo by to však způsobit žádné nedorozumění.

Dnešní matematika je celá vybudována z několika primitivních pojmů a axiomů teorie množin – nebo přinejmenším se většina matematiků snaží ji takovou mít. Tak například pojem „roviny" se modeluje jako kartézský součin $\mathbf{R} \times \mathbf{R}$, přitom reálná čísla se zavádějí jako jisté podmnožiny čísel racionálních, racionální čísla se vytvářejí z čísel přirozených, a ta se konečně definují jako jisté speciální množiny vybudované z množiny prázdné. (To je v každodenní matematice vidět málokdy, ale když se podíváte do nějaké knihy o základech matematiky, určitě to tam najdete.)

Předchozí definice ilustruje, že i pojem nakreslení grafu se dá zavést takto logicky přesně a lze jej tudíž zahrnout do logické konstrukce matematiky.

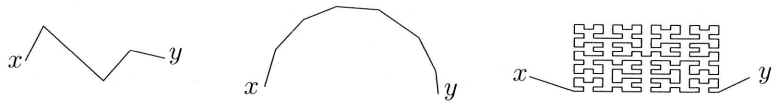
Tak, teď máme přesnou definici rovinného grafu. Jak se na jejím základě dokáže, že třeba graf $K_{3,3}$ není rovinný?

Přesný důkaz vyžaduje některé pojmy a výsledky týkající se křivek v rovině, které patří do odvětví matematiky zvaného *topologie*. (Topologie se dá považovat za součást geometrie, pokud geometrii pojmeme

dostatečně široce.) Topologie je krásný a důležitý obor matematiky, ale v běžných úvodních kurzech matematiky se z ní obvykle probere jen velmi málo, takže bychom museli zavádět poměrně rozsáhlý a složitý technický aparát. Navíc, jak už jsme říkali, důkazy některých „intuitivně zřejmých" tvrzení jsou překvapivě dlouhé a obtížné (o nejdůležitějším z takových tvrzení budeme mluvit v příští sekci).

Potíže v právě zmíněných důkazech pramení hlavně ze značné obecnosti pojmu oblouk. Teorii rovinných grafů lze vystavět i jiným, technicky o dost jednodušším způsobem, kdy se omezíme na nakreslení pomocí lomených čar (tedy přinejmenším pokud bereme v úvahu jen konečné grafy).

Kreslení lomenými čarami: cesta méně přirozená, ale snazší. Uvažme lomenou čáru spojující dva body x a y v rovině, která je tvořena konečným počtem úseček a sama sebe neprotíná. Viz příklady na obrázku:



Pro stručnost takové lomené čáře říkejme *lomenice*.

Lomenice je speciálním případem oblouku, ale protože sestává z konečně mnoha úseček, je to podstatně jednodušší matematický objekt než oblouk.

Nyní můžeme definovat *lomenicové nakreslení grafu* tak, že v definici 6.2.2 všude nahradíme oblouky lomenicemi. Podobně můžeme zavést *lomenicově rovinný graf* a lomenicové analogie dalších pojmů.

Z praktického hlediska není mezi kreslením obecnými oblouky a kreslením lomenicemi rozdíl. Nepoznáme, jestli je oblouk nakreslený na papíře opravdu zakřivený nebo jestli je ve skutečnosti tvořen mnoha maličkými úsečkami – nemluvě o tom, že třeba oblouk v tištěném obrázku je udělán z drobných teček a na ještě mikroskopičtější úrovni se každá kresba rozpadá na jednotlivé atomy.

Z teoretického hlediska je příjemný následující výsledek.

6.2.3 Fakt. *Z každého rovinného nakreslení grafu (tj. nakreslení pomocí oblouků) lze získat i lomenicově rovinné nakreslení téhož grafu. Tudíž třída všech lomenicově rovinných grafů splývá s třídou všech rovinných grafů.*

Důkaz zde podávat nebudeme. Dá se najít například v článku [29] a čtenář, znalý základů matematické analýzy, se o něj může sám pokusit ve cvičení 1.

Je tedy lepší definovat rovinné grafy pomocí oblouků, nebo pomocí lomenic? Obě cesty mají výhody i nevýhody.

Kreslení pomocí oblouků je definice elegantní, standardní a všeobecně přijatá. Všechna geometrická tvrzení, potřebná k vybudování teorie rovinných grafů, byla řádně dokázána a důkazy jsou k dispozici v literatuře, i když nejsou úplně jednoduché. Této definice se budeme držet i v naší kapitole o rovinných grafech.

Kreslení pomocí lomenic je šikovné pro rychlé a přitom logicky přesné vybudování teorie rovinných grafů na elementární úrovni. V následující sekci předvedeme ukázku geometrického důkazu s lomenicemi.

Cvičení

1.* Dokažte fakt 6.2.3 podle následujícího návodu. Vezmeme rovinné nakreslení pomocí obecných oblouků a pro každý vrchol v v tomto nakreslení zvolíme kruh K_v se středem ve v a s poloměrem tak malým, že do K_v nezasahují žádné jiné vrcholy ani žádné hrany s výjimkou těch, které mají ve v koncový bod. Nyní části hran mimo sjednocení všech K_v aproximujeme lomenicemi (s využitím spojitosti oblouků) a části hran uvnitř K_v nahradíme úsečkami, spojujícími v s příslušným bodem hranice K_v.

6.3 Jordanova věta o kružnici

Jordanova věta o kružnici praví, zhruba řečeno, že každé rovinné nakreslení grafové kružnice rozděluje rovinu na dvě oblasti. Než ji vyslovíme přesně, připravíme si několik definic.

Topologická kružnice[3] je uzavřená křivka v rovině neprotínající sebe sama. Formálně se topologická kružnice definuje jako oblouk, jehož koncové body splývají, tj. spojitý obraz intervalu $[0,1]$ při zobrazení $f : [0,1] \to \mathbf{R}^2$, které je prosté až na to, že $f(0) = f(1)$. Nebude-li hrozit nedorozumění, budeme místo topologická kružnice říkat jenom kružnice.

Dále buď $U \subset \mathbf{R}^2$ množina, zatím libovolná. Definujeme relaci $\approx$ na U tak, že $x \approx y$ právě tehdy, když existuje oblouk $\gamma \subseteq U$ s koncovými body x a y (tedy z y se dá dojít do x, aniž by se opustila U). Dá se ověřit, že $\approx$ je ekvivalence (cvičení 1). Potom definujeme *komponenty obloukové souvislosti* množiny U jako třídy ekvivalence $\approx$.

6.3.1 Věta (Jordanova věta o kružnici). *Nechť κ je topologická kružnice. Potom její doplněk $\mathbf{R}^2 \setminus \kappa$ má právě dvě komponenty obloukové souvislosti, z nichž jedna je omezená množina a druhá neomezená množina, a κ je hranicí*[4] *obou těchto množin.*

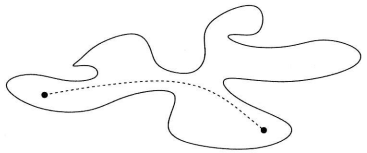
Jak souvisí tato věta s rovinným kreslením grafů? Jednoduše – kružnicím v grafu odpovídají v rovinném nakreslení topologické kružnice. Přesněji řečeno, srovnáním definic je snadné ověřit, že je-li G graf a $C \subseteq E(G)$ množina hran nějaké kružnice v G, potom pro každé rovinné nakreslení G tvoří sjednocení všech oblouků $\gamma(e)$ pro $e \in C$ topologickou kružnici.

Obtíže s Jordanovou větou. Jordanova věta jistě nepatří k nejtěžším výsledkům v matematice, ale žádný opravdu jednoduchý důkaz pro ni znám není. Zatím nejjednodušší je patrně důkaz Thomassenův z článku [29].

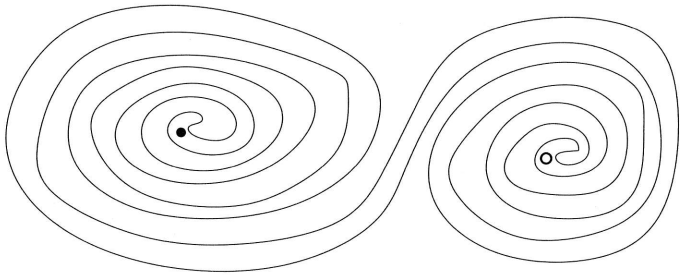
Proč by měl být důkaz obtížný, když věta vypadá na první pohled tak zřejmá? Pro některé kružnice v rovině je tvrzení evidentní,

[3] Jiný používaný název je *jednoduchá uzavřená křivka*, nebo taky *Jordanova křivka*.

[4] *Hranice* množiny $X \subseteq \mathbf{R}^2$ je množina všech bodů $x \in \mathbf{R}^2$, ke kterým existují libovolně blízké body z X a zároveň i libovolně blízké body z $\mathbf{R}^2 \setminus X$.



pro jiné už méně evidentní (zkuste najít oblouk mezi body ○ a ●, který neprotíná kružnici):



Nemohlo by se stát, že když bude kružnice ještě mnohem složitější, tvrzení platit přestane?

Takové případy, kdy zdánlivě zřejmá tvrzení ve skutečnosti neplatí, se v matematice vyskytují. Ukazuje to například tvrzení uvedené níže, které Jordanovu větu trochu připomíná.

V Jordanově větě o kružnici je rovina rozdělena do tří množin U_1, U_2, a X, kde X je topologická kružnice a U_1 a U_2 jsou dvě komponenty obloukové souvislosti $\mathbf{R}^2 \setminus X$ takové, že X je společnou hranicí U_1 a U_2.

Uvažme teď následující tvrzení: „Rovina se nedá rozdělit na čtyři neprázdné množiny U_1, U_2, U_3 a X tak, že hranice každé U_i je přesně X (celá X a nic než X).“

Intuitivně zřejmé? Možná, ale *nepravdivé* – takové množiny existují a krásné příklady se přirozeně vyskytují v komplexní dynamice v souvislosti s Newtonovou metodou a Juliovými množinami vhodných mnohočlenů. Pokud by to někoho zajímalo, doporučujeme tato hesla vyhledat třeba na Internetu.

Tento příklad s Jordanovou větou o kružnici přímo nesouvisí, ale ilustruje, že v rovině se mohou dít věci, které by člověk na první pohled nečekal.

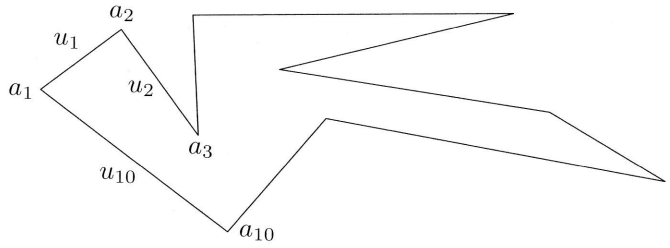
Obecnou Jordanovu větu zde nedokážeme (nedokazuje se ani v jiných učebnicích teorie grafů – výjimkou potvrzující pravidlo je monografie Mohara a Thomassena [22] o rovinných grafech). Dokážeme ale verzi pro kreslení lomenými čarami, což je i první a důležitý krok v důkazech obecné Jordanovy věty.

Lomenicová Jordanova věta. Definujeme *lomenicovou kružnici* jako uzavřenou lomenou čáru, která je tvořena konečně mnoha úsečkami a sama sebe neprotíná. Lomenicová kružnice odpovídá grafové kružnice v lomenicově rovinných nakresleních, podobně jako topologické kružnice odpovídá grafové kružnici v rovinných nakresleních.

Abychom se úplně vyhnuli pojmu oblouku, nebudeme také používat ekvivalenci $\approx$, ale zavedeme novou ekvivalenci $\cong$. Pro danou množinu $U \subseteq \mathbf{R}^2$ a body $x, y \in \mathbf{R}^2 \setminus U$ platí $x \cong y$, právě když se x a y dají uvnitř U spojit lomenicí. Poznamenejme, že v případech, které nás budou zajímat, bude U otevřená množina (tj. s každým svým bodem obsahuje i nějaké jeho malé okolí) a v takovém případě jsou ekvivalence $\approx$ a $\cong$ totožné – viz cvičení 2.

6.3.2 Věta (Jordanova věta pro lomenicové kružnice). *Nechť κ je lomenicová kružnice. Potom její doplněk $\mathbf{R}^2 \setminus \kappa$ má právě dvě komponenty lomenicové souvislosti (tj. třídy ekvivalence $\cong$), z nichž jedna je omezená množina a druhá neomezená množina, a κ je hranicí obou těchto množin.*

Důkaz. Podle definice sestává κ z konečně mnoha úseček, které označíme $u_1, u_2, \ldots, u_n$ v pořadí, jak následují za sebou při obcházení κ. Koncové body úsečky u_i nechť jsou a_i a a_{i+1}, přičemž bod a_{n+1} je totožný s a_1:



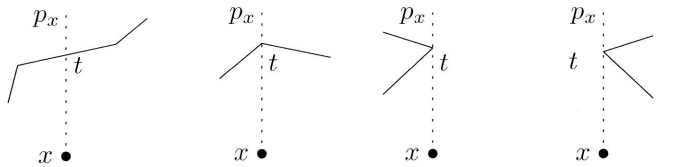
Důkaz má dvě nezávislé části: nejdříve dokážeme, že existují aspoň dvě komponenty lomenicové souvislosti (neboli že existují dva body $x_0, y_0 \in \mathbf{R}^2 \setminus \kappa$, které nelze spojit lomenicí), a potom, že existují nejvýš dvě komponenty.

Aspoň dvě komponenty. Plán této části je následující: pro každý bod $x \in \mathbf{R}^2 \setminus \kappa$ definujeme číslo $ind(x) \in \{0, 1\}$ a dokážeme, že pokud x a y lze spojit lomenicí, potom $ind(x) = ind(y)$. Pak ještě najdeme body x_0 a y_0, pro něž platí $ind(x_0) \neq ind(y_0)$, a tím bude tato část hotova.

Než začneme s definicí $ind(x)$, najdeme přímku s, která není rovnoběžná s žádnou z úseček $u_1, \ldots, u_n$. Taková jistě existuje, protože zmíněné úsečky určují konečně mnoho směrů, kdežto v rovině máme k dispozici nekonečně mnoho směrů. V dalším budeme pro snazší vyjadřování předpokládat, že přímka s je svislá, tj. rovnoběžná s osou y – pokud by nebyla, můžeme soustavu souřadnic otočit.

Pro bod $x \in \mathbf{R}^2 \setminus \kappa$ uvažme polopřímku p_x, která začíná v x a směřuje svisle vzhůru (a speciálně je rovnoběžná s přímkou s). Z volby s plyne, že p_x protíná κ v konečně mnoha bodech, neboť každou z úseček u_i protne nanejvýš jednou.

Průsečíky p_x s κ rozlišíme na *vhodné* a *nevhodné*. Pokud je průsečík $t \in p_x \cap \kappa$ vnitřním bodem některé u_i, potom je vhodný, a pokud t splývá s některým z bodů a_i, je vhodný právě tehdy, když úsečky u_{i-1} a u_i vycházející z a_i směřují na různé strany polopřímky p_x:[5]



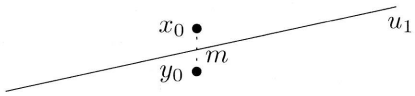
Teď položíme $ind(x) = 0$, pokud je počet vhodných průsečíků polopřímky p_x s κ *sudý*, a $ind(x) = 1$, pokud je tento počet *lichý*.

[5]Pro $i = 1$ úsečkou u_{i-1} myslíme samozřejmě u_n. Podobné konvence budeme mlčky používat i ve zbytku důkazu.

Rádi bychom ověřili, že jsou-li $x, y \in \mathbf{R}^2 \setminus \kappa$ dva body spojené nějakou lomenicí γ neprotínající κ, potom platí $ind(x) = ind(y)$. Stačí se zabývat případem, kdy je γ tvořena jedinou úsečkou xy – když totiž γ sestává z m úseček xb_1, b_1b_2,..., $b_{m-1}y$, potom z výsledku pro jednu úsečku postupně dostaneme $ind(x) = ind(b_1)$, $ind(b_1) = ind(b_2)$ atd., a tedy i $ind(x) = ind(y)$.

Uvažme bod z, který se po úsečce xy pohybuje od x k y, a zkoumejme, jak se mění počet vhodných průsečíků polopřímky p_z s lomenicovou kružnicí κ. Tento počet se může měnit jedině v (konečně mnoha) okamžicích, kdy p_z prochází některým z bodů a_i. Přesněji řečeno, počet vhodných průsečíků se mění jedině tehdy, když p_z projde vrcholem tvořícím nevhodný průsečík, a při průchodu každým takovým nevhodným průsečíkem dva vhodné průsečíky buď přibudou, nebo ubudou. Tudíž počet vhodných průsečíků se může měnit jen o sudé číslo, a proto se $ind(z)$ nemění vůbec. Takže $ind(x) = ind(y)$.

Nyní víme, že pokud $x \approxeq y$, potom $ind(x) = ind(y)$. Zbývá dokázat, že funkce ind nabývá na $\mathbf{R}^2 \setminus \kappa$ obou možných hodnot. Uvažme třeba střed m úsečky u_1, nechť x_0 je bod svisle nad m takový, že úsečka mx_0 protíná κ jedině v bodě m, a podobně nechť y_0 je bod „těsně pod“ m:

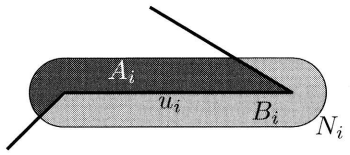


Potom p_{y_0} má právě o jeden vhodný průsečík s κ více než p_{x_0}, totiž o m, a tedy $ind(x_0) \neq ind(y_0)$. Tudíž ekvivalence $\approxeq$ má aspoň dvě třídy a první část důkazu je hotova.

Nejvýš dvě komponenty. Zvolíme kladné číslo ε tak malé, že každá z úseček u_i má od všech bodů $a_1, a_2, \ldots, a_n$ s výjimkou svých koncových bodů a_i a a_{i+1} vzdálenost větší než ε. (Takové ε existuje, protože každý bod a_j, $j \neq i, i+1$, má od u_i nějakou kladnou vzdálenost, a tedy stačí ε vzít menší než minimum z konečně mnoha kladných vzdáleností.)

Označme N_i množinu všech bodů $x \in \mathbf{R}^2 \setminus \kappa$, které mají od úsečky u_i vzdálenost nejvýš ε, a položme $N = N_1 \cup N_2 \cup \cdots \cup N_n$ (to je

vlastně „otevřené ε-okolí“ množiny κ). Každá N_i má tvar (protáhlého) stadiónu, z něhož je vyňata úsečka u_i a části úseček u_{i-1} a u_{i+1}:



Je důležité si všimnout, že díky volbě ε žádná jiná z úseček u_j do množiny N_i zasahovat nemůže – to doporučujeme promyslet pořádně.

Každá z množin N_i má dvě části, označené v obrázku A_i a B_i, které jsou lomenicově souvislé (kdybychom to chtěli dokázat opravdu přesně, mohli bychom prostředky eukleidovské geometrie explicitně popsat lomenici z maximálně tří úseček, která spojí dva dané body uvnitř A_i, a podobně pro B_i). Dále A_i i B_i obě protínají jak N_{i-1}, tak N_{i+1}. Z toho dostáváme, že i množina N má nanejvýš dvě komponenty lomenicové souvislosti.

Na závěr ověříme, že každý bod $x \in \mathbf{R}^2 \setminus \kappa$ lze spojit s nějakým bodem $y \in N$ úsečkou neprotínající κ. Pokud $x \in N$, není co dokazovat. Pro $x \notin N$ vezmeme libovolný bod $z \in \kappa$. Když postupujeme po úsečce xz z bodu x směrem k z, narazíme na nějaký bod y z množiny N dříve, než na množinu κ, poněvadž N obsahuje všechny body, které mají od κ vzdálenost nejvýš ε. Tudíž $\mathbf{R}^2 \setminus \kappa$ má skutečně nejvýš dvě komponenty lomenicové souvislosti a druhá část je hotova.

Ještě zbývá maličkost: dokázat, že κ tvoří hranici každé z komponent. Malou obměnou argumentu na konci první části se snadno ukáže, že je-li z libovolný vnitřní bod některé z úseček u_i, najdeme libovolně blízko k z jak body x splňující $ind(x) = 0$, tak body y splňující $ind(y) = 1$. Jak víme, takové body leží v různých komponentách $\mathbf{R}^2 \setminus \kappa$. □

Cvičení

1.* Buď U množina v rovině a nechť $x, y, z \in U$ jsou body takové, že x a y se dají spojit obloukem v U a y a z se dají spojit obloukem v U. Dokažte, že x a z se také dají spojit obloukem v U. (Na to jsou potřeba jisté základy z analýzy.)

2.* (I toto cvičení patří spíše do analýzy.) Buď $U \subseteq \mathbf{R}^2$ *otevřená* množina. Dokažte, že pokud body $x, y \in U$ lze uvnitř U spojit obloukem, lze je spojit i lomenicí. Návod: oblouk je potřeba pokrýt konečně mnoha kruhy, z nichž každý je obsažen v U.

6.4 Stěny a Eulerův vztah

V dalším textu budeme rovinným nakreslením myslet rovinné nakreslení pomocí oblouků, jako v definici 6.2.2 (a jak to naznačují i naše obrázky grafů). Tato definice se používá ve všech pokročilejších pracích o rovinných grafech a je matematicky i esteticky elegantnější a pro praxi vhodnější než alternativní definice pomocí lomenic.

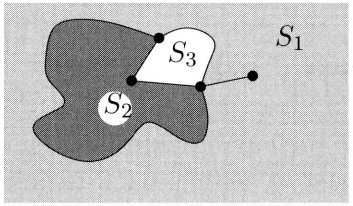
Potom ale nemůžeme dokázat všechna tvrzení, potřebná v geometrické části důkazů, jako například Jordanovu větu – jak jsme už zmiňovali, nemáme na to prostor ani matematické prostředky. Proto budeme v dalším výkladu postupovat poněkud neformálně. Budeme spoléhat na intuitivní představu a některá (platná!) geometrická tvrzení budeme jen předkládat k uvěření (na rozdíl od všech ostatních kapitol této knihy, kde výsledky řádně dokazujeme).

Naštěstí intuitivní představa v teorii kreslení grafů téměř nikdy nezavádí na scestí. Všechna potřebná tvrzení jsou také přesně dokázána v literatuře (viz například knihu Mohara a Thomassena [22]). Tyto důkazy do diskrétní matematiky vlastně ani nepatří a nejsou z jejího hlediska příliš zajímavé.

> Při studiu pokročilejší matematiky prakticky ani nelze projít důkazy všech potřebných výsledků. Dnešní matematik občas spoléhá na práci svých předchůdců, aniž by ji celou ověřoval.

Zájemci o přesné vybudování základů teorie rovinných grafů se také mohou pustit alternativní cestou lomenicových nakreslení. Lomenicovou Jordanovu větu jsme již dokázali a u tvrzení, která budeme probírat v dalším, zpravidla není nijak zvlášť těžké dokázat příslušné lomenicové verze.

Stěny rovinného nakreslení. Nechť $G = (V, E)$ je rovinný graf s daným rovinným nakreslením. Uvažme množinu všech bodů roviny, které neleží v žádném z oblouků nakreslení. Tato množina se rozpadne na konečný počet souvislých oblastí (představte si, že rovinu podél nakreslených hran rozstříháme):



Tyto oblasti budeme nazývat *stěny* uvažovaného rovinného nakreslení grafu G. Oblast rozprostírající se do nekonečna, jako je S_1 na našem obrázku, se nazývá *vnější stěna* (nebo *neomezená stěna*) nakreslení a všechny ostatní stěny se nazývají *vnitřní stěny* (nebo *omezené stěny*).

Definice stěny se dá formálně vyslovit na základě definic z částí 6.2 a 6.3. Pro dané rovinné nakreslení $G = (V, E)$ buď $X = \bigcup_{e \in E} \gamma(e)$ sjednocení všech oblouků nakreslení. Potom stěny nakreslení jsou komponenty obloukové souvislosti množiny $\mathbf{R}^2 \setminus X$.

Jordanovu větu o kružnici můžeme nyní přeformulovat následovně: každé rovinné nakreslení (grafové) kružnice má právě dvě stěny, přičemž sjednocení všech oblouků nakreslení je jejich společnou hranicí.

Zdůrazněme ještě, že stěny jsou definovány *pro dané rovinné nakreslení*. Pro nerovinné grafy se stěny většinou vůbec nedefinují, a ani pro rovinný graf bychom neměli mluvit o stěnách, aniž bychom zvolili nějaké rovinné nakreslení.

Eulerův vztah. Existuje v podstatě jediný základní kvantitativní vztah pro rovinné grafy; dá se říci, že všechny ostatní výsledky tento vztah ve větší či menší míře využívají. Je to zároveň vztah nejstarší, Euler jej znal v roce 1752, a někdy se tvrdí, že pochází dokonce od Descartesa z r. 1640. Původní tvrzení se ovšem týkalo mnohostěnů místo rovinných grafů (vztah mezi rovinnými grafy a mnohostěny probereme v části 6.6).

6.4.1 Věta (Eulerův vzorec). *Nechť $G = (V, E)$ je souvislý rovinný graf a nechť s je počet stěn nějakého rovinného nakreslení G. Potom platí*

$$|V| - |E| + s = 2.$$

Speciálně počet stěn nezávisí na způsobu rovinného nakreslení.

Předpoklad souvislosti G je důležitý. Jednoduchým zobecněním následujícího důkazu se dá ukázat, že když graf má k komponent souvislosti, potom $|V| - |E| + s = k + 1$ (viz cvičení 1).

Důkaz. Postupujme indukcí podle počtu hran grafu G. Je-li $E = \emptyset$, potom G jakožto souvislý graf má jediný vrchol, tudíž $|V| = 1$ a $s = 1$, a vzorec platí. Nechť $|E| \geq 1$; rozlišíme dvě možnosti:

1. Graf G neobsahuje kružnici. Potom je to strom a tedy máme $|V| = |E| + 1$ (viz větu 5.1.4). Přitom $s = 1$, jelikož rovinné nakreslení stromu má jedinou (neomezenou) stěnu.

2. Nějaká hrana $e \in E$ je obsažena v kružnici. V tom případě je graf $G - e$ souvislý. Podle indukčního předpokladu pro něj platí Eulerův vzorec (přitom bereme nakreslení $G - e$, které vznikne z uvažovaného nakreslení G vymazáním hrany e).

   Hrana e v nakreslení G sousedí se dvěma různými stěnami S a S', neboť kružnice obsahující e rozděluje rovinu na dvě části (podle Jordanovy věty o kružnici!). Tyto stěny se po vymazání e stanou stěnou jedinou. Takže vrácením hrany e zpět do nakreslení se počet hran i stěn zvýší o 1 a počet vrcholů se nemění, pročež Eulerův vzorec platí i pro G. □

O geometrické části důkazu. Právě uvedený důkaz je příkladem důkazu zčásti neformálního, kde používáme některá intuitivně zřejmá geometrická tvrzení, aniž bychom je přesně zdůvodnili.

Všimněme si například, že z Eulerova vztahu jiné vyplývá, že rovinné nakreslení kružnice má právě dvě stěny, což je hlavní tvrzení Jordanovy věty o kružnici. Takže při opravdu přesném důkazu Eulerova vztahu se nemůžeme vyhnout dokazování této věty.

Dalším speciálním případem Eulerova vztahu je tvrzení, že rovinné nakreslení stromu má jen jedinou stěnu. To jsme přijali jako zjevné, ale ve skutečnosti není důkaz o mnoho lehčí než důkaz Jordanovy věty o kružnici.

Navíc jsme indukční krok založili na skutečnosti, že hrana e obsažená v kružnici sousedí s právě dvěma stěnami. Pokud by celý graf sestával pouze z této kružnice, potom nám Jordanova věta o kružnici říká, že existují právě dvě stěny a e je částí hranice jich obou. Ale co když tam jsou mimo tuto kružnici další hrany? Nemohla by e třeba ležet na hranici tří (nebo nekonečně mnoha) stěn? Dále, i když e sousedí s právě dvěma stěnami, jak se tvrdí, proč se tyto po odstranění e spojí v stěnu jedinou?

Jak jsme uvedli na začátku sekce, důkazy těchto tvrzení existují v literatuře (a pro matematika trochu zkušeného v topologii roviny nepředstavují zásadní problém).

Řádně dokázat jejich lomenicové verze by po průpravě s lomenicovou Jordanovou větou nemělo být příliš těžké a čtenář se může aspoň o některý z takových důkazů sám pokusit.

Cvičení

1. Zobecněte důkaz věty 6.4.1 a dokažte, že pro jakékoli rovinné nakreslení grafu $G = (V, E)$ s k komponentami souvislosti platí $|V| - |E| + f = k + 1$.

2.* Dokažte, že každé lomenicově rovinné nakreslení stromu má jen jedinou stěnu (můžete se inspirovat druhou částí důkazu Jordanovy věty pro lomenicové kružnice).

6.5 Maximální počet hran rovinného grafu

Velmi důležitou vlastností rovinných grafů je to, že mohou mít jen poměrně málo hran: rovinný graf na $n \geq 3$ vrcholech nikdy nemá víc než $3n - 6$ hran.

6.5.1 Věta.

(i) Nechť $G = (V, E)$ je rovinný graf s aspoň třemi vrcholy. Potom $|E| \leq 3|V| - 6$.

(ii) Neobsahuje-li uvažovaný rovinný graf trojúhelník (tj. K_3 jako podgraf) a má-li aspoň 3 vrcholy, potom $|E| \leq 2|V| - 4$.

Následuje jeden důležitý a často využívaný důsledek této věty:

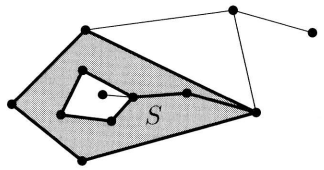
6.5.2 Důsledek. *Každý rovinný graf má nějaký vrchol stupně nejvýš 5. Každý rovinný graf bez trojúhelníků má vrchol stupně nejvýš 3.* □

První důkaz věty 6.5.1. Začneme částí (i) a po malé změně důkazu dostaneme také (ii).

Zvolíme nějaké rovinné nakreslení grafu G. Rozlišíme dva případy: buď G neobsahuje žádné kružnice, nebo obsahuje kružnici aspoň jednu.

V prvním případě je G strom nebo disjunktní sjednocení stromů (les), takže $|E| \leq |V| - 1$. Vzhledem k tomu, že pro všechna $n \geq 3$ máme $n - 1 \leq 3n - 6$, tvrzení (i) v tomto případě platí.

V dalším tedy předpokládáme, že G obsahuje aspoň jednu kružnici, a tedy jeho rovinné nakreslení má aspoň dvě stěny. Pro stěnu S uvažovaného rovinného nakreslení označme $E_S \subseteq E$ množinu těch hran grafu G, které leží na její hranici. Viz následující obrázek, kde jsou hrany z E_S vytaženy tučně.



Teď chceme ukázat, že každá stěna S má na hranici aspoň 3 hrany, tj. $|E_S| \geq 3$ (všimněme si, že v předchozím případě, G bez kružnice, by toto platit nemuselo – proto jsme onen případ diskutovali zvlášť).

Zhruba řečeno, E_S nemůže mít méně než 3 hrany, protože 2 hrany nestačí na oddělení S od ostatních stěn. Přesněji se to dá říct následovně. Když z uvažovaného rovinného nakreslení G vymažeme všechny hrany, které nepatří do E_S, dostaneme rovinné nakreslení grafu $G_S =$

(V, E_S), v němž je S stále stěnou (vymazání hrany totiž nemůže žádnou stěnu zmenšit a vymazání hrany mimo E_S nemůže ke stěně S ani nic přidat). Protože nakreslení grafu G mělo aspoň dvě stěny, má nakreslení grafu G_S také aspoň dvě stěny, a tudíž obsahuje kružnici. Každá kružnice má aspoň 3 hrany, a tedy skutečně $|E_S| \geq 3$.

Nyní nerovnosti $|E_S| \geq 3$ sečteme přes všechny stěny S a dostaneme $\sum_S |E_S| \geq 3s$, kde s je počet stěn. Vzhledem k tomu, že každá hrana náleží jedné nebo dvěma stěnám, máme také $\sum_S |E_S| \leq 2|E|$. Tedy platí nerovnost

$$s \leq \frac{2}{3}|E|. \tag{6.1}$$

Teď bychom rádi využili Eulerův vzorec. Náš graf nemusí být souvislý, tak musíme použít jeho obecnější verzi pro rovinné grafy s k komponentami zmíněnou za větou 6.4.1. Z té je vidět, že

$$|E| \leq |V| + s - 2.$$

Veličinu s na pravé straně odhadneme pomocí nerovnosti (6.1), což dává $|E| \leq |V| + \frac{2}{3}|E| - 2$, a po jednoduché úpravě dojdeme k $|E| \leq 3|V| - 6$.

To dokazuje část (i) věty. V důkazu části (ii) si všimneme, že v prvním případě (pro G bez kružnic) máme $n - 1 \leq 2n - 4$ pro všechna $n \geq 3$, a tedy odhad $|E| \leq 2|V| - 4$ v tomto případě platí. V opačném případě, když G kružnici obsahuje, dostaneme $|E_S| \geq 4$ pro všechny stěny S, protože kružnice v G_S nemůže být trojúhelník. Potom místo (6.1) získáme nerovnost $s \leq \frac{1}{2}|E|$ a po dosazení za s do Eulerova vzorce spočítáme, že $|E| \leq 2|V| - 4$, jak jsme tvrdili. □

Druhý důkaz. Teď si ukážeme ještě jiný důkaz věty 6.5.1, který je sice delší než ten první, ale v jistém smyslu přirozenější a dokazuje i trochu silnější tvrzení. Začneme s výsledkem, který je zajímavý sám o sobě.

6.5.3 Tvrzení. *Nechť G je 2-souvislý rovinný graf. Potom je každá stěna v libovolném nakreslení grafu G ohraničena nějakou kružnicí grafu G, tedy množina hran ležících na hranici stěny tvoří kružnici v grafu G.*

Důkaz. Postupujeme matematickou indukcí podle počtu hran grafu G, přičemž použijeme tvrzení 4.7.5 – charakterizaci 2-souvislých grafů. Je-li G trojúhelník, potom tvrzení zřejmě platí (podle Jordanovy věty o kružnici).

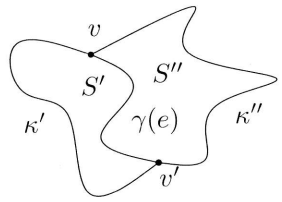
Nechť $G = (V, E)$ je souvislý rovinný graf s aspoň 4 vrcholy. Podle tvrzení 4.7.5 buď existuje hrana $e \in E$ taková, že graf $G' = G - e$ je 2-souvislý, nebo existuje 2-souvislý graf $G' = (V', E')$ a hrana $e \in E'$ tak, že $G = G'\%e$, kde $\%$ značí operaci dělení hrany.

Protože G je rovinný graf, je graf G' v obou případech opět rovinný.

Protože graf G' je 2-souvislý, můžeme použít indukčního předpokladu. Každá stěna v libovolném rovinném nakreslení grafu G' je tedy ohraničena nějakou kružnicí grafu G'.

Uvažme první případ, kdy $G' = G - e$, $e = \{v, v'\}$. Máme-li dáno libovolné rovinné nakreslení grafu G, dostaneme z něj vynecháním hrany e i rovinné nakreslení grafu G'. Vrcholy v a v' jsou v grafu G spojeny hranou e, a tedy leží na hranici nějaké stěny S v uvažovaném nakreslení G'. Označme κ_S kružnici v G' ohraničující stěnu S.

Jak je vidět na následujícím obrázku, hrana e rozděluje S na dvě nové stěny S' a S'':



Stěny S' a S'' jsou oblastmi kružnic $\kappa' \cup \{e\}$ a $\kappa'' \cup \{e\}$, kde κ' a κ'' jsou oblouky, které spojují v s v' a dohromady tvoří kružnici κ_S. Tudíž jsou všechny stěny v libovolném rovinném nakreslení G ohraničeny kružnicemi, jak jsme tvrdili. Tím je dokončen indukční krok v prvním případě, kdy $G = G' + e$.

Druhý případ je snazší: Jestliže $G = G'\%e$ a každá stěna G' je oblastí nějaké kružnice, potom G má tutéž vlastnost, jak plyne bezprostředně z definice operace dělení hrany. Tím je důkaz ukončen. □

Z tvrzení 6.5.3 vyplývá, že se 2-souvislé rovinné grafy chovají svým způsobem lépe než rovinné grafy obecně. Ale ještě mnohem lépe se chovají vrcholově 3-souvislé rovinné grafy. Ty mají v podstatě jednoznačné nakreslení na sféře (až na spojitou deformaci sféry a zrcadlení) a v mnoha směrech se s nimi lépe pracuje. Když se dokazují věty nebo navrhují algoritmy týkající se rovinných grafů, je většinou vhodné nejprve vyřešit 3-souvislé grafy a potom se snažit zpracovat obecný případ s využitím rozkladu daného grafu na 3-souvislé části. To zde ale nebudeme dále rozebírat.

Říkáme, že $G = (V, E)$ je *maximální rovinný graf*, pokud G je rovinný graf, ale po přidání jakékoli hrany graf rovinný být přestane, tj. pro žádnou $\bar{e} \in \binom{V}{2} \setminus E$ není $G + \bar{e}$ rovinný. Druhý důkaz věty 6.5.1 je založený na následujícím lemmatu:

6.5.4 Lemma. *Nechť G je maximální rovinný graf na $n \geq 3$ vrcholech. Potom je každá stěna (včetně vnější) ve všech rovinných nakresleních G trojúhelník (tj. je ohraničena kružnicí délky 3).*

Proto se maximální rovinné grafy někdy nazývají také *triangulace*.

Než začneme lemma dokazovat, podíváme se, jak z něj vyplývá věta 6.5.1(i). Postupuje se stejně jako v závěru prvního důkazu.

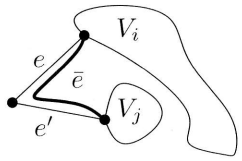
Vzhledem k tomu, že chceme omezit počet hran shora, můžeme předpokládat, že daný rovinný graf $G = (V, E)$ je maximální rovinný (pokud ne, můžeme hrany přidávat, dokud graf maximální rovinný nebude). Potom uvážíme nějaké rovinné nakreslení G a písmenem s označíme počet stěn. Protože všechny stěny jsou trojúhelníky, patří každá hrana do právě dvou stěn a $2|E| = 3s$. Protože je G (zjevně) souvislý, platí pro něj Eulerův vzorec $|E| = |V| + s - 2$, z čehož po dosazení $s = \frac{2}{3}|E|$ dostaneme $|E| = 3|V| - 6$.

Všimněte si, že jsme dokázali dokonce víc než jen větu 6.5.1(i): víme ještě také, že *nerovnost $|E| \leq 3|V| - 6$ platí s rovností právě tehdy, když je G maximální rovinný graf.*

Důkaz lemmatu 6.5.4. Nejdříve dokážeme (sporem), že maximální rovinný graf musí být vrcholově 2-souvislý.

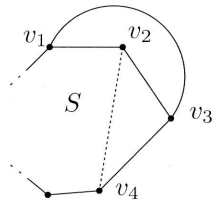
Pokud je G nesouvislý, můžeme zřejmě dvě různé komponenty souvislosti spojit novou hranou, takže G není maximální rovinný.

Pokud je G souvislý, ale není 2-souvislý, je v něm nějaký vrchol v, po jehož odstranění se graf rozpadne na komponenty souvislosti $V_1, V_2, \ldots, V_k$, $k \geq 2$ (zde využíváme předpoklad, že G má aspoň tři vrcholy!). Zvolíme dvě hrany e a e', které v spojují se dvěma různými komponentami souvislosti V_i, V_j tak, že e a e' jsou nakresleny vedle sebe (v cyklickém uspořádání okolo v). Jejich koncové vrcholy se dají spojit novou hranou $\bar{e}$, aniž by se narušila rovinnost:



Maximální rovinný graf s aspoň třemi vrcholy je tedy 2-souvislý a podle tvrzení 6.5.3 je každá stěna ohraničena kružnicí.

Zbývá dokázat, že každá stěna je ohraničena trojúhelníkem. Předpokládejme pro spor, že hraniční kružnice nějaké stěny S má $t \geq 4$ vrcholů $v_1, \ldots, v_t$. Není-li vrchol v_1 spojen hranou s vrcholem v_3, můžeme hranu $\{v_1, v_3\}$ přikreslit dovnitř stěny S. Je-li $\{v_1, v_3\} \in E(G)$, musí jít nakreslení této hrany vnějškem stěny S. Proto $\{v_2, v_4\} \notin E(G)$ (jinak by $\{v_1, v_3\}$ i $\{v_2, v_4\}$ musely obě být vně stěny S a křížily by se). Můžeme tedy přikreslit hranu $\{v_2, v_4\}$ dovnitř stěny S, viz obrázek:



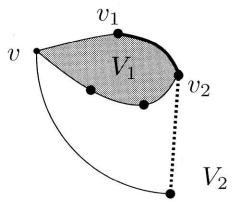
□

Druhý důkaz věty 6.5.1(ii). Tentokrát definujeme *maximální rovinný graf bez trojúhelníků* jako graf, který je rovinný a neobsahuje trojúhelník, ale přidáním libovolné hrany vznikne trojúhelník, nebo graf přestane být rovinný, nebo obojí.

Stačí dokázat, že *každá stěna v libovolném rovinném nakresleních maximálního rovinného grafu G bez trojúhelníků je ohraničena kružnicí délky aspoň* 4 – potom budeme vědět, že $2|E| \leq 4s$ a po stejném výpočtu z Eulerova vzorce jako v důkazu části (i) budeme hotovi.

Opět ověříme, že G je (vrcholově) 2-souvislý. Můžeme zase předpokládat, že G je souvislý. Není-li G 2-souvislý, má nějaký vrchol v, jehož odstraněním se G rozpadne na komponenty $V_1, \ldots, V_k$, $k \geq 2$. Jistě můžeme přidat nějakou hranu jdoucí mezi různými komponentami tak, aby G zůstal rovinný; pro některé hrany by tím však mohl vzniknout trojúhelník – to v případě, že bychom spojovali vrcholy, které oba sousedí s v. Musíme tedy postupovat obezřetněji. Jsou-li všechny komponenty V_i jednobodové, je G strom, a pro něj vzorec platí.

Předpokládejme tedy, že $|V_1| \geq 2$, a uvažme stěnu S takovou, která má na hranici nějaký vrchol V_1 i vrchol nějaké jiné komponenty V_i jako na obrázku:



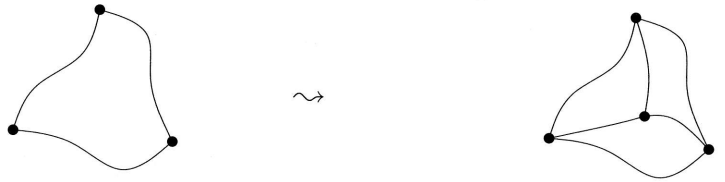
(Na tomto obrázku je S vnější stěna, $i = 2$ a komponenta V_2 má jediný vrchol.) Komponenta V_1 ale musí mít na hranici stěny S aspoň jednu hranu, nazvěme ji $\{v_1, v_2\}$, a protože G nemá trojúhelník, nemohou oba vrcholy v_1 i v_2 být zároveň spojeny s v. Takže můžeme uvnitř S spojit nějaký vrchol V_i s v_1 nebo s v_2, aniž bychom vytvořili trojúhelník.

Tudíž můžeme předpokládat, že G je 2-souvislý graf. V takovém případě je každá stěna ohraničena kružnicí. Každá taková kružnice má délku aspoň 4 a jsme hotovi. □

Typický chybný důkaz. Řekněmě, že máme rovinné nakreslení grafu s $n \geq 3$ vrcholy, v němž je každá stěna ohraničena třemi hranami, a

chceme dokázat, že takový graf má $3n-6$ hran. Studenti někdy přicházejí s (chybným) řešením podobným následujícímu.

*** **Chybně** *** Postupujeme indukcí podle n. Pro $n = 3$ se jedná o jediný trojúhelník s třemi hranami a třemi vrcholy, tvrzení tedy platí. Dále předpokládejme, že tvrzení platí pro všechny rovinné grafy G na n vrcholech. Do takového grafu G přidáme vrchol do nějaké stěny a spojíme jej s třemi vrcholy té stěny jako na následujícím obrázku:



Tak dostaneme graf G' na $n+1$ vrcholech. Počet hran grafu G je podle indukčního předpokladu $3n-6$ a přidali jsme 3 hrany nové. Tudíž G' má $3(n+1)-6$ hran a tvrzení platí i pro grafy na $n+1$ vrcholech. *** **konec chybného důkazu** ***

Problém je ale v tom, že ne všechny možné rovinné grafy G' na $n+1$ vrcholech a s trojúhelníkovými stěnami se dají zkonstruovat z nějakého G pomocí uvedené operace. Například všechny vrcholy grafu pravidelného osmistěnu (viz obr. 6.1 na str. 216) mají stupeň 4, kdežto v grafech vytvořených uvedenou operací z menších grafů je vždy aspoň jeden vrchol stupně 3.

Cvičení

1. Ukažte, že odhad $|E| \leq 2|V| - 4$ pro rovinné grafy bez trojúhelníků je obecně nejlepší možný. Tedy pro nekonečně mnoho n zkonstruujte rovinné grafy bez trojúhelníků s n vrcholy a $2n-4$ hranami.

2. (a) Ukažte, že libovolné nakreslení rovinného grafu s $n \geq 3$ vrcholy má nejvýš $2n-4$ stěn.

   (b) Ukažte, že pokud uvažovaný graf navíc neobsahuje trojúhelníky, je počet stěn maximálně $n-2$.

3. Řádně odvoďte důsledek 6.5.2 z věty 6.5.1.

4. Dokažte, že rovinný graf, jehož každý vrchol má stupeň aspoň 5, musí mít nejméně 12 vrcholů.

5. Množinou vrcholů *úplného k-partitního grafu* $K_{n_1,n_2,\ldots,n_k}$ je sjednocení $V = V_1 \dot\cup V_2 \dot\cup \cdots \dot\cup V_k$ disjunktních množin $V_1, \ldots, V_k$, kde $|V_i| = n_i$. Každý vrchol $v \in V_i$ je spojen se všemi vrcholy $V \setminus V_i$ pro $i = 1, 2, \ldots, k$. Popište všechny k-tice přirozených čísel $(n_1, n_2, \ldots, n_k)$, $k = 1, 2, \ldots$, pro které je graf $K_{n_1,n_2,\ldots,n_k}$ rovinný.

6.* Mějme maximální rovinný graf $G = (V, E)$ bez trojúhelníků (tj. takový rovinný graf bez trojúhelníků, že pro každou dvojici $\bar e in \binom{V}{2} \setminus E$ je graf $G + \bar e$ nerovinný nebo obsahuje trojúhelník). Dokažte, že každá stěna je čtyřúhelník nebo pětiúhelník.

7. Nechť $G = (V, E)$ je 2-souvislý rovinný graf s nejméně 3 vrcholy. Označme n_i počet vrcholů stupně i, a s_i počet stěn (v nějakém nakreslení) ohraničených kružnicí délky i.

   (a)* Dokažte, že

$$\sum_{i\geq 1}(6-i)n_i = 12 + 2\sum_{j\geq 3}(j-3)s_j,$$

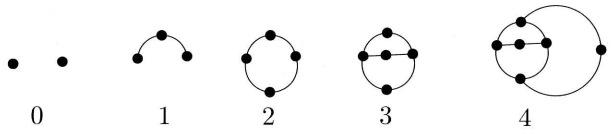
   neboli

$$5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 - n_7 - 2n_8 - \cdots = 12 + 2s_4 + 4s_5 + 6s_6 + \cdots.$$

   (b) Z toho odvoďte, že každý rovinný graf s aspoň 3 vrcholy obsahuje aspoň 3 vrcholy stupně nejvýš 5.

8.* Pro jaké hodnoty k umíte dokázat následující tvrzení? *Existuje n_0 takové, že každý rovinný graf na alespoň n_0 vrcholech obsahuje aspoň k vrcholů stupně maximálně 5.* Mohlo by platit pro *všechna* k?

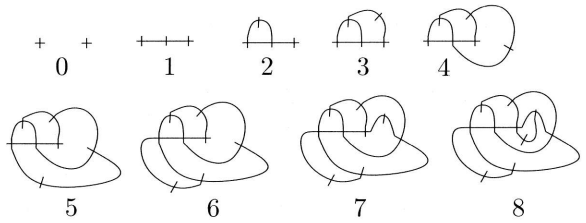
9. (Hra „šprouti“) Následující hru vynalezli J. H. Conway a M. S. Paterson. Anglicky se nazývá *sprouts* („výhonky“). Na papíře je na začátku nakresleno n puntíků (hra je zajímavá už pro malá n, třeba 5). Hráči se střídají v tazích, kdo nemá tah prohraje. V každém tahu hráč spojí dva puntíky obloukem, a někam na tento oblouk nakreslí nový puntík. Puntík se smí použít jako konec nového oblouku jen, pokud z něj vycházejí nanejvýš 2 již nakreslené čáry, a nový oblouk nesmí protnout již nakreslené oblouky (v každém okamžiku máme tedy rovinné nakreslení grafu s maximálním stupněm 3; puntík na nově přidaném oblouku má už stupeň 2). Například:



   (a) Dokažte, že pro n počátečních puntíků má hra nanejvýš $3n - 1$ tahů (při jakékoli strategii hráčů).

   (b)* Dokažte, že pro n počátečních puntíků má hra nejméně $2n$ tahů (při jakékoli strategii hráčů).

   (c)* („Podvodní šprouti“[6]) Modifikujme hru následovně: Místo puntíků se kreslí křížky, a nové oblouky se připojují k ramenům křížků (vrcholy mohou tentokrát mít maximální stupeň 4). Na nový oblouk se křížek přikresluje přeškrtnutím. Viz obrázek:



   Dokažte, že tato hra má vždy přesně $5n - 2$ tahů (takže se dá snadno předem určit kdo vyhraje).

10. Uvažme množinu L sestávající z n přímek v rovině (žádné 2 nejsou rovnoběžné, ale mnoho jich může procházet jedním bodem). Nakreslením těchto přímek vzniknou vrcholy (průsečíky přímek), hrany (části přímek mezi průsečíky, včetně nekonečných polopřímek), a stěny (souvislé části roviny po odebrání přímek).

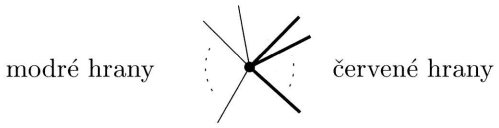
    (a)* Vyjádřete počet hran pomocí počtu vrcholů a počtu stěn.

    (b) Dokažte, že pokud všechny přímky neprocházejí jediným bodem, potom existuje nejvýš n stěn ohraničených jen dvěma hranami.

    (c)* Dokažte, že pokud všechny přímky neprocházejí jedním bodem, pak existuje aspoň jeden průsečík, jímž procházejí právě 2 přímky (to je takzvaný *Sylvesterův problém*).

[6] V originále „Brussels sprouts“; pro čtenáře, který by se chtěl věnovat překladům z angličtiny, může být užitečné vědět, že to znamená růžičková kapusta.

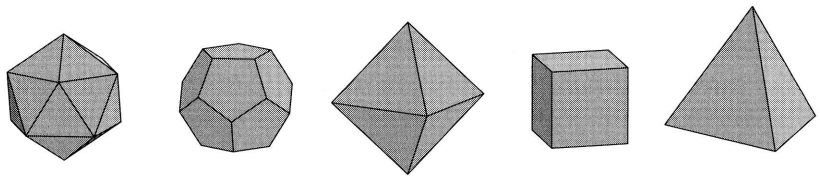
11.** Uvažme libovolné rovinné nakreslení grafu. Předpokládejme, že každé hraně je přiřazena jedna ze dvou barev (červená nebo modrá). Dokažte, že existuje vrchol následujícího typu:



(červené hrany tvoří jeden souvislý úsek při obcházení vrcholu, a podobně modré hrany; jedna ze skupin hran může být i prázdná).

6.6 Platónská tělesa

Antická škola myslitelů spojovaná s Platónovým jménem měla v obzvláštní vážnosti vysoce pravidelné geometrické útvary, takzvané *pravidelné mnohostěny*, které hledala dokonce i v základech stavby vesmíru. (Ostatně i Kepler považoval za jeden ze svých nejdůležitějších objevů teorii – patrně chybnou – podle níž jsou rozestupy mezi drahami planet určeny geometrií pravidelných mnohostěnů.) Pravidelný mnohostěn je trojrozměrné konvexní[7] těleso, ohraničené konečným počtem stěn – shodných pravidelných mnohoúhelníků, jichž se v každém vrcholu stýká stejný počet. Jednou z příčin zmíněného zájmu o pravidelné mnohostěny je patrně jejich výlučnost. Už ve starověku se vědělo, že jich je jen 5 typů: pravidelný čtyřstěn, krychle, pravidelný osmistěn, dvanáctistěn a dvacetistěn (čtenář jistě pozná, který je který).



Ty znali již staří Řekové.

[7]Konvexita znamená, že jsou-li x, y libovolné dva body tělesa, leží i celá úsečka xy uvnitř tělesa, tedy že povrch není nikde „prohnutý dovnitř".

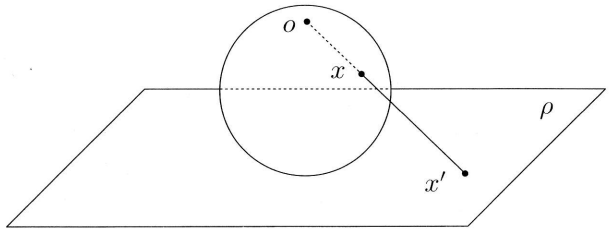
Pokud podmínky pravidelnosti trochu zmírníme (nebudeme trvat na konvexitě, povolíme dva typy stěn atp.), nebo pokud přejdeme do vyšší dimenze, můžeme se setkat s mnoha dalšími zajímavými a krásnými geometrickými ;útvary. Výzkum v této oblasti je stále aktivní.

Pomocí Eulerova vzorce ukážeme, že kromě pěti platónských těles žádné jiné pravidelné mnohostěny existovat nemohou. (To, že zmíněné pravidelné mnohostěny skutečně existují, není samozřejmé a musí se to ověřit geometrickou konstrukcí, čímž se zde zabývat nebudeme.)

Mnohostěny a rovinné grafy. Prvním krokem v dokazování neexistence jiných pravidelných těles bude převedení mnohostěnu na rovinný graf.

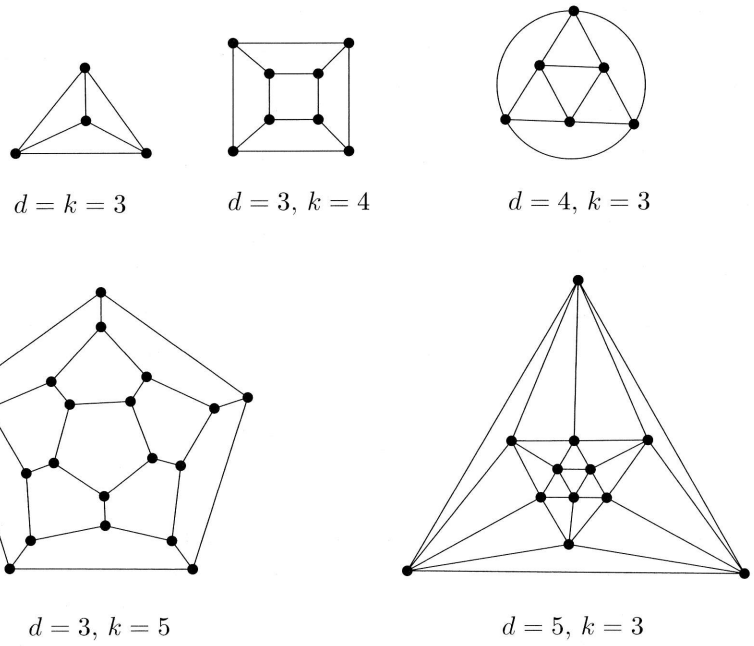
Umístíme zkoumaný mnohostěn dovnitř koule tak, aby střed koule ležel uvnitř mnohostěnu. Promítneme jej ze středu na povrch koule (představte si, že hrany mnohostěnu jsou vyrobeny z drátu a doprostřed namontujeme žárovičku). Tak dostaneme nakreslení nějakého grafu na povrchu koule, čili na sféře, bez křížení hran.

Nyní ukážeme, že graf je rovinný, právě když jej můžeme bez křížení hran nakreslit na povrch koule Opět použijeme vhodnou projekci, tentokrát to bude *stereografická projekce*. Kouli umístíme v třírozměrném prostoru tak, aby se dotýkala promítací roviny ρ, a bod koule nejvzdálenější od roviny ρ („severní pól") označíme o:



Potom stereografická projekce přiřazuje každému bodu $x \neq o$ na povrchu koule bod x' v rovině ρ, kde x' je průsečík přímky ox s rovinou ρ. (Pro bod o se projekce nedefinuje.) Toto je bijekce mezi povrchem koule bez bodu o a rovinou ρ.

Uvažme nějaké nakreslení grafu G na povrchu koule bez křížení hran. Můžeme předpokládat, že o neleží na žádném z oblouků nakres-



Obrázek 6.1: Grafy platónských těles.

lení (pokud by ležel, můžeme sféru vhodně pootočit). Pak stereografickou projekcí dostaneme rovinné nakreslení G – křížení hran nemohou vzniknout díky bijektivitě. Obráceně, z každého rovinného nakreslení vznikne zpětnou projekcí nakreslení na sféře bez křížení hran.

Takto můžeme každý trojrozměrný konvexní mnohostěn převést na rovinné nakreslení grafu. Vrcholy mnohostěnu přejdou na vrcholy grafu, hrany mnohostěnu na hrany grafu, a stěny mnohostěnu na stěny tohoto grafu (odtud také termíny „vrcholy“ a „hrany“ grafu a „stěny“ rovinného nakreslení pocházejí). Pro 5 vyjmenovaných pravidelných mnohostěnů tak obdržíme grafy na obr. 6.1.

Pro každý pravidelný mnohostěn je ve vzniklém rovinném nakreslení zřejmě stejný stupeň d u všech vrcholů (přičemž $d \geq 3$) a každá stěna má na hranici stejný počet vrcholů $k \geq 3$. Neexistence dalších

pravidelných mnohostěnů tedy vyplyne z následujícího:

6.6.1 Tvrzení. *Nechť G je graf s rovinným nakreslením, kde každý vrchol má stupeň $d \geq 3$ a každá stěna má $k \geq 3$ vrcholů. Potom G je isomorfní jednomu z grafů na obr. 6.1.*

Důkaz. Označme n počet vrcholů, m počet hran, a s počet stěn rovinného grafu $G = (V, E)$. Nejprve využijeme vztah $\sum_{v \in V} \deg_G(v) = 2|E|$ (tvrzení 4.4.1), který se v našem případě konkretizuje na

$$dn = 2m.$$

Podobně získáme rovnost

$$ks = 2m.$$

(Dvěma způsoby počítáme počet uspořádaných dvojic (e, S), kde S je stěna grafu G a $e \in E$ je hrana ležící na její hranici. Každá hrana přispěje 2 takovými dvojicemi, poněvadž je každá stěna je ohraničena kružnicí, a každá stěna přispěje k dvojicemi.)

Z právě odvozených vztahů vyjádříme n a s pomocí m a dosadíme do Eulerova vzorce:

$$2 = n - m + s = \frac{2m}{d} - m + \frac{2m}{k}.$$

K rovnici přičteme m, vydělíme ji $2m$ a máme

$$\frac{1}{d} + \frac{1}{k} = \frac{1}{2} + \frac{1}{m}.$$

Jsou-li tedy d i k známa, jsou ostatní parametry (m, n a s) již určeny jednoznačně. Zjevně $\min(d, k) = 3$, protože jinak $\frac{1}{d} + \frac{1}{k} \leq \frac{1}{2}$. Jestliže $d = 3$, potom $\frac{1}{k} - \frac{1}{6} = \frac{1}{m} > 0$, tedy $k \in \{3, 4, 5\}$. Podobně pro $k = 3$ dostaneme $d \in \{3, 4, 5\}$. Tedy nastane jedna z následujících možností:

d	k	n	m	f
3	3	4	6	4
3	4	8	12	6
3	5	20	30	12
4	3	6	12	8
5	3	12	30	20

Nyní je snadné se přesvědčit, že v každém z uvedených případů je graf hodnotami d, k, n, m, s určen jednoznačně a je isomorfní jednomu z grafů na obr. 6.1. □

Poznamenejme ještě, že vztah mnohostěnů v trojrozměrném prostoru a rovinných grafů je těsnější, než by se mohlo zdát. Jak jsme viděli, z každého (konvexního) mnohostěnu dostaneme rovinný graf. Dosti těžká *Steinitzova věta* tvrdí, že pro libovolný vrcholově 3-souvislý rovinný graf G (tj. graf, který po vymazání libovolných 2 vrcholů zůstává souvislý) existuje konvexní trojrozměrný mnohostěn, jehož grafem je právě G. Velmi pěkné shrnutí teorie konvexních mnohostěnů podává Ziegler [31].

Cvičení

1. Najděte příklad (jiný než platónská tělesa) třídimenzionálního konvexního mnohostěnu, jehož všechny stěny jsou shodné s týmž pravidelným mnohoúhelníkem.

   *Dokážete najít všechny možné příklady?

6.7 Kuratowského věta

Úplně na začátku našeho výkladu o rovinných grafech a vlastně i na úplném začátku celé knihy jsme zkoumali otázku, proč $K_{3,3}$ není rovinný graf. Teď na ni můžeme snadno odpovědět pomocí obecného výsledku, věty 6.5.1. Skutečně, $K_{3,3}$ je graf bez trojúhelníků se 6 vrcholy, takže kdyby měl být rovinný, mohl by mít maximálně 8 hran podle části (ii) zmíněné věty, ale přitom má hran 9.

Dalším malým příkladem nerovinného grafu je K_5, úplný graf na 5 vrcholech. Jeho nerovinnost plyne z věty 6.5.1(i), jelikož rovinný graf s pěti vrcholy může mít hran maximálně 9, zatímco K_5 jich má 10.

Ale $K_{3,3}$ a K_5 nejsou jen tak nějaké náhodné příklady nerovinných grafů. V jistém smyslu jsou to ty nejdůležitější příklady: vystupují v pozoruhodné kombinatorické charakterizaci rovinných grafů, charakterizaci, která je čistě grafově-teoretická a nepoužívá naprosto žádné geometrické pojmy.

Abychom mohli tento výsledek formulovat, připomeňme pojem dělení grafu z oddílu 4.7 a učiňme následující jednoduché pozorování: *Graf G je rovinný, právě když jeho libovolné dělení je rovinný graf.*

6.7.1 Věta (Kuratowského věta). *Graf G je rovinný, právě když žádný jeho podgraf není isomorfní dělení grafu $K_{3,3}$ ani dělení grafu K_5.*

Větu je snadno ukázat v jednom směru (pokud G je rovinný, tak nemůže obsahovat dělení nerovinného grafu), opačná implikace je však složitější a v tomto textu ji dokazovat nebudeme.

Z této věty plyne, že nerovinnost libovolného nerovinného grafu můžeme prokázat tím, že v něm najdeme nějaké dělení K_5 nebo $K_{3,3}$. Z algoritmického hlediska, tj. chceme-li skutečně testovat rovinnost grafu na počítači a případně hledat rovinná nakreslení, takový způsob ale příliš vhodný není.

Jsou sice známy algoritmy pro testování, zda vstupní graf obsahuje dělení nějakého pevně daného (malého) grafu, ale ty jsou velmi složité a poměrně nepraktické. Pro testování rovinnosti a hledání „pěkných" rovinných nakreslení byla vynalezena řada efektivních metod, i když jsou také komplikované. Takovými metodami se například dá testovat rovinnost grafu na n vrcholech v čase $O(n)$.

Co se týče „pěkných" nakreslení, je známo, že se každý rovinný graf na n vrcholech dá nakreslit tak, že všechny vrcholy mají celočíselné souřadnice mezi 1 a n a všechny hrany jsou úsečky. Shrnutí výsledků z této oblasti spolu s dalšími odkazy sepsal Kant [16]. Mnoho zajímavých problémů souvisejících s kreslením grafů také ale zůstává otevřených. Neví se například (v době, kdy tuto knihu píšeme), zda se každý rovinný graf dá nakreslit tak, že všechny hrany jsou úsečky s celočíselnými délkami. (To uvádíme jako příklad, jak snadno se někdy v diskrétní matematice dají formulovat i těžké problémy.)

Kuratowského věta charakterizuje rovinné grafy tím, že vymezuje dvě „překážky rovinnosti", konkrétně přítomnost dělení K_5 nebo dělení $K_{3,3}$. V posledních desetiletích bylo objeveno mnoho výsledků v podobném duchu, popisujících různé třídy grafů pomocí konečné množiny „překážek". Překážkami obvykle nebývají zakázaná dělení nějakých grafů, ale spíš takzvané *zakázané minory* (viz cvičení 6.8.9). Tímto a podobnými postupy byly vyřešeny mnohé významné problémy teorie grafů včetně četných otázek týkajících se efektivity algoritmů a v současnosti tato oblast,

zvaná *strukturální teorie grafů*, tvoří jedno z nejdynamičtějších a nejúspěšnějších odvětví moderní teorie grafů. Příkladem pokroku v tomto oboru je práce Robertsona, Seymoura a Thomase [26], ve které byl podobnými metodami vyřešen dlouhodobě otevřený problém.

Cvičení

1. (a) V grafu na obr. 4.2 (str. 130) vlevo nalezněte buď dělení grafu K_5, nebo dělení grafu $K_{3,3}$.
   (b) Je graf na obr. 4.2 uprostřed rovinný?
   (c) Je graf na obr. 9.1(b) (str. 284) rovinný?
2.* Uvažme (ne nutně rovinné) nakreslení úplného grafu K_n, kde všechny hrany jsou nakresleny jako úsečky. Ukažte, že aspoň $\frac{1}{5}\binom{n}{4}$ dvojic hran se protíná. (Využijte nerovinnosti grafu K_5.)

6.8 Barvení map – problém čtyř barev

Uvažme politickou mapu, na níž jsou vyznačeny hranice států:

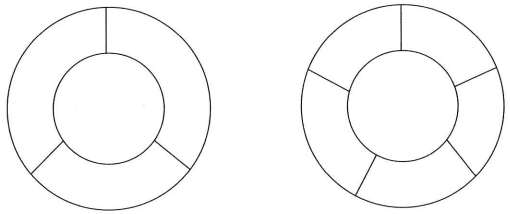


Předpokládejme, že každý stát tvoří souvislou oblast ohraničenou nějakou topologickou kružnicí (proto jsme na naši schematickou mapu nenakreslili ostrovy jako Sardinie, Sicílie, Korsika atd. a taky jsme vynechali Rusko – v době psaní této kapitoly stát nesouvislý!). Dvě oblasti pokládáme za sousední, jestliže mají společný aspoň kousek hranice, tj. nestačí, když se hranice dotýkají jen v jednom nebo několika bodech (takové případy se na mapách stejně vyskytují jen velmi vzácně). Každý stát na mapě chceme vybarvit nějakou barvou, a to tak, že sousedící státy nikdy nedostanou stejnou barvu (jak je na politických mapách zvykem). Kolik barev budeme určitě potřebovat? Pro uvedenou mapu stačí 4 barvy (zkuste takové obarvení najít!).

Jedním z nejznámějších kombinatorických problémů je následující otázka:

6.8.1 Úloha (Problém čtyř barev). *Je možno každou mapu obarvit 4 barvami?*

Čtyři je určitě minimální počet barev, který připadá obecně v úvahu. To je ilustrováno výše uvedenou mapou (uvažte např. Lucembursko nebo Rakousko) a následujícími příklady:



Zde dokážeme, že každou mapu lze obarvit 5 barvami. Přesto, že je tento výsledek znám už od konce 19. století, problém čtyř barev byl rozřešen (kladně) teprve roku 1976.

Všechny známé důkazy toho, že každou mapu lze obarvit 4 barvami, jsou obtížné a podstatně závisí na probírání mnoha případů počítačem. Zatím se nikomu nepodařilo důkaz udělat ručně, i když původní důkaz byl velmi zjednodušen v roce 1995 (Robertson a spol. [25]). V roce 2004 Gonthier [11] zkonstruoval důkaz, který je plně ověřitelný

počítačem: Větu zapsal v jistém formálním jazyce, a v témže jazyce vygeneroval i důkaz, jehož správnost se dá plně automaticky ověřit pomocí poměrně jednoduchého obecného programu. Jedině to, že formální zápis skutečně vyjadřuje znění věty, musí v tomto postupu stále zkontrolovat člověk.

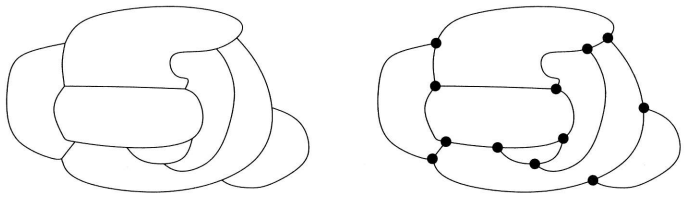
Některé základní myšlenky důkazů věty o čtyřech barvách se objevují i ve dvou důkazech „věty o pěti barvách", jež vzápětí popíšeme.

Problém čtyř barev vypadá jako otázka geometrická, ale dá se přeformulovat ryze kombinatoricky. Barvení map totiž jednoduše souvisí s barvením grafů. Nejdřív definujeme barevnost pro libovolný graf.

6.8.2 Definice (Barevnost grafu). *Buď $G = (V, E)$ graf, k přirozené číslo. Zobrazení $b : V \to \{1, 2, \ldots, k\}$ nazveme* obarvením grafu G pomocí k barev, *pokud pro každou hranu $\{x, y\} \in E$ platí $b(x) \neq b(y)$.* Barevnost *grafu G, označovaná $\chi(G)$, je minimální počet barev potřebný pro obarvení G.*

Barevnost grafu patří mezi základní kombinatorické pojmy, v našem úvodním textu se o ní však zmíníme pouze v tomto článku.

Matematicky můžeme mapu chápat jako nakreslení nějakého rovinného grafu, přičemž státy na mapě jsou stěny tohoto grafu (vrcholy grafu budou body ležící na hranici alespoň 3 států a hranami budou odpovídající části oblouků mezi jednotlivými vrcholy):



Je vidět, že přitom mohou vzniknout i násobné hrany.

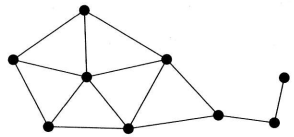
Abychom převedli problém barvení mapy, čili barvení stěn rovinného nakreslení grafu, na barevnost grafu ve smyslu právě uvedené definice, zavedeme tzv. duální graf. Představte si, že bychom v každém státě tečkou označili hlavní město. Hlavní města sousedních států by spojovala dálnice vedoucí po území těchto dvou států a překračující

jejich společnou hranici. Potom by hlavní města byla vrcholy duálního grafu a dálnice by tvořily jeho hrany.

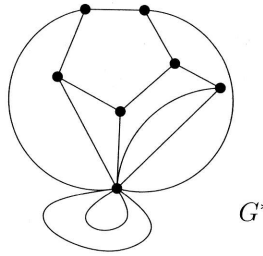
Budeme také obecně potřebovat násobné hrany a smyčky; připomeňme si tedy jeden způsob jejich zavedení. Graf s násobnými hranami můžeme chápat jako trojici (V, E, ε), kde V, E jsou nějaké (disjunktní) množiny a $\varepsilon : E \to \binom{V}{2} \cup V$ je zobrazení přiřazující hraně dvojici jejích konců, příp. smyčce její jediný vrchol (podrobněji se tento způsob reprezentace násobných hran a smyček probíral v části 4.5). Teď můžeme pokročit k matematické definici duálního grafu:

6.8.3 Definice (Duální graf). *Nechť G je graf s daným rovinným nakreslením, s množinou vrcholů V, množinou hran E a množinou stěn S. Definujme graf tvaru (S, E, ε), kde ε se definuje předpisem $\varepsilon(e) = \{S_i, S_j\}$, jestliže hrana e je společnou hranicí stěn S_i a S_j (přičemž se může stát, že $S_i = S_j$, jestliže z obou stran hrany e je táž stěna). Tento graf (S, E, ε) nazýváme* (geometrickým) duálem *grafu G a značíme jej G^*.*

Zde je příklad grafu a jeho duálu:



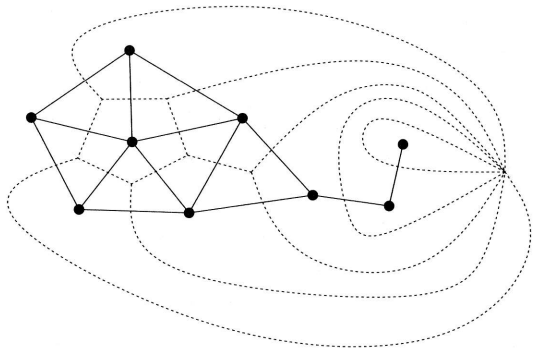
G



G^*

Jak jsme již naznačili neformálním popisem s městy a dálnicemi, můžeme graf G^* znázornit společně s nakreslením grafu G. Uvnitř každé stěny S grafu G zvolíme bod b_S, a každé hraně e přiřadíme oblouk, protínající hranu e a spojující body b_S a $b_{S'}$, kde S a S' jsou stěny přiléhající k hraně e.

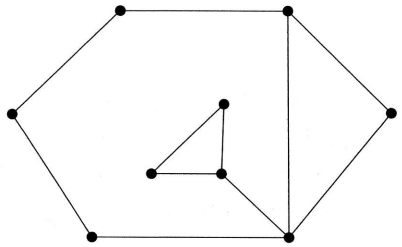
Tento oblouk leží celý ve stěnách S a S'. Tím získáme nakreslení grafu G^*:



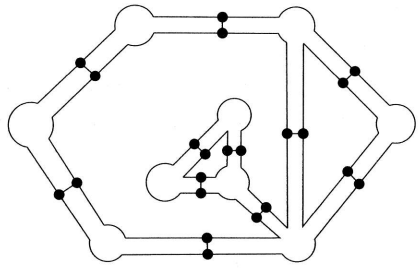
Z tohoto způsobu kreslení duálního grafu plyne jeho rovinnost. Další příklady najde čtenář na obr. 6.1 (str. 216): grafy krychle a pravidelného osmistěnu jsou navzájem duální, podobně grafy dvanáctistěnu a dvacetistěnu, a konečně graf pravidelného čtyřstěnu (čili K_4) je duální sám k sobě.

Máme-li tedy mapu, již chápeme jako nakreslení nějakého grafu G, potom je otázka obarvitelnosti mapy pomocí k barev ekvivalentní s obarvitelností duálního grafu G^* pomocí k barev.

Na druhé straně platí, že každý rovinný graf se vyskytne jako podgraf vhodného duálního grafu. Důkaz naznačíme pouze obrázkem. Například graf



je obsažen v duálu grafu



(Jinak by se také dalo argumentovat tím, že každý rovinný graf je isomorfní duálu svého duálu.) Takto lze převést problematiku barvení map na na otázky týkající se barevnosti rovinných grafů. Speciálně můžeme přeformulovat:

6.8.4 Úloha (Problém čtyř barev podruhé). *Platí $\chi(G) \leq 4$ pro každý rovinný graf G?*

Dokážeme slabší výsledek:

6.8.5 Tvrzení (Věta o 5 barvách). *Pro každý rovinný graf G platí $\chi(G) \leq 5$.*

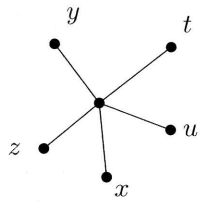
První důkaz. Postupujeme indukcí dle počtu vrcholů grafu $G = (V, E)$. Pro $|V| \leq 5$ je tvrzení triviální.

Podle důsledku 6.5.2 víme, že v každém rovinném grafu existuje vrchol v stupně nejvýš 5. Jestliže $\deg_G(v) < 5$, potom uvažme graf $G' = G - v$ a použijme pro něj indukčního předpokladu: je-li graf G' obarvený pomocí barev $1, 2, \ldots, 5$, potom v přiřaďme nějakou barvu $i \in \{1, 2, \ldots, 5\}$, jež se nevyskytuje mezi barvami (nejvýš 4) sousedů vrcholu v. Tak dostaneme obarvení grafu G pěti barvami.

Velmi podobná argumentace vlastně již dokazuje, že barevnost rovinného grafu je nejvýš 6, takže se ve zbytku důkazu budeme snažit těchto 6 zlepšit na 5.

Také je poučné na základě tohoto důkazu sestavit algoritmus na barvení rovinných grafů nejvýš 6 barvami (nebo s vylepšením z následujícího nejvýš 5 barvami). Uvědomte si, že takový algoritmus obarvuje vrchol v s malým stupněm až nakonec, když jsou všechny ostatní vrcholy už obarveny!

Zbývá vyšetřit případ, kdy $\deg_G(v) = 5$. Uvažme graf G s pevně zvoleným rovinným nakreslením a nechť t, u, x, z, y jsou vrcholy spojené s vrcholem v hranou, vypsané v pořadí, v němž příslušné hrany vycházejí z vrcholu v (např. ve směru hodinových ručiček).



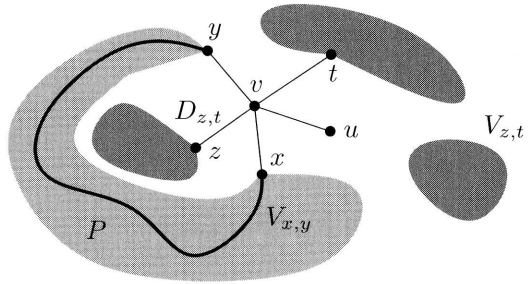
Uvažme opět obarvení $b' : V(G') \to \{1, 2, \ldots, 5\}$ grafu $G' = G - v$ pomocí 5 barev (zaručené indukčním předpokladem). Jestliže se mezi barvami sousedů vyskytují maximálně čtyři barvy, můžeme vrcholu v přiřadit barvu různou od barev jeho sousedů. Předpokládejme tedy, že sousedi v mají všech 5 různých barev. Uvažme vrcholy x a y, a nechť $V_{x,y}$ je množina všech vrcholů grafu G', které mají buď barvu $b'(x)$ nebo barvu $b'(y)$. Zřejmě $x, y \in V_{x,y}$. Rozlišíme dva případy podle toho, zda v grafu G' existuje cesta z x do y používající jen vrcholy z množiny $V_{x,y}$, nebo neexistuje.

1. Taková cesta neexistuje. Označme $D_{x,y}$ množinu těch vrcholů $s \in V(G')$, které jsou v grafu G' spojeny s vrcholem x cestou, používající pouze vrcholy z množiny $V_{x,y}$ (D jako dosažitelné vrcholy). Speciálně platí $y \notin D_{x,y}$. Definujme nové obarvení b grafu G' předpisem:

$$b(s) = \begin{cases} b'(s) & \text{pokud } s \notin D_{x,y} \\ b'(y) & \text{pokud } s \in D_{x,y} \text{ a } b'(s) = b'(x) \\ b'(x) & \text{pokud } s \in D_{x,y} \text{ a } b'(s) = b'(y) \end{cases}$$

(to znamená, že na množině $D_{x,y}$ zaměníme barvy). Zřejmě b je opět obarvení, a protože $b(x) = b(y) = b'(y)$, můžeme položit $b(v) = b'(x)$. Tedy b je obarvení grafu G pěti barvami.

2. Nyní předpokládáme, že z x do y existuje cesta P, jejíž všechny vrcholy jsou prvky množiny $V_{x,y}$. V tom případě uvážíme dvojici vrcholů z, t a definujeme množinu $V_{z,t}$ jako množinu všech těch vrcholů, které jsou obarveny pomocí barev $b'(t)$ a $b'(z)$. Množiny $V_{x,y}$ a $V_{z,t}$ jsou disjunktní. Nakreslení cesty P spolu s hranami $\{v, x\}$ a $\{v, y\}$ tvoří kružnici:



Ta má jeden z bodů z, t uvnitř a druhý vně, a proto každá cesta ze z do t musí používat některý vrchol zmíněné kružnice. Tudíž neexistuje cesta ze z do t používající pouze vrcholy množiny $V_{z,t}$ a můžeme zkonstruovat obarvení grafu G pěti barvami stejně jako v případě 1, jenom místo vrcholů x, y začneme s vrcholy t, z.

Tím je první důkaz věty o pěti barvách hotov. □

Kontrakce hran. Než začneme s druhým důkazem, zavedeme další důležitou grafovou operaci. Buď $G = (V, E)$ graf (ne nutně rovinný) a $e \in E$ jeho hrana. *Kontrakce* hrany e znamená, že oba vrcholy hrany e „slepíme" do jednoho nového vrcholu a odstraníme případné násobné hrany, které při lepení vznikly. Výsledný graf budeme značit $G.e$ a formálně bude definován takto:

$$G.e = (V', E'),$$

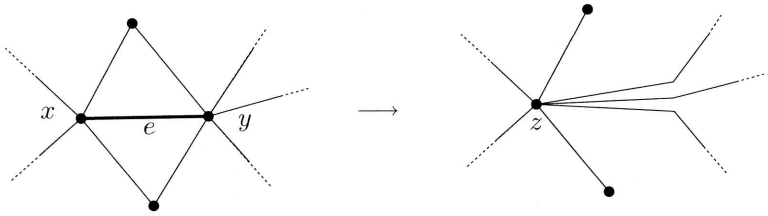
kde $e = \{x, y\}$ a

$$\begin{aligned} V' &= (V \setminus \{x, y\}) \cup \{z\} \\ E' &= \{e \in E;\ e \cap \{x, y\} = \emptyset\} \cup \\ &\qquad \{\{z, t\};\ t \in V \setminus \{x, y\},\ \{t, x\} \in E \text{ nebo } \{t, y\} \in E\}; \end{aligned}$$

přitom $z \notin V$ značí nový vrchol.

Lemma. *Je-li G rovinný graf a $e \in E(G)$, je graf $G.e$ opět rovinný.*

Neformální důkaz. Viz obrázek:



□

Druhý důkaz tvrzení 6.8.5. Postupujeme opět indukcí podle počtu vrcholů uvažovaného rovinného grafu $G = (V, E)$. Začneme stejně jako v prvním důkazu.

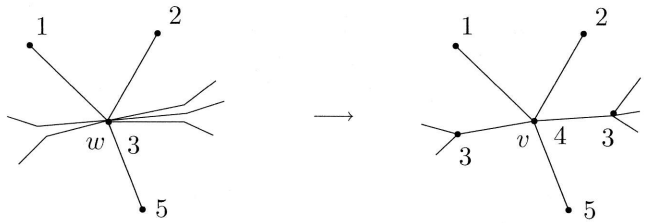
Můžeme tedy předpokládat, že $G = (V, E)$ je rovinný graf s alespoň 6 vrcholy, v němž každý vrchol má stupeň alespoň 5. Zvolme vrchol v stupně 5. Protože je graf G rovinný, neobsahuje K_5 jako podgraf, a tedy existuje dvojice sousedů vrcholu v, jež netvoří hranu. Označme nějakou takovou dvojici sousedů x, y, a zbývající tři sousedy t, u a z.

Uvažme graf G' vzniklý z G kontrakcí hran $\{x, v\}$ a $\{y, v\}$ (tj. trojice vrcholů x, y, v je nahrazena jediným novým vrcholem w, což zobecňuje definici kontrakce hrany zjevným způsobem).

Tento graf je opět rovinný, a má méně vrcholů než G, tedy podle indukčního předpokladu existuje nějaké jeho obarvení b' pomocí 5 barev. V této situaci definujeme obarvení b grafu G takto:

$$b(s) = \begin{cases} b'(s), & \text{pro } s \notin \{x, y, v\}, \\ b'(w), & \text{pro } s \in \{x, y\}, \\ i \in \{1, \ldots, 5\} \setminus \{b'(w), b'(u), b'(t), b'(z)\}, & \text{pro } s = v. \end{cases}$$

Viz obrázek:



situace v G' situace v G

Je snadné nahlédnout, že takto definované zobrazení b je skutečně obarvením grafu G. □

Ve cvičení 11 je nastíněn ještě další důkaz.

Cvičení

1. Dokažte, že
$$\chi(G) \leq 1 + \max\{\deg_G(x); x \in V(G)\}$$
pro každý (konečný) graf $G = (V, E)$.

2. Pro graf G položte $\delta(G) = \min\{\deg_G(v);\ v \in V\}$ (*minimální stupeň* v G). Dokažte $\chi(G) \leq 1 + \max\{\delta(G');\ G' \subseteq G\}$, kde $G' \subseteq G$ značí, že G' je podgrafem G.

3.* Graf G nazveme *vnějškově rovinným*, existuje-li jeho nakreslení, v němž hranice některé ze stěn obsahuje všechny vrcholy (můžeme předpokládat, že tuto vlastnost má stěna vnější). Dokažte, že každý vnějškově rovinný graf má barevnost nejvýš 3.

4. Buď G rovinný graf, který neobsahuje K_3 jako podgraf. Dokažte, že $\chi(G) \leq 4$. (Grötsch dokázal těžkou větu, která říká, že pro všechny rovinné grafy bez trojúhelníka platí dokonce $\chi(G) \leq 3$.)

5. Na základě některého ze dvou uvedených důkazů sestavte algoritmus pro obarvení daného rovinného grafu 5 barvami. Můžete předpokládat, že jeho rovinné nakreslení je zadáno následovně: pro každý vrchol v grafu G máme cyklický seznam sousedů v sepsaný podle pořadí, jak odpovídající hrany v nakreslení vycházejí z v.

6. (a) Uvažme hladový algoritmus pro barvení grafů. Zvolíme libovolně jeden z dosud neobarvených vrcholů a obarvíme nejmenší barvou (barvy jsou přirozená čísla $1, 2, \ldots$), která není použita na žádném z dosud

obarvených sousedů. Pro všechna čísla K nalezněte graf G, pro který existuje obarvení dvěma barvami (tj. je bipartitní), ale právě popsaný algoritmus jej někdy (tj. při nešikovném pořadí barvení vrcholů) obarví alespoň K barvami.

(b) Dokážete najít rovinný graf G s vlastnostmi jako v (a)?

(c) Algoritmus můžeme vylepšit následujícím způsobem: ze zatím neobarvených vrcholů vybereme ten, který má nejvyšší stupeň a obarvíme jej stejně jako v (a). Ukažte, že pořád existují grafy G jako v (a).

(d) Můžete si zahrát i hru na toto téma. Hráči navrhují verze hladového algoritmu na barvení grafů a protivníci se snaží nacházet grafy, které algoritmus obarví nešikovně.

7. Dokažte, že každý graf G má aspoň $\binom{\chi(G)}{2}$ hran.

8. (a)* Uvažme rovinný graf, jehož všechny stupně jsou sudé. Ukažte, že mapa vzniklá jeho rovinným nakreslením se dá obarvit dvěma barvami.

   (b)* Pomocí (a) ukažte, že neexistuje žádné rovinné nakreslení grafu, kde všechny stupně vrcholů jsou sudé, všechny vnitřní stěny jsou trojúhelníky (tj. ohraničené kružnicemi délky 3) a vnější stěna je pětiúhelník.

9.* Řekněme, že graf H je *minor* grafu G, pokud je možné z grafu G vytvořit graf isomorfní grafu H opakovaným použitím následujících operací: vymazání hrany, vymazání izolovaného vrcholu, kontrakce hrany. Z Kuratowského věty odvoďte: *Graf G je rovinný právě tehdy, když ani K_5, ani $K_{3,3}$ není minorem G.*

10. (Výběrová barevnost) Nechť $G = (V, E)$ je graf a předpokládejme, že pro každý vrchol $v \in V$ je dán konečný seznam přirozených čísel $L(v)$. Zobrazení $b : V \to \mathbf{N}$ se nazývá *výběrové obarvení* (vzhledem k daným seznamům $L(v)$, $v \in V$), pokud pro všechny vrcholy $v \in V$ platí $b(v) \in L(v)$ a pro všechny hrany $\{v, v'\} \in E$ platí $b(v) \neq b(v')$. *Výběrová barevnost* grafu G (označovaná $\chi_\ell(G)$) je nejmenší číslo k takové, že pro libovolný systém seznamů $L(v)$, $v \in V$, splňující $|L(v)| \geq k$ pro všechna $v \in V$, má G výběrové obarvení.

    (a) Nalezněte příklad grafu s $\chi_\ell(G) > \chi(G)$.

    (b)* Pro všechna přirozená čísla k zkonstruujte bipartitní graf G, pro který $\chi_\ell(G) > k$.

    Poznámka. Existuje rovinný graf G s $\chi_\ell(G) = 5$. Tedy „výběrová verze“ věty o čtyřech barvách neplatí.

11.* Pojem výběrového obarvení z předchozího cvičení se používá v krátkém a pozoruhodném Thomassenově důkazu věty o pěti barvách 6.8.5, který naznačíme v tomto cvičení.

Dokažte následující tvrzení indukcí dle počtu vrcholů:

Nechť $G = (V, E)$ je graf s daným rovinným nakreslením a nechť $L(v)$, $v \in V$, jsou seznamy, přičemž platí následující:

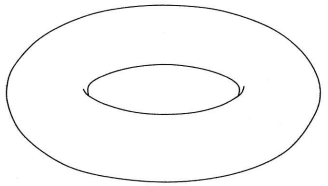
- Hranicí neomezené stěny je kružnice C s vrcholy $v_1, v_2, \ldots, v_k$ (číslováno po obvodu).
- Všechny omezené stěny jsou trojúhelníky.
- $L(v_1) = \{1\}$, $L(v_2) = \{2\}$.
- $|L(v_i)| = 3$ pro $i = 3, 4, \ldots, k$.
- $|L(v)| = 5$ pro všechny ostatní vrcholy kromě v_i (tj. ležící uvnitř hraniční kružnice C).

Potom G má výběrové obarvení vzhledem k seznamům $L(v)$.

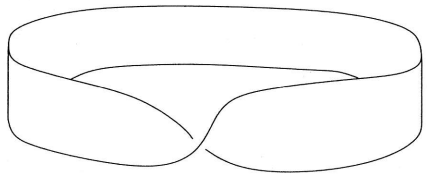
Tento důkaz nevyužívá ani Eulerův vzorec, ani přítomnost vrcholu s malým stupněm. Je to příklad matematické indukce *par excellence.*

6.9 Kreslení grafů na plochách

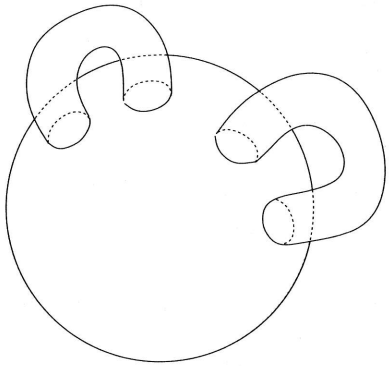
Graf G můžeme nakreslit i na jiné „plochy“, než je rovina, např. na sféru (tj. povrch koule), na anuloid (někdy zvaný též torus),



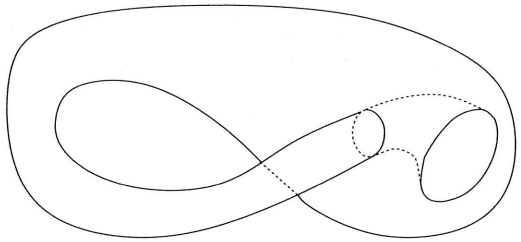
na Möbiův list,



na sféru s „dvěma ušima“

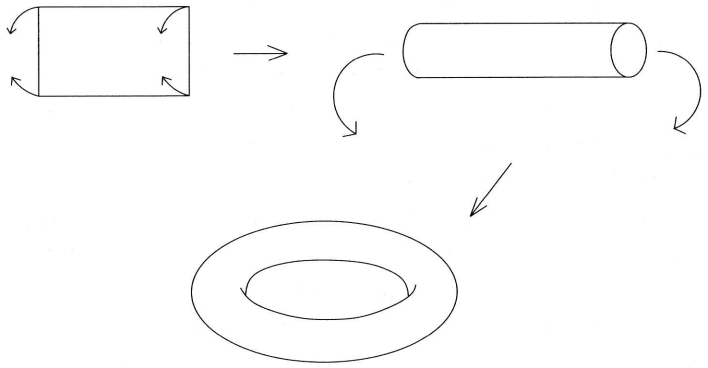


(což je po vhodné deformaci totéž jako povrch „tlusté osmičky“), nebo na tzv. *Kleinovu láhev*:

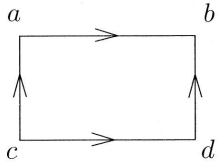


Takové plochy se dají vytvářet „slepováním“ a vhodnou deformací z rovinného mnohoúhelníka. Ve výše uvedených příkladech, s výjimkou sféry se dvěma ušima, vyjdeme vždy z obdélníka a vhodně ztotožníme (slepíme) jeho strany. Tento postup je i základem přesné definice těchto ploch (již zde neuvádíme).

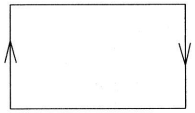
Tak například anuloid lze vytvořit následujícím způsobem:



neboli ztotožníme protější hrany obdélníka $abcd$, přičemž strana ab se slepí se stranou dc a strana ad se stranou bc. Orientace při lepení se obvykle vyznačuje šipkami; šipky na následujícím obrázku znamenají, že při slepování stran ad a bc přijde bod a k bodu b a bod d k bodu c.

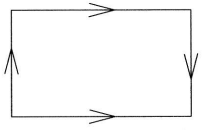


Möbiův list vyrobíme takhle:



(ztotožníme pouze hrany označené šipkou tak, že směr obou šipek souhlasí).

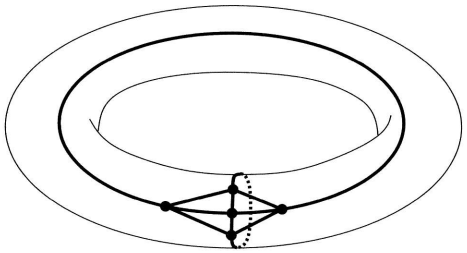
Kleinova láhev vznikne následovně:



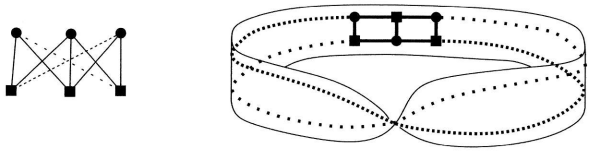
Tohle ve skutečnosti není poctivý návod na výrobu Kleinovy láhve, protože ve třídimenzionálním eukleidovském prostoru se podle něj postupovat nedá. Naznačené lepení nelze realizovat v $\mathbf{R}^3$, aniž by obdélník protínal sám sebe (jako na našem obrázku Kleinovy láhve). Matematicky nicméně definice Kleinovy láhve poslepováním smysl dává a například v $\mathbf{R}^4$ se tato plocha vytvořit dá.

Platí obecná věta, která zaručuje, že se každá uzavřená plocha (která nemá žádné „hraniční body“ a nikde „neutíká do nekonečna“, čemuž se odborně říká „kompaktní 2-dimenzionální varieta bez okraje“) dá vytvořit pomocí vhodného poslepování a deformace pravidelného konvexního mnohoúhelníka. Navíc, pokud má uvažovaná plocha dvě strany (Möbiův list i Kleinova láhev mají jenom jednu stranu!), potom ji lze spojitě deformovat na nějakou sféru s konečně mnoha ušima. Velmi pěkně a názorně jsou základy této teorie a řada souvisejících věcí popsány například v knize [28].

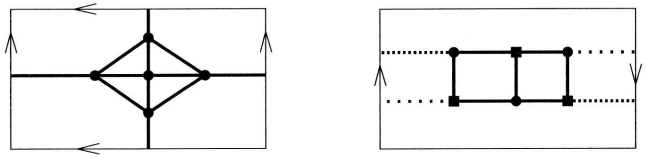
Grafy můžeme rozlišovat podle plochy, na niž je lze nakreslit bez křížení hran. Jak víme, ani graf K_5 (úplný graf na 5 vrcholech), ani graf $K_{3,3}$ (úplný bipartitní graf na $3+3$ vrcholech) není rovinný. Přitom ale například K_5 lze nakreslit na torus:



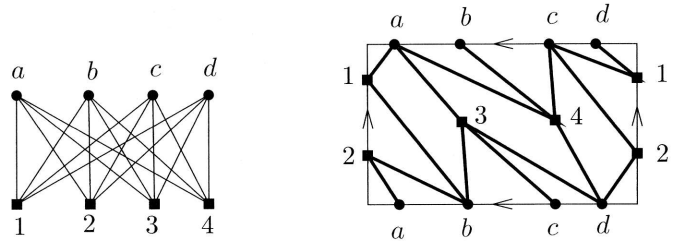
a $K_{3,3}$ na Möbiův list:



Jak jsme řekli, tyto plochy můžeme vyrábět vhodným slepováním hran obdélníků. Abychom nemuseli přepínat svou prostorovou představivost, můžeme kreslení na plochách převést na modifikované rovinné kreslení, kde hrany mohou „přeskakovat“ mezi slepovanými stranami. Právě uvedená nakreslení lze potom znázornit takto:



Poznamenejme, že na torus lze nakreslit dokonce graf $K_{4,4}$

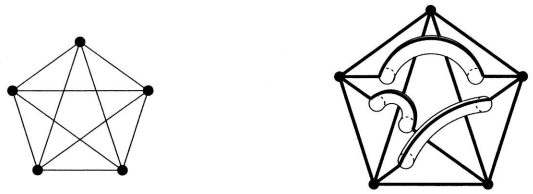


(K_7 se dá nakreslit také, viz cvičení 1). Obecně platí

6.9.1 Tvrzení. *Každý graf lze nakreslit na sféru s dostatečným počtem „uší“.*

(Toto tvrzení je třeba chápat intuitivně, neb jsme přesnou definici sféry s ušima nepodali.)

Neformální důkaz. Nakresleme graf $G = (V, E)$ na povrch koule, třeba i s křížením hran. Nechť $e_1, \ldots, e_n$ jsou všechny hrany, které se kříží s nějakou jinou hranou. Pro každou hranu e_i přidejme „ucho“, které pro ni bude sloužit jako „most“ přes ostatní hrany. Tyto mosty přidáváme tak, aby byly disjunktní a přitom hrany nakreslené na příslušných přemostěních se již nekřížily:



Vzhledem k tomu, že máme co činit pouze s konečným počtem hran, takové mosty snadno najdeme. □

Následující definice má tedy smysl:

6.9.2 Definice. *Minimální počet „uší", které je třeba přidat ke sféře, aby na vzniklou plochu bylo možno nakreslit graf G bez křížení hran, nazýváme* rod[8] *grafu G.*

V oddílu 6.8 jsme se zabývali otázkou barvení rovinných grafů. Jak jsme ukázali v oddílu 6.6, rovinné grafy jsou právě ty, které se dají nakreslit na sféru bez křížení hran, tedy grafy rodu 0.

Viděli jsme, že se vrcholy každého rovinného grafu dají obarvit pěti barvami, aniž by sousední vrcholy někdy byly obarveny stejnou barvou, a zmínili jsme se o velmi těžké větě o čtyřech barvách, která říká, že čtyři barvy vždycky stačí.

Podobně můžeme zkoumat otázku barevnosti grafů i na jiných plochách. Tato otázka je dnes beze zbytku vyřešena: maximální barevnost grafu G rodu k je rovna číslu

$$\left\lfloor \frac{7+\sqrt{1+48k}}{2} \right\rfloor .$$

Je pozoruhodné, že případ rodu 0, neboli rovinných grafů, je zdaleka nejtěžší – pro ostatní rody je tento výsledek (Heawoodův vzorec) mnohem snazší a byl dokázán dávno před vyřešením problému čtyř barev.

Cvičení

1. (a) Přesvědčte se, že obrázek v textu skutečně dává nakreslení $K_{4,4}$ na anuloid.
   (b) Nalezněte nakreslení grafu K_6 na anuloid.
   (c)* Nakreslete K_7 na anuloid.

[8]Pojem rodu se primárně používá pro plochy. Například rod sféry s ušima je roven počtu uší. Je zajímavé, že 2-dimenzionální plochy se začaly systematicky studovat v souvislosti s algebraickými rovnicemi! Množina všech nulových bodů (v komplexním oboru) mnohočlenu ve dvou proměnných je typicky 2-dimenzionální plocha, jejíž rod je pro různé vlastnosti mnohočlenu zásadní. Náročná oblast matematiky, která v tomto duchu zkoumá algebraické rovnice, se nazývá *algebraická geometrie*. (Pěkný úvod do tohoto předmětu napsali Cox, Little a O' Shea [8].)

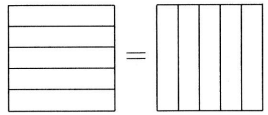
7

Počítání dvěma způsoby

Počítání dvěma způsoby používali například účetní, když ještě neměli počítače. Když chtěli bezchybně sečíst tabulku čísel, sčítali jednou napřed po sloupcích a jednou napřed po řádcích; pokud počítali správně, vyšlo totéž. Matematicky vyjádřeno, je-li A libovolná matice $n \times m$, platí

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij} = \sum_{j=1}^{m}\sum_{i=1}^{n} a_{ij},$$

schematicky



Jinak řečeno, v takovéto dvojité sumě můžeme podle potřeby zaměnit pořadí sumace. Na této prosté myšlence je založeno mnoho matematických triků a důkazů; v těch složitějších jsou pochopitelně navíc další nápady a obraty, hlavně se většinou musí přijít na to, co vlastně počítat dvěma způsoby.

7.1 Princip sudosti

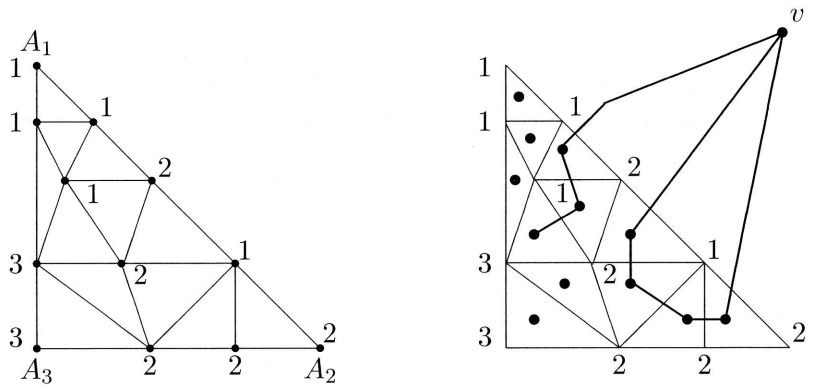
V části 4.4 jsme nahlédli, že *libovolný graf má sudý počet vrcholů lichého stupně.* (To platí i pro grafy s násobnými hranami.) Důkaz byl vlastně typické počítání dvěma způsoby (počítali jsme „konce hran"). Pomocí tohoto tvrzení jsme mohli někdy snadno vyloučit některé vektory jako možné skóre grafu, třeba vektor $(3,3,3,3,3)$. Tvrzení lze však použít i mnohem zajímavěji, například na důkaz existence nějakého objektu. K takovému účelu je vyslovíme v takovémto tvaru: *Víme-li, že graf G má aspoň jeden vrchol lichého stupně, potom musí mít aspoň 2 takové vrcholy.* Aplikace následuje.

Nakresleme do roviny velký trojúhelník s vrcholy označenými A_1, A_2, A_3 a rozdělme jej libovolně na konečný počet menších trojúhelníčků (jako na obr. 7.1(a)). Žádný trojúhelníček nesmí mít vrchol uvnitř strany jiného trojúhelníčku, tj. díváme-li se na obrázek jako na nakreslení rovinného grafu, jsou všechny vnitřní stěny trojúhelníky. Přiřaďme dále každému vrcholu velkého i malých trojúhelníků jedno z čísel 1,2,3: vrchol A_i dostane vždy číslo i, $i = 1,2,3$, a všechny vrcholy ležící na straně A_iA_j velkého trojúhelníka dostanou jen čísla i a j; mimo těchto pravidel je přiřazení naprosto libovolné.

7.1.1 Tvrzení (Spernerovo lemma – rovinná verze). *V popsané situaci vždy existuje trojúhelníček, jehož vrcholy dostanou čísla 1, 2 a 3.*

Důkaz. Definujeme pomocný graf G, viz obr. 7.1(b). Jeho vrcholy budou stěny nakreslené triangulace, tj. všechny trojúhelníčky a také vnější stěna. Na obrázku jsme vrcholy znázornili kroužky zakreslenými do příslušných stěn; vrchol vnější stěny je označen v. Dva vrcholy, tj. stěny, budou spojeny hranou, pokud spolu hraničí přes stranu některého trojúhelníčku, a pokud *koncové vrcholy této strany mají čísla 1 a 2.* To se týká i vnějšího vrcholu v: ten bude spojen se všemi trojúhelníčky přiléhajícími k obvodu velkého trojúhelníka stranou 12.

Stupeň trojúhelníčku v grafu G je nenulový pouze tehdy, je-li jeden z vrcholů očíslován 1 a jeden 2. Má-li zbývající vrchol také číslo 1 nebo



(a) (b)

Obrázek 7.1: Situace ve Spernerově lemmatu (a), odpovídající graf stěn (b).

2, je stupeň 2. Pokud zbývající vrchol má číslo 3, je stupeň 1, a *to je jediný případ, kdy je stupeň lichý.* Ukážeme nyní, že vrchol v (vnější stěna) má v grafu G lichý stupeň; tím pádem existuje v G ještě jiný vrchol lichého stupně, a to je hledaný trojúhelníček očíslovaný 1,2,3.

Hrany grafu G mohou zřejmě křižovat pouze stranu A_1A_2 velkého trojúhelníka. Podle pravidel očíslování jsou na této straně povoleny jen vrcholy trojúhelníčků s čísly 1 a 2. Napíšeme-li libovolnou posloupnost jedniček a dvojek začínající 1 a končící 2, potom počet míst, kde končí úsek jedniček a začíná úsek dvojek nebo obráceně je lichý (jdeme-li odleva doprava, po sudém počtu změn mezi jedničkami a dvojkami jsme v jedničce). Proto je stupeň v je lichý. □

Spernerovo lemma není jen samoúčelná hříčka, s jeho pomocí se dá dokázat tzv. Brouwerova věta o pevném bodě. Než řekneme, co tvrdí, uvedeme velmi jednoduchou větu o pevném bodě jako motivaci.

7.1.2 Tvrzení. *Pro každou spojitou funkci $f : [0,1] \to [0,1]$ existuje bod $x \in [0,1]$ takový, že $f(x) = x$.*

Takové x se jmenuje *pevný bod* funkce f. Tvrzení můžeme dokázat

takto: funkce $g(x) = f(x) - x$ je spojitá, $g(0) \geq 0$, $g(1) \leq 0$ a intuitivně se zdá celkem zřejmé, že graf spojité funkce g nemůže osu x nijak přeskočit a tedy ji musí protnout, čili g nabývá někde v intervalu $[0, 1]$ hodnoty 0. Odvodit to logicky přesně z vlastností reálných čísel dá trochu práce, příslušné tvrzení se jmenuje Darbouxova věta.

Obecně, věty o pevném bodě tvrdí, že za jistých okolností má nějaká funkce f pevný bod, tj. existuje x takové, že $f(x) = x$. Taková tvrzení jsou klíčová v mnoha oblastech matematiky (i aplikované). Odvozují se z nich různé výsledky zaručující, že nějaká rovnice má řešení a podobně, a hrají dokonce roli například i v teorii sémantiky programů.

V Brouwerově větě o pevném bodě je jednorozměrný interval z tvrzení 7.1.2 nahrazen trojúhelníkem v rovině, čtyřstěnem v třídimenzionálním prostoru nebo jejich analogií ve vyšších dimenzích. Zde dokážeme pouze dvoudimenzionální verzi (protože jsme dokázali jenom dvoudimenzionální Spernerovo lemma, ale viz cv. 2). Důkaz patří spíše do matematické analýzy. Zde se jej pokusíme formulovat tak, abychom z analýzy potřebovali co nejméně; věci, které potřebovat budeme, připomeneme.

Nechť Δ označuje trojúhelník v rovině. Pro určitost vezmeme pravoúhlý rovnoramenný trojúhelník s vrcholy $A_1 = (0, 1)$, $A_2 = (1, 0)$ a $A_3 = (0, 0)$ (jako na obr. 7.1(a)). Funkce $f : \Delta \to \Delta$, jak je nejspíš čtenáři známo, se nazývá *spojitá*, pokud pro každé $a \in \Delta$ a pro každé $\varepsilon > 0$ existuje $\delta > 0$ tak, že je-li $b \in \Delta$ libovolný bod vzdálený od a nejvýš o δ, potom $f(a)$ a $f(b)$ mají vzdálenost nejvýš ε (heslovitě: f zobrazuje blízké body na blízké body).

7.1.3 Věta (Brouwerova věta o pevném bodě v rovině). *Každá spojitá funkce $f : \Delta \to \Delta$ má pevný bod.*

Důkaz. Zavedeme tři pomocné reálné funkce $\beta_1, \beta_2, \beta_3$ na trojúhelníku Δ: Je-li $a \in \Delta$ bod o souřadnicích (x, y), bude

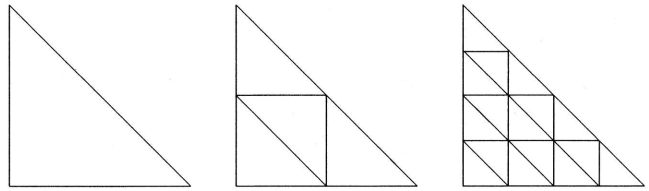
$$\beta_1(a) = y, \quad \beta_2(a) = x, \quad \beta_3(a) = 1 - x - y.$$

Podstatné vlastnosti těchto funkcí, které si hned napíšeme, jsou $\beta_i(a) \geq 0$ a $\beta_1(a) + \beta_2(a) + \beta_3(a) = 1$ pro každé $a \in \Delta$.

Dále definujeme 3 množiny $M_1, M_2, M_3 \subseteq \Delta$:

$$M_i = \{a \in \Delta;\ \beta_i(a) \geq \beta_i(f(a))\}, \quad i = 1, 2, 3.$$

Pro představu, M_i je množina těch bodů, které funkce f nevzdálí od strany protilehlé vrcholu A_i.



Obrázek 7.2: Zjemňování triangulace.

Všimneme si, že každý bod $p \in M_1 \cap M_2 \cap M_3$ je pevným bodem funkce f. (Pokud by funkce f bodem p někam pohnula, vždy jej vzdálí od některé ze stran; formálně přesný důkaz přenecháváme čtenářově píli.) Naším cílem je tedy najít bod ve zmíněném průniku.

Uvažme posloupnost jemnějších a jemnějších triangulací trojúhelníku Δ (první 3 triangulace jsou nakresleny na obr. 7.2). Pro každou triangulaci očíslujeme vrcholy trojúhelníčků čísly 1,2,3. Budeme požadovat, aby vrchol očíslovaný i patřil do množiny M_i, a dále aby očíslování bylo podle pravidel ve Spernerově lemmatu. Musíme se přesvědčit, že to vždy jde udělat.

Vrchol A_1 je vůbec nejvzdálenější od své protilehlé strany, takže funkce f jej nemůže ještě vzdálit. Proto $A_1 \in M_1$, takže tomuto vrcholu můžeme přidělit číslo 1 (podobně pro A_2, A_3). Každý bod a na straně A_1A_2 má $\beta_1(a) + \beta_2(a) = 1$, tedy $f(a)$ nemůže zároveň splňovat $\beta_1(f(a)) > \beta_1(a)$ a $\beta_2(f(a)) > \beta_2(a)$. Odtud $a \in M_1 \cup M_2$, neboli nic nám nebrání očíslovat vrcholy na straně A_1A_2 jen jedničkami a dvojkami (podobně pro ostatní strany). Konečně každý bod Δ patří do aspoň jedné z množin M_i, protože žádný bod nelze vzdálit od všech tří stran současně (formální ověření opět vynecháme).

Tím jsme připraveni aplikovat Spernerovo lemma 7.1.1. Každá z triangulací má tedy trojúhelníček očíslovaný 1,2,3. Označme vrcholy nějakého takového trojúhelníčku pro j-tou z oněch zjemňujících se triangulací symboly $a_{j,1}$, $a_{j,2}$ a $a_{j,3}$, a to ještě tak, že vždy $a_{j,i} \in M_i$.

Uvážíme posloupnost bodů $(a_{1,1}, a_{2,1}, a_{3,1}, \ldots)$. Tady potřebujeme, že z této posloupnosti můžeme vybrat nějakou nekonečnou konvergentní podposloupnost. Ale z každé posloupnosti bodů v trojúhelníku se dá vybrat nekonečná konvergentní podposloupnost (tato vlastnost trojúhelníka – sdílená například i každou omezenou a uzavřenou podmnožinou roviny – se nazývá *kompaktnost*). Řekněme, že jsme vybrali takovou pod-

posloupnost $(a_{j_1,1}, a_{j_2,1}, a_{j_3,1}, \ldots)$, $j_1 < j_2 < j_3 < \ldots$, a bod, k němuž konverguje, pojmenujeme p.

Bod p náleží do množiny M_1. Podle definice M_1 totiž pro každé $a_{j_k,1}$ máme $\beta_1(a_{j_k,1}) \geq \beta_1(f(a_{j_k,1}))$, a podle základních vět o limitách se taková neostrá nerovnost mezi spojitými funkcemi zachovává přechodem k limitě.

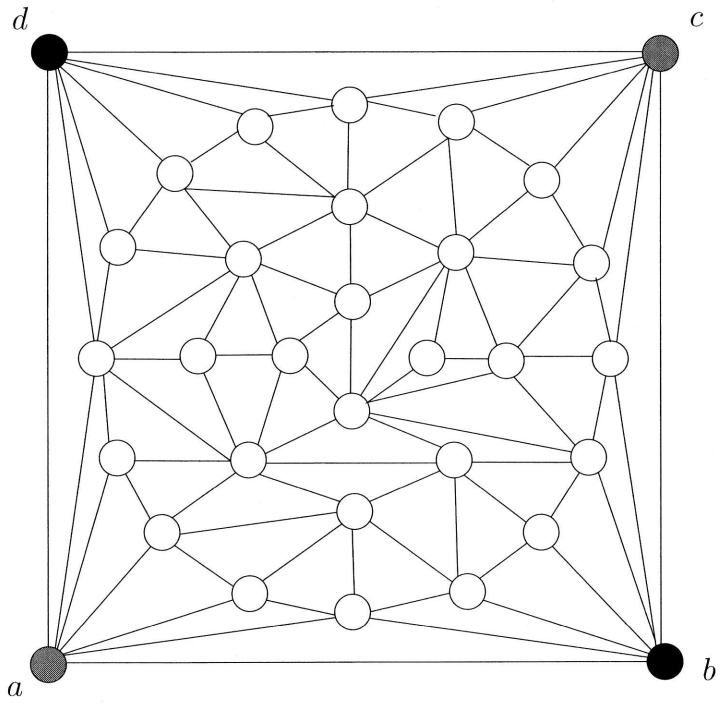
Poněvadž průměr trojúhelníčků v použitých triangulacích se zmenšoval k nule, musí i posloupnosti ostatních vrcholů, to znamená $(a_{j_1,2}, a_{j_2,2}, a_{j_3,2}, \ldots)$ a $(a_{j_1,3}, a_{j_2,3}, a_{j_3,3}, \ldots)$ konvergovat k bodu p, takže také $p \in M_2$ a $p \in M_3$. Bod p je kýžený pevný bod funkce f. □

Složitější věty podobného typu (jako například, že zobrazíme-li povrch koule spojitě do roviny, nějaké dva protilehlé body se musí zobrazit na sebe) se dokazují v odvětví matematiky zvaném *algebraická topologie*. Potřebuje se k tomu většinou poměrně složitý technický aparát, ale v jádru takových důkazů je často nějaký argument založený na sudosti/lichosti apod.

Ukážeme ještě jeden pěkný příklad úvahy pomocí principu sudosti. Budeme analyzovat jednu hru (podobnou hře HEX). Na hracím plánu, jaký je nakreslen na obr. 7.3 (ale triangulace uvnitř čtverce může být libovolná), se hraje následující hra. Hráči pro sebe zabírají políčka (tj. kroužky na hracím plánu); např. A je zamalovává světlejší barvou – na našem obrázku šedou – a B černě. Na začátku má A zabraná a a c, B má b a d, střídají se v tazích, A začíná, a v jednom tahu může hráč zabrat jedno libovolné dosud nezabrané políčko. Hráč A vyhraje, podaří-li se mu obsadit všechna políčka nějaké cesty z a do c, B usiluje o cestu z b do d. Kdyby se stalo, že hráč, který je na tahu, už nemá kam táhnout, ale ani jeden z hráčů svoji cestu nedokončil, hra by končila remízou.

7.1.4 Tvrzení. *Tato hra na hracím plánu uvedeného typu (vnější stěna čtverec, všechny vnitřní trojúhelníky) nemůže skončit remízou.*

Důkaz. Pro spor předpokládejme, že remíza nastala, nechť A je množina políček zabraných hráčem A a B množina políček zabraných hráčem B.



Obrázek 7.3: Hrací plán.

Označíme políčka čísly 1,2,3 podle takovéhoto pravidla: Jedničkou bude označeno políčko, které je v A a vede z něj cesta do políčka a, jejíž všechna políčka leží v A. Dvojkou označíme políčka z B, která lze spojit s b cestou ležící celou v B, a trojka připadne zbývajícím políčkům. Podle předpokladu pak budou c i d mít označení 3 (jinak by jeden z hráčů býval vyhrál).

Nyní se ukáže, že existuje některá vnitřní trojúhelníková stěna, jejíž políčka jsou označena 1,2 a 3. To bude spor: Políčko s číslem 3 nemůže být v A, protože sousedí s políčkem označeným 1, do kterého tedy vede cesta z a používající jen políček v A, a takovou cestu bychom mohli protáhnout do onoho políčka s číslem 3 (a to by správně mělo

mít číslo 1). Z podobného důvodu není políčko s číslem 3 ani v B – spor.

Jak se ukáže existence trojúhelníka označeného 1,2,3? Přesně jako Spernerovo lemma. Ještě jedno velmi podobné tvrzení je ve cvičení 1. □

Poznamenejme, že uvedený důkaz podstatně využívá toho, že všechny vnitřní stěny hracího plánu jsou trojúhelníkové, a vnější stěna má jen 4 vrcholy a, b, c, d. Povolíme-li například čtyřúhelníkové vnitřní stěny, remíza v principu nastat může.

Cvičení

1. Mějme nakreslený rovinný graf, jehož každá stěna včetně vnější je trojúhelník (tj., má 3 vrcholy). Každému vrcholu přiřadíme, zcela libovolně, některé z čísel 1,2,3. Dokažte, že existuje sudý počet stěn, jejichž vrcholy mají všechna 3 čísla.

2. (Spernerovo lemma v dimenzi 3)

   (a) Uvažme čtyřstěn $A_1A_2A_3A_4$, a nějaké jeho rozdělení na malé čtyřstěny tak, že každá stěna každého z malých čtyřstěnů buď leží na stěně velkého čtyřstěnu, nebo tvoří zároveň stěnu ještě jednoho malého čtyřstěnu. Očíslujeme vrcholy malých čtyřstěnů čísly 1,2,3,4 tak, že A_i dostane i, na hraně A_iA_j se vyskytují pouze i a j, a ve stěně $A_iA_jA_k$ jenom i, j a k. Dokažte, že potom existuje malý čtyřstěn očíslovaný 1,2,3,4.

   (b) Vyslovte a dokažte 3-dimenzionální verzi Brouwerovy věty o pevném bodě (o zobrazení čtyřstěnu do sebe).

3. K tématu vět o pevném bodě náleží dosti známá úloha o turistovi stoupajícím na horu. Turista tedy jednoho dne ráno v 6:00 začne stoupat na horu. Na vrchol dorazí v 6:00 večer, přenocuje tam (v budce k tomu účelu tam vystavěné, řekněme) a druhý den zase v 6:00 vyrazí po přesně stejné trase zpět, cestou se zastavuje, rozhlíží a podobně, takže do výchozího místa přijde zase v 6 večer. Má se dokázat, že na některém místě trasy byl v oba dny přesně ve stejný čas.

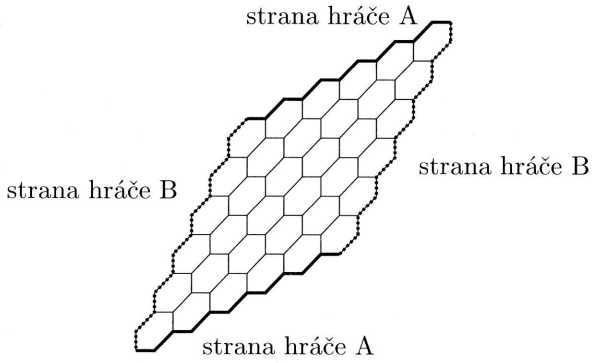
4. Uvažme hru jako v tvrzení 7.1.4.

   (a)* Dokažte, že vždy buď hráč A nebo hráč B má vyhrávající strategii (tj., pokud neudělá chybu, vyhraje, ať už druhý hraje jakkoli).

   (b) Najděte příklad hracího plánu (splňující podmínky jako v tvrzení 7.1.4) takového, že vyhrávající strategii má hráč B.

   (c)* Dokažte, že je-li hrací plán symetrický vzhledem k otočení o pravý úhel kolem středu (tj. jeví se stejně z pohledu hráče A i hráče B), potom má vyhrávající strategii vždy hráč A.

5. Hru HEX, jak možná čtenář ví, vynalezl Piet Hein. Hrací plán vypadá zhruba následovně:



   Hráči střídavě obsazují prázdná políčka svými figurkami. Cílem hráče A je spojit jeho dvě strany souvislým řetězcem políček, a podobně B chce spojit své dvě strany. Objevte a vysvětlete souvislost této hry s verzí hry HEX diskutované v textu.

7.2 Spernerova věta o nezávislém systému množin

Ano, v této kapitole potkáváme jméno Sperner už podruhé, ale Spernerova věta, již dokážeme, bude o něčem zcela jiném než Spernerovo lemma z předchozí části. Bude o n-prvkové množině X a nějakém systému $\mathcal{M}$ jejích podmnožin. Systém $\mathcal{M}$ nazveme *nezávislý*, pokud v něm nejsou žádné dvě různé množiny A, B takové, že $A \subset B$. Než budete číst dál, zkuste najít nezávislý systém množin na čtyřprvkové množině. Jaký největší počet množin může takový systém obsahovat?

7.2.1 Věta (Spernerova věta). *Libovolný nezávislý systém podmnožin n-prvkové množiny má nejvýš $\binom{n}{\lfloor n/2 \rfloor}$ množin.*

To je vlastně věta o částečně uspořádaných množinách. Uvažme totiž množinu 2^X (tj., systém všech podmnožin množiny X). Relace $\subseteq$, „býti podmnožinou", je částečným uspořádáním na množině 2^X; je to dokonce jeden z nejdůležitějších příkladů částečně uspořádaných množin, viz část 2.3. Nezávislý systém podmnožin je množinou po dvou neporovnatelných prvků v uspořádané množině $(2^X, \subseteq)$. Množina po dvou neporovnatelných prvků v částečně uspořádané množině se nazývá *nezávislá množina* nebo též *antiřetězec* . Spernerova věta tedy omezuje $\alpha(2^X, \subseteq)$, tj. maximální možnou velikost nezávislé množiny v $(2^X, \subseteq)$.

Spernerova věta dává nejlepší možný horní odhad, neboť opravdu existují nezávislé systémy s právě $\binom{n}{\lfloor n/2 \rfloor}$ množinami. Jeden takový nezávislý systém je systém všech podmnožin množiny X velikosti právě $\lfloor n/2 \rfloor$.

Důkaz věty 7.2.1. Nejprve definujeme, co je to *řetězec* podmnožin množiny X: je to každá posloupnost podmnožin množiny X, která je tvaru $A_1 \subset A_2 \subset \cdots \subset A_k$. V řeči uspořádání na 2^X je to prostě lineárně uspořádaná podmnožina částečně uspořádané množiny $(2^X, \subseteq)$.

Základní pozorování je, že každý řetězec má s libovolným nezávislým systémem podmnožin společnou nejvýš jednu množinu. Kdyby se nám například podařilo ukázat, že celá uvažovaná uspořádaná množina se dá vyjádřit jako sjednocení nejvýš r řetězců, potom žádná nezávislý systém nemá více než r množin. V našem důkazu nicméně využijeme uvedené pozorování trochu složitějším způsobem.

Uvažme množinu všech *maximálních řetězců* v $(2^X, \subseteq)$, kde maximální řetězec je řetězec, ke kterému už nelze nic přidat tak, aby zůstal řetězcem. Je snadné nahlédnout, jak maximální řetězce vypadají: obsahují jednu podmnožinu X každé z možných velikostí, tj., mají tvar

$$\emptyset \subset \{x_1\} \subset \{x_1, x_2\} \subset \{x_1, x_2, x_3\} \subset \ldots \subset \{x_1, x_2, \ldots, x_n\}, \qquad (7.1)$$

kde $x_1, x_2, \ldots, x_n$ jsou všechny prvky X vypsané v nějakém pořadí. Každý takový maximální řetězec tudíž určuje pořadí prvků X, a obráceně, z každého pořadí dostaneme právě jeden maximální řetězec. Proto maximálních řetězců je stejně jako permutací, neboli $n!$.

Nechť $\mathcal{M}$ je libovolný nezávislý systém množin. Utvořme všechny uspořádané dvojice $(\mathcal{R}, M)$, kde $M \in \mathcal{M}$ a $\mathcal{R}$ je maximální řetězec, obsahující M. Budeme počet takových dvojic počítat dvěma způsoby.

Z jedné strany, podle zmíněného pozorování, každý řetězec obsahuje nejvýš jednu $M \in \mathcal{M}$, takže uvažovaných dvojic $(\mathcal{R}, M)$ není více než maximálních řetězců, tedy než $n!$.

Z druhé strany, vezmeme jednu množinu $M \in \mathcal{M}$ a ptáme se, v kolika maximálních řetězcích je obsažena. Maximální řetězec tvaru (7.1) obsahuje M jako jednu ze svých množin, právě když $\{x_1, x_2, \ldots, x_k\} = M$, kde $k = |M|$. Prvky množiny M můžeme stále ještě uspořádat $k!$ způsoby, čímž volíme počátečních k množin řetězce, a prvky mimo M můžeme uspořádat $(n-k)!$ způsoby, čímž je dán zbytek řetězce. Celkem je tedy M obsažena v $k!(n-k)!$ maximálních řetězcích. Počet uvažovaných uspořádaných dvojic $(\mathcal{R}, M)$ je proto roven

$$\sum_{M \in \mathcal{M}} |M|!(n - |M|)!,$$

přitom podle předchozího způsobu počítání je tento počet nejvýš $n!$. Vydělíme-li vzniklou nerovnost číslem $n!$, dostaneme

$$\sum_{M \in \mathcal{M}} \frac{|M|!(n-|M|)!}{n!} = \sum_{M \in \mathcal{M}} \frac{1}{\binom{n}{|M|}} \leq 1.$$

Využijeme toho, že $\binom{n}{\lfloor n/2 \rfloor}$ je aspoň tak velké jako libovolné kombinační číslo tvaru $\binom{n}{k}$ (viz část 3.5). Proto

$$1 \geq \sum_{M \in \mathcal{M}} \frac{1}{\binom{n}{|M|}} \geq |\mathcal{M}| \frac{1}{\binom{n}{\lfloor n/2 \rfloor}},$$

a odtud $|\mathcal{M}| \leq \binom{n}{\lfloor n/2 \rfloor}$. □

Ještě jeden důkaz Spernerovy věty. Spernerova věta se dá dokazovat několika podstatně odlišnými metodami. Popíšeme ještě dvě z nich. První z nich chytře pokrývá 2^X řetězci speciálního typu. Mějme nějaký řetězec v $(2^X, \subseteq)$, j. posloupnost do sebe zařazených množin

$M_1 \subset M_2 \subset \cdots \subset M_t$. Nazvěme takový řetězec *symetrickým*, jestliže pro nějaké k obsahuje množiny velikostí právě $k, k+1, \ldots, n-k$. *Rozklad na symetrické řetězce* bude pak vyjádření 2^X jako disjunktního sjednocení několika symetrických řetězců.

Je vidět, že libovolný rozklad na symetrické řetězce (existuje-li vůbec) sestává z přesně $\binom{n}{\lfloor n/2 \rfloor}$ symetrických řetězců, jelikož každý symetrický řetězec obsahuje právě jednu množinu velikosti $\lfloor n/2 \rfloor$. Každý řetězec má s nezávislým systémem množin nejvýš jednu společnou množinu (na tom byl založen i předchozí důkaz Spernerovy věty). Spernerova věta tudíž vyplývá z následujícího:

Tvrzení. *Pro každou konečnou množinu X existuje rozklad na symetrické řetězce.*

Důkaz. Předpokládejme, že $X = \{1, 2, \ldots, n\}$. Základem důkazu je takováto konstrukce:

Každé podmnožině $M \subseteq X$ přiřadíme posloupnost $(m_1, m_2, \ldots, m_n)$ levých a pravých závorek „(“ „)“ předpisem

$$m_i = \begin{cases} \text{„(“} & \text{jestliže } i \in M \\ \text{„)“} & \text{jestliže } i \notin M. \end{cases}$$

Tak například pro $n = 7$ a množinu $M = \{2, 6\}$ máme

$$(m_1, \ldots, m_7) = \text{„)()))()“}.$$

Posloupnost závorek je zcela obecná (tedy ne správně uzávorkovaná). Můžeme ji však „částečně uzávorkovat“: nejdříve spárujeme všechny dvojice „()“ stojící bezprostředně vedle sebe, a dále pokračujeme v párování dosud nepoužitých závorek stejným způsobem (přičemž již spárované závorky ignorujeme). Dva příklady:

$$) \underbrace{(\,)}\,) \,) \underbrace{(\,)}$$

$$) \,) \,) \,(\underbrace{(\,)\,\underbrace{(\,)}\,)}\,(\,.$$

Při tomto postupu samozřejmě mohou některé závorky zůstat nespárovány. Z pravidla částečného závorkování nicméně plyne, že posloupnost zbývajících závorek má na začátku jen pravé závorky a potom, od jistého místa, už jen levé závorky.

Řekneme, že dvě posloupnosti závorek mají *stejné částečné uzávorkování*, pokud spárované závorky jsou v obou posloupnostech stejné (i na stejných pozicích). Tak je tomu například pro posloupnosti tří následujících množin: (podmnožin množiny $\{1, 2, \ldots, 11\}$):

$$\begin{array}{lll} M_1 = \{4,5,6,8,11\} & \ldots &) \,) \,) \,(\,(\,(\,)\,(\,)\,)\,(\\ M_2 = \{5,6,8,11\} & \ldots &) \,) \,) \,) \,(\,(\,)\,(\,)\,)\,(\\ M_3 = \{5,6,8\} & \ldots &) \,) \,) \,) \,(\,(\,)\,(\,)\,) \,) \end{array}$$

Jediný způsob, jak se mohou dvě posloupnosti závorek se stejným částečným uzávorkováním lišit, je že jedna z nich má zleva více nespárovaných levých závorek, nebo zprava více nespárovaných pravých závorek. Z toho je snadno vidět, že dvě množiny se stejným částečným uzávorkováním (příslušných posloupností) musí být jedna podmnožinou druhé.

Definujeme nyní na množině 2^X ekvivalenci $\sim$ předpisem $M \sim M'$ právě když M i M' mají stejné částečné uzávorkování. Tvrdíme, že třídy této ekvivalence jsou symetrické řetězce. Ověření necháváme jako cvičení. Tím jsme ještě jednou dokázali Spernerovu větu. □

Nakonec předvedeme ještě jeden důkaz Spernerovy věty. Ten je zajímavý tím, že se v něm vlastně vůbec nepočítá s kombinačními čísly, ačkoliv Spernerova věta o nich hovoří. Místo toho se využívá značné symetrie uspořádané množiny $(2^X, \subseteq)$.

Začneme trochu obecnější definicí. Mějme nějaké uspořádané množiny $(X, \leq)$ a $(Y, \preceq)$. Zobrazení $f : X \to Y$ nazveme *isomorfismem* uspořádaných množin, jestliže f je bijekce a pro každé dva prvky $x, y \in X$ platí $x \leq y$ právě když $f(x) \preceq f(y)$. Isomorfismus uspořádané množiny $(X, \leq)$ s ní samotnou se jmenuje *automorfismus*. Automorfismus zachovává všechny vlastnosti, které můžeme definovat pomocí relace $\leq$. Tak například x je největším prvkem nějaké podmnožiny $A \subseteq X$, právě když $f(x)$ je největším prvkem množiny $f(A)$.

Třetí důkaz Spernerovy věty. Nechť X je daná konečná množina s n prvky. Každá permutace $f : X \rightarrowtail\!\!\!\!\!\twoheadrightarrow X$ indukuje zobrazení $f^{\#} : 2^X \to 2^X$, dané předpisem $f^{\#}(A) = \{f(x);\, x \in A\}$. Je zřejmé, že $f^{\#}$ je bijekce[1] $2^X \to 2^X$, a dokonce automorfismus uspořádané množiny $(2^X, \subseteq)$.

Uvažme nyní nějaký systém $\mathcal{M}$ podmnožin množiny X. Pro každou permutaci f množiny X můžeme uvážit systém $\{f^{\#}(M);\, M \in \mathcal{M}\}$, tedy

[1] V části 1.5 jsme přijali konvenci, podle níž se pro obraz množiny může použít stejné formy zápisu jako pro obraz prvku, tj. v našem případě bychom mohli množinu $\{f(x);\, x \in A\}$ zapsat též jako $f(A)$. Momentálně ale bude lepší přísněji rozlišovat mezi obrazem prvku a obrazem množiny. Proto jsme zavedli odlišné značení, $f^{\#}$, pro zobrazení množin

systém obrazů množin z $\mathcal{M}$ při zobrazení $f^{\#}$. Definujeme tak vlastně nové zobrazení

$$f^{\#\#} : 2^{2^X} \to 2^{2^X}$$

(tj. množinovým systémům přiřazuje množinové systémy) předpisem

$$f^{\#\#}(\mathcal{M}) = \{f^{\#}(M);\ M \in \mathcal{M}\}.$$

Zobrazení $f^{\#\#}$ je opět bijekce.

Na systémech množin, tj. na množině 2^{2^X}, zavedeme teď relaci $\lhd$ následujícím předpisem:

$$\mathcal{M} \lhd \mathcal{N} \quad \Leftrightarrow \quad \text{pro každé } M \in \mathcal{M} \text{ existuje } N \in \mathcal{N} \text{ tak, že } M \subseteq N.$$

Všimněte si, že relace $\lhd$ je něco jiného než inkluze mezi systémy množin. Je to relace větší (tedy z $\mathcal{M} \subseteq \mathcal{N}$ plyne $\mathcal{M} \lhd \mathcal{N}$). Čtenář může sám ověřit, že relace $\lhd$ je reflexivní a transitivní. Nemusí to však být relace antisymetrická (najděte příklad na tříprvkové množině X, abyste se přesvědčili, že pojmu rozumíte).

Písmenem Ξ budeme značit množinu všech nezávislých systémů na množině X (tedy $\Xi \subset 2^{2^X}$). Tvrdíme, že relace $\lhd$ zúžená na množinu Ξ již antisymetrická je, a tudíž to je částečné uspořádání. Když totiž $\mathcal{M}$ a $\mathcal{N}$ jsou nezávislé systémy a platí $\mathcal{M} \lhd \mathcal{N}$ i $\mathcal{N} \lhd \mathcal{M}$, uvažme libovolnou množinu $M \in \mathcal{M}$. Systém $\mathcal{N}$ musí obsahovat nějakou $M' \supseteq M$, a pak také $\mathcal{M}$ obsahuje nějakou $M'' \supseteq M'$. Máme tedy $M, M'' \in \mathcal{M}$, $M \subseteq M''$, a proto (z nezávislosti) $M = M'' = M'$, takže $M \in \mathcal{N}$. Tím jsme ukázali $\mathcal{M} \subseteq \mathcal{N}$, a symetricky dostaneme $\mathcal{N} \subseteq \mathcal{M}$, neboli $\mathcal{M} = \mathcal{N}$. Proto $(\Xi, \lhd)$ je uspořádaná množina.

Dále tvrdíme, že pro každou permutaci f je zobrazení $f^{\#\#}$ automorfismem uspořádané množiny $(\Xi, \lhd)$ – ověření přenecháváme čtenáři (tím si ověří i své zvládnutí pojmů jako Ξ a $f^{\#\#}$).

Základem důkazu Spernerovy věty je takovéto lemma:

7.2.2 Lemma. *Označme $\Xi_0 \subseteq \Xi$ množinu všech nezávislých systémů, které mají největší možný počet množin (mezi všemi nezávislými systémy). Množina Ξ_0 má největší prvek, $\mathcal{N}_0$, vzhledem k uspořádání $\lhd$. To znamená, že pro každé $\mathcal{M} \in \Xi_0$ platí $\mathcal{M} \lhd \mathcal{N}_0$.*

Důkaz lemmatu. Protože nezávislých systémů na množině X je pouze konečně mnoho, stačí dokázat, že pro libovolné dva systémy $\mathcal{M}, \mathcal{M}' \in \Xi_0$ existuje systém $\mathcal{N} \in \Xi_0$ splňující $\mathcal{M} \lhd \mathcal{N}$ a $\mathcal{M}' \lhd \mathcal{N}$.

Pro libovolné $\mathcal{M}, \mathcal{M}' \in \Xi_0$ uvažme systém $\bar{\mathcal{M}} = \mathcal{M} \cup \mathcal{M}'$. Poněvadž jak $\mathcal{M}$, tak $\mathcal{M}'$ jsou nezávislé systémy množin, má nejdelší řetězec v $\bar{\mathcal{M}}$ (vzhledem k uspořádání $\bar{\mathcal{M}}$ inkluzí) délku nejvýš 2. Označme dále $\bar{\mathcal{M}}_{\min}$ systém všech množin z $\bar{\mathcal{M}}$, pro něž $\bar{\mathcal{M}}$ už neobsahuje žádnou jejich vlastní podmnožinu, jinak řečeno systém všech množin z $\bar{\mathcal{M}}$ minimálních vzhledem k $\subseteq$. Podobně zavedeme systém $\bar{\mathcal{M}}_{\max}$ jako systém všech množin z $\bar{\mathcal{M}}$ maximálních vzhledem k $\subseteq$. Chceme ověřit, že $\bar{\mathcal{M}}_{\max}$ splňuje podmínky kladené výše na systém $\mathcal{N}$.

Oba systémy $\bar{\mathcal{M}}_{\min}$ i $\bar{\mathcal{M}}_{\max}$ jsou nezávislé, a $\bar{\mathcal{M}} = \bar{\mathcal{M}}_{\min} \cup \bar{\mathcal{M}}_{\max}$. Zřejmě také $\bar{\mathcal{M}}_{\max} \rhd \mathcal{M}$ a $\bar{\mathcal{M}}_{\max} \rhd \mathcal{M}'$. Zbývá ověřit $|\bar{\mathcal{M}}_{\max}| = |\mathcal{M}|$. Všimneme si, že z nezávislosti $\mathcal{M}$ a $\mathcal{M}'$ plyne $\mathcal{M} \cap \mathcal{M}' \subseteq \bar{\mathcal{M}}_{\min} \cap \bar{\mathcal{M}}_{\max}$. Proto

$$\begin{aligned} |\bar{\mathcal{M}}_{\min}| + |\bar{\mathcal{M}}_{\max}| &= |\bar{\mathcal{M}}_{\min} \cup \bar{\mathcal{M}}_{\max}| + |\bar{\mathcal{M}}_{\min} \cap \bar{\mathcal{M}}_{\max}| \\ &\geq |\mathcal{M} \cup \mathcal{M}'| + |\mathcal{M} \cap \mathcal{M}'| = |\mathcal{M}| + |\mathcal{M}'|, \end{aligned}$$

a tedy kdyby $|\bar{\mathcal{M}}_{\max}| < |\mathcal{M}| = |\mathcal{M}'|$, potom bychom měli $|\bar{\mathcal{M}}_{\min}| > |\mathcal{M}|$, a systémy $\mathcal{M}$ a $\mathcal{M}'$ by neměly maximální velikost. Tím je lemma dokázáno.

Zbývá dokončit důkaz Spernerovy věty. Uvažme největší prvek $\mathcal{N}_0$ množiny $(\Xi_0, \lhd)$. Pro každou permutaci f množiny X zobrazuje příslušný indukovaný automorfismus $f^{\#\#}$ množinu Ξ_0 (nezávislé systémy maximální velikosti) na ni samotnou, a tedy zobrazuje i její maximální prvek $\mathcal{N}_0$ na něj samotný: $f^{\#\#}(\mathcal{N}_0) = \mathcal{N}_0$. Odtud však plyne, že jestliže do $\mathcal{N}_0$ patří aspoň jedna k-prvková množina, potom tam už musí patřit *všechny* k-prvkové množiny, neboli $\binom{X}{k} \subseteq \mathcal{N}_0$. K systému $\binom{X}{k}$ už nejde přidat žádnou množinu tak, aby zůstal nezávislým, takže $\mathcal{N}_0 = \binom{X}{k}$. Z maximality kombinačních čísel $\binom{n}{\lfloor n/2 \rfloor}$ a $\binom{n}{\lceil n/2 \rceil}$ pak vyplývá, že $\mathcal{N}_0 = \binom{X}{\lceil n/2 \rceil}$. □

Cvičení

1. Řekneme, že systém $\mathcal{N}$ podmnožin X je *polonezávislý*, neobsahuje-li žádné 3 množiny A, B, C takové, že $A \subset B \subset C$.

   (a) Podobnou metodou jako v důkazu Spernerovy věty dokažte, že $|\mathcal{N}| \leq 2\binom{n}{\lfloor n/2 \rfloor}$, kde $n = |X|$.

   (b) Ukažte, že pro liché n odhad z (a) nelze zlepšit.

2. Pro přirozené číslo n definujte uspořádanou množinu $(D_n, |)$, kde D_n značí množinu všech dělitelů čísla n a $|$ je relace dělitelnosti.
   (a) Jaký je nejdelší řetězec v této množině pro $n = 10!$?
   (b) Kolik má tato množina maximálních řetězců (tj. takových, které již nejdou prodloužit) pro $n = 10!$?
   (c) Kolik prvků má největší antiřetězec v této množině pro $n = 720$?
3. Ověřte, že třídy ekvivalence $\sim$ definované ve druhém důkazu Sperneovy věty jsou doopravdy symetrické řetězce.
4.* Dokažte, že množinové systémy $\binom{X}{\lfloor n/2 \rfloor}$ a $\binom{X}{\lceil n/2 \rceil}$ jsou jediné nezávislé systémy na n-prvkové množině s největším možným počtem množin.
5. Určete, kolik má množina $(2^X, \subseteq)$ automorfismů.
6. Dokažte, že pro každou konečnou částečně uspořádanou množinu $(P, \leq)$ existuje nezávislá množina maximální možné velikosti, který se všemi automorfismy množiny $(P, \leq)$ zobrazuje sama na sebe (je jejich *pevným bodem*).
7.* Nechť $a_1, \ldots, a_n$ jsou reálná čísla, $|a_i| \geq 1$. Nechť $p(a_1, \ldots, a_n)$ značí počet vektorů $(\varepsilon_1, \ldots, \varepsilon_n)$, kde $\varepsilon_i = \pm 1$, pro něž
$$-1 < \sum_{i=1}^{n} \varepsilon_i a_i < 1.$$
   Dokažte, že $p(a_1, \ldots, a_n) \leq \binom{n}{\lfloor n/2 \rfloor}$ pro každé $a_1, \ldots, a_n$, a že pro jistou volbu a_i nastane rovnost. (Toto je jedna z prvních aplikací Spernerovy věty – tzv. Littlewoodův-Offordův problém.)
8. Nechť n je přirozené číslo, které není dělitelné žádnou druhou mocninou přirozeného čísla. Určete maximální možnou velikost množiny dělitelů čísla n, které se navzájem nedělí (tj., $\max |M|$, kde $x \in M \Rightarrow x|n$ a $x, y \in M$, $x \neq y \Rightarrow x \not| y$).

7.3 Extremální věta: grafy bez čtyřcyklů

V oddílu 4.8 jsme zjišťovali, jaký je největší možný počet hran grafu s n vrcholy, který neobsahuje jako podgraf žádný trojúhelník. Zde budeme vyšetřovat velmi podobně vypadající úlohu: Jaký je největší možný počet hran grafu s n vrcholy, který neobsahuje žádný podgraf

isomorfní grafu $K_{2,2}$ (neboli kružnici délky 4)? Podgraf zde uvažujeme v neindukovaném smyslu, takže například úplný graf na 4 vrcholech zakázaný podgraf $K_{2,2}$ obsahuje.

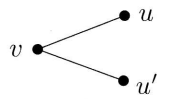
Mohlo by se zdát, že zakázat $K_{2,2}$ bude mít podobný účinek jako zakázat trojúhelník, ale kupodivu se odpovědi na tyto dvě otázky zásadně liší. Graf neobsahující trojúhelník může mít až $\lfloor n^2/4 \rfloor$ hran, tedy přibližně polovinu z $\binom{n}{2}$ (to je počet hran úplného grafu na n vrcholech, tedy maximální možný počet hran beze všech omezení). Naproti tomu, jak brzy uvidíme, zakázáním $K_{2,2}$ omezíme počet hran mnohem více, zhruba na $n^{3/2}$. To je pro velká n počet nepatrný v porovnání s $\binom{n}{2}$ (nebo i s $n^2/4$).

Obě úlohy náležejí do *extremální teorie grafů*, která v obecnosti vyšetřuje maximální možný počet hran grafu na n vrcholech, který neobsahuje daný zakázaný podgraf, nebo obecněji žádný podgraf z dané zakázané množiny grafů. V kapitole o stromech jsme se také setkali s úlohou tohoto typu: Viděli jsme, že graf na n vrcholech neobsahující žádnou kružnici (tedy les) má nanejvýš $n - 1$ hran.

Teď přistoupíme k hlavnímu výsledku této části.

7.3.1 Věta. *Buď G graf s n vrcholy. Neobsahuje-li G graf $K_{2,2}$ jako podgraf, potom má nejvýše $\frac{1}{2}(n^{3/2} + n)$ hran.*

Důkaz. Pišme $V = V(G)$. Budeme dvěma způsoby počítat velikost množiny M všech dvojic $(\{u, u'\}, v)$, kde $v \in V$, $\{u, u'\} \in \binom{V}{2}$ a v je spojen hranou jak s u tak s u'. Jinými slovy, počítáme (neindukované) podgrafy tvaru



Pro pevnou dvojici $\{u, u'\}$ může existovat pouze jediný vrchol $v \in V$ spojený s u i s u' (kdyby byly dva takové vrcholy, v a v', seděl by na vrcholech u, u', v, v' podgraf isomorfní $K_{2,2}$). Proto $|M| \leq \binom{n}{2}$.

Nyní uvážíme všechny prvky $(\{u, u'\}, v)$ z množiny M pro jeden pevný vrchol $v \in V$. Každá dvojice $\{u, u'\}$ sousedů vrcholu v přispěje jeden prvek M, proto vrchol v stupně d přispěje $\binom{d}{2}$ prvky.

Označíme-li tedy $d_1, d_2, \ldots, d_n$ stupně jednotlivých vrcholů z V, dostáváme $|M| = \sum_{i=1}^{n} \binom{d_i}{2}$.

Spojením s předchozím odhadem máme

$$\sum_{i=1}^{n} \binom{d_i}{2} \leq \binom{n}{2}. \tag{7.2}$$

Přitom počet hran uvažovaného grafu je $E = \frac{1}{2}\sum_{i=1}^{n} d_i$. Zbytek důkazu je již čistě manipulace s nerovnostmi, která se dá dělat mnoha různými způsoby.

Zde ukážeme jeden důkaz, další je naznačen ve cvičení 5 (ten je trochu složitější, ale snáze se zobecní). Nejdříve potřebujeme jednu (důležitou) nerovnost:

7.3.2 Tvrzení (Cauchyho-Schwarzova nerovnost). *Pro libovolná reálná čísla $x_1, \ldots, x_n$ a $y_1, \ldots, y_n$ platí*

$$\sum_{i=1}^{n} x_i y_i \leq \sqrt{\sum_{i=1}^{n} x_i^2}\sqrt{\sum_{i=1}^{n} y_i^2}.$$

Cauchyho-Schwarzova nerovnost má názorný geometrický význam. Interpretujeme-li totiž $x = (x_1, \ldots, x_n)$ a $y = (y_1, \ldots, y_n)$ jako vektory v n-dimenzionálním euklidovském prostoru, je levá strana nerovnosti jejich *skalární součin*, zatímco pravá strana je součin jejich délek. Přitom dobře známý vzorec z vektorového počtu říká, že kosinus úhlu dvou vektorů je roven jejich skalárnímu součinu dělenému součinem jejich délek. Cauchyho-Schwarzova nerovnost tedy vyjadřuje, že kosinus úhlu je vždy nejvýš 1 (rozmyslete si to aspoň pro případ $n = 2$, tj. v rovině).

Cauchyho-Schwarzova nerovnost se většinou probírá v analýze i v lineární algebře, ale proč neuvést dva hezké důkazy?

První důkaz: z AG nerovnosti. Pišme $X = \sum_{i=1}^{n} x_i^2$ a $Y = \sum_{i=1}^{n} y_i^2$. Pokud $X = 0$, pak všechna x_i jsou 0 a nerovnost platí, a podobně pro $Y = 0$. Mějme teď $X > 0$ a $Y > 0$ a definujme $a_i = x_i^2/X$, $b_i = y_i^2/Y$. Nerovnost mezi aritmetickým a geometrickým průměrem, viz důkaz věty 3.4.1, praví $\sqrt{a_i b_i} \leq (a_i + b_i)/2$. Sečtením těchto nerovností pro $i = 1, 2, \ldots, n$ vychází na levé straně

$$\sum_{i=1}^{n} \sqrt{a_i b_i} = \sum_{i=1}^{n} \frac{|x_i y_i|}{\sqrt{XY}},$$

zatímco pravá strana dává

$$\frac{1}{2}\left(\frac{1}{X}\sum_{i=1}^{n} x_i^2 + \frac{1}{Y}\sum_{i=1}^{n} y_i^2\right) = \frac{1}{2}(1+1) = 1.$$

Takže $\sum_{i=1}^{n} \frac{|x_i y_i|}{\sqrt{XY}} \leq 1$, a po vynásobení výrazem $\sqrt{XY}$ máme Cauchyho-Schwarzovu nerovnost. □

Druhý důkaz: kouzlo s diskriminantem. Považujme čísla x_i a y_i za pevně zvolená, a definujme funkci p proměnné t předpisem

$$p(t) = \sum_{i=1}^{n} (x_i + t y_i)^2.$$

Po umocnění závorek a sloučení členů se stejnou mocninou t je vidět, že $p(t)$ je kvadratická funkce tvaru $p(t) = at^2 + bt + c$, kde $a = \sum_{i=1}^{n} y_i^2$, $b = \sum_{i=1}^{n} 2x_i y_i$ a $c = \sum_{i=1}^{n} x_i^2$. Na druhé straně je hodnota $p(t)$ součtem čtverců, a tedy nezáporná pro všechna t.

Kdyby měla kvadratická rovnice $at^2 + bt + c = 0$ kladný diskriminant, měla by dva reálné kořeny, a byla by na části reálné osy záporná. Tudíž diskriminant je nekladný, neboli $b^2 - 4ac \leq 0$. Kdo si do tohoto vztahu dosadí za a, b, c, zjistí, že vyjde přesně Cauchyho-Schwarzova nerovnost. □

Tím nejsou důkazy Cauchyho-Schwarzovy nerovnosti zdaleka vyčerpány – další jsou například ve cvičení 4.

Dokončení důkazu věty 7.3.1. Zřejmě můžeme předpokládat, že náš graf nemá izolované vrcholy, tedy $d_i \geq 1$ pro každé i. Potom platí $\binom{d_i}{2} \geq (d_i - 1)^2/2$, takže z (7.2) dostaneme

$$\sum_{i=1}^{n} (d_i - 1)^2 \leq n^2.$$

Použijeme nyní Cauchyho-Schwarzovu nerovnost s $x_i = d_i - 1$, $y_i = 1$. Dostaneme

$$\sum_{i=1}^{n} (d_i - 1) \leq \sqrt{\sum_{i=1}^{n} (d_i - 1)^2}\sqrt{n} \leq \sqrt{n^2}\sqrt{n} = n^{3/2},$$

takže $E = \frac{1}{2}\sum_{i=1}^{n} d_i \leq \frac{1}{2}(n^{3/2} + n)$. □

Cvičení

1. Dokažte, že pro libovolné $t \geq 2$ je maximální počet hran grafu neobsahujícího $K_{2,t}$ jako podgraf nejvýš $\frac{1}{2}(\sqrt{t-1}\, n^{3/2} + n)$.

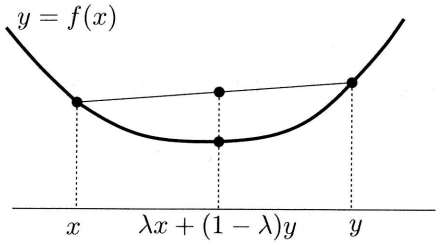
2. Nechť $S_1, S_2, \ldots, S_n$ jsou nějaké podmnožiny nějaké n-prvkové množiny X. Předpokládejme, že platí $|S_i \cap S_j| \leq 1$ pro každé i, j, $1 \leq i < j \leq n$. Ukažte, že některá z množin S_i má nanejvýš $O(\sqrt{n})$ prvků.

3. Nechť A je n-prvková množina, B je m-prvková množina, a nechť G je bipartitní graf na $A \cup B$, jehož každá hrana spojuje vrchol z A s vrcholem z B. Dokažte, že neobsahuje-li G graf $K_{2,2}$ jako podgraf, potom má nejvýš $O(m\sqrt{n} + n)$ hran.

4. (a) Dokažte Cauchyho-Schwarzovu nerovnost indukcí podle n (napřed ji umocněte na druhou).

   (b) Dokažte Cauchyho-Schwarzovu nerovnost přímo: vyjděte z nerovnosti $\sum_{i,j=1}^{n}(x_i y_j - x_j y_i)^2 \geq 0$ a upravte.

5. (a) Nechť $f : \mathbf{R} \to \mathbf{R}$ je *konvexní funkce*, tj. pro pro libovolné $x, y \in \mathbf{R}$ a $\lambda \in [0,1]$ platí $f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda) f(y)$. Geometricky to znamená, že spojíme-li libovolné dva body na grafu této funkce úsečkou, leží část grafu mezi těmito body pod zmíněnou úsečkou:



   Dokažte indukcí, že potom pro libovolná reálná čísla $x_1, x_2, \ldots, x_n$ platí

$$f(\tfrac{1}{n}x_1 + \tfrac{1}{n}x_2 + \cdots + \tfrac{1}{n}x_n) \leq \tfrac{1}{n}f(x_1) + \tfrac{1}{n}f(x_2) + \cdots + \tfrac{1}{n}f(x_n).$$

   (b) Definujte funkci f předpisem

$$f(x) = \begin{cases} 0 & \text{pro } x \leq 1 \\ x(x-1)/2 & \text{pro } x > 1. \end{cases}$$

   Dokažte, že f je konvexní.

   (c) Dokažte ze vztahu (7.2) větu 7.3.1 pomocí (a) a (b) (napřed odvoďte $nf(2E/n) \leq \binom{n}{2}$).

6.* Podobnou metodou jako ve cvičení 5 odvoďte, že neobsahuje-li graf na n vrcholech $K_{3,3}$ jako podgraf, má nejvýš $const.n^{5/3}$ hran.

8

Počet koster

8.1 Cayleyho formule

Pro daný graf G označme $\kappa(G)$ počet všech koster G. V této kapitole předkládáme čtenáři několik důkazů následujícího výsledku:

8.1.1 Věta (Cayleyho formule). *Pro každé $n \geq 2$ je $\kappa(K_n)$, tj. počet stromů na daných n vrcholech, roven n^{n-2}.*

Ačkoli pro $\kappa(K_n)$ vyjde taková pěkná jednoduchá formule, není znám žádný úplně přímočarý způsob, jak její správnost nahlédnout. Postupem času se přišlo na celou řadu důkazů, jejichž základní myšlenky se od sebe podstatně odlišují, ale každý z nich je založen na umném triku nebo vyplývá z netriviální teorie. Shromáždili jsme několik důkazů do této kapitoly, hlavně jako ilustraci myšlenkového bohatství matematiky.

Rozhodně nechceme tvrdit, že věta 8.1.1 patří k vůbec nejdůležitějším v matematice. Na druhé straně, počet koster grafu (a související teorie) má řadu teoretických i praktických aplikací, a začal se studovat v souvislosti s elektrickými obvody.

Jako ilustraci uvedeme bez důkazu „elektrotechnický“ význam počtu koster. Představme si, že daný graf G je elektrický obvod, kde každá hrana je vodič s jednotkovým odporem (a vrcholy znamenají prostě spojení konců dohromady). Jsou-li x, y vrcholy spojené hranou, potom odpor, který bychom mezi nimi v tomto obvodu naměřili, je roven počtu

koster G obsahujících hranu $\{x, y\}$, dělenému celkovým počtem koster $\kappa(G)$. Přímo tento výsledek není ovšem pro přímou aplikaci příliš užitečný (málokdy máme všechny odpory stejné), ale existuje příslušné zobecnění na grafy s ohodnocenými hranami.

V celé kapitole bude množina V vrcholů uvažovaného úplného grafu rovna $\{1, 2, \ldots, n\}$.

Cvičení

1. Dokažte, že počet navzájem neisomorfních stromů na n vrcholech je nejméně e^n/n^3 (viz též cvičení 5.2.5!).

2.* Předpokládejte platnost věty 8.1.1, a určete počet koster úplného grafu na n vrcholech bez jedné hrany.

3. Označme $T_n = \kappa(K_n)$. Dokažte rekurentní vzorec

$$(n-1)T_n = \sum_{k=1}^{n-1} k(n-k)\binom{n-1}{k-1} T_k T_{n-k}.$$

Poznámka: také z této rekurence se dá věta 8.1.1 odvodit, ale není to jen tak.

4.* Spočítejte $\kappa(K_{n,m})$ (počet koster úplného bipartitního grafu). Pokuste se aplikovat některou z metod z následujících oddílů (např. 8.5, 8.2).

8.2 Důkaz přes skóre

Ukážeme

8.2.1 Tvrzení. *Nechť $d_1, d_2, \ldots, d_n$ jsou kladná celá čísla se součtem $2n-2$. Potom počet koster grafu K_n, v nichž každý vrchol i má stupeň právě d_i (pro $i = 1, 2, \ldots, n$) je roven*

$$\frac{(n-2)!}{(d_1-1)!(d_2-1)!\ldots(d_n-1)!}.$$

Důkaz. Indukcí podle n. Pro $n = 1, 2$ je tvrzení triviální, nechť tedy $n > 2$. Protože součet d_i je menší než $2n$, existuje i takové, že $d_i = 1$.

Po případném přejmenování vrcholů můžeme předpokládat, že $d_n = 1$. (Jinak řečeno: když dokážeme tvrzení za předpokladu $d_n = 1$, bude pak dokázáno i pro libovolnou hodnotu d_n.)

Buď $\mathcal{T}$ množina všech koster grafu K_n, v nichž má každý vrchol i stupeň d_i. Rozdělme kostry z $\mathcal{T}$ do $n-1$ skupin: $\mathcal{T}_j$ budou ty kostry z $\mathcal{T}$, ve kterých je vrchol n spojen s vrcholem j. Nyní uvažme kostru z nějakého $\mathcal{T}_j$, a vymažme z ní vrchol n společně s (jedinou) hranou do něj zasahující. Tím dostaneme kostru grafu K_{n-1}, v níž je stupeň vrcholu i roven d_i pro $i \neq j$ a $d_j - 1$ pro $i = j$. Je snadno vidět, že to definuje bijekci mezi množinou koster $\mathcal{T}_j$ a množinou $\mathcal{T}'_j$ všech koster grafu K_{n-1} se stupni $d_1, d_2, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_{n-1}$ (protože různé kostry z $\mathcal{T}_j$ dávají různé kostry z $\mathcal{T}'_j$, a z každé kostry z $\mathcal{T}'_j$ můžeme dostat kostru z $\mathcal{T}_j$ tím, že přidáme vrchol n a spojíme jej s vrcholem j).

Podle indukčního předpokladu pak máme

$$|\mathcal{T}_j| = |\mathcal{T}'_j| = \frac{(n-3)!}{(d_1-1)!\cdots(d_{j-1}-1)!(d_j-2)!(d_{j+1}-1)!\cdots(d_{n-1}-1)!} =$$

$$= \frac{(n-3)!(d_j-1)}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!}.$$

Tento vzorec platí i když $d_j = 1$ (pak dává 0, což souhlasí s tím, že žádná kostra se stupněm $d_j - 1 = 0$ u vrcholu j neexistuje).

Proto hledaný počet koster na n vrcholech se stupni $d_1, d_2, \ldots, d_n$, kde $d_n = 1$, je roven

$$\sum_{j=1}^{n} |\mathcal{T}_j| = \sum_{j=1}^{n-1} \frac{(n-3)!(d_j-1)}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!} =$$

$$= \left(\sum_{j=1}^{n-1}(d_j-1)\right) \frac{(n-3)!}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!} =$$

$$= \frac{(n-2)(n-3)!}{(d_1-1)!(d_2-1)!\cdots(d_{n-1}-1)!}.$$

Protože $d_n = 1$, můžeme do jmenovatele beze škody přidat činitel $(d_n - 1)! = 0! = 1$, a tím jsme udělali indukční krok. □

Nyní dokážeme větu 8.1.1. Budeme sčítat přes všechna možná skóre, a využijeme přitom multinomické věty 3.3.4:

$$\kappa(K_n) = \sum_{\substack{d_1,d_2,\dots,d_n\geq 1\\ d_1+d_2+\cdots+d_n=2n-2}} \frac{(n-2)!}{(d_1-1)!(d_2-1)!\cdots(d_n-1)!} =$$

$$= \sum_{\substack{k_1+k_2+\cdots+k_n=n-2\\ k_1,\dots,k_n\geq 0}} \frac{(n-2)!}{k_1!k_2!\cdots k_n!} = \underbrace{(1+1+\cdots+1)}_{n\times}{}^{n-2} = n^{n-2}.$$

□

Cvičení

1. (a)* Najděte počet stromů (na daných n vrcholech), v nichž každý vrchol má stupeň 1 nebo 3.

   (b)* Co když připustíme stupně 1, 2 a 3?

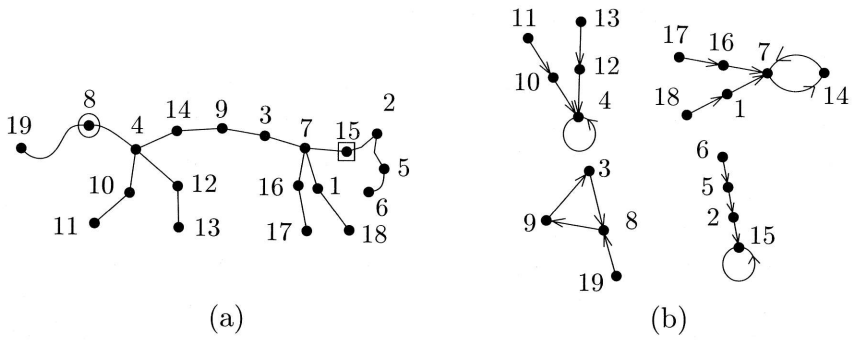
8.3 Důkaz s obratlovci

Definujeme, co je *obratlovec* na množině vrcholů V uvažovaného úplného grafu K_n (viz obr. 8.1(a)): je to kostra, u níž navíc je jeden vrchol označen čtverečkem a jeden vrchol kroužkem (nevylučujeme, že týž vrchol je označen čtverečkem i kroužkem). Označme množinu všech obratlovců písmenem $\mathcal{O}$.

Z každé kostry můžeme stvořit právě n^2 různých obratlovců, proto počet všech koster je roven $|\mathcal{O}|/n^2$. Ukážeme nyní

8.3.1 Lemma. *Existuje bijekce F mezi množinou $\mathcal{O}$ všech obratlovců a množinou všech zobrazení množiny V do sebe.*

Počet zobrazení n-prvkové množiny do sebe je n^n, obratlovců je podle lemmatu stejně, a tudíž koster je n^{n-2}.



Obrázek 8.1: (a) Obratlovec na 19 vrcholech, (b) jemu odpovídající graf zobrazení.

Důkaz lemmatu. Konstrukci bijekce F ukážeme na příkladu na obr. 8.1. Vyjdeme z obratlovce O nakresleného na obrázku (a). Označené vrcholy □ a ◯ jsou spojeny jedinou cestou, kterou nazveme *páteř*. Vypišme si čísla vrcholů páteře do řádky v pořadí podle velikosti, a potom do další řádky znovu v pořadí, jak jdou od ◯ k □:

3	4	7	8	9	14	15
8	4	14	9	3	7	15

Definujeme nyní na vrcholech páteře pomocný orientovaný graf P: uděláme šipku z každého vrcholu z horní řádky do vrcholu napsaného pod ním v dolní řádce. Poněvadž z každého vrcholu vychází právě jedna šipka a také do každého vrcholu jedna šipka vchází, je graf P disjunktním sjednocením orientovaných cyklů (případně samotných vrcholů se smyčkou). Můžeme také říci, že páteř definuje permutaci svých vrcholů a P sestává právě z cyklů této permutace, viz část 3.2. V našem příkladu jsou posloupnosti vrcholů těchto cyklů, srovnané v pořadí podle šipek, $(3, 8, 9)$, (4), $(7, 14)$ a (15).

Podíváme se nyní zpátky na obratlovce O. Odebereme-li z něj na chvíli všechny hrany páteře, rozpadne se na jednotlivé komponenty (opět stromy). Orientujme hrany každé komponenty tak, že směřují k (jedinému) vrcholu páteře v této komponentě. Tím vznikne další

množina orientovaných hran na množině V. Definujeme nyní orientovaný graf G na množině V, jehož hranami budou jednak právě definované orientované hrany komponent, jednak všechny hrany pomocného grafu P. Na obrázku je to velmi názorné: nakreslíme cykly grafu P, a potom ke každému vrcholu (původně z páteře) přikreslíme strom, který přes něj byl zavěšen na páteři obratlovce, viz obrázek (b).

Tvrdíme nyní, že výsledný orientovaný graf G je grafem zobrazení, to znamená, že z každého vrcholu vychází právě jedna hrana. Pro vrcholy páteře jsme to již konstatovali. Pro ostatní vrcholy je to proto, že v obratlovci O z nich vede jediná cesta do páteře. Definujeme tedy konečně zobrazení $f = F(O) : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, příslušející obratlovci O: pro každé i, což je vrchol grafu G, položíme $f(i) = j$, kde j je ten vrchol G, do nějž jde šipka z i. V našem konkrétním příkladě bychom dostali zobrazení $1 \mapsto 7$, $2 \mapsto 15$, $3 \mapsto 8$, $4 \mapsto 4$, $5 \mapsto 2$, $6 \mapsto 5$, $7 \mapsto 14$, $8 \mapsto 9$, $9 \mapsto 3$, $10 \mapsto 4$, $11 \mapsto 10$, $12 \mapsto 4$, $13 \mapsto 12$, $14 \mapsto 7$, $15 \mapsto 15$, $16 \mapsto 7$, $17 \mapsto 16$, $18 \mapsto 1$ a $19 \mapsto 8$. Takto každý obratlovec určuje zobrazení.

Zbývá ještě ukázat, že z takto sestrojeného zobrazení lze původního obratlovce zpětně rekonstruovat, a že každé zobrazení se dostane z nějakého obratlovce. To ponecháme do cvičení. □

Cvičení

1. Pro dané zobrazení f konečné množiny V do V definujeme *graf* f, což je orientovaný graf s množinou vrcholů V a hranami z každého $i \in V$ do $f(i)$ (takový graf jsme používali v důkazu výše). Dokažte, že každá komponenta takového grafu je orientovaným cyklem, na jehož vrcholy jsou případně přivěšeny stromy s hranami orientovanými směrem k tomuto cyklu.

2. Popište, jak se ze zobrazení $f = F(O) : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ zpětně získá výchozí obratlovec O, a dokažte, že každé zobrazení $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ se dostane jako $F(O)$ pro nějakého obratlovce O (s využitím cvičení 1).

3.* Nechť $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ je funkce. Navrhněte algoritmus, který pro dané i najde délku periody posloupnosti $(i, f(i), f(f(i)), \ldots)$ (tj. v řeči grafu zobrazení f, délku cyklu, do nějž se dostaneme po šipkách z bodu i), přičemž používá jen konstantní velikost paměti (nezávislou na délce periody). Přitom máte k dispozici podprogram (černou skříňku), vypočítávající hodnoty f.

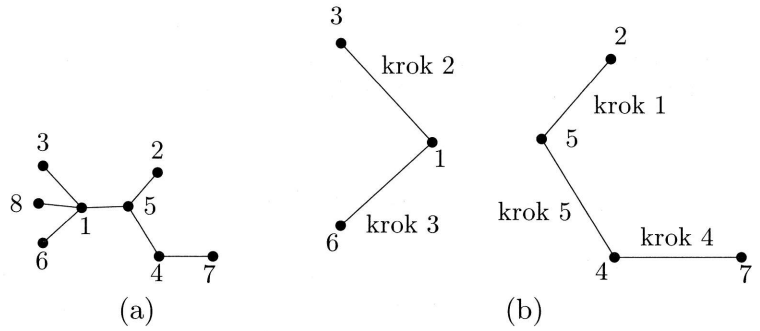
8.4 Důkaz pomocí Prüferova kódu

Ukážeme, jak každou kostru grafu K_n zakódovat $(n-2)$-člennou posloupností, jejíž každý člen je některé z čísel $1, 2, \ldots, n$. Toto kódování bude definovat bijekci mezi všemi kostrami a všemi posloupnostmi uvedeného typu. Poněvadž takových posloupností je zřejmě n^{n-2}, bude tím dokázána věta 8.1.1.

Mějme danou kostru T; příklad viz obr. 8.2(a). Popíšeme, jak sestrojit posloupnost $P = P(T) = (p_1, p_2, \ldots, p_{n-2})$, tzv. Prüferův kód kostry T. Základní myšlenka[1] je, že ze stromu T budeme postupně otrhávat listy, dokud z něj nezbude jen jediná hrana. Budeme tedy konstruovat pomocnou posloupnost stromů $T_0 = T, T_1, T_2, \ldots, T_{n-2} = K_2$ a přitom vyrábět posloupnost P. Předpokládejme, že už jsme zkonstruovali T_{i-1} (na začátku máme $T_0 = T$). Jak víme, má aspoň 1 list (vrchol stupně 1). Vezmeme nejmenší z listů T_{i-1} (připomeňme, že vrcholy T jsou čísla $1, 2, \ldots, n$), a utvoříme T_i odstraněním tohoto listu z T_{i-1}, spolu s příslušnou hranou. Přitom definujeme i-tý člen, p_i, konstruované posloupnosti jako *souseda právě utrženého listu* (tedy nikoliv jako list sám, to je hlavní trik!). Uděláme-li toto pro $i = 1, 2, \ldots, n-2$, definovali jsme posloupnost $P = P(T)$.

Předpokládejme teď, že daná posloupnost P vznikla výše uvedenou konstrukcí z nějaké (nám dosud neznámé) kostry T. Odvodíme, jak zpětně vytvořit T. Ptejme se nejdříve, jak z posloupnosti P poznat, který vrchol kostry T byl utržen jako první; označme jej ℓ_1 (musel to být list). Zřejmě ℓ_1 se nesmí vyskytovat nikde v posloupnosti P (protože do P se zapisují jen vrcholy dosud přítomné v otrhaném stromě). Dále, každý vrchol, který není obsažen v množině $\{p_1, p_2, \ldots, p_{n-2}\}$, musí být listem stromu T (jinak bychom od něj v některé fázi odtrhli list, a tím by se octl v posloupnosti P). Podle pravidla otrhávání listů

[1] Trochu vandalská.



Obrázek 8.2: (a) Kostra s kódem $(5, 1, 1, 4, 5, 1)$, (b) postup její rekonstrukce z kódu.

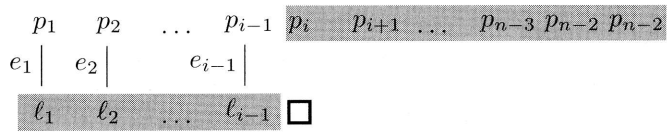
je tudíž ℓ_1 minimum z množiny $\{1, 2, \ldots, n\} \setminus \{p_1, p_2, \ldots, p_{n-2}\}$. Tato množina je vždy neprázdná, a proto je minimum dobře definováno. Můžeme nyní ℓ_1 nakreslit jako první vrchol kostry, a připojit k němu hranou vrchol p_1 (viz obr. 8.2(b)).

Dále postupujeme podobně; známe-li již listy $\ell_1, \ell_2, \ldots, \ell_{i-1}$ utržené v krocích 1 až $i-1$, budeme určovat list ℓ_i. Nemůže to být žádný z vrcholů $p_i, p_{i+1}, \ldots, p_{n-2}$, a ovšem ani z $\ell_1, \ldots, \ell_{i-1}$ – bude to tedy minimum z množiny $\{1, 2, \ldots, n\} \setminus \{p_i, p_{i+1}, \ldots, p_{n-2}, \ell_1, \ell_2, \ldots, \ell_{i-1}\}$ (ta je zase neprázdná). Takto určený list ℓ_i připojíme hranou k vrcholu p_i. Není-li ℓ_i dosud nakreslen, nakreslíme jej ovšem také, podobně pro p_i. Prvních 5 kroků konstrukce je znázorněno na obr. 8.2(b), v 6. kroku bychom dokreslili hranu $\{1, 5\}$.

Po $n-2$ krocích jsme nakreslili $n-2$ hran kostry T, jmenovitě všechny, které byly při otrhávání odstraněny, a zbývá určit, která byla poslední zbývající hrana. Jeden její konec musí ovšem být p_{n-2}, tedy soused posledně odtrženého listu, a druhý konec je ten vrchol, který se nevyskytuje mezi všemi odtrženými listy $\ell_1, \ldots, \ell_{n-2}$ a je různý od p_{n-2}. Na obr. 8.2 to bude hrana $\{1, 8\}$. Tím je metoda rekonstrukce popsána. Ještě ji pro přehlednost jednou shrňme.

Použijeme dvouřádkového zápisu. Do prvního řádku zapíšeme čísla $p_1, p_2, \ldots, p_{n-3}, p_{n-2}, p_{n-2}$ (tedy $n-1$ čísel, přičemž p_{n-2} na konci se

opakuje – tímto opakováním se elegantně zahrne poslední, výjimečný krok do obecného pravidla). Do druhého řádku postupně vyplňujeme čísla $\ell_1, \ell_2, \ldots, \ell_{n-1}$. Byla-li již vyplněna ℓ_1 až ℓ_{i-1}, pak číslo ℓ_i je nejmenší takové, jež se nevyskytuje mezi předchozími čísly v dolním řádku ani mezi čísly v horním řádku od $i$té pozice (včetně) vpravo:



Na silně orámovanou pozici přijde nejmenší číslo, které není mezi čísly vyznačenými šedě. Hrany $e_1, e_2, \ldots$ rekonstruované kostry spojují vždy vrchol z horního řádku s vrcholem napsaným pod ním.

Pro libovolnou $(n-2)$-člennou posloupnost P vytvoří právě uvedený algoritmus nějaký graf G na množině vrcholů $\{1, 2, \ldots, n\}$ s $n-1$ hranami. Též víme, že pokud posloupnost P pocházela z nějaké kostry T, platí $G = T$. Náš úkol ale ještě nekončí: Musíme se přesvědčit, že vzniklý graf G je *vždycky* strom, a že jeho zpětným překódováním do posloupnosti dostaneme tu posloupnost, z níž jsme vyšli.

Označme $G_i = (\{1, 2, \ldots, n\}, \{e_i, e_{i+1}, \ldots, e_{n-1}\})$. Z algoritmu vyplňování dolního řádku je vidět, že do vrcholu ℓ_i zasahuje hrana e_i a žádná z hran $e_{i+1}, \ldots, e_{n-1}$ už do ℓ_i zasahovat nemůže, takže ℓ_i má v G_i stupeň 1. Tedy G_i vznikne z G_{i+1} přidáním listu, a z tvrzení 5.1.3 o postupné výstavbě stromu vidíme, že G je strom. Obecněji, G_i je strom plus $i-1$ izolovaných vrcholů.

Zbývá ověřit, že ℓ_i je nejmenší z listů grafu G_i. Podle definice ℓ_i by menší list mohl být jedině mezi $\ell_1, \ldots, \ell_{i-1}$ nebo mezi $p_i, \ldots, p_{n-2}$. První skupina nepřichází v úvahu (poněvadž $\ell_1, \ldots, \ell_{i-1}$ mají v G_i stupně 0). Uvažme vrchol p_k, $i < k \leq n-2$. V grafu G_k je to soused listu ℓ_k, a protože G_k sestává z izolovaných vrcholů a jedné další komponenty, která má aspoň 2 hrany, má p_k v grafu G_k stupeň minimálně 2. Takže ani v G_i není p_k listem.

Tudíž ℓ_i je nejmenší list v G_i, a G_{i+1} opravdu vznikne z G_i podle procedury Prüferova kódování kostry. Důkaz věty 8.1.1 je hotov. □

8.5 Důkaz pracující s determinanty

Dva důkazy věty 8.1.1 uvedené v tomto oddílu jsou založeny na lineární algebře, a ilustrují pěkný kombinatorický význam determinantu matice. Jsou o něco těžší než předchozí důkazy (a potřebují se v nich základní věty o determinantech), zato ale určují počet koster pro libovolný graf.

Buď G libovolný graf s vrcholy $1, 2, \ldots, n$, $n \geq 2$, a hranami e_1, e_2, $\ldots$, e_m. Zavedeme $n \times n$ matici Q, zvanou *Laplaceova matice* grafu G, jejíž prvky q_{ij} jsou určeny následujícím předpisem:

$$\begin{aligned} q_{ii} &= \deg_G(i) && i = 1, 2, \ldots, n \\ q_{ij} &= \begin{cases} -1 & \text{pro } \{i,j\} \in E(G) \\ 0 & \text{jinak} \end{cases} && i, j = 1, 2, \ldots, n,\ i \neq j. \end{aligned}$$

Brzy se nám bude hodit pozorování, že součet všech řádků Laplaceovy matice je vždy nulový vektor.

Dále nechť Q_{ij} značí matici $(n-1) \times (n-1)$, která vznikne z matice Q vyškrtnutím i-tého řádku a j-tého sloupce. Platí následující pozoruhodná

8.5.1 Věta. *Pro každý graf G platí $\kappa(G) = \det Q_{11}$.*

Věta ve skutečnosti říká, že $\kappa(G) = \det Q_{ii}$ pro libovolný vrchol i grafu G, neboť vrcholy grafu si můžeme očíslovat jak chceme. Obecněji dokonce platí $\kappa(G) = |\det Q_{ij}|$ pro libovolná i a j. To tady nebudeme dokazovat, důkaz je naznačen ve cvičení.

Než začneme větu dokazovat, odvoďme z ní větu 8.1.1. Pro $G = K_n$ má Laplaceova matice na diagonále všude čísla $n-1$, a mimo diagonálu -1. Vymažeme-li první řádek a první sloupec, dostaneme $(n-1) \times (n-1)$ matici tvaru

$$\begin{pmatrix} n-1 & -1 & -1 & \ldots & -1 \\ -1 & n-1 & -1 & \ldots & -1 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ -1 & -1 & -1 & \ldots & n-1 \end{pmatrix}.$$

Determinant spočítáme šikovnými řádkovými a sloupcovými úpravami: odečteme-li od všech řádků kromě prvního první řádek, a potom k prvnímu sloupci přičteme součet všech ostatních, vznikne matice, která na diagonále má $1, n, n, n, \ldots, n$ a všude pod diagonálou nuly. Determinant je pak součin diagonálních prvků, čili n^{n-2}.

Větu 8.5.1 dokážeme dvěma způsoby. První z nich je kratší a grafovější. Druhý využívá víc lineární algebry a asi je z něj trochu lépe vidět, proč věta platí.

První důkaz věty 8.5.1. Dělá se indukcí, a aby fungovala, potřebujeme tvrzení věty zesílit. Budeme je dokazovat i pro multigrafy, neboli grafy s násobnými hranami. Ty jsme zmiňovali v oddílu 4.5: každá dvojice vrcholů může být spojena libovolným počtem hran (žádnou, jednou, nebo několika). Jsou-li vrcholy u a v spojeny více hranami, potom kostry odlišujeme podle toho, kterou z nich užijí. Následující multigraf má kupříkladu 6 koster:

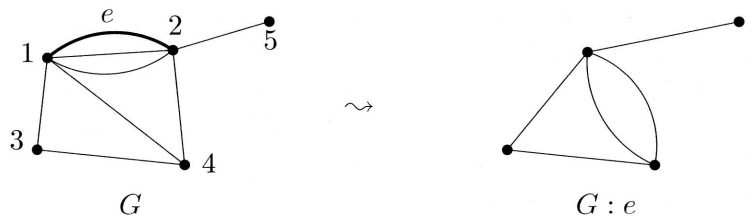


Smyčky v našich grafech připouštět nebudeme, poněvadž nemají na počet koster vliv. Jak vypadá Laplaceova matice multigrafu? Jsou-li vrcholy u a v spojeny m hranami, potom $q_{uv} = -m$. Diagonální prvek q_{uu} je pak stupeň vrcholu u včetně násobností hran (například prostřední vrchol grafu na předchozím obrázku má stupeň 5).

Dále budeme spoléhat na vzoreček

$$\kappa(G) = \kappa(G - e) + \kappa(G : e), \tag{8.1}$$

kde e je libovolná hrana grafu G, $G - e$ je graf po jejím odebrání, a $G : e$ značí graf po *kontrakci* hrany e. To znamená, že hrana e se z G vynechá a její koncové vrcholy se pak slepí do jednoho vrcholu. Touto operací se mohou objevit nové násobné hrany – to je rozdíl proti operaci kontrakce hrany zavedené v části 6.8. Pokud ale byly slepené vrcholy spojeny více hranami než jenom e, tyto hrany se zruší (mohly by se místo toho stát smyčkami na slepeném vrcholu, ale zde smyčky neuvažujeme). Na obrázku je příklad kontrakce:



Abychom nahlédli vzoreček (8.1), všechny kostry grafu G rozdělíme do dvou skupin. První skupina jsou kostry neobsahující hranu e, které přesně odpovídají kostrám grafu $G-e$ a přispějí člen $\kappa(G-e)$. Druhá skupina jsou kostry obsahující e, a ty jsou ve vzájemně jednoznačné korespondenci s kostrami $G:e$, jak naznačuje obrázek



a jak si čtenář může v klidu rozvážit, a je jich tedy $\kappa(G:e)$.

Ještě potřebujeme rozmyslet, co operace odebrání hrany a kontrakce hrany udělají s Laplaceovou maticí. Přesněji řečeno, předpokládáme, že hrana e má koncové vrcholy 1 a 2, a podíváme se, jak se změní matice Q_{11}. Pro odebrání hrany je to velmi jednoduché: označíme-li Q' Laplaceovu matici grafu $G-e$, pak Q'_{11} vznikne z Q_{11} zmenšením prvku v levém horním rohu o 1 (protože odebrání e ovlivní jedině pozice $(1,1)$, $(1,2)$, $(2,1)$ a $(2,2)$ v Laplaceově matici, a nás zajímá Laplaceova matice po vymazání prvního řádku i sloupce).

Při kontrakci hrany e vrcholy 1 a 2 zaniknou a místo nich se objeví nový vrchol, vzniklý jejich slepením. Očíslujme vrcholy grafu $G:e$ třeba tak, že slepený vrchol má číslo 1 a starý vrchol číslo $i \geq 3$ teď má číslo $i-1$, a nechť Q'' značí Laplaceovu matici $G:e$ při tomto očíslování. Je snadno vidět, že $Q''_{11} = Q_{11,22}$, což značí matici Q po vymazání prvního a druhého sloupce a prvního a druhého řádku.

Například pro graf G na předchozích dvou obrázcích máme

$$Q_{11} = \begin{pmatrix} 5 & 0 & -1 & -1 \\ 0 & 2 & -1 & 0 \\ -1 & -1 & 3 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}, \quad Q''_{11} = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Teď zahájíme vlastní důkaz indukcí. Budeme dokazovat, že pro každý multigraf G s nanejvýš m hranami platí $\kappa(G) = \det Q_{11}$, indukcí podle m.

Pokud v multigrafu G z vrcholu číslo 1 nevychází žádná hrana, máme $\kappa(G) = 0$. První řádek Laplaceovy matice je celý nulový, a jelikož řádky Laplaceovy matice mají vždy nulový součet, má i matice Q_{11} nulový součet řádků. Proto $\det Q_{11} = 0$ a dokazované tvrzení platí. Speciálně tím dostáváme platnost případu $m = 0$ jako základ indukce.

Zajímavější je druhý případ, kdy z vrcholu číslo 1 vychází aspoň jedna hrana. Jednu takovou hranu zvolíme a pojmenujeme ji e, a zvolíme očíslování ostatních vrcholů tak, aby druhý koncový vrchol byl 2. Značí-li Q, Q' a Q'' po řadě Laplaceovy matice grafů G, $G-e$ a $G:e$ jako v předchozím, podle vzorečku (8.1) a podle indukčního předpokladu máme

$$\kappa(G) = \kappa(G-e) + \kappa(G:e) =$$

$$= \det Q'_{11} + \det Q''_{11} = \det Q'_{11} + \det Q_{11,22}.$$

Jak známo, determinant matice je lineární funkcí každého řádku, a matice Q_{11} vznikne z Q'_{11} přičtením vektoru $e_1 = (1,0,0,\ldots,0)$ k prvnímu řádku. Tedy $\det Q_{11} = \det Q'_{11} + \det R$, kde R má v prvním řádku vektor e_1 a ostatní řádky se shodují s Q_{11}. Nyní podle vzorce pro rozvoj determinantu podle řádku platí $\det R = \det Q_{11,22}$, takže $\det Q'_{11} + \det Q_{11,22} = \det Q'_{11} + \det R = \det Q_{11}$. To je konec indukčního kroku a také prvního důkazu věty 8.5.1. Ještě podotkněme, že jsme potřebovali jen velmi speciální případ vzorce pro rozvoj determinantu podle řádku, kdy v tom řádku je jedna jednička a jinak samé nuly, a tento případ je ihned vidět z definice determinantu. □

Druhý důkaz věty 8.5.1. Nejdříve pevně zvolíme libovolnou *orientaci* $\vec{G}$ grafu G, tj. pro každou hranu e_k vybereme jeden její vrchol jako *začátek* a druhý jako *konec* (terminologie pro orientované grafy se probírá v části 4.6). Příslušnou orientovanou hranu budeme značit také e_k. Je zajímavé, že pro důkaz nějakou orientaci potřebujeme, přestože výsledek na ní nebude záležet!

Definujeme teď pomocnou matici $D = D_{\vec{G}}$ (zvanou *matice incidence* pro zvolenou orientaci $\vec{G}$). Bude mít n řádků (odpovídají vrcholům grafu $\vec{G}$) a m sloupců (odpovídají hranám $\vec{G}$), a bude zadána takto:

$$d_{ik} = \begin{cases} -1 & \text{je-li } i \text{ začátek hrany } e_k \\ 1 & \text{je-li } i \text{ konec hrany } e_k \\ 0 & \text{jinak, tedy pro } i \notin e_k \end{cases}$$

Všimněme si, že matice D má v každém sloupci právě jednu 1, jednu -1 a zbytek 0, speciálně tedy součet všech řádek je nulový vektor.

Připomeňme, že je-li A matice, značí A^T matici k ní transponovanou, tj. A^T má na místě (i,j) prvek a_{ji}. Označme dále B matici vzniklou z D odebráním prvního řádku. Nejprve uvedeme do souvislosti matici D a Laplaceovu matici grafu G:

8.5.2 Lemma. *Platí $DD^T = Q$ a $BB^T = Q_{11}$ (kde $D = D_{\vec{G}}$ pro nějakou libovolnou orientaci $\vec{G}$ grafu G).*

Důkaz. Podle definice násobení matic je prvek v pozici (i,j) v součinu DD^T roven $\sum_{k=1}^{m} d_{ik}d_{jk}$. Pro $i = j$ je $d_{ik}d_{jk} = d_{ik}^2$ rovno 1, pokud i je začátek nebo konec hrany e_k, a 0 jinak, tedy uvedený součet je právě stupeň vrcholu i v grafu G. Pro $i \neq j$ je součin $d_{ik}d_{jk}$ nenulový v jediném případě, totiž když $e_k = \{i,j\}$, a tehdy je roven -1. Srovnáním s definicí Laplaceovy matice vidíme, že $DD^T = Q$. Druhá rovnost v lemmatu plyne prostě z definice násobení matic. □

Teď první souvislost koster s determinanty:

8.5.3 Lemma. *Buď T nějaký graf na množině vrcholů $\{1,2,\ldots,n\}$ s $n-1$ hranami ($n \geq 2$), a $\vec{T}$ nějaká jeho orientace. Buď $D_{\vec{T}}$ matice incidence orientovaného grafu $\vec{T}$, a nechť C označuje matici vzniknou z matice $D_{\vec{T}}$ vynecháním jejího prvního řádku. Potom* $\det C$ *má jednu z hodnot* 0, 1, -1, *a je nenulový právě když T je strom (tj. kostra úplného grafu na $\{1,2,\ldots,n\}$).*

Důkaz povedeme indukcí podle n, počtu vrcholů. Pro $n = 2$ je situace jednoduchá – T má jedinou hranu a je tedy kostrou, a jediný prvek matice C je 1 nebo -1.

Uvažme tedy obecné $n > 2$, a rozlišme dva případy podle toho, jestli některý z vrcholů $2,3,\ldots,n$ má v grafu T stupeň 1.

Nejprve předpokládejme že takový vrchol stupně 1 existuje. Můžeme případně přečíslovat vrcholy tak, aby stupeň 1 měl vrchol n. To znamená, že matice C má v posledním řádku jediný nenulový prvek (rovný 1 nebo -1), a sice v k-tém sloupci.

Podle vzorce z lineární algebry pro rozvoj determinantu podle řádku matice, použitého na i-tý řádek naší $(n-1)\times(n-1)$ matice C, můžeme psát

$$\det C = \sum_{j=1}^{n-1} (-1)^{i+j} c_{ij} \det C_{ij},$$

(C_{ij} je matice C po vynechání i-tého řádku a j-tého sloupce). Speciálně, vezmeme-li $i = n-1$, máme pouze jediný nenulový člen (protože pouze prvek v k-tém sloupci je nenulový):

$$\det C = (-1)^{n-1+k} c_{n-1,k} \det C_{n-1,k},$$

a tedy $|\det C| = |\det C_{n-1,k}|$.

Tuto zmenšenou matici $C' = C_{n-1,k}$ můžeme dostat vymazáním prvního řádku z incidenční matice $D_{\vec{T}'}$ menšího orientovaného grafu $\vec{T}'$, vzniklého z $\vec{T}$ vynecháním vrcholu n a hrany e_k. Podle indukčního předpokladu tedy víme, že $|\det C'|$ je 1 nebo 0 podle toho, je-li T' (tj. „neorientovaná verze“ $\vec{T}'$) kostra nebo ne. Protože jsme ale z T odstranili vrchol stupně 1 (list), je T' kostra právě když T je kostra. Tím

jsme udělali indukční krok pro případ, že některý z vrcholů $2, 3, \ldots, n$ má v T stupeň 1.

Přejděme k druhému případu, kdy žádný z vrcholů $2, 3, \ldots, n$ nemá v T stupeň 1. Nejprve nahlédneme, že za této situace má T izolovaný vrchol (kdyby tomu tak nebylo, má vrchol 1 stupeň aspoň 1 a ostatní vrcholy stupeň aspoň 2, tedy součet stupňů je aspoň $2n-1$, na což $n-1$ hran grafu T nestačí).

Z existence izolovaného vrcholu vyplývá, že T není kostra; k završení důkazu potřebujeme ukázat, že $\det C = 0$. Je-li izolovaným vrcholem některý z $2, 3, \ldots, n$, určuje v matici C nulový řádek. Je-li izolovaným vrcholem 1, je součet všech řádků matice C roven nulovému vektoru (protože součet všech řádek matice $D_{\vec{T}}$ je nulový). V obou případech máme $\det C = 0$. □

Podle právě dokázaného lemmatu teď víme, že počet koster grafu G je přesně roven počtu čtvercových $(n-1)\times(n-1)$ podmatic matice B s nenulovým determinantem. K dokončení důkazu věty 8.5.1 využijeme jednoho tvrzení o determinantech.

8.5.4 Věta (Binetova-Cauchyho věta). *Nechť A je libovolná matice s n řádky a m sloupci. Potom*

$$\det(AA^T) = \sum_I \det(A_I)^2,$$

kde se sčítá přes všechny n-prvkové podmnožiny $I \in \binom{\{1,2,\ldots,m\}}{n}$, a kde A_I značí matici vzniklou z A vyškrtáním všech sloupců, jejichž indexy neleží v I.

Pro úplnost uvedeme důkaz této věty, ale nejdříve se podíváme, jak z ní plyne věta 8.5.1. S tím, co už víme, je to velmi prosté. Podle lemmatu 8.5.2 a potom podle věty 8.5.4 je

$$\det Q_{11} = \det(BB^T) = \sum_{I\in\binom{\{1,2,\ldots,m\}}{n-1}} \det(B_I)^2,$$

a podle lemmatu 8.5.3 vidíme, že posledně uvedený výraz je právě počet koster G. □

Důkaz věty 8.5.4. Označme $M = AA^T$. Rozvineme determinant matice M podle definice, tedy

$$\det M = \sum_\pi \operatorname{sgn}(\pi) \prod_{i=1}^n m_{i,\pi(i)},$$

kde se sčítá přes všechny permutace π množiny $\{1, 2, \ldots, n\}$, a kde $\operatorname{sgn}(\pi)$ značí *znaménko* permutace π (pro každou permutaci je $+1$ nebo -1). Definice znaménka zde nebudeme přímo potřebovat, proto si připomeneme pouze následující

8.5.5 Fakt. *Pro libovolnou permutaci π množiny $\{1, 2, \ldots, n\}$ a indexy i, j, $1 \le i < j \le n$, označme symbolem $\pi_{i\leftrightarrow j}$ permutaci, jejíž hodnota pro i je $\pi(j)$, hodnota pro j je $\pi(i)$ a hodnoty pro všechna ostatní čísla se shodují s hodnotami π. Potom platí $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi_{i\leftrightarrow j})$.* □

Do rozvoje determinantu M dosadíme hodnoty prvků m_{ij}, tedy $m_{ij} = \sum_{k=1}^m a_{ik}a_{jk}$, a roznásobíme každý ze součinů. Dostáváme

$$\det M = \sum_\pi \operatorname{sgn}(\pi) \sum_{k_1,k_2,\ldots,k_n=1}^m \prod_{i=1}^n a_{i,k_i}a_{\pi(i),k_i}.$$

Přejdeme nyní k zápisu, který bude v dalším lépe vyhovovat. Volbu n-tice sumačních indexů $k_1, \ldots, k_n$ ve vnitřní sumě můžeme chápat jako volbu zobrazení $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$, kde $f(i) = k_i$. V tomto novém zápisu tedy máme

$$\det M = \sum_\pi \operatorname{sgn}(\pi) \sum_{f:\{1,2,\ldots,n\}\to\{1,2,\ldots,m\}} \prod_{i=1}^n a_{i,f(i)}a_{\pi(i),f(i)}.$$

V uvedené sumě dále zaměníme pořadí sumace; napřed budeme sčítat podle funkce f, a potom podle permutace π. Přitom ještě pro pohodlnější zápis zavedeme označení

$$P(f,\pi) = \prod_{i=1}^{n} a_{i,f(i)} a_{\pi(i),f(i)},$$

$$S(f) = \sum_{\pi} \operatorname{sgn}(\pi) P(f,\pi)$$

a potom máme

$$\det M = \sum_{f:\{1,2,\dots,n\}\to\{1,2,\dots,m\}} S(f).$$

Klíčové pro celý důkaz je následující

8.5.6 Lemma. *Pokud funkce $f : \{1,2,\dots,n\} \to \{1,2,\dots,m\}$ není prostá, potom $S(f) = 0$ (pro libovolnou volbu matice A).*

Důkaz lemmatu: Nechť i, j jsou indexy takové, že $f(i) = f(j)$. Potom pro libovolnou permutaci π jsou součiny $P(f,\pi)$ a $P(f,\pi_{i\leftrightarrow j})$ (kde užíváme označení z faktu 8.5.5) stejné. Probíhá-li π všechny permutace, potom také $\pi_{i\leftrightarrow j}$ probíhá všechny permutace, takže máme

$$S(f) = \sum_{\pi} \operatorname{sgn}(\pi_{i\leftrightarrow j}) P(f,\pi_{i\leftrightarrow j}) = \sum_{\pi} -\operatorname{sgn}(\pi) P(f,\pi) = -S(f),$$

tedy $S(f) = 0$ jak tvrdí lemma. □

Dokončení důkazu věty 8.5.4. Podle lemmatu můžeme psát

$$\det(AA^T) = \sum_{f:\{1,2,\dots,n\}\hookrightarrow\{1,2,\dots,m\}} S(f),$$

kde se sčítá přes všechny *prosté* funkce z $\{1,2,\dots,n\}$ do $\{1,2,\dots,m\}$.

Zvolme nyní nějakou množinu $I \in \binom{\{1,2,\dots,m\}}{n}$, a počítejme

$$\det(A_I)^2 = \det(A_I)\det(A_I^T) = \det(A_I A_I^T).$$

Tento determinant můžeme rozvinout přesně stejným postupem, jak jsme to udělali pro determinant AA^T; tentokrát dostaneme

$$\det(A_I A_I^T) = \sum_{f:\{1,2,\dots,n\}\hookrightarrow I} S(f).$$

Máme tedy

$$\sum_{I\in\binom{\{1,2,\dots,m\}}{n}} \det(A_I)^2 = \sum_{I\in\binom{\{1,2,\dots,m\}}{n}} \sum_{f:\{1,2,\dots,n\}\hookrightarrow I} S(f) =$$

$$\sum_{f:\{1,2,\dots,n\}\hookrightarrow\{1,2,\dots,m\}} S(f) = \det(AA^T)$$

(předposlední rovnost plyne z toho, že prostá funkce

$$f : \{1,2,\dots,n\}\hookrightarrow\{1,2,\dots,m\}$$

jednoznačně určuje n-prvkovou množinu I svých hodnot). Tím je věta 8.5.4 dokázána. □

Cvičení

1. V tomto cvičení G je graf na n vrcholech, Q jeho Laplaceova matice, a Q^* značí matici, jejíž prvek v pozici (i,j) je roven $(-1)^{i+j}\det Q_{ij}$.

   (a) Ukažte $\det Q = 0$.

   (b) Ukažte, že je-li graf G souvislý, má jeho Laplaceova matice hodnost $n-1$.

   (c)* Ukažte, že pro nesouvislý graf G má Laplaceova matice hodnost nejvýš $n-2$. Z toho odvoďte, že pro nesouvislý G je Q^* nulová matice.

   (d) Ukažte, že je-li G souvislý a $x \in \mathbf{R}^n$ je libovolný vektor, pak $Qx = 0$ právě když x je násobkem vektoru $(1,1,\dots,1)$.

   (e)* Dokažte, že součin QQ^* je nulová matice. Pomocí (d) pak odvoďte, že všechny prvky matice Q^* jsou stejné.

2. Řešte cvičení 2 k úvodu této kapitoly pomocí věty 8.5.1.

3.* Buď G (neorientovaný) graf, a M jeho matice incidence; tj., má-li G vrcholy $v_1, v_2, \ldots, v_n$ a hrany $e_1, e_2, \ldots, e_k$, pak M je $n \times m$ matice splňující

$$m_{ik} = \begin{cases} 1 & \text{jestliže } v_i \in e_k \\ 0 & \text{jinak.} \end{cases}$$

Dokažte, že následující dvě podmínky jsou ekvivalentní:

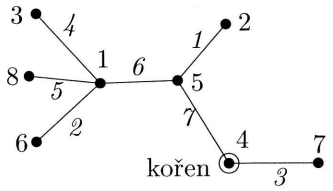
(i) G je bipartitní.

(ii) Libovolná čtvercová podmatice M (vzniklá z M vypuštěním některých řádků a sloupců) má determinant 0,1 nebo -1 (matice M s touto vlastností se jmenuje *unimodulární*).

8.6 Důkaz zatím asi nejjednodušší

I v dobře prozkoumaných oblastech matematiky je stále co objevovat. Tak například zcela nedávno našel matematik-statistik Jim Pitman z Kalifornské university v Berkeley nový, velmi jednoduchý důkaz Cayleyho formule. Zazáří v něm počítání dvěma způsoby, zdánlivě velmi jednoduchý trik, o jehož užitečnosti jsme se již přesvědčili v předchozí kapitole. Nepoužije se přímo, ale na vhodné zjemnění původní úlohy.

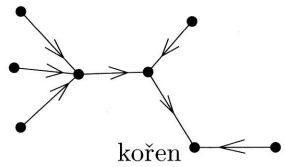
V tomto důkazu Cayleyho formule budeme dvěma způsoby počítat *povykosy*. Co je to povykos? Zkrácený název pro *po*stup *výr*oby *ko*řenového *s*tromu (o kořenových stromech viz část 5.2). Formálně je povykos definován jako uspořádaná trojice $(T, r, č)$, kde T je strom na množině vrcholů $V = \{1, 2, \ldots, n\}$, $r \in V$ je jeho kořen, a $č$ je očíslování hran, neboli bijekce $č : E(T) \to \{1, 2, \ldots, n-1\}$. Na obrázku je příklad povykosu:



Můžeme si představovat, že začneme s prázdným grafem na množině vrcholů V a vyrábíme kořenový strom postupným přidáváním hran; očíslování $č$ kóduje pořadí přidávání hran. Pro každý strom T můžeme

kořen r volit n způsoby a pro očíslování hran $č$ je $(n-1)!$ možností, takže počet povykosů je $n(n-1)!\,\kappa(K_n)$.

Pro druhý způsob počítání povykosů budeme kořenový strom uvažovat jako orientovaný strom, kde všechny šipky směřují ke kořenu:



Naopak, každá orientace stromu, pro niž existuje právě jeden vrchol, který není počátkem žádné šipky, odpovídá jednoznačně kořenovému stromu (zmíněný jediný vrchol je kořen). I povykos teď budeme interpretovat v této orientované podobě, a budeme počítat, kolik povykosů můžeme dostat, začneme-li z prázdného orientovaného grafu a budeme postupně přidávat šipky v $n-1$ krocích.

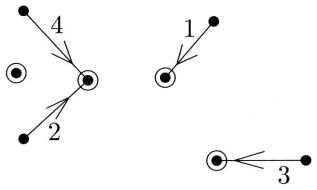
První šipka musí spojovat dva různé vrcholy, a tudíž ji můžeme přidat $n(n-1)$ způsoby. Pro druhou šipku máme ještě další omezující podmínku: nesmí vycházet z téhož vrcholu jako šipka první. Jaká jsou obecně omezení na přidání další šipky?

(A) Nesmíme vytvořit kružnici (v neorientovaném smyslu), tedy nová šipka musí spojovat dvě různé komponenty již vytvořeného grafu (komponenty se opět myslí bez ohledu na orientaci).

(B) Na konci musí z každého vrcholu až na jediný vycházet nějaká šipka, přičemž máme k dispozici celkem $n-1$ šipek. Nesmíme tedy promarnit ani jedinou, a každá nová šipka musí vycházet z vrcholu, z nějž dosud žádná šipka nevycházela.

Klíčové pozorování je, že *v každé komponentě již vytvořeného grafu je právě jeden vrchol, z nějž nevychází žádná šipka*. To je proto, že komponenta má nějakých m vrcholů a $m-1$ hran, a z každého vrcholu vychází nejvýš jedna šipka, neboť jsme i v předchozím postupu dodržovali podmínku (B).

Po přidání k šipek s dodržením (A) a (B) má graf $n-k$ komponent (ověřte). Obrázek ukazuje situaci po přidání čtyř šipek podle povykosu na prvním obrázku:



Další šipka, číslo $k+1$, může nyní vést do libovolného vrcholu v nějaké z komponent, a vycházet musí z kořene některé jiné komponenty, a pro její přidání máme proto $n(n-k-1)$ možností.

Každý takový postup dává po $n-1$ krocích právě jeden povykos. Proto povykosů je

$$\prod_{k=0}^{n-2} n(n-k-1) = (n-1)!\, n^{n-1}.$$

Porovnáním obou výrazů pro počet povykosů dostáváme Cayleyho vzorec $\kappa(K_n) = n^{n-2}$. □

9

Konečné projektivní roviny

Matematika se často zajímá o objekty, vyznačující se v nějakém smyslu velkou pravidelností, mnoha symetriemi atd. (viz například pravidelné mnohostěny v části 6.6). V této kapitole se budeme zabývat jistými hodně pravidelnými systémy konečných množin, tzv. konečnými projektivními rovinami, a s nimi úzce souvisejícími čtvercovými tabulkami čísel, tzv. ortogonálními latinskými čtverci.

9.1 Definice a vlastnosti konečné projektivní roviny

Konečná projektivní rovina bude množinový systém s jistými speciálními vlastnostmi.

9.1.1 Definice (Konečná projektivní rovina). *Nechť X je nějaká konečná množina, a nechť $\mathcal{P}$ je systém podmnožin množiny X. Dvojice $(X, \mathcal{P})$ se nazývá* konečná projektivní rovina, *pokud splňuje následující axiomy:*

(P0) Existuje čtyřbodová množina $\check{C} \subseteq X$ taková, že $|P \cap \check{C}| \leq 2$ pro každou množinu $P \in \mathcal{P}$.

(P1) Každé dvě různé množiny $P_1, P_2 \in \mathcal{P}$ se protínají právě v jednom bodě, tj. $|P_1 \cap P_2| = 1$.

(P2) Pro každé dva různé body $x_1, x_2 \in X$ existuje právě jedna množina $P \in \mathcal{P}$ taková, že $x_1 \in P$ a $x_2 \in P$.

Je-li $(X, \mathcal{P})$ konečná projektivní rovina, budeme prvkům X říkat *body* a množinám z $\mathcal{P}$ *přímky*. Vztah $x \in P$ (kde $x \in X$ a $P \in \mathcal{P}$) budeme vyjadřovat obratem „bod x leží na přímce P“ nebo taky „přímka P prochází bodem x“. Vyjádříme-li axiomy (P0)–(P2) v této řeči, začnou se podobat povědomým geometrickým tvrzením. Axiom (P1) říká, že každé dvě (různé) přímky se protínají právě v jednom bodě, a (P2) praví, že každými dvěma různými body prochází právě jediná přímka. Axiom (P0) potom požaduje existenci 4 bodů, z nichž žádné 3 neleží na přímce. Jsou-li $a, b \in X$ dva body konečné projektivní roviny, budeme jedinou přímku $P \in \mathcal{P}$ obsahující a i b značit symbolem $\overline{ab}$. Jsou-li $P, P' \in \mathcal{P}$ dvě přímky, budeme jediný bod jejich průniku nazývat jejich *průsečíkem*.

Konečné projektivní roviny jsou konečnou analogií tzv. projektivní roviny (přesněji *reálné projektivní roviny* známé z geometrie. Zmíněná terminologie („projektivní rovina“, „přímky“) poukazuje na tuto analogii. Krátce tedy odbočíme a nastíníme, co je reálná projektivní rovina (což beztak patří k všeobecnému matematickému vzdělání).

V obvyklé (euklidovské) rovině se každé dvě přímky protínají v jednom bodě, až na jednu výjimku – rovnoběžky se neprotínají nikde. V mnoha geometrických úvahách je taková výjimka dosti nepříjemná, neboť vyžaduje rozbor různých speciálních případů v důkazech i v analytických výpočtech. Reálná projektivní rovina je vhodné rozšíření euklidovské roviny o množinu dalších bodů, nazývající se *body v nekonečnu*. Populárně řečeno, každému směru přímek v rovině odpovídá jeden bod v nekonečnu, v němž se všechny přímky rovnoběžné s tímto směrem protínají. Všechny body v nekonečnu leží na jedné společné *přímce v nekonečnu*. Tím se dosáhne toho, že nyní se skutečně každé dvě přímky protínají právě v jednom bodě (který ovšem může ležet v nekonečnu).

Body v nekonečnu zde nejsou nějakou filosofickou záhadností, projektivní rovina je matematickou konstrukcí trochu podobného typu, jako třeba konstrukce racionálních čísel z celých čísel nebo reálných čísel z racionálních, tedy jakési zúplnění. Zájemci najdou tuto konstrukci v části 9.2.

Každé dvě přímky v reálné projektivní rovině se protínají právě v jednom bodě (to je podmínka (P1)), a každými dvěma body prochází právě jedna přímka (to je podmínka (P2)). Mnoho geometrických úvah a konstrukcí v reálné projektivní rovině (zhruba řečeno ty konstrukce, které lze provést samotným pravítkem) se opírá pouze o tyto dva axiomy.

Analogie konečných projektivních rovin s reálnou projektivní rovinou je užitečná jako motivace pojmů a často i pro intuici. Nesmí se však zapomínat, že přísně vzato konečná projektivní rovina je pouze systém konečných množin s vlastnostmi (P0)–(P2), a nelze na ni automaticky přenášet různé další geometrické pojmy a představy. Nejdůležitější rozdíl asi je, že zatímco body na obyčejné geometrické přímce jsou přirozeně uspořádány „podél“ přímky, v konečné projektivní rovině žádné takové přirozené uspořádání nemáme.

9.1.2 Příklad. *Nejmenší konečná projektivní rovina má 7 bodů a 7 přímek (všechny přímky jsou tříbodové) a nazývá se* Fanova rovina. *Je znázorněna na obrázku 9.1(a): body jsou vyznačeny puntíky 1–7, a trojice bodů každé přímky je spojena úsečkou, v jednom případě kruhovým obloukem*[1]*; tyto spojnice jsou označeny a–g.*

Fanova rovina je užitečný matematický objekt, často je nejmenším protipříkladem na různě domněnky apod.

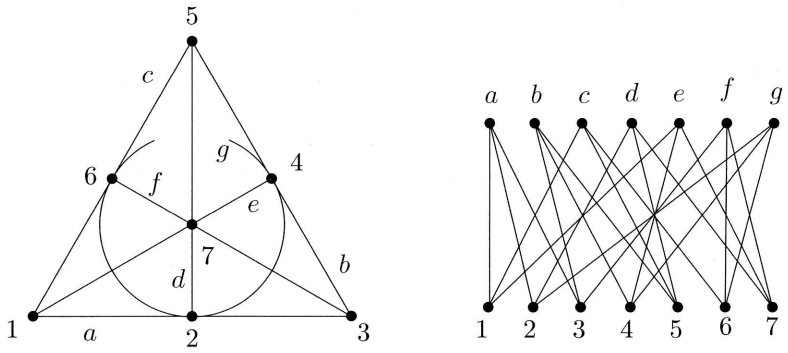
Dokážeme teď několik tvrzení, která ilustrují, že při konstrukci projektivní roviny máme mnohem menší svobodu, než je na první pohled patrné.

9.1.3 Tvrzení. *Buď $(X, \mathcal{P})$ konečná projektivní rovina. Pak všechny její přímky mají stejný počet bodů, tj. $|P| = |P'|$ pro každé $P, P' \in \mathcal{P}$.*

Důkaz. Zvolme libovolné 2 přímky $P, P' \in \mathcal{P}$. Nejprve dokážeme pomocné tvrzení: *Existuje bod $z \in X$, neležící na P ani na P'.*

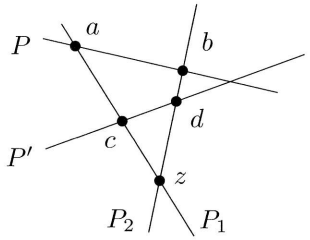
> *Důkaz pomocného tvrzení.* Uvažme množinu $\check{C} \subseteq X$ jako v axiomu (P0); máme $|P \cap \check{C}| \leq 2$, $|P' \cap \check{C}| \leq 2$. Pokud $\check{C}$ není obsaženo v $P \cup P'$, jsme hotovi. Jediná zbývající možnost je, že P protíná $\check{C}$ ve dvou bodech (označme je a, b), a P' protíná $\check{C}$ ve dvou zbývajících bodech (označme je c, d). Uvážíme potom přímky $P_1 = \overline{ac}$ a $P_2 = \overline{bd}$. Nechť z je bod, v němž se P_1 a P_2 protínají.

[1] Dá se ukázat, že sedmici bodů nelze nakreslit do roviny tak, aby každá trojice odpovídající přímce ve Fanově rovině ležela na euklidovské přímce – viz cvičení 6.



Obrázek 9.1: Fanova rovina (a), a její graf incidence (b).

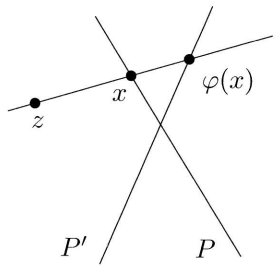
Následující geometrický obrázek situaci ilustruje:



Musíme ale dávat dobrý pozor, abychom v našem důkazu používali jedině podmínek (P0)–(P2), a na intuitivní geometrickou představu podle obrázku nespoléhali – koneckonců konečné projektivní roviny vypadají v mnoha ohledech úplně jinak než „obyčejná“ rovina.

Tvrdíme, že $z \notin P \cup P'$. Přímky P a P_1 se protínají v jediném bodě, totiž v a, takže kdyby $z \in P$, muselo by být $z = a$. To ale není možné, poněvadž pak by přímka P_2 obsahovala body $z = a$, b a d, tedy 3 body z $\check{C}$, což je zakázáno podmínkou (P0). Proto $z \notin P$, a analogicky se ukáže $z \notin P'$. Tím je dokázáno pomocné tvrzení.

Ukážeme teď, že přímky P a P' jsou stejně velké; za tím účelem definujeme zobrazení $\varphi : P \to P'$, o němž se pak ověří, že je to bijekce. Obraz $\varphi(x)$ bodu $x \in P$ definujeme jako průsečík přímek $\overline{zx}$ a P', kde z je bod jako v pomocném tvrzení. Obrázek tomu opět dodá názornosti:



Podle axiomů (P1) a (P2) je bod $\varphi(x)$ dobře definován. Přitom je-li $y \in P'$ libovolný bod, uvažme přímku $\overline{zy}$, a buď x její průsečík s přímkou P. Pak $\overline{zy}$ a $\overline{zx}$ je tatáž přímka, a proto máme $y = \varphi(x)$. Zobrazení φ je tedy bijekce, a proto $|P| = |P'|$. □

9.1.4 Definice (Řád projektivní roviny). Řádem *konečné projektivní roviny* $(X, \mathcal{P})$ *rozumíme číslo* $|P| - 1$, *kde* $P \in \mathcal{P}$ *je libovolná přímka (podle předchozího tvrzení řád nezávisí na tom, kterou konkrétní přímku* P *vybereme).*

Například Fanova rovina je řádu 2 (přímky jsou tříbodové), a dá se dokázat, že je to jediná projektivní rovina řádu 2 (až na případné přejmenování bodů, tj. až na isomorfismus).

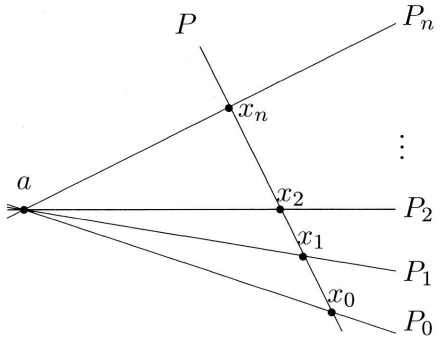
Budeme pokračovat v dokazování vlastností konečných projektivních rovin.

9.1.5 Tvrzení. *Pro každou projektivní rovinu* $(X, \mathcal{P})$ *řádu* n *platí:*

(i) *Každým bodem* $x \in X$ *prochází právě* $n + 1$ *přímek.*

(ii) $|X| = n^2 + n + 1$.

(iii) $|\mathcal{P}| = n^2 + n + 1$.



Obrázek 9.2: Ilustrace k důkazu 9.1.5(ii).

Důkaz (i). Uvažme libovolný bod $x \in X$. Nejdříve nahlédneme, že existuje přímka P jím neprocházející. Je-li totiž $\check{C}$ konfigurace 4 bodů jako v (P0) a a, b, c jsou 3 její body různé od x, potom aspoň jedna z přímek $\overline{ab}$ a $\overline{ac}$ neobsahuje x, jak se snadno zkontroluje. Každým z $n+1$ bodů takové přímky P prochází právě jedna přímka obsahující též x. Přitom každá přímka, procházející bodem x, protne P v nějakém bodě y, a tedy je to přímka tvaru $\overline{xy}$, takže bodem x prochází přesně $n+1$ přímek.

Důkaz (ii). Zvolíme nějakou přímku $P = \{x_0, x_1, x_2, \ldots, x_n\} \in \mathcal{P}$ a bod $a \notin P$, viz obr. 9.2. Označme P_i přímku $\overline{ax_i}$, $i = 0, 1, \ldots, n$. Podle (P1) se každé dvě z těchto přímek, P_i a P_j, protínají právě v jednom bodě, a tím je právě a. Přímky $P_0, P_1, \ldots, P_n$ mají každá kromě a ještě dalších n bodů, a celkem tedy obsahují $(n+1)n+1 = n^2+n+1$ různých bodů. Ukážeme, že libovolný bod $x \in X$ již leží na některé přímce P_i; tím bude dokázáno tvrzení (ii).

Body x a a můžeme podle (P2) proložit nějakou přímku Q. Tato přímka protne, podle (P1), přímku P v některém bodě x_i, a podle (P2) (jednoznačnost) je tedy totožná s přímkou P_i.

Důkaz části (iii) nyní vynecháme. Řekneme si v dalším jeden důležitý princip, podle něhož uvidíme, že (iii) plyne okamžitě z toho, co jsme už dokázali. □

Dualita. Heslovitě se dualita dá vyjádřit jako „záměna rolí bodů a přímek". Abychom to mohli formulovat přesně, zavedeme nejdříve obecnou definici. Mějme nějaký (zatím libovolný) systém $\mathcal{S}$ podmnožin množiny X. Definujeme *duální množinový systém* $(Y, \mathcal{T})$ k systému $(X, \mathcal{S})$. Prvky tohoto nového množinového systému budou množiny z $\mathcal{S}$, tj. $Y = \mathcal{S}$. Pro každý bod $x \in X$ zařadíme do systému $\mathcal{T}$ množinu všech množin $S \in \mathcal{S}$ takových, že $x \in S$. Tím dostaneme soubor $\mathcal{T}$ podmnožin $\mathcal{S}$, jehož množiny odpovídají bodům z X. Zapsáno formulí, máme

$$\mathcal{T} = \Big\{ \{S \in \mathcal{S};\ x \in S\};\ x \in X \Big\}.$$

Jestliže například $X = \{1,2,3\}$ a $\mathcal{S} = \{A, B\}$, kde $A = \{1,2\}$ a $B = \{1,3\}$, potom duální systém $(Y, \mathcal{T})$ bude mít $Y = \mathcal{S} = \{A, B\}$, $\mathcal{T} = \{\{A,B\}, \{A\}, \{B\}\}$.

Ještě jinak si můžeme představit konstrukci duálního množinového systému takto: Definujeme na množině $X \cup \mathcal{S}$ bipartitní graf, tzv. *graf incidence*, v němž každá množina $S \in \mathcal{S}$ bude spojena hranou právě se všemi svými body $x \in S$ (a tudíž bod $x \in X$ bude spojen právě se všemi množinami jej obsahujícími). Stručně můžeme říci, že hrany grafu odpovídají relaci náležení. Pro Fanovu rovinu (což je jistý množinový systém) je tento graf nakreslen na obr. 9.1(b) (vrcholy jsou popsány označením příslušných bodů a přímek)[2]. Potom uvedený přechod k duálnímu systému prostě znamená, že ty vrcholy bipartitního grafu, které jsme dříve chápali jako body, budeme nyní chápat jako množiny, a obráceně, tj. na obrázku bychom jenom překlopili graf vzhůru nohama. V kontextu konečných projektivních rovin se tedy zaměňují body za přímky a přímky za body (podobná dualita se používá i v reálné projektivní rovině).

9.1.6 Tvrzení. *Množinový systém duální ke konečné projektivní rovině je opět konečná projektivní rovina.*

Důkaz. Buď $(X, \mathcal{P})$ konečná projektivní rovina, a $(Y, \mathcal{Q})$ množinový systém k ní duální. Pro něj je potřeba ověřit podmínky (P0)–(P2). Začneme podmínkou (P0). Přeložíme-li ji do řeči výchozího systému

[2] Tento graf se jmenuje *Heawoodův graf* a je to pěkný a zajímavý příklad grafu – i když naše nakreslení moc pěkně nevypadá; dokážete najít hezčí?

$(X, \mathcal{P})$, znamená to, že máme najít 4 přímky $P_1, P_2, P_3, P_4 \in \mathcal{P}$, z nichž žádné 3 nemají společný bod. Uvažme 4-bodovou množinu $\check{C} = \{a, b, c, d\} \subseteq X$ jako v podmínce (P0), a definujme $P_1 = \overline{ab}$, $P_2 = \overline{cd}$, $P_3 = \overline{ad}$, $P_4 = \overline{bc}$. Podíváme-li se na libovolné 3 z těchto 4 přímek, mají vždy 2 z nich společný nějaký bod z $\check{C}$, jímž třetí z nich neprochází. Proto libovolné 3 z přímek $P_1, \ldots, P_4$ mají prázdný průnik. Tím jsme ověřili (P0) pro duální množinový systém.

Přeložíme-li podobně podmínku (P1) pro duální systém, zjistíme, že se požaduje následující: jsou-li $x, x' \in X$ dva různé body, potom existuje právě jedna přímka $P \in \mathcal{P}$ obsahující oba – a to je přesně podmínka (P2) pro $(X, \mathcal{P})$. Podobně zjistíme, že (P2) pro duální systém vyplývá z (P1) pro původní systém $(X, \mathcal{P})$. □

Teď tedy můžeme množinový systém duální ke konečné projektivní rovině oprávněně nazvat *duální projektivní rovina*. Z tvrzení 9.1.5(i) vyplývá, že přechodem k duální projektivní rovině se zachovává řád. Také je vidět, že části (ii) a (iii) tvrzení 9.1.5 jsou navzájem duální, a pokud jsme dokázali jedno z nich, musí platit i druhé.

Obecně, máme-li nějaké pravdivé tvrzení o projektivní rovině řádu n, a zaměníme v něm všude navzájem slova „bod“ a „přímka“, dostaneme opět pravdivý výrok. Přitom ovšem musíme náležitě interpretovat příslušné pojmy, například kde v původním výroku bylo „přímky P_1, P_2 se protínají v bodě x“, bude nyní „body x_1, x_2 jsou spojeny přímkou P“ apod. To je tedy jakýsi „recept na výrobu vět“ a nazývá se *princip duality*. Všimli si ho geometři studující reálnou projektivní rovinu.

Cvičení

1. (a) Najděte příklad množinového systému $(X, \mathcal{P})$ na konečné množině X, který splňuje podmínky (P1), (P2), ale nesplňuje (P0).

   (b) Najděte X a $\mathcal{P}$ jako v (a), kde navíc $|X| \geq 10$, $|\mathcal{P}| \geq 10$, a každá $P \in \mathcal{P}$ má aspoň 2 body.

2. Nechť X je konečná množina a $\mathcal{P}$ systém jejích podmnožin, splňující podmínky (P1), (P2) a následující (P0′):

   Existují aspoň 2 různé přímky $P_1, P_2 \in \mathcal{P}$, z nichž každá má aspoň 3 body.

   Dokažte, že potom $(X, \mathcal{P})$ je konečná projektivní rovina.

3.* Popište všechny množinové systémy $(X, \mathcal{P})$ (kde $X \neq \emptyset$ je konečné), splňující (P1),(P2), ale nikoli (P0).

4. Dokažte část (iii) tvrzení 9.1.5 přímo, bez použití duality.

5.* Nechť $n \geq 2$ a X je množina s $n^2 + n + 1$ prvky a $\mathcal{P}$ je systém tvořený $n^2 + n + 1$ jejími $(n+1)$-prvkovými podmnožinami, z nichž každé 2 se protínají nejvýš v jednom bodě.

   (a) Dokažte, že každá dvojice bodů z X je obsažena v právě jedné množině z $\mathcal{P}$.

   (b) Dokažte, že každým bodem prochází nejvýš $n + 1$ množin.

   (c) Dokažte, že každým bodem prochází právě $n + 1$ množin.

   (d) Dokažte, každé 2 množiny z $\mathcal{P}$ se protínají.

   (e) Ověřte, že $(X, \mathcal{P})$ je projektivní rovina řádu n.

   (V tomto cvičení se hojně využije počítání dvěma způsoby.)

6. Ukažte, že Fanovu rovinu nelze vnořit do „obyčejné“ (euklidovské) roviny, to znamená, že neexistuje 7 přímek a 7 bodů v euklidovské rovině tak, že každá dvojice bodů leží na jedné z přímek a každá dvojice přímek má průsečík v jednom z bodů. Využijte cvičení 6.5.10.

9.2 Konstrukce projektivních rovin

Projektivní roviny řádu 2, 3, 4 a 5 existují, ale žádná projektivní rovina řádu 6 neexistuje! (Dokázat to je dost pracné, musí se rozebrat velmi mnoho případů nebo použít nesnadnou větu.) Projektivní roviny řádů 7,8, a 9 opět existují, řádu 10 nikoliv. Kde je v tom nějaká pravidelnost? Konečná projektivní rovina řádu n existuje, kdykoliv existuje konečné těleso[3] s přesně n prvky, což je právě když n je mocninou nějakého prvočísla. Speciálně tedy existují projektivní roviny libovolně velkých řádů.

[3] V algebraickém smyslu, tj. množina s operacemi sčítání, odčítání, násobení a dělení splňující jisté podmínky; viz dodatek o algebře.

Pro n dělitelné aspoň dvěma různými prvočísly sice n-prvkové těleso neexistuje, ale neví se, zda nemůže přesto existovat nějaká projektivní rovina řádu n. Je známo, že pokud číslo n dává při dělení 4 zbytek 1 nebo 2 a přitom se nedá napsat jako součet dvou čtverců celých čísel, potom projektivní rovina řádu n neexistuje (je to dost těžká věta). To například vylučuje existenci projektivní roviny řádu 6 nebo 14 a mnoha dalších řádů, ale zdaleka nepokrývá všechny možné řády, např. o $n = 10$ nebo 12 to nic neříká.

Existence konečné projektivní roviny řádu 10 je také vyloučena. Tyto výsledky mají zajímavou historii. Pro řád 6 se neexistenci projektivní roviny pokoušel dokázat už Euler, ale podařilo se to až kolem roku 1900 G. Tarrymu. Pro řád 10 se to prokázalo nedávno neobyčejně rozsáhlými výpočty na počítačích (dokonce armádních, totiž armády Spojených států). Pro nejbližší vyšší řád, 12, je existence projektivní roviny stále otevřený problém. Je sice jasné, že takový problém se dá vyřešit probráním konečně mnoha poměrně malých konfigurací, nicméně počet konfigurací je pro soudobou výpočetní techniku příliš obrovský.

Algebraická konstrukce projektivní roviny. Pro zájemce uvedeme, jak se zkonstruuje projektivní rovina. Obzvlášť nás samozřejmě budou zajímat konečné projektivní roviny, ale půvab konstrukce je i v tom, že přesně stejně funguje pro reálnou projektivní rovinu.

Nejdříve konstrukci popíšeme formálně, což může vypadat trochu složitě, protože body výsledné projektivní roviny budou třídy jisté ekvivalence na množině uspořádaných trojic. Když si ale člověk na tyto definice trochu zvykne, ověřit axiomy projektivní roviny není zvlášť těžké. V reálném případě má konstrukce docela názornou geometrickou interpretaci, již zmíníme na závěr. Někomu může geometrická představa pomoci lépe se ve formální konstrukci orientovat, jiného může třeba ještě víc zmást, takže necháváme na čtenáři, jak moc se na ni spolehne.

Konstrukce vychází z nějakého tělesa K. Pro reálnou projektivní rovinu (tj. vhodné rozšíření obvyklé euklidovské roviny o body v nekonečnu) se vezme za K těleso $\mathbf{R}$ všech reálných čísel. Budeme-li za K volit n-prvkové těleso, zkonstruujeme konečnou projektivní rovinu řádu n. Průběžně budeme konstrukci ilustrovat pro tříprvkové těleso K, tj. množinu $\{0, 1, 2\}$ s operacemi sčítání a násobení modulo 3.

Nejprve uvážíme množinu $T = K^3 \setminus \{(0,0,0)\}$, čili množinu všech uspořádaných trojic (x, y, t), kde $x, y, t \in K$ a x, y, t nejsou všechna zároveň rovna nule. Na T definujeme ekvivalenci $\approx$ takto: $(x_1, y_1, t_1) \approx (x_2, y_2, t_2)$ právě když existuje nenulové $\lambda \in K$ takové, že $x_2 = \lambda x_1$, $y_2 = \lambda y_1$ a $t_2 = \lambda t_1$ (není těžké ověřit, že to opravdu je ekvivalence). Body konstruované projektivní roviny budou třídy této ekvivalence. Takto vyrobená projektivní rovina[4] se v literatuře zpravidla označuje PK^2, kde místo K se případně píše konkrétní těleso; např. reálná projektivní rovina se značí $P\mathbf{R}^2$.

Abychom získali o projektivní rovině lepší představu, vybereme si z každé třídy ekvivalence $\approx$ jednu trojici jako reprezentanta. Jako reprezentanty vezmeme ty trojice, *jejichž poslední nenulová složka je rovna* 1. Budou to tedy trojice tvaru $(x, y, 1)$, $(x, 1, 0)$ $(x, y \in K)$ a trojice $(1, 0, 0)$; je snadné si rozmyslet, že každá jiná trojice je ekvivalentní některé z uvedených, a naopak že žádné dvě trojice zmíněných tvarů nemohou být ekvivalentní.

Bylo by nepohodlné mluvit stále o třídách ekvivalence. Proto nadále budeme říkat „bod (x, y, t)“ pro nějakou trojici z T, a budeme tím myslet celou třídu ekvivalence $\approx$ obsahující tento bod.

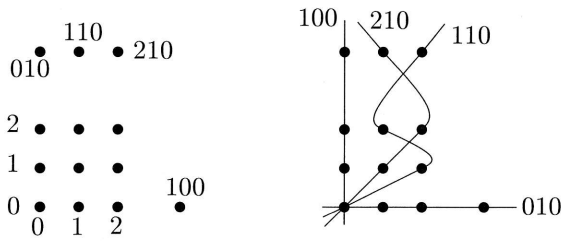
Je-li K n-prvkové těleso, můžeme spočítat, kolik dostaneme bodů. Bodů tvaru $(x, y, 1)$ je n^2, bodů tvaru $(x, 1, 0)$ je n a navíc jeden bod $(1, 0, 0)$ – dohromady tedy n^2+n+1 jak to má být. Pro $n = 3$ jsou všechny body nakresleny na obr. 9.3 vlevo; body tvaru $(x, y, 1)$ jsou popsány hodnotami x, y na souřadnicových osách, ostatní body přímo příslušnými trojicemi.

Teď je třeba definovat přímky. Pro každou trojici $(a, b, c) \in K^3 \setminus \{(0,0,0)\}$ definujeme přímku $P(a, b, c)$ jako množinu bodů (x, y, t) naší projektivní roviny, splňujících rovnici

$$ax + by + ct = 0. \tag{9.1}$$

Dvě ekvivalentní trojice (x, y, t) a $(\lambda x, \lambda y, \lambda t)$ tuto rovnici buď obě zároveň splňují nebo obě zároveň nesplňují, tedy jsme skutečně definovali jistou množinu bodů projektivní roviny. Je také vidět, že pro každé nenulové $\lambda \in K$, trojice $(\lambda a, \lambda b, \lambda c)$ definuje stejnou přímku jako trojice (a, b, c). Na trojicích definujících přímky tedy máme přesně stejnou ekvi-

[4] Pro konečné těleso jsme ještě nedokázali, že touto konstrukcí dostaneme projektivní rovinu ve smyslu definice 9.1.1, dokonce jsme ještě ani nedefinovali, co jsou přímky, takže přísně vzato bychom neměli konstruovaný objekt nazývat projektivní rovinou. Ale k takové přísnosti zde snad není důvod.



Obrázek 9.3: Ilustrace ke konstrukci projektivní roviny řádu 3.

valenci jako na trojicích, definujících body, a můžeme pro tyto trojice vybrat stejné reprezentanty, jako jsme to udělali pro body, tj. trojice s poslední nenulovou složkou rovnou 1. Na obrázku 9.3 vpravo jsou vyznačeny a popsány příslušnými trojicemi všechny přímky, procházející bodem $(0,0,1)$.

Abychom ukázali, že pro n-prvkové těleso jsme opravdu zkonstruovali projektivní rovinu řádu n, je třeba ověřit podmínky (P0)–(P2). Začneme podmínkou (P1) (2 přímky se protínají v 1 bodě). Nechť tedy (a_1,b_1,c_1) a (a_2,b_2,c_2) jsou dvě trojice definující přímky, a předpokládejme, že nejsou ekvivalentní, tj. jedna není násobkem druhé.

Mohli bychom teď přímo vypočítat bod, který je jejich průsečíkem, a ověřit jeho jednoznačnost. Uvedeme jiný důkaz, pomocí základních výsledků z lineární algebry (zkusí-li si čtenář udělat důkaz přímým výpočtem, bude si pak možná lineární algebry cenit více než předtím).

Dívejme se na trojice (a_1,b_1,c_1) a (a_2,b_2,c_2) jako na třírozměrné vektory nad tělesem K. Oba jsou nenulové, a to, že jeden není násobkem druhého, tedy znamená, že jsou lineárně nezávislé. Proto matice

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$$

má hodnost 2. Podívejme se nyní na sloupce této matice jako na dvourozměrné vektory. Především víme, že všechny tři jsou lineárně závislé; existují tedy nějaká 3 čísla $x,y,t \in K$, aspoň jedno z nich nenulové, taková, že

$$x(a_1,a_2)+y(b_1,b_2)+t(c_1,c_2)=(0,0). \tag{9.2}$$

Rozepíšeme-li to po složkách, znamená to přesně to, že bod (x,y,t) leží na obou uvažovaných přímkách.

Na druhé straně, protože hodnost matice je 2, musí existovat 2 sloupcové vektory, které jsou lineárně nezávislé; nechť jsou to třeba (a_1,a_2) a (b_1,b_2). Z toho plyne, že pro každý vektor (u,v) má rovnice $x(a_1,a_2)+y(b_1,b_2)=(u,v)$ jen jediné řešení. Jinými slovy, předepíšeme-li hodnotu t v rovnici (9.2), jsou x a y už dána jednoznačně, a tedy všechna řešení této rovnice jsou násobky jediného vektoru, což znamená, že uvažované přímky se protínají v jediném bodě.

Uvedený argument se dá říci ještě trochu učeněji a stručněji: Zobrazení přiřazující vektoru $(x,y,t) \in K^3$ vektor

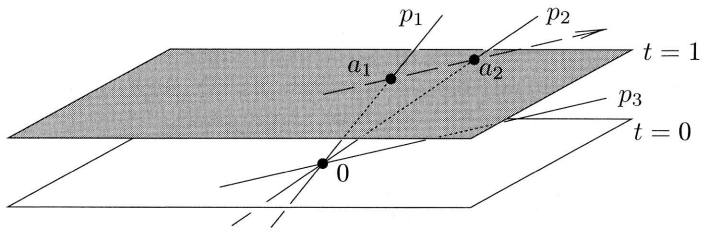
$$x(a_1,a_2)+y(b_1,b_2)+t(c_1,c_2) \in K^2$$

má hodnost 2, čili je na a tedy jeho jádro je 1-dimenzionální.

Tak jsme dokázali (P1). Podmínku (P2) bychom mohli dokazovat podobně, nebo můžeme rovnou říci, že v rovnici (9.1) jsou role trojice (x,y,t) a trojice (a,b,c) zcela symetrické, tedy mezi body a přímkami máme (opět) dualitu. Konečně ověření (P0) přenecháváme čtenáři. □

Geometrická interpretace. Jak jsme zmiňovali na začátku kapitoly, základní myšlenka konstrukce reálné projektivní roviny je doplnit obyčejnou euklidovskou rovinu o body v nekonečnu, přičemž každému směru přímek v euklidovské rovině odpovídá jeden bod v nekonečnu (ne dva!), kde se všechny tyto rovnoběžné přímky protínají.

Teď si představme, že ona obyčejná euklidovská rovina, již chceme doplňovat o body v nekonečnu, je umístěna v trojrozměrném prostoru se souřadnicovým systémem (x,y,t) jako vodorovná rovina $t=1$, na obrázku znázorněná šedě:



Každý bod a této roviny odpovídá jedné přímce $p=\overline{0a}$ procházející počátkem trojrozměrného prostoru, například bodu a_1 na obrázku je přiřazena přímka p_1. Obráceně, každá přímka procházející počátkem trojrozměrného prostoru odpovídá právě jednomu bodu šedé roviny, ovšem s výjimkou vodorovných přímek, jako je třeba p_3. Dále si všimneme, že

když přímku p_1 začneme naklánět do polohy p_2 a dále směrem k vodorovné poloze p_3, ubíhá odpovídající bod v šedé rovině do nekonečna. Není tedy nepřirozené si představovat, že vodorovné přímky jako p_3 odpovídají bodům v nekonečnu, které bychom rádi k naší euklidovské rovině přidali. A zde se udělá jeden z typických triků moderní matematiky – místo abychom vysvětlovali, co jsou to ty body v nekonečnu, jimž odpovídají ony vodorovné přímky, zapomeneme na původní euklidovskou rovinu a řekneme, že body projektivní roviny *jsou* přímky v trojrozměrném prostoru procházející počátkem. (V popsané konstrukci jsme to úplně tak neřekli, ale bod projektivní roviny tam byla množina tvaru $\{(\lambda x, \lambda y, \lambda t);\ \lambda \in K \setminus \{0\}\}$, což geometricky je přesně přímka v K^3 procházející počátkem, až na to, že počátek sám jsme z ní pro technické pohodlí odebrali.) Přímky projektivní roviny pak odpovídají rovinám v trojrozměrném prostoru procházející počátkem, to už necháme k dorozmyšlení čtenáři. Prohlašovat přímky za body může znít podivně, ale čtenář, který svědomitě absolvoval například úvodní kurs analýzy, už mohl na podobné podivnosti přivyknout, například když mu vysvětlili, že reálné číslo je množina racionálních čísel, případně že racionální číslo je třída ekvivalence na množině uspořádaných dvojic celých čísel, a podobně.

Poznámka. Uvedená konstrukce může vzbudit dojem, že body v nekonečnu se nějak odlišují od ostatních. Ve skutečnosti jsou všechny body rovnocenné, a nekonečno můžeme v jistém smyslu umístit kam chceme – projektivní rovina vypadá „lokálně všude stejně".

Cvičení

1.** Dokažte neexistenci projektivní roviny řádu 6. (Můžete si pomoci počítačovým programem, který probere a vyloučí konfigurace přicházející v úvahu. Musí se postupovat obratně, protože např. probírání všech systémů 43 sedmic na 43 bodech by trvalo příliš dlouho.)

9.3 Ortogonální latinské čtverce

Latinský čtverec řádu n je čtvercová tabulka $n \times n$, v níž v každém políčku je zapsáno jedno číslo z množiny $\{1, 2, \ldots, n\}$ a taková, že každé číslo se v každém řádku i sloupci vyskytuje právě jednou. Dva latinské čtverce 3×3 jsou znázorněny na obr. 9.4(a).

1	2	3
2	3	1
3	1	2

(a)

1	2	3
3	1	2
2	3	1

1 1	2 2	3 3
2 3	3 1	1 2
3 2	1 3	2 1

(b)

Obrázek 9.4: Dva ortogonální latinské čtverce řádu 3 (a), a jejich položení přes sebe (b).

Nyní řekneme, co to znamená, že dva latinské čtverce téhož řádu jsou *ortogonální*: Představme si, že jeden ze čtverců je nakreslen na průhledné fólii, a že jej položíme přes druhý čtverec tak, že odpovídající políčka jsou nad sebou (obr. 9.4(b) znázorňuje takové položení čtverců z (a) přes sebe). Tím vznikne n^2 uspořádaných dvojic, každá z nich je tvořena číslem ze spodního čtverečku a odpovídajícím číslem z horního čtverečku. Čtverce jsou ortogonální, pokud se žádná dvojice neopakuje. Protože všech možných uspořádaných dvojic čísel od 1 do n je také n^2, musí se dokonce každá dvojice objevit právě jednou.

9.3.1 Věta. *Nechť M je množina latinských čtverců řádu n, z nichž každé dva jsou navzájem ortogonální. Potom $|M| \leq n - 1$.*

Důkaz. Nejdříve jedno pozorování. Nechť A, B jsou dva ortogonální latinské čtverce řádu n, a nechť π je nějaká permutace čísel $1, 2, \ldots, n$. Utvořme nový latinský čtverec A', který v políčku (i, j) bude mít číslo $\pi(a_{ij})$, kde a_{ij} je číslo v políčku (i, j) čtverce A. Z definice ortogonality není těžké nahlédnout, že potom i A' a B budou ortogonální latinské čtverce. Toto pozorování můžeme vyjádřit heslem „ortogonalita latinských čtverců se nezmění přejmenováním symbolů v jednom z nich".

Mějme nyní latinské čtverce $A_1, A_2, \ldots, A_t$, z nichž každé 2 jsou ortogonální. Pro každé A_i zvolíme tu permutaci čísel $1, 2, \ldots, n$, je-

již aplikací na čísla v políčcích A_i se dosáhne toho, že v první řádce budou stát čísla $1, 2, \ldots, n$ *v pořadí podle velikosti*; výsledný čtverec označíme A'_i. Podle uvedeného pozorování budou $A'_1, \ldots, A'_t$ stále po dvou ortogonální. Podívejme se nyní, jaká čísla mohou stát v prvním políčku druhé řádky čtverců $A'_1, \ldots, A'_t$. Především tam nemůže být číslo 1, protože to už je v prvním sloupci použito. Dále, žádné dva čtverce A'_i, A'_j nemohou mít v uvažované pozici $(2,1)$ stejná čísla. Kdyby totiž měly, položením A'_i, A'_j přes sebe vznikne v pozici $(2,1)$ dvojice stejných čísel, řekněme (k,k), ale tato dvojice také vznikne na k-tém místě prvního řádku! Tedy každé z čísel $2, 3, \ldots, n$ může na pozici $(2,1)$ stát jen v jednom z A'_i, a proto $t \leq n-1$. □

Následující věta dává do souvislosti konečné projektivní roviny a latinské čtverce.

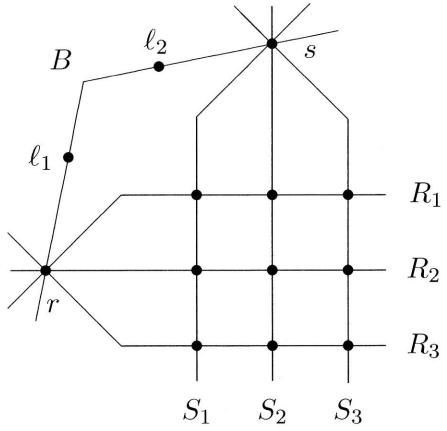
9.3.2 Věta. *Pro $n \geq 2$, projektivní rovina řádu n existuje právě když existuje soubor $n-1$ po dvou ortogonálních latinských čtverců řádu n.*

Poznamenejme jen, že existence projektivní roviny řádu 10 byla vyloučena právě přes hledání ortogonálních latinských čtverců řádu 10.

Důkaz nebudeme dělat do detailů, ale popíšeme si příslušnou konstrukci. Řekněme, že máme dáno $n-1$ ortogonálních latinských čtverců L_1, L_2, $\ldots$, L_{n-1} řádu n, budeme vyrábět projektivní rovinu řádu n. Zvolíme 2 body projektivní roviny, r a s, přímku B je spojující, a zbývající body na přímce B označíme $\ell_1, \ldots, \ell_{n-1}$. Potom nazveme $R_1, \ldots, R_n$ zbývající přímky procházející bodem r (mimo B) a $S_1, \ldots, S_n$ zbývající přímky bodem s. Nyní každý z dosud neoznačených bodů je průsečíkem některé dvojice přímek R_i a S_j. Schematicky je situace znázorněna na obr 9.5 (pro $n = 3$).

Body konstruované projektivní roviny mimo bodů r, s, ℓ_1, ℓ_2, $\ldots$, ℓ_{n-1} máme sestaveny do čtverce $n \times n$; pozice bodu v tomto čtverci bude odpovídat pozici políčka v latinském čtverci; tak např. 2. políčko v 3. řadě latinského čtverce odpovídá v projektivní rovině průsečíku přímek S_2 a R_3.

To, co jsme dosud označili a zakreslili, musí být stejné v každé projektivní rovině řádu n; nyní podle latinských čtverců doplníme přímky procházející body $\ell_1, \ldots, \ell_{n-1}$; jak označení napovídá, přímky procházející



Obrázek 9.5: Konstrukce projektivní roviny z latinských čtverců

bodem ℓ_i budou určeny čtvercem L_i. Přímky bodem ℓ_i budou odpovídat jednotlivým číslům (symbolům) v latinském čtverci L_i. Kdyby např. L_1 byl latinský čtverec na obr. 9.4 vlevo, potom bodem ℓ_1 budou procházet takovéto přímky: přímka odpovídající číslu 1 v latinském čtverci, ta obsahuje mimo ℓ_1 body $R_1 \cap S_1$, $R_2 \cap S_3$ a $R_3 \cap S_2$, tj. body odpovídající políčkům s 1, dále přímka odpovídající číslu 2, s body $R_1 \cap S_2$, $R_2 \cap S_1$ a $R_3 \cap S_3$, a konečně podobně utvořená přímka odpovídající číslu 3.

Tím jsme popsali konstrukci projektivní roviny, zbývá ověřit axiomy. Snadno spočteme, že celkový počet bodů i přímek je $n^2 + n + 1$. Podle cvičení 5 v části 9.1 stačí ověřit, že každé 2 přímky se protínají nejvýš v 1 bodě. Přitom se využije jak toho, že každý L_i je latinský čtverec, tak toho, že každé 2 z použitých čtverců jsou ortogonální; přenecháváme to do cvičení.

Obrácený postup, konstrukce $n-1$ ortogonálních latinských čtverců z projektivní roviny, sleduje totéž schéma. V projektivní rovině libovolně zvolíme body r, s, a zafixujeme další označení jako na obr. 9.5. Potom i-tý latinský čtverec L_i vyplníme podle přímek procházející bodem ℓ_i. Tolik k důkazu věty 9.3.2. □

Cvičení

1. Projděte konstrukci v důkazu věty 9.3.2 pro $n = 2$ (kdy existuje jen 1 latinský čtverec), ověřte, že vznikne Fanova rovina.
2. Ověřte, že každé 2 přímky zkonstruované v důkazu věty 9.3.2 se protínají nejvýš v 1 bodě, a uveďte, kde se využije vlastnosti latinského čtverce a kde ortogonality.
3. Ukažte, že obrácená konstrukce v důkazu věty 9.3.2 opravdu dává $n-1$ ortogonálních latinských čtverců.
4. Definujme *osvobozený čtverec* řádu n jako čtvercovou tabulku $n \times n$, v jejímž každém políčku je některé z čísel $1, 2, \ldots, n$. Ortogonalitu pro osvobozené čtverce definujeme stejně jako pro čtverce latinské. Pro nějaké číslo $t \geq 0$, uvažme následující dvě podmínky:

   (i) Existuje t navzájem ortogonálních latinských čtverců řádu n.

   (ii) Existuje $t+2$ navzájem ortogonálních osvobozených čtverců řádu n.

   (a) Dokažte, že z (i) plyne (ii).

   (b)* Dokažte, že z (ii) plyne (i).
5. Buď T konečné těleso s n prvky, které označíme $t_0, t_1, \ldots, t_{n-1}$, přičemž $t_0 = 0$, $t_1 = 1$. Pro $k = 1, 2, \ldots, n-1$ definujme $n \times n$ matice $L^{(k)}$, přičemž prvek matice $L^{(k)}$ v pozici (i, j), je roven $t_i t_k + t_j$ (násobení a sčítání v tomto vzorci je v tělese T). Dokažte, že $L^{(1)}$, $\ldots$, $L^{(n-1)}$ jsou navzájem ortogonální latinské čtverce řádu n. (Tím se pomocí věty 9.3.2 podá také jiná konstrukce projektivní roviny řádu n.)
6. Pro $m \leq n$ definujme *latinský* $m \times n$ *obdélník* jako obdélníkovou tabulku $m \times n$, v jejímž každém políčku je zapsáno jedno číslo z množiny $\{1, 2, \ldots, n\}$ tak, že v žádném řádku ani sloupci se čísla neopakují. Spočítejte počet všech možných latinských $2 \times n$ obdélníků.

9.4 Použití konečných projektivních rovin

Konečné projektivní roviny mají řadu aplikací v matematice i mimo ni; několik jich zmiňme. Projektivní rovina je velmi stejnorodá, to znamená, že každé dva body (nebo i např. každé dvě dvojice bodů) jsou zcela rovnocenné. Proto se konečné projektivní roviny a jejich

zobecnění, tzv. *bloková schémata*, používají jako schémata organizace různých pokusů, viz část 13.1. Podobná použití mají i latinské čtverce. Motocyklové závody jednotlivců na ploché dráze se rozepisují podle schématu daného projektivní rovinou řádu 4 (k čemuž však nejspíše organizátoři závodů dospěli empiricky); podrobněji se o této souvislosti lze dočíst v knížce [15]. Konečné projektivní roviny se objevují v teorii šifer a kódů, tzv. kryptografii.

V samotné matematice slouží konečné projektivní roviny jako příklady množinových systémů s mnoha pozoruhodnými vlastnostmi. Hledáme-li pro nějakou domněnku o množinových systémech protipříklad nebo naopak chceme-li příklad množinového systému cosi splňujícího, často neprohloupíme, zkusíme-li jako jeden z prvních pokusů nějakou konečnou projektivní rovinu (to trochu připomíná situaci v teorii grafů, která má také svoji zásobárnu zajímavých grafů sloužících jako „notorické protipříklady“).

9.4.1 Příklad (Barvení dvěma barvami). *Buď X konečná množina bodů a $\mathcal{M}$ nějaký systém podmnožin X. Řekneme, že $(X, \mathcal{M})$ je* 2-obarvitelný, *pokud můžeme každý bod z X obarvit jednou ze dvou barev (např. červenou nebo bílou) tak, že v každé množině z $\mathcal{M}$ se vyskytují body obou barev. Nejmenší počet tříbodových množin, z nichž lze utvořit systém, jenž není* 2-obarvitelný, *je* 7, *a jediný takový systém je projektivní rovina řádu* 2. *Více o tom v příkladu 10.1.3*

9.4.2 Příklad. Věta 7.3.1 praví, že je-li G graf na m vrcholech neobsahující $K_{2,2}$ jako podgraf, potom G má nejvýš $\frac{1}{2}(m^{3/2} + m)$ hran. Pomocí konečných projektivních rovin ukážeme, že tento odhad je obecně téměř nejlepší možný: pro nekonečně mnoho hodnot m existuje graf na m vrcholech s aspoň $0.35\, m^{3/2}$ hranami neobsahující $K_{2,2}$ jako podgraf.

Důkaz. Vezmeme projektivní rovinu řádu n, a uvážíme její graf incidence (jako v odstavci o principu duality v části 9.1). Budeme tedy mít celkem $m = 2(n^2 + n + 1)$ vrcholů. Každá z $n^2 + n + 1$ přímek má $n + 1$ bodů, takže tento graf má

$$(n^2 + n + 1)(n + 1) \geq (n^2 + n + 1)^{3/2} = m^{3/2}/2^{3/2} \approx 0.35 m^{3/2}$$

hran.

Co by znamenalo, kdyby uvažovaný graf incidence obsahoval $K_{2,2}$? V pojmech projektivní roviny by to říkalo, že existují dva body x, x' a dvě přímky P, P' takové, že $\{x, x'\} \subseteq P \cap P'$, to ale v projektivní rovině není možné. □

Poznámka. Konstanta 0.35 se dá ještě poněkud vylepšit, viz cvičení 2.

Cvičení

1. Dokažte tvrzení z příkladu 9.4.1: Fanova rovina není 2-obarvitelná.
2. Nechť n je mocnina prvočísla, a nechť K je n-prvkové těleso. Uvažte třídy ekvivalence $\approx$ na množině všech trojic z $K^3 \setminus \{(0,0,0)\}$ (zavedené v části 9.2). Tyto třídy budou vrcholy grafu G, a vrcholy (a,b,c) a (x,y,z) budou spojené hranou právě když $ax + by + cz = 0$. Ověřte
   (a) že tato definice je korektní,
   (b)* že definovaný graf neobsahuje $K_{2,2}$ jako podgraf,
   (c) že každý vrchol má aspoň n sousedů
   (d) a že je-li $m = n^2 + n + 1$ počet vrcholů, potom počet hran je aspoň $\frac{1}{2}m^{3/2} - m$.

10

Pravděpodobnostní důkazy

Čtenář asi zná nějaké úlohy na počítání pravděpodobnosti nějakého jevu (v jiných kapitolách je ostatně několik takových také roztroušeno). Nejčastěji to asi budou příklady, které jsou takzvaně „ze života“ nebo to aspoň předstírají: ve školských úlohách se nejčastěji hovoří o hracích kostkách, kartách, mincích, v učebnicích z let padesátých bychom možná našli otázky o zmetcích mezi hutními výrobky, apod. V téhle kapitole chceme ukázat pozoruhodnou matematickou aplikaci, totiž jak se některá tvrzení dají dokazovat pomocí pravděpodobnosti, ačkoli v nich o pravděpodobnosti ani náhodnosti není ani zmínka.

10.1 Důkazy počítáním

Ve dvou úvodních příkladech se zatím o pravděpodobnosti mluvit nebude.

10.1.1 Příklad. *Uvažme balíček 32 karet srovnaných tak, jak přišly z továrny. Budeme ho míchat tzv. řezáním: rozdělíme jej na 2 stejně velké části, a smísíme karty z jedné části s kartami z druhé části, přičemž pořadí karet z každé části se zachová. Dokážeme, že opakujeme-li to nejvýš 4×, nemůžeme dostat všechna možná pořadí karet (což naznačuje, že takové míchání nemůže dát opravdu náhodné pořadí).*

Důkaz. Celkem je 32! možných pořadí karet. Spočítáme, kolika pořadí se dá dosáhnout popsaným mícháním. Kolika způsoby můžeme smísit oddělené poloviny (říkejme jim třeba levá a pravá polovina) balíčku? Známe-li pořadí v levé i pravé polovině, a udáme-li, které z karet smíšeného balíčku pocházejí z levého balíčku, můžeme již rekonstruovat pořadí ve smíšeném balíčku. Možných pořadí po prvním smísení je tedy $\binom{32}{16}$, a po 4 smíseních můžeme dostat maximálně $\binom{32}{16}^4$ pořadí. Výpočtem se můžeme přesvědčit, že toto číslo je menší než 32!, a tedy určitě existuje nějaké pořadí, které čtyřmi smíseními nedostaneme. □

Uvedený výsledek ovšem nepraví, že 5 smíseními bychom už všechna pořadí dostat mohli. To už je komplikovanější otázka, o které už zde dále nic neřekneme.

10.1.2 Příklad. *Booleovská funkce n proměnných* je libovolné zobrazení $f : \{0,1\}^n \to \{0,1\}$, tj. každé možné kombinaci n nul a jedniček přiřazuje 0 nebo 1. Můžeme ji zadat tabulkou hodnot, ale i všelijakými jinými způsoby. Například libovolný počítačový program, který přečte n bitů ze vstupu a na jejich základě vydá jednu z odpovědí ANO/NE, realizuje jistou booleovskou funkci n proměnných. Zde se budeme zabývat zadáním booleovských funkcí formulemi, jaké čtenář patrně zná z výrokového počtu.

Logická formule v n proměnných bude utvořena ze symbolů proměnných $x_1, x_2, \ldots, x_n$ (každý z nich se může několikrát opakovat), logických spojek & (konjunkce), $\vee$ (disjunkce), $\Rightarrow$ (implikace), $\Leftrightarrow$ (ekvivalence), $\neg$ (negace) a závorek. Ne každá posloupnost těchto symbolů je ovšem logická formule; formule musí splňovat jednoduchá syntaktická pravidla, správné uzávorkování apod., přesná podoba těchto pravidel pro nás nebude podstatná. Jedna taková formule ve třech proměnných je třeba $(x_1 \& x_2) \vee (x_3 \& \neg x_1)$. Každá logická formule v n proměnných definuje booleovskou funkci n proměnných, a není příliš těžké dokázat, že každá booleovská funkce se dá definovat formulí. Otázka nyní je, jak musí být taková formule dlouhá.

Ukážeme, že existuje booleovská funkce n proměnných, která se nedá definovat žádnou formulí s méně než $2^n/\log_2(n+8)$ symboly.

Skutečně, všech možných funkcí n proměnných je 2^{2^n}, zatímco formulí v n proměnných složených z nejvýš m symbolů není více než $(n+8)^m$, protože na každém z m pozic ve formuli je jeden z $n+7$ možných symbolů nebo případně mezera (tím jsme započítali i spoustu nesmyslných řetězců symbolů, ale hrubý horní odhad postačí). Pokud $2^{2^n} > (n+8)^m$, existuje nějaká funkce, která se nedá vyjádřit formulí s nejvýš m symboly; po logaritmování této nerovnosti vyjde $m \geq 2^n/\log_2(n+8)$. □

Podobně můžeme uvažovat definici funkce pomocí programu v nějakém programovacím jazyce, nebo pomocí tzv. logického obvodu (integrované obvody tvořící např. procesory počítačů jsou v podstatě takové logické obvody). Ve všech takových případech se dá počítáním jednoduše dokázat, že existují funkce exponenciální složitosti (např. vyžadující exponenciálně dlouhý text programu).

Uvedené příklady mají společné schéma. Máme nějakou množinu objektů, a chceme ukázat, že mezi nimi existuje nějaký „dobrý“ objekt (s nějakou požadovanou vlastností). Spočítáme, kolik je všech objektů, a odhadneme shora, kolik je špatných objektů (nemajících požadovanou vlastnost). Pokud vyjde, že špatných objektů je méně než všech, musí existovat nějaký dobrý objekt.

> Pozoruhodným rysem této metody je, že žádný dobrý objekt nesestrojíme, ani se nic nedozvíme o tom, jak vypadá, pouze víme, že existuje – je to tedy metoda nekonstruktivní. V příkladu 10.1.1 jsme dokázali, že nějaké pořadí se čtyřmi smíseními nedostane, ale žádné konkrétní takové pořadí jsme nenašli. V příkladu 10.1.2 jsme nezjistili, jak by „složitá“ booleovská funkce (nemající krátkou formuli) měla vypadat. To je dost častá situace u důkazů tohoto typu.

Argument o dobrých a špatných objektech můžeme přeformulovat do řeči pravděpodobnosti. Představme si, že náhodně zvolíme jeden objekt z uvažované množiny. Ukážeme-li, že s nenulovou pravděpodobností bude dobrý, znamená to, že aspoň jeden dobrý objekt existuje. Ve složitějších případech se řeč pravděpodobností stává přehlednější než počítání objektů, a můžeme použít různých pokročilejších metod teorie pravděpodobnosti, jejichž vyjádření v řeči počítání objektů by

bylo nesmírně neohrabané. Řeč pravděpodobnosti použijeme v následujícím příkladu. Pokud by byl čtenář na rozpacích nad některými pojmy týkajícími se pravděpodobnosti, může si napřed přečíst další sekci.

2-barvení. Buď X konečná množina bodů a $\mathcal{M}$ nějaký systém podmnožin X. Řekneme, že $\mathcal{M}$ je *2-obarvitelný*, pokud můžeme každý bod z X obarvit jednu ze dvou barev (např. černou nebo bílou) tak, že v každé množině z $\mathcal{M}$ se vyskytují body obou barev (viz též příklad 9.4.1). Otázka, které systémy množin jsou 2-obarvitelné, souvisí s řadou aplikací a intenzívně se studuje. Zde se budeme zabývat následující situací.

10.1.3 Úloha. *Předpokládejme, že každá množina z $\mathcal{M}$ má přesně k prvků. Jaký je nejmenší počet, $m(k)$, množin v systému $\mathcal{M}$, který není 2-obarvitelný?*

Tak například pro $k = 2$ jsou množiny dvojice bodů, takže uvažované systémy nejsou nic jiného než grafy. Snadno zjistíme, že $m(2) = 3$; jediný příklad systému 3 dvojic, který nejde 2-obarvit, je úplný graf na 3 vrcholech. Už pro $k = 3$ už je ale otázka daleko těžší.

Příklad 9.4.1 ukazuje systém 7 trojic, který není 2-obarvitelný, proto $m(3) \leq 7$. Ve skutečnosti $m(3) = 7$; abychom to dokázali, musíme demonstrovat, že každý systém tvořený 6 nebo méně trojicemi lze 2-obarvit. Ukážeme to pravděpodobností metodou. Začneme obecným tvrzením, které pro $k = 3$ dá slabší výsledek, a potom pro speciální případ $k = 3$ postup vylepšíme.

10.1.4 Věta. *Platí $m(k) \geq 2^{k-1}$, tj. každý systém k-prvkových množin tvořený méně než 2^{k-1} množinami lze 2-obarvit.*

Důkaz. Nechť $\mathcal{M}$ je systém k-prvkových podmnožin nějaké množiny X, $|\mathcal{M}| = m$. Obarvíme každý bod X černě nebo bíle následujícím náhodným postupem: pro každý bod $x \in X$ jednou hodíme mincí (na které padá rub i líc se stejnou pravděpodobností), padne-li líc, obarvíme x bíle, padne-li rub, obarvíme x černě.

Buď $M \in \mathcal{M}$ některá z k-tic v uvažovaném systému. Jaká je pravděpodobnost, že v našem náhodném obarvení dostanou všechny body M stejnou barvu? Pravděpodobnost, že všech k bodů množiny M bude zároveň bílých, je zřejmě 2^{-k}, a zrovna tak pravděpodobnost, že všechny body M budou černé, je 2^{-k}. Celkem tedy pravděpodobnost, že M je jednobarevná, je rovna $2 \times 2^{-k} = 2^{1-k}$, a proto pravděpodobnost, že aspoň jedna z množin v $\mathcal{M}$ je jednobarevná, je nejvýš $m\,2^{1-k}$. Pokud toto číslo je ostře menší než 1, čili $m < 2^{k-1}$, znamená to, že s nenulovou pravděpodobností naše náhodné obarvení bude 2-obarvení systému $\mathcal{M}$. Proto *zcela určitě* existuje aspoň jedno 2-obarvení (kdyby žádné neexistovalo, nemůže se při náhodném obarvení objevit s nenulovou pravděpodobností). Tím je věta dokázána. □

Jak dobrý je dohad na $m(k)$ v právě dokázané větě? Ví se, že pro velká k funkce $m(k)$ roste řádově zhruba jako 2^k, takže tato věta dává celkem správnou představu. Na druhé straně pro $k = 3$ dostaneme jenom odhad $m(k) \geq 4$, což má k správné hodnotě 7 ještě dosti daleko. Dvěma dalšími triky postup vylepšíme.

10.1.5 Věta. $m(3) \geq 7$.

Důkaz uděláme ve dvou krocích, jen první z nich je pravděpodobnostní.

10.1.6 Lemma. *Nechť X je nejvýš 6-prvková množina, nechť $\mathcal{M}$ je systém nejvýš 6 trojic na X. Potom $\mathcal{M}$ je 2-obarvitelný.*

Důkaz. V případě potřeby přidáme ke X další body tak, aby měla přesně 6 bodů. Náhodně zvolenou trojici bodů z X obarvíme bíle, zbývající 3 body obarvíme černě, existuje tedy $\binom{6}{3} = 20$ možností obarvení. Je-li M libovolná trojice, pouze 2 z možných obarvení ji ponechají jednobarevnou, tedy pravděpodobnost, že M bude jednobarevná, je $\frac{1}{10}$. Pravděpodobnost, že některá ze 6 množin bude jednobarevná, tedy není větší než $\frac{6}{10} < 1$, proto existuje 2-obarvení. □

Týž důkaz ukazuje, že i každých 9 trojic na 6 bodech lze 2-obarvit.

Pro další krok potřebujeme definici. Nechť $(X, \mathcal{M})$ je nějaký systém množin, a nechť x, y jsou dva prvky z X. Řekneme, že x a y jsou *spojené*, pokud existuje množina $M \in \mathcal{M}$ obsahující zároveň x i y. Jsou-li x, y dva nespojené body, definujeme nový systém množin $(X', \mathcal{M}')$ vzniklý „slepením" bodů x a y. Neformálně, body x a y ztotožníme do jediného nového bodu, z, a z dáme do všech množin, do nichž předtím patřil x nebo y. Formálně zapsáno:

$$\begin{aligned} X' &= (X \setminus \{x, y\}) \cup \{z\}, \\ \mathcal{M}' &= \{M \in \mathcal{M};\ M \cap \{x, y\} = \emptyset\} \cup \\ &\quad \cup \{(M \setminus \{x, y\}) \cup \{z\};\ M \cap \{x, y\} \neq \emptyset\}. \end{aligned}$$

Všimněme si, že jsou-li body x a y nespojené, potom $(X', \mathcal{M}')$ bude opět systém trojic, a množina X' má o jeden bod méně než X. Dále tvrdíme, že *je-li $(X', \mathcal{M}')$ 2-obarvitelný, potom i $(X, \mathcal{M})$ je 2-obarvitelný*: Vezmeme totiž 2-obarvení množiny X', a obarvíme X stejně, přičemž x i y dostanou tu barvu, již měl „slepený" bod z. Je snadné si rozmyslet, že nemůže vzniknout žádná jednobarevná množina. K dokončení důkazu věty 10.1.5 stačí tedy ukázat následující:

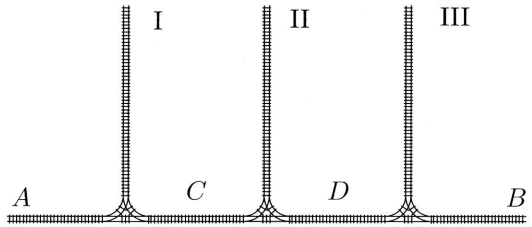
10.1.7 Lemma. *Nechť $(X, \mathcal{M})$ je systém 6 trojic, $|X| \geq 7$. Potom v X existují 2 nespojené body.*

Důkaz. Jedna trojice $M \in \mathcal{M}$ způsobí, že 3 dvojice bodů budou spojené, takže 6 trojic dá nejvýš $3 \times 6 = 18$ spojených dvojic. Přitom ale na 7-bodové množině je $\binom{7}{2} = 21$ dvojic bodů, takže některá z nich je nespojená (dokonce aspoň 3). □

Poznamenejme ještě, že přesná hodnota $m(4)$ již známa není, jsou k dispozici jen horní a dolní odhady. Přitom je snadné si rozmyslet, že tento problém se v principu dá vyřešit probráním konečného počtu konfigurací (systémů čtveřic). Jejich počet je ale tak obří, že je to nad síly všech superpočítačů.

Cvičení

1.* Na koleji A na následujícím obrázku stojí vlak s n vagóny (srovnanými v jistém pořadí). Vagóny se postupně přesunují na kolej B, přičemž každý vagón může nebo nemusí zajet na některé z postranních kolejí; požadujeme však, aby žádný vagón nepřejel žádnou z výhybek přilehajících ke kolejím A,B,C,D více než jednou (předpokládáme, že na každou postranní kolej se v případě potřeby vejdou všechny vagóny najednou).



Dokažte, že pro dost velké n nelze na koleji B docílit každé možné pořadí vagónů.

2. (a) Dokažte, že každou booleovskou funkci n proměnných lze vyjádřit logickou formulí.

   (b) Ukažte, že formuli v (a) lze volit délky nejvýš $Cn\,2^n$, pro vhodnou konstantu C. * Podaří se vám tento odhad ještě řádově zlepšit?

3. Dokažte, že každý systém nejvýš 14 čtveřic lze 2-obarvit:

   (a) Pro systém na nejvýš 14 bodech použijte náhodné obarvení (7 bílých a 7 černých bodů).

   (b) Pro systém na aspoň 15 bodech ukažte, že existuje nespojená dvojice.

4. Máme 27 pravých mincí a 1 falešnou, o trochu těžší než pravé mince. Ukažte, že na určení falešné mince potřebujeme aspoň 4 vážení na rovnoramenných vahách (bez použití závaží, tj. můžeme pouze porovnávat celkovou hmotnost některých k mincí s celkovou hmotností jiných k mincí; neobsahuje-li ani jedna skupina falešnou minci, výsledkem je rovnováha).

10.2 Konečné pravděpodobnostní prostory

Nyní je čas pohovořit o základních pojmech matematické teorie pravděpodobnosti. Omezíme se přitom jen na to, co budeme pro naše příklady potřebovat. V žádném případě není cílem nahradit kurs z teorie pravděpodobnosti, matematicky nebo informaticky vzdělaný člověk by o pravděpodobnosti určitě měl vědět podstatně více, než co uvedeme zde.

Pravděpodobnost je jeden z pojmů, který vystupuje jak v matematice, tak mimo matematiku, tj. „ve skutečném životě", „v praxi", nebo jak jinak ještě se to ještě může nazývat[1]. Definovat „skutečnou" pravděpodobnost je obtížné, a je to otázka filosofická. Matematika se ovšem jejímu řešení v podstatě vyhne: sestrojí totiž matematický model „skutečné" pravděpodobnosti, který je čistě matematickým objektem. Tento model má ve sobě zabudováno (jako axiomy) několik jednoduchých vlastností, odpozorovaných ze „skutečné" pravděpodobnosti (jako např. že pravděpodobnost, že nějaký jev nastane, plus pravděpodobnost, že tento jev nenastane, je dohromady 1), dále se s ním ale pracuje jako s jinými matematickými objekty, tedy všechny jeho vlastnosti, všechna tvrzení o něm a všechna pravidla pro počítání pravděpodobnosti jsou logicky odvozena z axiomů. Tento model je velmi užitečný a jeho předpovědi se shodují s chováním pravděpodobnosti v praxi, což ale to neznamená, že „skutečná" a matematická pravděpodobnost jsou totožné pojmy. Nadále budeme mluvit o pravděpodobnosti v matematickém smyslu, budeme se však odvolávat na příklady se „skutečnou" pravděpodobností jako motivaci jednotlivých pojmů a axiomů.

Základním pojmem v teorii pravděpodobnosti je *pravděpodobnostní prostor*. Omezíme se na konečné pravděpodobnostní prostory.

10.2.1 Definice. Konečným pravděpodobnostním prostorem *rozumíme dvojici* (Ω, P), *kde* Ω *je konečná množina, a* $P : 2^\Omega \to [0,1]$ *je funkce, přiřazující každé podmnožině* Ω *číslo z intervalu* $[0,1]$, *taková, že*

(i) $P(\emptyset) = 0$

(ii) $P(\Omega) = 1$

(iii) $P(A \cup B) = P(A) + P(B)$ *pro libovolné dvě* disjunktní *množiny* $A, B \subseteq \Omega$.

Množinu Ω si můžeme představovat jako množinu všech možných výsledků nějakého náhodného pokusu. Její prvky se nazývají *elementární jevy*. Kdyby tento pokus byl třeba jeden hod hrací kostkou, elementární jevy by byly „padla jednička", „padla dvojka",..., „padla šestka" (pro větší stručnost je můžeme např. označit $\omega_1, \ldots, \omega_6$). Podmnožiny Ω se jmenují *jevy*, tak třeba jeden jev by byl „padlo sudé číslo", neboli $\{\omega_2, \omega_4, \omega_6\}$. Z pochopitelných důvodů se prázdné množině říká *jev nemožný*, celému Ω *jev jistý*. Teorie pravděpodobnosti má své názvy i pro různé množinové pojmy a operace. Tak „$\omega \in A$" můžeme číst „nastal jev A" nebo obšírněji „elementární jev ω je příznivý jevu A"; „$\omega \in A \cap B$" interpretujeme jako „nastaly zároveň jevy A i B"; „$A \cap B = \emptyset$" můžeme vyjádřit jako „jevy A a B jsou neslučitelné" a podobně.

Je-li $A \subseteq \Omega$ jev, číslo $P(A)$ se nazývá *pravděpodobnost jevu* A. Axiomy (i)–(iii) vyjadřují vlastnosti, které od pravděpodobnosti přirozeně očekáváme. Z vlastnosti (iii) je snadno vidět, že hodnotu P stačí zadat na všech jednoprvkových jevech (množinách), a pravděpodobnost libovolného jevu je rovna součtu pravděpodobností jeho prvků, tedy elementárních jevů (přesněji, součtu pravděpodobností všech jeho jednoprvkových podmnožin, ale dovolíme si toto zkrácené vyjádření).

Nejjednodušším a možná nejdůležitějším konečným pravděpodobnostním prostorem je takový, v němž všechny elementární jevy mají stejnou pravděpodobnost, tj. funkce P je dána předpisem

$$P(A) = \frac{|A|}{|\Omega|}.$$

Takový prostor odráží tzv. *klasickou definici pravděpodobnosti*. V této definici (formulované Laplacem) se předpokládá, že všechny možné výsledky určitého náhodného pokusu jsou, na podkladě symetrie a homogenity, stejně možné. Je-li všech možných výsledků pokusu (elementárních jevů) n a výsledků příznivých nějakému jevu A je m, potom pravděpodobnost jevu A se definuje jako m/n. To se někdy heslovitě vyjadřuje rčením, že pravděpodobnost je počet případů příznivých ku počtu případů možných. Jako definice toho, co pravděpodobnost je, to není příliš uspokojivé (potíž je v obratu „stejně možné"), navíc to nezahrnuje nekonečné pravděpodobnostní prostory, ale v mnoha konkrétních případech je to přinejmenším užitečný návod, jak pravděpodobnost počítat.

[1] I v mimomatematickém významu myslíme ovšem pravděpodobnost jako veličinu, jako ve větě „Pravděpodobnost toho, že na hrací kostce padne šestka, je $\frac{1}{6}$.", nikoli jako ve třeba ve větě „Ten člověk pravděpodobně neví, že tramvaje teď jezdí jinudy.".

O nekonečných pravděpodobnostních prostorech. Tím, že jsme se omezili na konečné pravděpodobnostní prostory, jsme si situaci matematicky značně zjednodušili. Pro modelování mnoha zajímavých jevů je však nejpřirozenější pracovat s nekonečnými prostory. Tak například se můžeme ptát, zvolíme-li 5 náhodných bodů z intervalu $[0,1]$, jaká je pravděpodobnost, že každé dva budou od sebe vzdáleny aspoň o $\frac{1}{10}$ (a tisíce jiných otázek podobného typu). Potřebovali bychom především definovat pravděpodobnostní prostor, vystihující pojem „náhodný bod z intervalu $[0,1]$". Body, tj. elementární jevy, budou všechny body $[0,1]$. Přitom pravděpodobnost každého jednotlivého bodu musí být stejná, a protože bodů je nekonečně, musí být nulová! Funkci P tedy už nelze definovat jen jejím zadáním na jednoprvkových množinách, pravděpodobnost jevu A musí být jeho „míra" ve vhodném smyslu. To již je složitější pojem, který úzce souvisí s integrováním funkcí a dalšími otázkami matematické analýzy. S jinými nekonečnými pravděpodobnostními prostory operujeme (aniž je tak nazýváme) v částech 12.5 a 12.6.

Následují důležité konkrétní exempláře konečných pravděpodobnostních prostorů.

10.2.2 Definice (Náhodná posloupnost n nul a jedniček). *Tento prostor budeme značit $\mathcal{C}_n$. Jeho prvky (elementární jevy) jsou všechny n-prvkové posloupnosti nul a jedniček, jinak řečeno, množina $\{0,1\}^n$, a všechny mají stejnou pravděpodobnost. Protože $|\mathcal{C}_n| = 2^n$, je pravděpodobnost každého jevu A rovna $|A|/2^n$.*

Takový prostor modeluje třeba posloupnost n hodů mincí (rozumí se symetrickou mincí, kde rub i líc padají se stejnou pravděpodobností); padne-li v i-tém hodu líc, resp. rub, napíšeme na i-té místo posloupnosti jedničku, resp. nulu. Příkladem jevu by mohl být třeba jev $A =$„Líc padne právě $10\times$", jehož pravděpodobnost je $\binom{n}{10}/2^n$.

10.2.3 Definice (Náhodná permutace). *Prvky tohoto prostoru, označovaného $\mathcal{S}_n$, budou všechny permutace (tj. prostá zobrazení na) množiny $\{1,2,\ldots,n\}$, a pravděpodobnost jevu (podmnožiny) A je rovna $|A|/n!$.*

Tento prostor je modelem rozložení nějakých n různých předmětů v náhodném pořadí, třeba dobře zamíchaného balíčku karet.

10.2.4 Úloha. *Jaká je pravděpodobnost, že v náhodném pořadí karet bude červené eso předcházet červené sedmě?*

Přeformulováno v našem pravděpodobnostním modelu, jaká je pravděpodobnost jevu $A = \{\pi \in \mathcal{S}_n;\ \pi(1) < \pi(2)\}$? Mohli bychom ovšem poctivě spočítat permutace, pro něž $\pi(1) < \pi(2)$, ale můžeme také tuto pravděpodobnost určit jednoduchou úvahou: díky symetrii není možné, aby jeden z jevů „$\pi(1) < \pi(2)$" a „$\pi(1) > \pi(2)$" byl pravděpodobnější než druhý, a tedy hledaná pravděpodobnost je rovna $\frac{1}{2}$. Přesněji bychom takovou úvahu měli říci asi takto: mezi množinou A a $A' = \{\pi \in \Omega;\ \pi(1) > \pi(2)\}$ můžeme sestrojit bijekci, permutaci $\pi \in A$ přiřadíme permutaci π', která číslu 1 přiřazuje číslo $\pi(2)$, číslu 2 přiřazuje $\pi(1)$ a jinak se shoduje s π. Proto $|A| = |A'|$, a jelikož $\mathcal{S}_n = A \dot\cup A'$ (disjunktní sjednocení), je $P(A) = \frac{1}{2}$.

Teď jeden příklad pro oživení, možná s překvapivým řešením.

10.2.5 Úloha. *Představme si, že hrajeme následující hru. Protivník má 100 prázdných kartiček, a napíše na každou nějaké, zcela libovolné číslo podle svého uvážení. Potom je dobře zamíchá (nebo to může udělat nestranný pomocník), a zamíchaný balíček položí na stůl čísly dolů. Začneme si odebírat shora z balíčku jednu kartičku po druhé, a díváme se na jejich čísla. Po otočení kterékoli kartičky máme možnost hru ukončit. Přitom vyhrajeme, pokud na posledně otočené kartičce je napsáno největší číslo ze všech kartiček (vůbec všech, tedy jak již otočených, tak dosud neotočených!), jinak vyhraje soupeř. Je pro nás výhodné vsadit si na výhru v poměru 4:1 (např. vyhrajeme-li, bereme 400, prohrajeme-li, platíme 100)?*

Na první pohled se zdá, že to je v uvedeném poměru sázek velice nevýhodná hra. Ukážeme však, že při vhodné strategii je šance na výhru aspoň $\frac{1}{4}$, a tedy náš průměrný zisk v dlouhé sérii her je aspoň

$$\frac{1}{4} \times 400 - \frac{3}{4} \times 100 = 25.$$

Přidržme se takovéto strategie: prvních 50 kartiček otočíme v každém případě, jenom si pamatujeme, jaké na nich bylo největší číslo – označme jej M. Potom otáčíme další kartičky, a jakmile na některé bude číslo větší nebo rovné M, hru ukončíme. Když na žádné takové nenarazíme, skončíme až poslední kartičkou.

Tvrdíme, že pravděpodobnost výhry při této strategii je větší než $\frac{1}{4}$.

Pro jednoduchost předpokládejme, že všechna čísla na kartičkách jsou navzájem různá (modifikaci pro zcela libovolná čísla si může čtenář v případě zájmu rozmyslet sám). Potom uvedená strategie jistě vede k výhře, pokud

- největší číslo není mezi prvními 50 kartičkami
- a druhé největší číslo je na některé z prvních 50 kartiček.

Při uvedené strategii záleží očividně jen na pořadí čísel na kartičkách podle velikosti, a tedy můžeme předpokládat, že na kartičkách je náhodná permutace množiny $\{1, 2, \ldots, 100\}$, tj. elementární jev z výše definovaného prostoru $\mathcal{S}_{100}$. Zajímat nás pak bude jev

$$A = \{\pi \in \mathcal{S}_{100};\ \pi(100) > 50 \text{ a } \pi(99) \leq 50\}.$$

Tady bude užitečné dívat se na permutaci jako na pořadí. Pozici čísla 100 můžeme zvolit 50 způsoby, pozici 99 nezávisle na tom 50 způsoby, a pro každou takovou volbu pak zbývající čísla můžeme na zbývající pozice rozestavit 98! způsoby. Proto

$$P(A) = \frac{50 \times 50 \times 98!}{100!} = \frac{50 \times 50}{99 \times 100} \doteq 0.2525 > \frac{1}{4}.$$

Ještě několik poznámek. Jev A není jediná situace, kdy naše strategie vyhrává, proto pravděpodobnost A je jen dolní odhad pro šanci na výhru. Číslo 50 v popsané strategii optimalizuje pravděpodobnost jevu A, ale vezmeme-li v úvahu i jiné možnosti výhry, dostaneme poněkud lepší výsledky s jiným „prahovým" počtem kartiček; zde podrobnější analýzu už dělat nebudeme.

10.2.6 Definice (Náhodný graf). *Graf (obyčejný, neorientovaný) na množině vrcholů $V = \{1, 2, \ldots, n\}$ je zadán tím, že pro každou dvojici $\{i, j\} \in \binom{V}{2}$ specifikujeme, zda tvoří hranu nebo ne. Existuje tedy $2^{\binom{n}{2}}$ grafů (mnohé z nich jsou ovšem isomorfní, to nás zde ale nebude zajímat). Vybíráme-li náhodný G graf na V, přičemž všechny grafy jsou stejně pravděpodobné, můžeme na to nahlížet též jako na $\binom{n}{2}$ hodů symetrickou mincí – pro každou dvojici vrcholů hodíme mincí, zda se má stát hranou nebo ne. Příslušný pravděpodobnostní prostor $\mathcal{G}_n$ bude mít jako prvky všechny možné grafy na V, a všechny budou mít stejnou pravděpodobnost, totiž $2^{-\binom{n}{2}}$.*

Jako příklady jevů můžeme studovat nejrůznější grafové vlastnosti, jako jev S =„graf G je souvislý" nebo B =„graf G je bipartitní", a podobně. Vypočítat pravděpodobnosti takových jevů přesně je někdy obtížné, ale většinou nás zajímá jen nějaký přibližný odhad. Pro dva zmíněné jevy lze ukázat, že pro $n \to \infty$ se pravděpodobnost $P(S)$ velmi rychle blíží 1, zatímco pravděpodobnost $P(B)$ se velmi rychle blíží 0. To se někdy vyjadřuje frázemi „náhodný graf je skoro jistě souvislý" a „náhodný graf skoro jistě není bipartitní".

10.2.7 Úloha. *Dokažme, že náhodný graf skoro jistě není bipartitní, tj.* $\lim_{n\to\infty} P(B) = 0$.

Důkaz. Následující postup je poučný i pro mnoho jiných tvrzení tohoto typu. Jak víme, množinu vrcholů V bipartitního grafu lze rozdělit na dvě části, U a W, tak, že všechny hrany jsou mezi U a W. Pro danou podmnožinu $U \subseteq V$ označme B_U jev, že všechny hrany grafu G spojují vrcholy z U s vrcholy z $W = V \setminus U$. Je-li $k = |U|$, máme $k(n-k)$ dvojic $\{u, w\}$ s $u \in U$, $w \in V \setminus U$, tedy jev (množina) B_U sestává z $2^{k(n-k)}$ grafů, a proto $P(B_U) = 2^{k(n-k)-\binom{n}{2}}$. Není těžké se přesvědčit, že funkce $k \mapsto k(n-k)$ nabývá maxima pro $k = n/2$, a toto maximum je rovno $n^2/4$. Proto můžeme pro každé U odhadnout

$$P(B_U) \leq 2^{n^2/4-\binom{n}{2}} = 2^{-n(n-2)/4}.$$

Každý bipartitní graf patří některému B_U (pro vhodnou množinu U). Pro různé volby U nemusí být jevy B_U navzájem disjunktní, avšak pravděpodobnost sjednocení jevů je vždy nejvýš rovna součtu jejich pravděpodobností, a proto

$$P(B) \leq \sum_{U \subseteq V} P(B_U) \leq 2^n 2^{-n(n-2)/4} = 2^{-n(n-6)/4} \to 0.$$

□

V uvedeném výsledku jsme se zajímali o jistou kvalitativní vlastnost „velkého" náhodného grafu. To trochu připomíná např. otázky fyziky pevných látek; tam se totiž studují nějaké makroskopické vlastnosti souboru velkého množství mikroskopických částic. Předpokládá se přitom, že jednotlivé částice si vedou ve vhodném smyslu náhodně, a makroskopické vlastnosti jsou výslednicí jejich náhodného chování. I matematické metody studia takových souborů částic jsou příbuzné metodám pro náhodné grafy.

Nezávislé jevy. Musíme probrat ještě jeden klíčový pojem. Dva jevy A, B v nějakém pravděpodobnostním prostoru (Ω, P) se nazývají *nezávislé*, platí-li

$$P(A \cap B) = P(A)P(B).$$

Nezávislost znamená, že rozdělíme-li Ω na 2 části, A a jeho doplněk, jev B „rozřízne" obě tyto části v témže poměru. Jinak řečeno, kdybychom prvek $\omega \in \Omega$ volili náhodně nikoliv ze všech prvků Ω, ale jenom mezi prvky z A, byla by pravděpodobnost toho, že $\omega \in B$, přesně rovna $P(B)$ (za předpokladu $P(A) \neq 0$).

S nezávislými jevy se nejčastěji setkáme v takovéto situaci: prvky Ω, tj. elementární jevy, si můžeme představovat jako uspořádané dvojice, neboli Ω modeluje výsledek jednoho „složeného" experimentu, sestávajícího ze dvou experimentů konaných jeden po druhém. Předpokládejme, že průběh prvního experimentu nijak neovlivní průběh experimentu druhého. Je-li $A \subseteq \Omega$ nějaký jev, závisející jen na výsledku prvního experimentu (tj., známe-li tento výsledek, můžeme rozhodnout, zda A nastal nebo ne) a podobně B závisí jen na výsledku druhého experimentu, potom jevy A a B budou nezávislé.

Prostor $\mathcal{C}_n$ (náhodná posloupnost 0/1) je typickým zdrojem situací tohoto druhu. Zde máme složený experiment sestávající z n po sobě jdoucích hodů mincí, o nichž předpokládáme, že se navzájem nijak neovlivňují. Závisí-li tedy jev A např. jen na hodech se sudým pořadovým číslem („v suchých hodech nepadl žádný líc") a jev B jen na hodech s lichým pořadovým číslem („v lichých hodech padly aspoň 3 ruby"), budou takové jevy nezávislé. Podobně v prostoru $\mathcal{G}_n$ (náhodný graf) jsou jednotlivé hrany nezávislé, a např. jevy „graf G má aspoň jeden trojúhelník na vrcholech 1,2,...,10" a „graf G obsahuje nějakou lichou kružnici s vrcholy mezi $11, 12, \ldots, n$" jsou nezávislé.

Subtilnější situace můžeme demonstrovat na pravděpodobnostním prostoru $\mathcal{S}_n$ (náhodná permutace). Jevy $A = \{\pi(1) = 1\}$ a $B = \{\pi(2) = 1\}$ zjevně nezávislé nejsou (protože $P(A), P(B) > 0$, ale $A \cap B = \emptyset$, a tudíž $P(A \cap B) = 0$). Bude-li jev $C = \{\pi(2) = 2\}$, je vidět, že B a C určitě nejsou nezávislé, ale možná už není tak zřejmé, že ani A a C nejsou nezávislé: máme $P(A) = P(C) = \frac{1}{n}$, ale $P(A \cap C) = \frac{1}{n(n-1)} \neq P(A)P(C)$. Intuitivně, víme-li, že nastal A, tj. že $\pi(1) = 1$, vyloučili jsme tím zároveň jednu z n možností pro $\pi(2)$, a tedy $\pi(2)$ má malinko větší šanci být rovno 2. Naproti tomu jevy A a $D = \{\pi(2) < \pi(3)\}$ jsou nezávislé, jak se lze přesvědčit výpočtem příslušných pravděpodobností.

Pojem nezávislosti můžeme rozšířit i na více jevů $A_1, A_2, \ldots, A_n$.

10.2.8 Definice. *Jevy $A_1, \ldots, A_n \subseteq \Omega$ se nazývají* nezávislé, *pokud pro každou množinu indexů $I \subseteq \{1, 2, \ldots, n\}$ platí*

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i).$$

Speciálně tato definice požaduje, aby každé dva z těchto jevů byly nezávislé, ale musíme varovat, že z nezávislosti všech dvojic obecně neplyne nezávislost!

V prostorech $\mathcal{C}_n$ (náhodná posloupnost 0/1) i $\mathcal{G}_n$ (náhodný graf) máme typické situace s mnoha nezávislými jevy. Definujme jev A_i v prostoru $\mathcal{C}_n$, tvořený všemi posloupnostmi s jedničkou na i-tém místě. Pak jevy $A_1, \ldots, A_n$ jsou nezávislé. Obecněji, závisejí-li nějaké jevy na po dvou disjunktních skupinách složek posloupnosti, jsou nezávislé (důkaz vynecháme, není obtížný).

V různých pravděpodobnostních výpočtech a důkazech se příslušné pravděpodobnostní prostory zpravidla výslovně nepopisují, jen se s nimi mlčky pracuje. Přesto je samozřejmě důležité mít jasno v těchto základních pojmech.

Na závěr tohoto oddílu uvedeme ještě jeden pěkný pravděpodobnostní důkaz.

10.2.9 Úloha. *Uvažme turnaj n hráčů, řekněme v tenisu, v němž každý hraje s každým (a žádná dvojice neremizuje). Mají-li jednotliví hráči velké výkonnostní odstupy, můžeme čekat, že nejlepší s nich vyhraje se všemi, druhý nejlepší se všemi kromě prvního, atd., tj., turnaj přesvědčivě určí pořadí. Turnaj s vyrovnanými hráči ovšem může dopadnout složitějším způsobem. Může například turnaj dopadnout*

tak, aby pro každou trojici hráčů existoval nějaký jiný hráč, který je všechny porazil? *(Podobně se ovšem můžeme ptát pro libovolné k místo trojky.)*

Když si matematikové položili tuto otázku, dlouho se nedařilo najít řešení; konstrukce takových turnajů je obtížná. Pravděpodobnostní metodou se ukáže existence takového výsledku turnaje, pro dost velké n, poměrně snadno.

Uvažme náhodný turnaj, kde si představujeme, že výsledek každého zápasu je určen nestranným losem. Podíváme se na pevně zvolenou trojici hráčů x, y, z. Pravděpodobnost, že nějaký jiný hráč w s nimi se všemi vyhraje, je $2^{-3} = \frac{1}{8}$, tedy pravděpodobnost že w prohraje aspoň s jedním je $\frac{7}{8}$. Jaká je pravděpodobnost, že každý z $n-3$ hráčů w (různých od x, y, z) prohraje aspoň s jedním z x, y, z? Pro různé hráče w jsou výsledky jejich zápasů s x, y, z na sobě nezávislé, a tedy tato pravděpodobnost je $(\frac{7}{8})^{n-3}$. Trojici $\{x, y, z\}$ lze volit $\binom{n}{3}$ způsoby, proto pravděpodobnost, že pro aspoň jednu z těchto trojic x, y, z není žádný další hráč, jenž x, y i z porazil, je nejvýš $\binom{n}{3}(\frac{7}{8})^{n-3}$. Pro $n \geq 91$ je tato pravděpodobnost menší než 1, proto existuje nějaký výsledek turnaje n hráčů s požadovanou vlastností. □

Cvičení

1. Ukažte, že náhodný graf skoro jistě obsahuje trojúhelník (tím podáte jiné řešení příkladu 10.2.7).
2.* Ukažte, že náhodný graf je skoro jistě souvislý.
3. Najděte příklad 3 jevů v nějakém pravděpodobnostním prostoru takových, že každé dva jsou nezávislé, ale všechny 3 nezávislé nejsou.
4. Ukažte, že jsou-li A, B nezávislé jevy, pak také jejich doplňky $\Omega \setminus A$, $\Omega \setminus B$ jsou nezávislé.
5. (a) Ukažte podle definice, že jevy $A_1, \ldots, A_n$ v prostoru $\mathcal{C}_n$, definované v textu za definicí 10.2.8, jsou skutečně nezávislé.

   (b)* Buď (Ω, P) konečný pravděpodobnostní prostor, v němž existuje n nezávislých jevů $A_1, \ldots, A_n$ takových, že $0 < P(A_i) < 1$ pro každé i. Dokažte, že $|\Omega| \geq 2^n$.

6. Nechť (Ω, P) je konečný pravděpodobnostní prostor, v němž všechny prvky mají pravděpodobnost $1/|\Omega|$. Ukažte, že je-li $|\Omega|$ prvočíslo, pak žádné dva netriviální jevy (různé od $\emptyset$ a Ω) nejsou nezávislé.
7. Pro jednoduchost předpokládejme, že pravděpodobnost narození kluka i holky je stejná (což ve skutečnosti není zcela tak). O jisté rodině víme, že mají přesně dvě děti, a aspoň jedno z nich je kluk. Jaká je pravděpodobnost, že mají dva kluky?

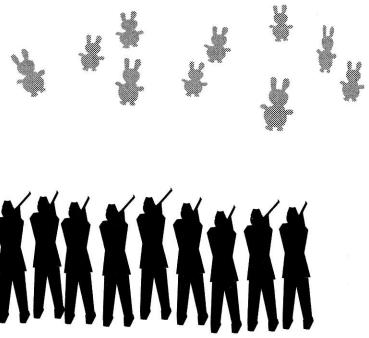
10.3 Střední hodnota

10.3.1 Definice. *Nechť (Ω, P) je nějaký konečný pravděpodobnostní prostor.* Náhodnou veličinou *na Ω nazveme každé zobrazení $f : \Omega \to \mathbf{R}$.*

Náhodná veličina f tedy přiřazuje každému elementárnímu jevu $\omega \in \Omega$ nějaké reálné číslo $f(\omega)$. Teď několik příkladů náhodných veličin:

10.3.2 Příklad (Počet jedniček). *Je-li $\mathcal{C}_n$ prostor všech n-prvkových posloupností nul a jedniček, můžeme definovat náhodnou veličinu f_1 takto: $f_1(s)$ je počet jedniček v posloupnosti s.*

10.3.3 Příklad (Počet živých zajíců). *Každý z n lovců zamíří na jednoho náhodně vybraného z n zajíců, a všichni naráz vystřelí. Náhodná veličina f_2 je počet přeživších zajíců (za předpokladu, že se každý lovec trefí). Formálně, pravděpodobnostní prostor zde bude množina všech zobrazení μ množiny $\{1, 2, \ldots, n\}$ do sebe, každé s pravděpodobností n^{-n}, a $f_2(\mu)$ je počet bodů mino obraz μ.*



10.3.4 Příklad (Počet levých maxim). *Na pravděpodobnostním prostoru $\mathcal{S}_n$ všech permutací na množině $\{1, 2, \ldots, n\}$, definujeme náhodnou veličinu f_3: $f_3(\pi)$ je počet* levých maxim *permutace π, tj. počet i takových, že $\pi(i) > \pi(j)$ pro všechna $j < i$. Představme si závod třeba ve vrhu koulí, a pro jednoduchost předpokládejme, že každý závodník podává stabilní výkon, tj., pokaždé hodí stejně. V první sérii hodů hází n závodníků v náhodném pořadí. Potom f_3 bude udávat, kolikrát se v této první sérii hodů měnil závodník s dosud nejlepším výkonem.*

10.3.5 Příklad (Složitost třídicího algoritmu). *A ještě jedna složitější náhodná veličina. Nechť A je nějaký třídicí algoritmus, to znamená, A dostane jako vstup n-tici čísel $x_1, \ldots, x_n$, a na výstup vypíše táž čísla setříděná podle velikosti. Předpokládejme, že počet kroků výpočtu algoritmu A závisí jen na pořadí vstupních čísel podle velikosti, takže si můžeme představovat, že na vstupu je nějaká permutace π čísel $\{1, 2, \ldots, n\}$ (tuto podmínku splňuje mnoho skutečně používaných algoritmů). Definujeme náhodnou veličinu f_4 na prostoru $\mathcal{S}_n$; $f_4(\pi)$ je počet kroků, vykonaných algoritmem A pro vstupní permutaci π.*

10.3.6 Definice. *Nechť (Ω, P) je konečný pravděpodobnostní prostor, f náhodná veličina na něm.* Střední hodnota *f bude reálné číslo, které značíme $\mathbf{E}f$ a definujeme předpisem*

$$\mathbf{E}f = \sum_{\omega \in \Omega} P(\{\omega\}) f(\omega)$$

(písmeno $\mathbf{E}$ je zkratka z anglického „expectation“, v překladu „očekávání“).

Střední hodnotu si můžeme představovat takto: opakujeme-li mnohokrát náhodnou volbu prvku z Ω, bude se průměrná hodnota f přes tyto náhodně zvolené prvky blížit $\mathbf{E}f$. Jsou-li speciálně všechny elementární jevy $\omega \in \Omega$ stejně pravděpodobné (jak je tomu téměř ve

všech našich příkladech), je střední hodnota f prostě aritmetický průměr všech hodnot f:

$$\mathbf{E}f = \frac{1}{|\Omega|} \sum_{\omega \in \Omega} f(\omega).$$

Pokračování příkladu 10.3.2 (Počet jedniček). Pro ilustraci vypočteme střední hodnotu náhodné veličiny f_1, počtu jedniček v náhodné n-členné posloupnosti nul a jedniček, podle definice. Veličina f_1 má hodnotu 0 pro jedinou posloupnost (samých nul), hodnotu 1 pro n posloupností,..., hodnotu k pro $\binom{n}{k}$ posloupností z $\mathcal{C}_n$. Proto

$$\mathbf{E}f_1 = \frac{1}{2^n} \sum_{k=1}^{n} \binom{n}{k} k.$$

Jak se počítá v příkladu 12.1.2, je suma na pravé straně rovna $n2^{n-1}$, takže $\mathbf{E}f_1 = n/2$. To ovšem souhlasí s intuicí, že při n hodech mincí v průměru padne polovina líců.

Hodnota $\mathbf{E}f_1$ se dá stanovit jednodušeji, následujícím trikem. Pro každou posloupnost $s \in \mathcal{C}_n$ uvažme posloupnost $\bar{s}$, která vznikne ze s záměnou jedniček na nuly a obráceně. Platí $f_1(s) + f_1(\bar{s}) = n$. Toho využijeme takto:

$$\mathbf{E}f_1 = 2^{-n} \sum_{s \in \mathcal{C}_n} f_1(s) = \frac{1}{2^n . 2} \sum_{s \in \mathcal{C}_n} (f_1(s) + f_1(\bar{s})) = 2^{-n-1} |\mathcal{C}_n| n = \frac{n}{2}.$$

Popíšeme nyní metodu, jíž se střední hodnota často dá spočítat velmi jednoduše (viděli jsme, že výpočet podle definice je i v jednoduchých případech pracný). Potřebujeme na to definici a jednoduchou větu.

10.3.7 Definice. *Buď $A \subseteq \Omega$ jev v nějakém pravděpodobnostním prostoru (Ω, P).* Indikátorem *jevu A nazveme náhodnou veličinu, $I_A : \Omega \to \{0, 1\}$, definovanou následovně*

$$I_A(\omega) = \begin{cases} 1 & \text{pro } \omega \in A \\ 0 & \text{pro } \omega \notin A. \end{cases}$$

10.3.8 Pozorování. *Pro každý jev A platí $\mathbf{E}I_A = P(A)$.*

Důkaz. Podle definice střední hodnoty je

$$\mathbf{E}I_A = \sum_{\omega\in\Omega} I_A(\omega)P(\{\omega\}) = \sum_{\omega\in A} P(\{\omega\}) = P(A).$$

□

Následující tvrzení je skoro škoda nazývat větou, jeho důkaz z definice je bezprostřední a přenecháváme jej čtenáři. Je to však tvrzení, které nám bude v dalším velice užitečné.

10.3.9 Věta (O linearitě střední hodnoty). *Buďte f a g libovolné náhodné veličiny na konečném pravděpodobnostním prostoru (Ω, P), α reálné číslo. Potom $\mathbf{E}(\alpha f) = \alpha\mathbf{E}f$, $\mathbf{E}(f+g) = (\mathbf{E}f) + (\mathbf{E}g)$.*

Zdůrazněme, že f a g mohou být naprosto libovolné, nemusí tedy být v žádném smyslu nezávislé nebo tak něco. Pokračujeme několika příklady toho, jak se 10.3.7–10.3.9 dají využít.

Další pokračování příkladu 10.3.2 (Počet jedniček). Spočítáme $\mathbf{E}f_1$, průměrný počet jedniček, asi nejelegantnějším způsobem. Jev A_i na prostoru $\mathcal{C}_n$ bude „v i-tém hodu padne líc", čili množina všech posloupností, majících na i-tém místě jedničku. Zřejmě $P(A_i) = \frac{1}{2}$ pro každé i. Všimněme si, že pro každou posloupnost $s \in \mathcal{C}_n$ platí $f_1(s) = I_{A_1}(s) + I_{A_2}(s) + \cdots + I_{A_n}(s)$ (triviální tvrzení jsme jen zapsali v trošku komplikovanějším značení). Z linearity střední hodnoty a pak z pozorování 10.3.8 dostaneme

$$\mathbf{E}f_1 = \mathbf{E}I_{A_1} + \mathbf{E}I_{A_2} + \cdots + \mathbf{E}I_{A_n} = P(A_1) + P(A_2) + \cdots + P(A_n) = \frac{n}{2}.$$

□

Pokračování příkladu 10.3.3 (Počet živých zajíců). Budeme počítat $\mathbf{E}f_2$, střední hodnotu počtu nezastřelených zajíců. Tentokrát

A_i bude jev „i-tý zajíc přežije", formálně A_i bude množina všech zobrazení μ, která nic nezobrazí na i. Pravděpodobnost, že j-tý lovec střelí i-tého zajíce je $\frac{1}{n}$, a protože lovci si vybírají nezávisle, je $P(A_i) = (1-1/n)^n$. Dále postupujeme jako v předchozím příkladě:

$$\mathbf{E}f_2 = \sum_{i=1}^{n} \mathbf{E}I_{A_i} = \sum_{i=1}^{n} P(A_i) = \left(1-\frac{1}{n}\right)^n n \approx \frac{n}{e}$$

(jak známo z analýzy, $(1-1/n)^n$ konverguje k e^{-1}). □

Pokračování příkladu 10.3.4 (Počet levých maxim). Budeme teď počítat střední hodnotu počtu levých maxim náhodné permutace, $\mathbf{E}f_3$. Zde A_i bude jev „i je levé maximum π", tj.

$$A_i = \{\pi;\ \pi(i) > \pi(j) \text{ pro } j = 1, 2, \ldots, i-1\}.$$

Tvrdíme, že $P(A_i) = \frac{1}{i}$. Nejnázornější je si představit, že náhodnou permutaci π vyrábíme takovýmto postupem: Začneme s „hromádkou" čísel $\{1, 2, \ldots, n\}$. Vytáhneme z hromádky jedno náhodně zvolené číslo, a prohlásíme jej za $\pi(n)$. Potom ze zbývajících čísel v hromádce vytáhneme další náhodné číslo, to bude $\pi(n-1)$, atd. Hodnota $\pi(i)$ se volí v okamžiku, kdy v hromádce zbývá právě i čísel. Pravděpodobnost, že jako $\pi(i)$ zvolíme největší z těchto i čísel (což je právě jev A_i), je tudíž $\frac{1}{i}$. Zbytek výpočtu je jako v předchozím:

$$\mathbf{E}f_3 = \sum_{i=1}^{n} \mathbf{E}I_{A_i} = \sum_{i=1}^{n} P(A_i) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Hodnota součtu převrácených hodnot, k němuž jsme dospěli, je přibližně $\ln n$, viz cvičení 3.4.12. □

Cvičení

1. Ukažte na příkladech, že pro libovolné náhodné veličiny f, g obecně neplatí ani jedna z rovností $\mathbf{E}(fg) = (\mathbf{E}f)(\mathbf{E}g)$, $\mathbf{E}(f^2) = (\mathbf{E}f)^2$, $\mathbf{E}(1/f) = 1/\mathbf{E}f$.

2. Dokažte, že pro libovolnou náhodnou veličinu f platí $\mathbf{E}(f^2) \geq (\mathbf{E}f)^2$.

3. Nechť $f(\pi)$ je počet pevných bodů permutace π (viz část 3.7). Spočtěte $\mathbf{E}f$ pro náhodnou permutaci $\pi \in \mathcal{S}_n$.

4. Buď π náhodná permutace množiny $\{1, 2, \ldots, n\}$.

   (a)* Určete střední délku cyklu π obsahujícího číslo 1.

   (b)* Určete střední počet cyklů π.

5. Hodíme $n\times$ po sobě desetikorunovou mincí, na níž padá lev i Hradčana s pravděpodobností $\frac{1}{2}$. Kolik je střední počet „sérií“ (série jsou souvislé úseky, kdy padá stejná strana)?

6. Předpokládejme, že jeden z milionu lidí má místo levé nohy kopyto, a že tito lidé jsou mezi populací náhodně rozděleni. Detektiv zjistil, že pachatelem zločinné finanční machinace je člověk s kopytem místo levé nohy žijící v Praze (předpokládejme 1 milion obyvatel). Policejní inspektor pak člověka s tímto anatomickým znakem zatkl. Jaká je teď pravděpodobnost, že v Praze žije aspoň jeden další takový člověk?

7.* V první nádobě je n červených kuliček a ve druhé n modrých kuliček. Vezmeme náhodně vybranou kuličku z první nádoby, náhodně vybranou kuličku z druhé nádoby, a dáme je do opačných nádob než ze kterých jsme je vytáhli. Dokažte, že opakujeme-li to $k\times$, je střední hodnota počtu červených kuliček v první nádobě rovna $\frac{1}{2}n\bigl(1+\bigl(1-\frac{2}{n}\bigr)^k\bigr)$.

10.4 Několik aplikací

V této části jsou shromážděny příklady – drobné matematické skvosty – na použití linearity střední hodnoty.

10.4.1 Věta (Existence velkých bipartitních podgrafů). *Buď G graf se sudým počtem, $2n$, vrcholů a s $m > 0$ hranami. Potom množinu $V = V(G)$ lze rozdělit na dvě disjunktní n-prvkové podmnožiny A a B tak, že více než $m/2$ hran G spojuje vrchol z A s vrcholem z B.*

Důkaz. Zvolme n-prvkovou množinu A náhodně mezi všemi n-prvkovými podmnožinami V, položme $B = V \setminus A$. Nechť X označuje počet hran grafu G jdoucích „napříč“, tj. tvaru $\{a, b\}$, kde $a \in A$, $b \in B$. Spočteme střední hodnotu $\mathbf{E}X$ náhodné veličiny X. Pro každou hranu $e = \{u, v\} \in E(G)$ definujeme jev N_e, který nastane pro všechny volby množiny A takové, že hrana e jde napříč, to znamená $|A \cap \{u, v\}| = 1$. Platí $X = \sum_{e \in E(G)} I_{N_e}$, a tedy $\mathbf{E}X = \sum_{e \in E(G)} P(N_e)$. Potřebujeme stanovit pravděpodobnost $P(N_e)$.

Celkem existuje $\binom{2n}{n}$ možností volby množiny A. Požadujeme-li, aby $u \in A$ a $v \notin A$, můžeme zbývajících $n-1$ prvků A zvolit $\binom{2n-2}{n-1}$ způsoby, a podobně pro symetrickou situaci $u \notin A$, $v \in A$. Proto

$$P(N_e) = \frac{2\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1} > \frac{1}{2}.$$

Odtud dostaneme $\mathbf{E}X = \sum_{e \in E(G)} P(N_e) > m/2$. Střední hodnota X je průměrem hodnot X přes všechny volby množiny A. Průměr nemůže být větší než maximum z těchto hodnot, a tedy existuje volba A, pro niž více než polovina hran jde napříč. □

Nezávislé množiny. V oddílu 4.8 jsme zjišťovali maximální možný počet hran grafu na n vrcholech, který neobsahuje žádný trojúhelník. Obecněji se můžeme ptát, kolik nanejvýš hran může mít graf na n vrcholech neobsahující jako podgraf K_k, čili úplný graf na k vrcholech. Na to přesně odpovídá Turánova věta, což je jeden ze základních výsledků extremální teorie grafů.

Tato věta se dá formulovat různými způsoby. Nejsilnější verze, již jsme v oddílu 4.8 dokázali pro speciální případ $k = 3$ (pro obecné k viz cvičení 4.8.5), přesně popisuje, jak musí graf s takovým maximálním možným počtem hran vypadat. Tady předvedeme elegantní pravděpodobnostní důkaz trošku slabšího výsledku, který jen omezuje zmíněný počet hran.

Turánova věta se nejčastěji používá v „obrácené“ podobě: *má-li graf na n vrcholech více než jistý počet hran, pak obsahuje K_k.* Vezmeme-li doplněk grafu G, tj. hrany budou právě tam, kde G hrany neměl, Turánova věta o něm tvrdí: *má-li graf na n vrcholech méně než jistý počet hran, pak obsahuje nezávislou množinu velikosti aspoň k* (nezávislá množina je množina vrcholů, mezi nimiž nejde žádná hrana). V této podobě zde větu zformulujeme a dokážeme.

10.4.2 Věta (Turánova věta). *Pro každý graf na n vrcholech platí*

$$\alpha(G) \geq \frac{n^2}{2|E(G)| + n},$$

kde $\alpha(G)$ značí velikost největší nezávislé množiny v grafu G.

Pravděpodobnostní metodu použijeme v důkazu takovéhoto lemmatu:

10.4.3 Lemma. *Pro každý graf G platí*

$$\alpha(G) \geq \sum_{v \in V(G)} \frac{1}{\deg_G(v) + 1}$$

($\deg_G(v)$ značí stupeň vrcholu v v grafu G).

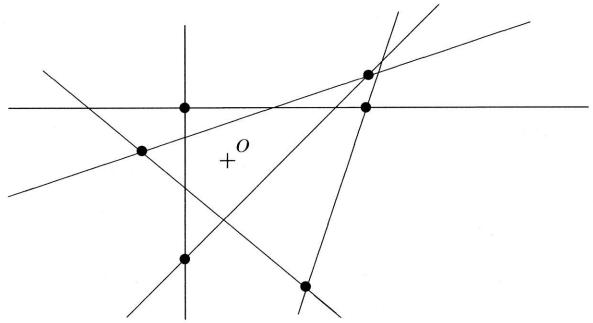
Důkaz. Předpokládejme, že vrcholy grafu G jsou $1, 2, \ldots, n$, a zvolme náhodnou permutaci π těchto vrcholů. Definujeme množinu $M \subseteq V(G)$ obsahující všechny vrcholy v takové, že pro všechny sousedy u vrcholu v platí $\pi(u) > \pi(v)$, tj., vrchol v je v uspořádání podle hodnot π menší než všichni jeho sousedi. Všimněme si, že množina M je nezávislá v grafu G, tedy $|M| \leq \alpha(G)$ pro libovolnou permutaci, a tudíž i $\mathbf{E}|M| \leq \alpha(G)$.

Pro každý vrchol v buď A_v jev „$v \in M$“. Je-li N_v množina všech sousedů vrcholu v, jsou všechna uspořádání množiny $N_v \cup \{v\}$ permutací π stejně pravděpodobná, a tedy pravděpodobnost, že v bude nejmenší z této množiny, je rovna $1/(|N_v| + 1) = 1/(\deg_G(v) + 1)$. Proto $P(A_v) = 1/(\deg_G(v) + 1)$, a můžeme počítat střední hodnotu jako již několikrát:

$$\alpha(G) \geq \mathbf{E}|M| = \sum_{v \in V(G)} \mathbf{E} I_{A_v} = \sum_{v \in V(G)} P(A_v) = \sum_{v \in V(G)} \frac{1}{\deg_G(v) + 1}.$$

□

Důkaz věty 10.4.2. To už je čistě počítání s nerovnostmi. Počet hran grafu $e = |E(G)|$ je polovina součtu stupňů všech vrcholů. Máme



Obrázek 10.1: Průsečíky úrovně 1 pro množinu přímek

tedy takovouto situaci: pro nezáporná reálná čísla $d_1, d_2, \ldots, d_n$ víme $\sum_{i=1}^{n} d_i = 2e$, a ptáme se, jaká je nejmenší možná hodnota součtu

$$\sum_{i=1}^{n} \frac{1}{d_i + 1}.$$

Lze ukázat, že tento součet je minimální pro $d_1 = \cdots = d_n = 2e/n$ (ponecháme do cvičení), a tehdy má hodnotu $n^2/(2e+n)$ jako v tvrzení věty. □

Počet průsečíků úrovně $\leq k$. Mějme množinu L sestávající z n přímek v rovině, z nichž žádné 3 se neprotínají v jednom bodě a žádné 2 nejsou rovnoběžné, a dále nějaký bod o, který neleží na žádné z přímek. Budeme se zabývat průsečíky přímek z L. Celkem je jich $\binom{n}{2}$ (každá dvojice přímek určuje právě 1 průsečík). Řekneme, že průsečík v má *úroveň* k, pokud úsečka ov protíná, kromě dvou přímek procházejících průsečíkem v, ještě k dalších přímek (obr. 10.1 znázorňuje všechny průsečíky úrovně 1). Kolik maximálně může být průsečíků úrovně nejvýš k, pro dané n a k? Tato otázka vzniká při analýze efektivity některých geometrických algoritmů. Následující věta dává horní odhad, který je nejlepší možný až na hodnotu konstanty úměrnosti:

10.4.4 Věta. *Existuje maximálně $3(k+1)n$ průsečíků úrovně nejvýš k.*

Důkaz. Nejdříve se podíváme na případ $k = 0$. Zjišťujeme, že průsečíky úrovně 0 jsou přesně vrcholy ohraničující konvexní mnohoúhelník, jenž obsahuje bod o. Protože každá přímka přispívá nejvýš jednou stranou tohoto mnohoúhelníka, je takových vrcholů nejvýš n. Toho využijeme v dalším. Přikročíme k obecnému případu.

Nechť p označuje jisté číslo v intervalu $(0, 1)$, jehož hodnotu vhodně zvolíme na konci důkazu. Představíme si takovýto náhodný pokus: Náhodně vybereme podmnožinu přímek $R \subseteq L$, přičemž každou přímku $\ell \in L$ dáme do R s pravděpodobností p, a výběry jednotlivých přímek jsou na sobě nezávislé.

Tady je asi na místě říci více o příslušném pravděpodobnostním prostoru. Je to zobecnění prostoru $\mathcal{C}_n$ z příkladu 10.2.2, modelujícího n hodů symetrickou mincí, na níž padá rub a líc se stejnou pravděpodobností, totiž $\frac{1}{2}$. V našem případě bychom používali jakousi nesymetrickou minci, na níž padá líc s pravděpodobností p a rub s pravděpodobností $1-p$. Pro každou přímku $\ell \in L$ bychom jednou hodili, a zahrnuli bychom ji do R jestliže padne líc. Formálně, náš pravděpodobnostní prostor je množina všech podmnožin $R \subseteq L$, a pravděpodobnost množiny $R \subseteq L$, tedy elementárního jevu, je $p^r(1-p)^{n-r}$, kde $r = |R|$ (abychom dostali právě množinu R, musí v určitých r hodech padnout líc a ve zbývajících $n-r$ hodech rub). To je příklad pravděpodobnostního prostoru, kde elementární jevy nemají všechny stejnou pravděpodobnost.

Vraťme se k naší geometrické situaci. Představme si, že bychom do roviny nakreslili jen přímky z takové náhodně vybrané podmnožiny R. Zavedeme náhodnou veličinu $f = f(R)$, což bude počet průsečíků přímek z R úrovně 0, jinak řečeno těch průsečíků, jimž žádná přímka z R nezabraňuje ve výhledu na bod o. Budeme dvěma způsoby počítat střední hodnotu $\mathbf{E}f$. Na jedné straně víme, podle poznámky na začátku důkazu, že pro každou konkrétní množinu R je $f(R) \le |R|$, a proto $\mathbf{E}f \le \mathbf{E}|R|$. Lze snadno spočítat (ponecháváme do cvičení), že $\mathbf{E}|R| = pn$.

Nyní jiný způsob počítání $\mathbf{E}f$. Pro každý průsečík v přímek z L definujeme jev A_v, který nastane, pokud v bude jedním z průsečíků

úrovně 0 přímek z R, tj. přispěje 1 k hodnotě $f(R)$. Jev A nastane, právě když jsou splněny tyto dvě podmínky:

- Obě přímky, určující průsečík v, padnou do R.
- Žádná z přímek, protínajících úsečku ov ve vnitřním bodě (tj. zakrývající bodu o výhled na bod v) nepadne do R.

Z toho je vidět, že $P(A_v) = p^2(1-p)^{u(v)}$, kde $u(v)$ značí úroveň průsečíku v.

Označme M množinu všech průsečíků přímek z L, a $M_k \subseteq M$ množinu průsečíků úrovně nejvýš k. Máme

$$\mathbf{E}f = \sum_{v\in M} \mathbf{E}I_{A_v} = \sum_{v\in M} P(A_v) \ge \sum_{v\in M_k} P(A_v) = \sum_{v\in M_k} p^2(1-p)^{u(v)} \ge$$

$$\ge \sum_{v\in M_k} p^2(1-p)^k = |M_k|p^2(1-p)^k.$$

Celkem jsme tedy odvodili $np \ge \mathbf{E}f \ge |M_k|p^2(1-p)^k$, neboli

$$|M_k| \le \frac{n}{p(1-p)^k}.$$

Zvolíme teď číslo p tak, abychom na pravé straně dostali co nejmenší hodnotu. Vhodná volba je například $p = 1/(k+1)$. Je známo, že pro každé $k \ge 1$ je $(1-\frac{1}{k+1})^k > e^{-1} > \frac{1}{3}$, takže vyjde $|M_k| \le 3(k+1)n$, jak se tvrdí ve větě. □

Poznamenejme ještě, že problém odhadnout maximální možný počet průsečíků úrovně *přesně* k je mnohem obtížnější a dosud nevyřešený.

Průměrný počet porovnání v algoritmu QUICKSORT. Známý třídící algoritmus QUICKSORT (česky „rychlotřídič"?), dostane-li jako vstup posloupnost prvků $(x_1, x_2, \ldots, x_n)$, pracuje takto: porovnáním s x_1 rozdělí ostatní prvky na dvě skupiny, na prvky menší než x_1 a prvky aspoň tak velké jako x_1 (přitom v obou skupinách zachová pořadí prvků jako bylo na vstupu). Každou skupinu pak zvlášť

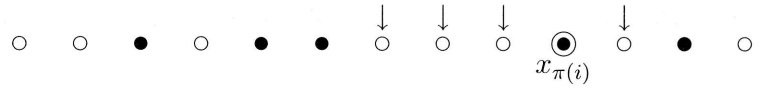
setřídí rekurzivním voláním sebe sama. Rekurze se zastaví u triviálně malých skupin (např. nejvýš dvouprvkových).

Tento algoritmus v nejhorším případě může potřebovat řádově až n^2 kroků (nejhorší, co mu můžeme provést, je dát mu již setříděnou posloupnost). V praxi je však velmi oblíben a bere se jako jeden z nejrychlejších třídících algoritmů. Jeden z důvodů je následující výsledek o jeho průměrném chování:

10.4.5 Věta. *Nechť $x_1 < x_2 < \ldots < x_n$ jsou tříděné prvky v pořadí podle velikosti. Buď π permutace množiny $\{1, 2, \ldots, n\}$, a nechť $T(\pi)$ značí počet porovnání (dvojic čísel podle velikosti) provedených algoritmem QUICKSORT pro vstupní posloupnost $(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$. Potom při náhodné volbě permutace π platí $\mathbf{E}T \leq 2n \ln n$.*

Důvod takového chování není těžké vidět. Jsou-li vstupní čísla srovnána náhodně, lze čekat, že první prvek většinou rozdělí ostatní na dvě zhruba stejně velké skupiny. Rekurze pak bude mít $\log n$ úrovní, a na každé úrovni se spotřebuje celkem $O(n)$ porovnání. To ale není pořádný důkaz. Následující elegantní analýza dává i správnou konstantu úměrnosti.

Důkaz. Nechť T_i je počet prvků porovnávaných s prvkem $x_{\pi(i)}$ ve fázi, kdy se stane dělicím prvkem. Například $T_1 = n - 1$, protože $x_{\pi(1)}$ je první prvek na vstupu a porovnávají se s ním všechny ostatní prvky. Pokud $\pi(2) < \pi(1)$, T_2 bude $\pi(1) - 2$, a pro $\pi(2) > \pi(1)$ je $T_2 = n - \pi(1) - 1$. Obecně si můžeme T_i představit podle obrázku:



Kroužky na tomto obrázku znázorňují $x_1, x_2, \ldots, x_n$ seřazené podle velikosti, plně jsou kresleny prvky s indexy $\pi(1), \pi(2), \ldots, \pi(i-1)$, dvojitě je označen $x_{\pi(i)}$, a prázdné jsou kroužky pro ostatní prvky. Není těžké si rozmyslet, že T_i je právě počet prázdných kroužků, které „vidí“ prvek $x_{\pi(i)}$, přičemž skrz plné kroužky vidět není.

Budeme hledat $\mathbf{E}T_i$. Představme si, že indexy probíráme pozpátku a sledujeme příslušný obrázek s plnými a prázdnými kroužky. Nejprve jsou všechny kroužky plné, postupně se jeden po druhém v náhodném pořadí vyprazdňují. V okamžiku, kdy zbývá i plných kroužků, vezmeme náhodně jeden zbývající plný kroužek, $x_{\pi(i)}$, a T_i bude počet prázdných kroužků, které vidí.

Použijeme jednoduché počítání dvěma způsoby. Každý *prázdný* kroužek vidí nejvýš dva plné kroužky. Proto celkový počet dvojic (plný kroužek, prázdný kroužek), které se vidí, je nejvýš $2(n-i)$. Na jeden z i plných kroužků tedy připadá v průměru nejvýš $\frac{2(n-i)}{i}$ prázdných kroužků, a to je potřebný odhad pro $\mathbf{E}T_i$. Z linearity střední hodnoty konečně dostáváme

$$\mathbf{E}T = \sum_{i=1}^{n} \mathbf{E}T_i \leq \sum_{i=1}^{n} \frac{2(n-i)}{i} = 2n \sum_{i=1}^{n} \frac{1}{i} - 2n \leq 2n \ln n$$

(součet převrácených hodnot jsme odhadli podle cvičení 3.4.12). □

Poznámky. Složitější analýzou se dá dokázat, že při náhodné vstupní permutaci je nepříznivé chování algoritmu (tj. počet porovnání podstatně větší než řádově $n \log n$) velmi málo pravděpodobné. Přesto skutečnost, že algoritmus pracuje špatně zrovna pro setříděné nebo skoro setříděné posloupnosti, je nepříjemná. Existuje řada verzí algoritmu QUICKSORT, které se různými modifikacemi snaží toto odstranit. Modifikace se týkají způsobu výběru prvku, podle nějž se ostatní prvky rozdělí.

Cvičení

1. Odvoďte z věty 10.4.2, že graf na n vrcholech bez trojúhelníků má nejvýš $n^2/4$ hran (to dává další důkaz věty 4.8.1).

2.* Ukažte, že jsou-li $d_1, \ldots, d_n$ nezáporná reálná čísla se součtem 1, potom výraz $\sum_{i=1}^{n} 1/(d_i + 1)$ je minimální pro $d_1 = d_2 = \ldots = d_n = \frac{1}{n}$.

3. Nechť podmnožina $R \subseteq L$ je zvolena náhodně jako v důkazu věty 10.4.4. Ukažte $\mathbf{E}|R| = pn$.

4.* Uvažme přímky jako ve větě 10.4.4, z nichž navíc žádná není svislá, a předpokládejme také, že bod o leží pod všemi přímkami. Řekneme, že průsečík v je *špice*, pokud jedna z přímek jej definujících má kladnou směrnici (zleva doprava stoupá) a druhá má zápornou směrnici (zleva doprava klesá). Dokažte, že existuje nejvýš $6(k+1)^2$ špic úrovně nejvýš k.

11

Řád z nepravidelnosti: Ramseyova věta

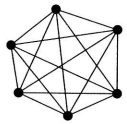
Paul Erdős (1913–1996), slavný matematik dvacátého století a bezpochyby jeden z nejvýznamnějších tvůrců diskrétní matematiky v její dnešní podobě, rád vyprávěl následující historku: Rentgenové paprsky objevil Wilhelm Conrad Röntgen v roce 1895. Ale podobný efekt zpozoroval již před Röntgenem anglický fyzik Sir William Crookes, kterému záhadně zčernaly fotografické desky v blízkosti trubice, již dnes nazýváme Crookesova. Crookes si toho všiml a vydal laborantům pokyn desky u trubic napříště neukládat.

Poučení z toho plyne dvojí. Za prvé, štěstěna přeje objevitelům, kteří jsou na objev připraveni (a tento bod Erdős zdůrazňoval). A za druhé, rozhodující objevy mají často zdánlivě nicotné počátky. Velké teorie někdy začínají efekty, které jsou prahové, které téměř nevnímáme. Ale musíme být připraveni.

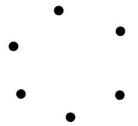
I matematika a informatika mají své objevy, které se mnohdy projevují nenápadně jako nepodstatné kuriozity. V této kapitole uvedeme jednu takovou zvláštnost. Týká se grafů, které mají pouhých 6 vrcholů.

Začněme následující populární formou výsledku: Šest lidí se sejde na večírku. Někteří se vzájemně znají, jiní se neznají, protože se třeba

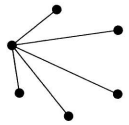
vidí poprvé. Večírky mohou vypadat například takto



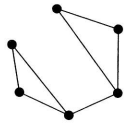
sraz maturantů
po 50 letech



seznamovací
večírek



večírek
ctitelů



jednání dvou
mafiánských bossů

(účastníky jsme znázornili puntíky, dvojice známých jsme spojili čarami, a ejhle – máme grafy na šesti vrcholech!). Nebo i mnoha dalšími způsoby, které by se nám sem ani všechny nevešly. Ale ať už je večírek jakýkoliv, vždy na něm bude trojice účastníků, která se navzájem zná (tedy trojice řekněme přátel) nebo trojice účastníků navzájem cizích. Můžeme s jistotou tvrdit, že jedna z těchto možností musí vždycky nastat, i když nelze předem říct, která.

Toto skromné tvrzení, dalo by se říci hříčka, je zárodkem celé teorie – *Ramseyovy teorie*, z níž v této kapitole uvidíme malý kousek. V následujícím oddílu dokážeme tvrzení pro večírky se šesti účastníky, což není tak snadné, jak by se mohlo na první pohled zdát, a v oddílu 11.2 dokážeme Ramseyovu větu pro grafy, která ukazuje, že zvláštnost na 6 vrcholech zase taková zvláštnost není. Další překvapení v Ramseyově větě skryté potkáme v oddíle 11.3: ukážeme, že Ramseyova věta platí jen pro množiny skutečně obrovské. Jako kombinatorický princip je to tedy nástroj velmi neefektivní a obtížný. Ukážeme to přístupem, vysvětleným v kapitole 10 – pravděpodobnostní metodou.

11.1 Večírky se šesti

Dokažme nyní tvrzení o večírcích se šesti účastníky. Večírek si samozřejmě můžeme představit jako graf, kde vrcholy odpovídají účastníkům a hrany grafu dvojicím, které se znají. Předpokládáme, že známost je vztah symetrický. Podobně jako v oddílu 2.4 zaveďme následující značení: $\omega(G)$ nechť označuje maximální počet vrcholů úplného

podgrafu G a $\alpha(G)$ nechť je maximální počet vrcholů nezávislé množiny vrcholů G, tj. množiny vrcholů, v níž žádné dva nejsou spojeny hranou.

Dokážeme následující větu.

11.1.1 Věta. *Nechť G je graf s alespoň 6 vrcholy. Potom $\alpha(G) \geq 3$ nebo $\omega(G) \geq 3$.*

Důkaz. Zvolme libovolně jeden z vrcholů grafu G a označme jej u. Nechť $A \subseteq V(G) \setminus \{u\}$ je množina vrcholů, které nejsou s u spojeny hranou; formálně $A = \{v \in V(G);\ v \neq u, \{u,v\} \notin E(G)\}$. Nechť $B = V(G) \setminus A \setminus \{u\}$ sestává z vrcholů, které s u spojeny jsou. Protože $|V(G)| \geq 6$, musí některá z množin A, B mít nejméně 3 prvky. Rozlišíme tedy dva případy.

1. *Případ* $|A| \geq 3$. Nechť A obsahuje vrcholy x, y, z. Jestliže každé dva z nich tvoří hranu grafu G, potom $\{x,y,z\}$ je úplný podgraf dokazující $\omega(G) \geq 3$. V opačném případě nechť například $\{x,y\} \notin E(G)$. Potom však $\{u,x,y\}$ je nezávislá množina v grafu G, a tedy $\alpha(G) \geq 3$.

2. *Případ* $|B| \geq 3$. Postupujeme obdobně: Buď žádná dvojice vrcholů z B netvoří hranu, a tudíž $\alpha(G) \geq 3$, nebo existují dva vrcholy $x, y \in B$, které tvoří hranu v G. Potom však množina $\{u,x,y\}$ je úplný podgraf G, a tedy $\omega(G) \geq 3$. □

Všimněte si, kolik možností jsme museli rozlišit, abychom dokázali větu pro grafy se 6 vrcholy. Přitom výsledek sám zní jako hříčka. Záhy však uvidíme, že je speciálním případem obecnějších tvrzení. Uvědomte si, že v důkazu věty 11.1.1 jsme rovněž použili speciální případ (pro $t = 2, n_1 = n_2 = 3$) následujícího tvrzení, v české literatuře nazývaného *Dirichletův princip*[1].

11.1.2 Věta (Dirichletův princip). *Nechť $n_1, n_2, \ldots, n_t$ jsou přirozená čísla, nechť X je množina s nejméně $1 + \sum_{i=1}^{t}(n_i - 1)$ prvky,*

[1] V anglické literatuře pigeonhole principle a v německé Schubfachprinzip.

a nechť množiny $X_1, X_2, \ldots, X_t$ tvoří rozklad množiny X. Potom existuje i takové, že X_i má velikost alespoň n_i.

11.2 Ramseyova věta pro grafy

Zde je slíbené zobecnění věty 11.1.1 pro „větší večírky".

11.2.1 Věta (Ramseyova věta pro grafy). *Nechť graf G má alespoň $\binom{k+\ell-2}{k-1}$ vrcholů. Potom $\omega(G) \geq k$ nebo $\alpha(G) \geq \ell$.*

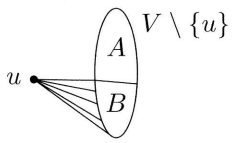
Všimněte si, že podmínka věty je symetrická v k a ℓ, poněvadž $\binom{k+\ell-2}{k-1} = \binom{k+\ell-2}{\ell-1}$.

Dosadíme-li do věty $k = \ell = 3$, dostáváme, že každý graf G se $\binom{4}{2} = 6$ vrcholy splňuje $\omega(G) \geq 3$ nebo $\alpha(G) \geq 3$, což je právě věta 11.1.1. Pozornému čtenáři rovněž neunikne, jak je následující důkaz obdobný důkazu věty 11.1.1.

Důkaz. Postupujme indukcí dle $k + \ell$. Pokud $k = 1$ nebo $\ell = 1$, je snadno vidět, že tvrzení platí. (A jeho platnost není těžké nahlédnout ani pro $k = 2$ nebo $\ell = 2$, ale tento případ není nutné řešit zvlášť.)

Teď předpokládejme, že $k, \ell \geq 2$ a že tvrzení platí pro $k, \ell - 1$ a také pro $k-1, \ell$. Položíme $n = \binom{k+\ell-2}{k-1}$, $n_1 = \binom{k+\ell-3}{k-1}$ a $n_2 = \binom{k+\ell-3}{k-2}$. Podle Pascalova vzorce (3.5) pro součet binomických koeficientů máme $n = n_1 + n_2$, což přepíšeme do tvaru $n = 1 + ((n_1 - 1) + (n_2 - 1) + 1)$, který napovídá schéma důkazu.

Nechť $G = (V, E)$ je libovolný graf s n vrcholy. Chceme ukázat, že $\omega(G) \geq k$ nebo $\alpha(G) \geq \ell$. Zvolme některý vrchol $u \in V$. Rozdělíme zbývající vrcholy na dvě podmnožiny A a B podle toho, zda jsou nebo nejsou spojeny s vrcholem u, viz obrázek:



Formálně

$$A = \{v \in V \setminus \{u\};\ \{u, v\} \notin E\}$$

$$B = \{v \in V \setminus \{u\};\ \{u, v\} \in E\}.$$

Podle Dirichletova principu platí $|A| \geq n_1$ nebo $|B| \geq n_2$. Pokud $|A| \geq n_1$, použijeme indukčního předpokladu pro dvojici $(k, \ell - 1)$. Dostaneme, že graf G_A indukovaný množinou A splňuje $\omega(G_A) \geq k$ nebo $\alpha(G_A) \geq \ell - 1$. V prvním případě rovněž $\omega(G) \geq k$. Ve druhém případě libovolná nezávislá množina $I \subset A$ tvoří spolu s vrcholem u nezávislou množinu $I \cup \{u\}$ v grafu G, a tedy $\alpha(G) \geq \alpha(G_A) + 1 \geq \ell$.

V případě $|B| \geq n_2$ postupujeme obdobně, a opět dostaneme, že $\omega(G) \geq k$ nebo $\alpha(G) \geq \ell$. Tím je učiněn indukční krok. □

Právě dokázaná věta umožňuje zavést následující definici: Označme $r(k, \ell)$ minimální číslo n takové, že každý graf G s n vrcholy splňuje $\omega(G) \geq k$ nebo $\alpha(G) \geq \ell$. Číslo $r(k, \ell)$ se nazývá *Ramseyovo číslo.* Věta nám zaručuje, že tato definice má smysl, že $r(k, \ell)$ existuje pro každé $k \geq 1$ a $\ell \geq 1$.

Shrňme hodnoty Ramseyových čísel, které jsme odvodili nebo které je snadné nahlédnout:

$$\begin{aligned} r(1,\ell) &= 1, & r(k,1) &= 1 \\ r(2,\ell) &= \ell, & r(k,2) &= k \\ r(3,3) &= 6. \end{aligned}$$

Kromě těchto hodnot je známa jen hrstka dalších. Například platí $r(4,4) = 18$, zatímco $r(5,5)$ je hodnota dosud neznámá, přes usilovnou snahu lidí i počítačů.

V následujícím článku uvedeme dolní odhad čísel $r(k, k)$.

Cvičení

1. (a) Ověřte, že z věty 11.2.1 plyne následující tvrzení: Pro každé n existuje N takové, že je-li X množina s N prvky a $\binom{X}{2} = E_1 \cup E_2$ je libovolný rozklad na 2 části, potom aspoň jeden z grafů (X, E_1) a (X, E_2) obsahuje úplný podgraf s n vrcholy.

   (b) Dokažte předcházející cvičení pro libovolný rozklad množiny množiny $\binom{X}{2}$ na r částí $E_1, E_2, \ldots, E_r$. (Návod: postupujte indukcí podle r.)

2. Pro graf G definujeme $f(G) = \alpha(G)\cdot\omega(G)$ a položme $f(n) = \min f(G)$, kde minimum se týká všech grafů s n vrcholy.

   (a) Dokažte, že pro $n \in \{1,2,3,4,6\}$ platí $f(n) \geq n$.

   (b) Ukažte, že $f(5) < 5$.

   (c)* Pro přirozená čísla n, k, $1 < k \leq n/2$, definujme graf $C_{n,k}$: Začneme s C_n, tj. kružnicí délky n, a v ní pak spojíme hranami každou dvojici vrcholů, které v C_n měly vzdálenost nejvýš k. Pomocí těchto grafů (s vhodnou volbou k) dokažte, že $f(n) < n$ pro všechna $n \geq 7$.

3. Pro funkci $f(n)$ ve cvičení 2 dokažte, že je neklesající a že není shora omezená.

4. V článku 2.4 jsme zavedli značení $\alpha(P)$ a $\omega(P)$ pro částečně uspořádanou množinu P. Toto značení se podobá značení zavedenému v této kapitole. Dokažte, že $\alpha(P)$ a $\omega(P)$ lze vyjádřit jako $\alpha(G_P)$ a $\omega(G_P)$ pro vhodný graf G_P. (Návod: G_P se obvykle nazývá graf porovnatelnosti.)

   Tyto grafy G_P podle věty 2.4.5 (o dlouhém a širokém) splňují

   $$\alpha(G_P)\omega(G_P) \geq |V(G_P)|;$$

   srovnejte se cvičením 2.

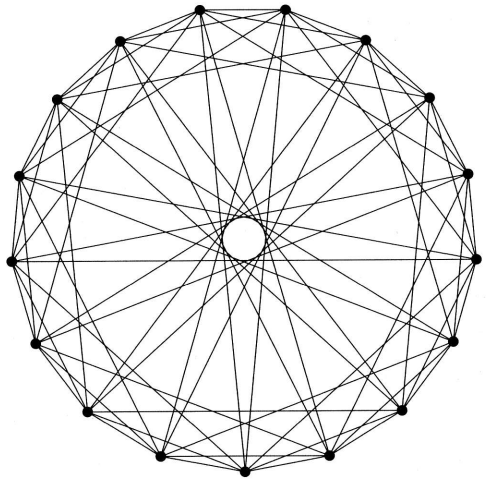
5. Dokažte, že pokud $k \leq k'$ a $\ell \leq \ell'$, potom $r(k,\ell) \leq r(k',\ell')$.

6.** Zkuste sami porozumět následujícímu zobecnění Ramseyovy věty pro rozklady konečných množin a dokázat je. *Pro každou trojici kladných celých čísel p, r, n existuje číslo N s následující vlastností: Je-li X libovolná množina s alespoň N prvky a je-li $\binom{X}{p} = A_1 \cup A_2 \cup \cdots \cup A_r$ libovolný rozklad, potom existuje n-prvková podmnožina $Y \subseteq X$ tak, že $\binom{Y}{p}$ je celé obsaženo v jedné třídě A_i rozkladu.* (Návod: postupujte indukcí dle p.)

11.3 Dolní odhad Ramseyových čísel

V tomto článku odvodíme jednu ze základních vlastností Ramseyových čísel, která ovlivňuje jejich zkoumání i použití. Ukážeme, že čísla $r(k,k)$, která zde pro stručnost označíme $r(k)$, rostou exponenciálně rychle. (Poznamenejme, že pro některá zobecnění Ramseyovy věty, o nichž zde nemluvíme, se dostanou ještě mnohem rychleji rostoucí

funkce.) Předtím, než přistoupíme k vlastnímu výsledku, si uvědomíme, co znamená dokázat dolní odhad pro Ramseyovo číslo $r(k)$: Tvrdíme-li $r(k) > n$, znamená to existenci jistého grafu G na n vrcholech, konkrétně takového, že $\omega(G) < k$ a $\alpha(G) < k$. (*Nestačí* tedy ověřit $n < \binom{2k-2}{k-1}$, protože výraz $\binom{2k-2}{k-1}$ z věty 11.2.1 je pouze horním odhadem pro $r(k)$, a $r(k)$ by mohlo být ještě podstatně menší.) Například nerovnost $r(3) > 5$ jsme dokázali pomocí grafu C_5. V předchozí sekci jsme bez důkazu zmínili, že $r(4) = 18$. Vztah $r(4) > 17$ je možno dokázat pomocí následujícího grafu:



Poznamenejme, že jak v případě $r(3) > 5$, tak v případě $r(4) > 17$ jsou grafy určeny jednoznačně až na isomorfismus. To naznačuje obtížnost dolních odhadů Ramseyových čísel.

Zde dokážeme dolní odhad pro $r(k)$ pravděpodobnostní metodou, o jejíchž základech pojednává kapitola 10. Je to jedno z prvních použití pravděpodobnostních důkazů v kombinatorice a matematice vůbec.

11.3.1 Věta. *Nechť k a n jsou čísla splňující $\binom{n}{k}\cdot 2^{1-\binom{k}{2}} < 1$. Potom $r(k) > n$.*

Pro jaká čísla k a n je uvedená podmínka splněna? Jak je v pravděpodobnostní metodě obvyklé, použijeme poměrně hrubé a jednoduché

odhady:

$$\binom{n}{k} \leq \frac{n^k}{k!} < \frac{n^k}{2^{k/2+1}}$$

(druhá nerovnost platí jen pro $k \geq 3$). Poznamenejme, že použitím přesnějších odhadů z kapitoly 3 nedostaneme výsledek o mnoho silnější. Výraz z věty 11.3.1 tedy odhadneme takto:

$$\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < \frac{n^k}{2^{k/2+1}} \cdot 2^{1-k(k-1)/2} = \left(\frac{n}{2^{k/2}}\right)^k.$$

Tedy pro $n = 2^{k/2}$ jsou podmínky věty splněny a dostáváme následující:

11.3.2 Důsledek. *Pro každé $k \geq 3$ platí $r(k) > 2^{k/2}$.*

Důkaz věty 11.3.1. Jako v kapitole 10 uvažme náhodný graf G na množině $V = \{1, \ldots, n\}$, kde každá z $\binom{n}{2}$ možných hran se objevuje s pravděpodobností $\frac{1}{2}$, nezávisle na ostatních. Nechť K je libovolná k-prvková podmnožina množiny V. Označme A_K jev, že vrcholy K indukují úplný podgraf v G. Zřejmě pravděpodobnost $P(A_K)$ jevu A_K je $2^{-\binom{k}{2}}$. Podobně označíme-li B_K jev, že vrcholy K tvoří nezávislou množinu v G, je $P(B_K) = 2^{-\binom{k}{2}}$. Tedy pravděpodobnost jevu C_K, že K je buďto úplný podgraf nebo nezávislá množina, je $2 \cdot 2^{-\binom{k}{2}} = 2^{1-\binom{k}{2}}$. Označme písmenem p pravděpodobnost, že v náhodném grafu G existuje k-prvková podmnožina K vrcholů, pro niž nastane jev C_K. Tuto pravděpodobnost je obtížné určit, protože pro různé množiny K nejsou jevy C_K nezávislé. Nám ale postačí shora odhadnout pravděpodobnost p součtem pravděpodobností jevů C_K:

$$p \leq \sum_{K \subseteq V, |K|=k} P(C_K)$$

(sčítá se přes všechny k-prvkové podmnožiny n-prvkové množiny V). Dostáváme tedy $p \leq \binom{n}{k} \cdot 2^{1-\binom{k}{2}}$, a tím pádem předpoklad věty zaručuje $p < 1$. To ovšem znamená, že musí existovat alespoň jeden graf na množině V, pro nějž jak α, tak ω jsou menší než k. □

Poznamenejme, že uvedený důkaz neposkytuje žádný návod, jak sestrojit graf dosvědčující nerovnost $r(k) > 2^{\frac{k}{2}}$. Nejenom to: přestože uvedený (slavný) důkaz P. Erdőse pochází z roku 1947, konstrukci takových grafů se nepodařilo nalézt dodnes, a tento dolní odhad Ramseyových čísel zůstává jedním z nejpřesvědčivějších dokladů síly pravděpodobnostní metody.

Cvičení

1. Dokažte, že $\sqrt{2} \leq \sqrt[k]{r(k)} \leq 4$.
2. Zkonstruujte graf G, který ukazuje, že $r(k) \geq (k-1)^2$.
3.* Graf dosvědčující $r(4) > 17$ může vypadat složitě, ale dá se snadno zapamatovat. Například si stačí pamatovat: 17; 1,2,4,8. Nebo také: Kvadratické zbytky modulo 17. Umíte tyto dva trochu záhadné návody objasnit?
4. Dokažte $r(4) = 18$ uvážením grafu na obrázku v textu a „vylepšením“ důkazu věty 11.2.1.

12

Vytvořující funkce

V této kapitole probereme jednu užitečnou početní techniku. Základní myšlenkou je sdružit se studovanou nekonečnou posloupností reálných čísel jistou spojitou funkci, tzv. vytvořující funkci této posloupnosti. Úlohy o posloupnostech lze pak řešit využitím různých operací s funkcemi a poznatků o funkcích. Takový přechod je velmi nesamozřejmý a mnohé aplikace vytvořujících funkcí, ač technicky nejsou příliš hluboké, můžeme právem nazvat podivuhodnými.

V tomto úvodním textu se dostaneme pouze k jednodušším příkladům, řešitelným i bez použití vytvořujících funkcí. V některých úlohách různé triky dokonce vedou k cíli rychleji než počítání přes vytvořující funkce (nemusí však být snadné na takové triky přijít). To by čtenáře nemělo odrazovat od zvládnutí technik s vytvořujícími funkcemi, neboť ty jsou mocným nástrojem i pro složitější problémy, kde jiné postupy selhávají nebo se stávají příliš složitými.

U některých řešení jsou alternativní postupy zmíněny, jinde jsou naznačeny ve cvičeních. Někdy čtenář možná najde ještě jednodušší řešení.

12.1 Kombinatorické aplikace mnohočlenů

Jak vynásobit mnohočleny $p(x) = x+x^2+x^3+x^4$ a $q(x) = x+x^3+x^4$? Třeba podle tohoto jednoduchého pravidla: vynásobíme každý člen

z $p(x)$ každým členem z $q(x)$, a všechny tyto součiny sečteme, přesněji řečeno sloučíme součiny se stejnými mocninami x. Součin takto vyjde $x^8 + 2x^7 + 2x^6 + 3x^5 + 2x^4 + x^3 + x^2$.

Ptejme se teď jinak: vybereme si nějakou mocninu x, například x^5, a chceme vědět, jaký bude její koeficient v součinu, aniž bychom celý součin počítali. Člen s x^5 se v součinu může objevit vynásobením nějakého členu x^i z $p(x)$ členem x^{5-i} z $q(x)$. Koeficient u x^5 v součinu bude tedy právě počet způsobů, kterými se dá vyhovující i zvolit. Jinak řečeno, koeficient u x^5 bude počet dvojic (i,j), kde $i \in \{1,2,3,4\}$ (to je „množina exponentů" mnohočlenu $p(x)$), $j \in \{1,3,4\}$ (to jsou exponenty v $q(x)$) a přitom $i + j = 5$.

To, co jsme právě řekli, vyjádříme trochu obecněji. Nechť I, J jsou konečné množiny přirozených čísel. Utvoříme mnohočleny $p(x) = \sum_{i \in I} x^i$ a $q(x) = \sum_{j \in J} x^j$ (všechny koeficienty v takových mnohočlenech jsou rovny 1). Potom pro každé přirozené číslo r platí

Počet řešení (i,j) rovnice

$$i + j = r$$

splňujících $i \in I$, $j \in J$ je roven koeficientu u x^r v součinu $p(x)q(x)$.

Další a zajímavější zobecnění tohoto pozorování je na součin 3 a více mnohočlenů. Ilustrujeme jej nejdřív na příkladu.

12.1.1 Úloha. *Kolika způsoby lze zaplatit částku* 21 *korun, máme-li* 6 *korunových mincí,* 5 *dvoukorun a* 4 *pětikoruny?*

Hledaný počet je zřejmě roven počtu řešení rovnice

$$i_1 + i_2 + i_3 = 21,$$

kde $i_1 \in \{0,1,2,3,4,5,6\}$, $i_2 \in \{0,2,4,6,8,10\}$, $i_3 \in \{0,5,10,15,20\}$ – i_1 je částka zaplacená korunami, i_2 částka zaplacená dvoukorunami a i_3 pětikorunami.

Tentokrát tvrdíme, že počet řešení této rovnice je roven koeficientu u x^{21} v součinu

$$\left(1 + x + x^2 + x^3 + x^4 + x^5 + x^6\right)\left(1 + x^2 + x^4 + x^6 + x^8 + x^{10}\right) \times$$
$$\times \left(1 + x^5 + x^{10} + x^{15} + x^{20}\right)$$

(samozřejmě poté, co ho roznásobíme a upravíme). Člen s x^{21} totiž dostáváme tak, že vezmeme nějaký člen x^{i_1} z první závorky, nějaký člen x^{i_2} ze druhé závorky a x^{i_3} ze třetí, přičemž $i_1 + i_2 + i_3 = 21$. Každý takový možný výběr přispěje 1 k uvažovanému koeficientu.

Čím nám toto pomůže v řešení úlohy? Z čistě praktického hlediska, usnadní to použití počítače na její řešení, máme-li ovšem k dispozici nějaký program pro násobení mnohočlenů (systémů pro počítání s formulemi, které zvládnou násobení mnohočlenů i mnoho dalších rutinních matematických úloh, existuje řada, mezi nejznámější patří Reduce, Maple, Mathematica, Macsyma, Derive, Mupad,...). Tak byla také zjištěna odpověď k tomuto příkladu: 9. Hledaný počet můžeme samozřejmě najít probráním všech možností (máme také jen celkem málo mincí), ale snadno se může stát, že na nějakou zapomeneme. Nejvýznamnější je však uvedený postup jako předehra ke složitějším metodám.

Kombinatorický význam binomické věty. Binomická věta tvrdí

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n. \tag{12.1}$$

Na levé straně máme součin n mnohočlenů, každý z nich je $1 + x$. Podle výše uvedeného, koeficient u x^r po roznásobení bude počet řešení rovnice

$$i_1 + i_2 + \cdots + i_n = r,$$

kde $i_1, i_2, \ldots, i_n \in \{0,1\}$. Ale každé řešení takové rovnice znamená vybrat r proměnných mezi $i_1, i_2, \ldots, i_n$, které budou rovny 1 – ostatní pak budou rovny 0. Takových výběrů je stejně jako r-prvkových podmnožin n-prvkové množiny, tedy $\binom{n}{r}$. To znamená, že koeficient při x^r v mnohočlenu $(1+x)^r$ je $\binom{n}{r}$. Právě jsme kombinatoricky dokázali binomickou větu!

Pohráváme-li si šikovně s mnohočlenem $(1+x)^n$ a jemu podobnými, můžeme odvodit hodnoty různých sum s binomickými koeficienty. Nejjednodušší příklad jsme viděli už v části 3.3, jmenovitě vzorce $\sum_{k=0}^{n}\binom{n}{k} = 2^n$ a $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$, které dostaneme dosazením $x = 1$, resp. $x = -1$ do (12.1).

12.1.2 Příklad. *Platí rovnost*

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$$

Důkaz. Tento vztah můžeme odvodit derivováním obou stran vzorce (12.1) jako funkce proměnné x. Na obou stranách musí samozřejmě vyjít týž mnohočlen. Derivováním levé strany dostaneme $n(1+x)^{n-1}$, derivováním pravé strany člen po členu obdržíme $\sum_{k=0}^{n} k\binom{n}{k}x^{k-1}$. Dosazením $x = 1$ vznikne požadovaná rovnost.

Příklad jiného typu je založen na rovnosti koeficientů ve dvou vyjádřeních téhož mnohočlenu.

Jiný důkaz tvrzení 3.3.3. Uvažme identitu

$$(1+x)^n(1+x)^n = (1+x)^{2n}.$$

Koeficient při x^n na pravé straně je $\binom{2n}{n}$. Na levé straně můžeme rozvinout obě mocniny $(1+x)^n$ podle binomické věty, a potom násobit dva vzniklé mnohočleny. Koeficient u x^n v jejich součinu můžeme vyjádřit jako $\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \cdots + \binom{n}{n}\binom{n}{0}$, a to musí být totéž jako koeficient na pravé straně, tj.

$$\sum_{i=0}^{n}\binom{n}{i}\binom{n}{n-i} = \binom{2n}{n}.$$

Tím jsme znovu dokázali tvrzení 3.3.3. □

Podobným způsobem lze spočítat i řadu dalších, komplikovanějších sum. Pokusíme-li se však o nějaké složitější výpočty, brzy začneme pociťovat jako nepříjemné omezení to, že pracujeme jen s mnohočleny, jež mají jen konečný počet členů. „Správným" nástrojem pro podobné aplikace se ukazují být analogie mnohočlenů, u nichž však připouštíme nekonečný počet mocnin proměnné x, tzv. mocninné řady.

Cvičení

1. V cukrárně prodávají 3 druhy zákusků – větrníky, kremrole a punčové dortíky. Kolika způsoby lze koupit 12 zákusků tak, aby se od každého druhu koupily aspoň 2 zákusky a přitom nejvýš 3 kremrole? Vyjádřete hledaný počet jako koeficient vhodné mocniny x ve vhodném součinu mnohočlenů.
2. Kolika způsoby lze rozdělit 10 stejných balónků 2 chlapečkům a 2 holčičkám, má-li každý chlapeček dostat aspoň 1 balónek a každá holčička nejméně 2? Vyjádřete hledaný počet jako koeficient vhodné mocniny x ve vhodném součinu mnohočlenů.
3. Dokažte multinomickou větu 3.3.4 podobnou úvahou, jako jsme zde dokazovali větu binomickou.
4. Spočtěte sumu v příkladu 12.1.2 vhodnou početní úpravou výrazu $k\binom{n}{k}$ a použitím binomické věty.
5. Spočítejte sumu $\sum_{i=0}^{n}(-1)^i\binom{n}{i}\binom{n}{n-i}$.

12.2 Rozšíření na nekonečné řady

Vlastnosti mocninných řad. *Mocninnou řadou* budeme rozumět nekonečnou řadu tvaru $a_0 + a_1x + a_2x^2 + \cdots$, kde $a_0, a_1, a_2, \ldots$ jsou reálná čísla a x je proměnná, nabývající reálných hodnot[1]. Uvedenou mocninnou řadu budeme zpravidla označovat $a(x)$.

Jednoduchým příkladem mocninné řady je

$$1 + x + x^2 + x^3 + \cdots \tag{12.2}$$

(všechna a_i jsou rovna 1). Ze vzorce pro součet geometrické řady víme, že pro každé $x \in (-1, 1)$ tato řada konverguje, a její součet je roven

[1] Velmi užitečné je též rozšíření na komplexní čísla a aplikace metod z teorie funkcí komplexní proměnné. Tak daleko se však v tomto úvodním textu nedostaneme.

$1/(1-x)$. V tomto smyslu řada (12.2) určuje funkci $1/(1-x)$. Obráceně, uvedená funkce v sobě naopak obsahuje veškerou informaci o řadě (12.2), protože koeficienty řady jsou, jak se může čtenář přesvědčit, právě koeficienty Taylorova rozvoje funkce $1/(1-x)$ v bodě 0. Takové převtělování nekonečné posloupnosti čísel ve funkci a zpět je klíčovým obratem v technice vytvořujících funkcí.

Následující tvrzení říká, že nerostou-li členy posloupnosti $(a_0, a_1, a_2, \ldots)$ příliš rychle, definuje příslušná nekonečná řada $a(x) = a_0 + a_1x + a_2x^2 + \cdots$ skutečně funkci reálné proměnné x (aspoň na malém okolí 0), a ze znalosti hodnot této funkce můžeme posloupnost $(a_0, a_1, a_2, \ldots)$ zpětně rekonstruovat.

12.2.1 Tvrzení. *Buď $(a_0, a_1, a_2, \ldots)$ posloupnost reálných čísel. Předpokládejme, že pro nějaké číslo K platí $|a_n| \leq K^n$ pro všechna $n \geq 1$. Potom pro každé $x \in (-\frac{1}{K}, \frac{1}{K})$ řada $a(x) = \sum_{i=0}^{\infty} a_i x^i$ konverguje (dokonce absolutně), a hodnota jejího součtu definuje tedy funkci proměnné x na uvedeném intervalu; tuto funkci budeme označovat též $a(x)$. Hodnotami funkce $a(x)$ na libovolně malém okolí 0 jsou všechny členy posloupnosti $(a_0, a_1, a_2, \ldots)$ jednoznačně určeny: funkce $a(x)$ má totiž v bodě 0 derivace všech řádů, a pro $n = 0, 1, 2, \ldots$ platí*

$$a_n = \frac{a^{(n)}(0)}{n!}$$

($a^{(n)}(0)$ značí n-tou derivaci funkce $a(x)$ v bodě 0).

Důkaz plyne z poznatků z matematické analýzy a zde jej nebudeme uvádět, podobně jako u několika dalších tvrzení v tomto oddílu. Nejpřirozenější důkazy se dostanou z teorie funkcí komplexní proměnné, která se zpravidla probírá až v pokročilejších přednáškách. Nicméně pro naše účely potřebujeme velice málo, a to se dá trochu pracněji dokázat i elementárně, ze základních vět o limitách a derivování. V následujících příkladech nebudeme pro uvažované mocninné řady předpoklad tvrzení 12.2.1 výslovně ověřovat. V mnoha případech můžeme tomu uniknout následujícím alibistickým způsobem: Najdeme-li jednou správné řešení úlohy pomocí vytvořujících funkcí jakkoli podezřelou metodou, můžeme potom ověřit správnost řešení jinak, třeba indukcí.

Teď konečně řekneme, co je vytvořující funkce:

12.2.2 Definice. *Nechť $(a_0, a_1, a_2, \ldots)$ je posloupnost reálných čísel.* Vytvořující funkcí *této posloupnosti*[2] *rozumíme mocninnou řadu*

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots .$$

Má-li posloupnost $(a_0, a_1, a_2, \ldots)$ jen konečně mnoho nenulových členů, její vytvořující funkce je mnohočlen. V předchozím oddílu jsme tedy různě využívali vytvořujících funkcí konečných posloupností (aniž jsme jim tak říkali).

Operace s posloupnostmi a jejich vytvořujícími funkcemi. Operace popsané dále můžeme použít pro nalezení šikovného vyjádření vytvořující funkce pro danou posloupnost (tj. pro otázky typu „Jaká je vytvořující funkce posloupnosti $(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots)$?“), nebo někdy i pro hledání posloupnosti pro danou vytvořující funkci (ptáme-li se třeba „Která posloupnost má vytvořující funkci $\ln(1-x)$?“). V dalším budou $(a_0, a_1, a_2, \ldots)$ a $(b_0, b_1, b_2, \ldots)$ posloupnosti a $a(x), b(x)$ jejich vytvořující funkce.

A. Sčítáme-li posloupnosti člen po členu, odpovídá tomu zřejmě *sčítání* vytvořujících funkcí, tj. posloupnost $(a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$ má vytvořující funkci $a(x) + b(x)$.

B. Jiná jednoduchá operace je *násobení reálným číslem* α: posloupnost $(\alpha a_0, \alpha a_1, \alpha a_2, \ldots)$ má vytvořující funkci $\alpha a(x)$.

C. Je-li n nějaké přirozené číslo, vytvořující funkce $x^n a(x)$ odpovídá posloupnosti

$$(\underbrace{0, 0, \ldots, 0}_{n\times}, a_0, a_1, a_2, \ldots) ;$$

[2] Obšírnější název používaný v literatuře je *obyčejná vytvořující funkce*. Jak toto napovídá, používají se i jiné typy vytvořujících funkcí, z nichž pro kombinatorické aplikace nejdůležitější jsou patrně *exponenciální vytvořující funkce*. Exponenciální vytvořující funkce posloupnosti $(a_0, a_1, a_2, \ldots)$ je mocninná řada $\sum_{i=0}^{\infty} a_i/i!$, tj. např. pro posloupnost $(1, 1, 1, \ldots)$ dostaneme exponenciální vytvořující funkci e^x. V dalším se omezíme na obyčejné vytvořující funkce.

to je velmi užitečné pro *posunutí posloupnosti doprava* o potřebný počet míst.

D. Co dělat, chceme-li naopak *posunout doleva*, neboli získat vytvořující funkci např. pro posloupnost $(a_3, a_4, a_5, \ldots)$? Je ovšem potřeba dělit x^3, ale nesmíme zapomenout odečíst první 3 členy; správná vytvořující funkce pro uvedenou posloupnost je

$$(a(x) - a_0 - a_1x - a_2x^2)/x^3.$$

E. *Dosazení αx za x*: Utvoříme-li funkci $c(x) = a(\alpha x)$, kde α je opět pevné reálné číslo, bude $c(x)$ vytvořující funkcí pro posloupnost $(a_0, \alpha a_1, \alpha^2 a_2, \ldots)$. Kupříkladu: Jak už víme, je $1/(1-x)$ vytvořující funkce posloupnosti samých jedniček, a podle právě uvedeného pravidla bude tedy $1/(1-2x)$ vytvořující funkcí pro posloupnost mocnin dvojky, $(1, 2, 4, 8, \ldots)$. Na této operaci je založen i trik pro nahrazení všech členů posloupnosti s lichým indexem nulou: jak se může čtenář přesvědčit, odpovídá funkce $(a(x) + a(-x))/2$ posloupnosti $(a_0, 0, a_2, 0, a_4, 0, \ldots)$.

F. Jinou možností je *dosazení x^n za x*. Tím vznikne posloupnost, v níž nk-tý člen bude roven k-tému členu původní posloupnosti, a všechny ostatní členy budou nulové. Tak např. funkce $a(x^3)$ dává posloupnost $(a_0, 0, 0, a_1, 0, 0, a_2, 0, 0, \ldots)$. Se složitějšími případy, jako je dosazení jedné mocninné řady do druhé, se v našich příkladech nesetkáme, ale v komplikovanějších úvahách se objevují také.

12.2.3 Úloha. *Jaká je vytvořující funkce posloupnosti*

$$(1, 1, 2, 2, 4, 4, 8, 8, \ldots),$$

tj. $a_n = 2^{\lfloor n/2 \rfloor}$*?*

Řešení. Jak jsme zmínili v E, posloupnost $(1, 2, 4, 8, \ldots)$ má vytvořující funkci $1/(1-2x)$. Podle F dostaneme vytvořující funkci $1/(1-2x^2)$ pro posloupnost $(1, 0, 2, 0, 4, 0, \ldots)$, a podle C odpovídá posloupnosti

$(0, 1, 0, 2, 0, \ldots)$ vytvořující funkce $x/(1-2x^2)$. Sečtením konečně dostaneme vytvořující funkci pro původní posloupnost, tj. odpověď je $(1+x)/(1-2x^2)$. □

G. Populární operace z matematické analýzy, *derivování a integrování* podle proměnné x, znamenají v řeči posloupností toto: derivace funkce $a(x)$, čili $a'(x)$, má jako svoji posloupnost

$$(a_1, 2a_2, 3a_3, \ldots),$$

člen s indexem k je $(k+1)a_{k+1}$ (mocninnou řadu derivujeme člen po členu, podobně jako mnohočlen). Vytvořující funkce $\int_0^x a(t)\mathrm{d}t$ odpovídá posloupnosti $(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \frac{1}{4}a_3, \ldots)$, pro $k \geq 1$ je člen s indexem k roven $\frac{1}{k}a_{k-1}$.

12.2.4 Úloha. *Jaká je vytvořující funkce pro posloupnost druhých mocnin* $(1^2, 2^2, 3^2, \ldots)$*, tj. posloupnost* $(a_0, a_1, a_2, \ldots)$*, kde* $a_k = (k+1)^2$*?*

Řešení. Začneme s posloupností samých jedniček, pro niž známe vytvořující funkci: $1/(1-x)$. První derivace této funkce, $1/(1-x)^2$, dává posloupnost $(1, 2, 3, 4, \ldots)$ podle bodu G. Druhá derivace je $2/(1-x)^3$, a její posloupnost je $(2\times1, 3\times2, 4\times3, \ldots)$ opět podle G; člen s indexem k je $(k+2)(k+1) = (k+1)^2+k+1$. My ale potřebujeme $a_k = (k+1)^2$, takže odečteme ještě vytvořující funkci pro posloupnost $(1, 2, 3, \ldots)$, a dostaneme

$$a(x) = \frac{2}{(1-x)^3} - \frac{1}{(1-x)^2}.$$

□

H. Nakonec jsme si nechali nejzajímavější operaci, totiž násobení vytvořujících funkcí. Součin $a(x)b(x)$ je vytvořující funkcí posloupnosti $(c_0, c_1, c_2, \ldots)$, kde čísla c_k jsou dána vztahy

$$\begin{aligned} c_0 &= a_0b_0 \\ c_1 &= a_0b_1 + a_1b_0 \\ c_2 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &\vdots \end{aligned}$$

obecně můžeme napsat

$$c_k = \sum_{i,j\geq 0;\ i+j=k} a_i b_j. \tag{12.3}$$

To se snadno zapamatuje – členy v součinu až do k-tého jsou tytéž jako v součinu mnohočlenů $(a_0 + a_1 x \cdots + a_k x^k)(b_0 + b_1 x + \cdots + b_k x^k)$.

Násobení vytvořujících funkcí má názornou kombinatorickou interpretaci, kterou nyní vysvětlíme na příkladu (pravda dětinském), přirozený příklad přijde v oddílu 12.4. Představme si, že máme zásobu stejných kostek, a že víme, že z i kostek můžeme a_i různými způsoby postavit hrad, a z j kostek můžeme b_j různými způsoby zbudovat pyramidu. Máme-li celkem k kostek, pak $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0$ bude počet způsobů, jak postavit nějaký hrad a zároveň nějakou pyramidu (přitom pyramida a hrad nemají nikdy společné kostky). Heslovitě řečeno, vytvořující funkci pro počet uspořádaných dvojic (hrad, pyramida) získáme jako součin vytvořující funkce pro počet hradů a vytvořující funkce pro počet pyramid.

Výchozí funkce. K práci s vytvořujícími funkcemi je užitečné mít, kromě různých operací, k dispozici i zásobu funkcí, pro něž známe příslušné mocninné řady. Příklady mocninných řad, uváděné v kursu diferenciálního počtu, mohou patřit do takové zásoby; tak třeba někdy se může hodit poznatek, že $-\ln(1-x)$ je vytvořující funkcí pro posloupnost $(0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots)$. My zde uvedeme jedno snadné tvrzení, které se využívá zvlášť často:

12.2.5 Tvrzení (Zobecněná binomická věta). *Pro libovolné reálné číslo r a nezáporné celé číslo k definujme kombinační číslo $\binom{r}{k}$ předpisem*

$$\binom{r}{k} = \frac{r(r-1)(r-2)\ldots(r-k+1)}{k!}$$

(speciálně klademe $\binom{r}{0} = 1$). Potom funkce $(1+x)^r$ je vytvořující funkcí pro posloupnost $\left(\binom{r}{0}, \binom{r}{1}, \binom{r}{2}, \binom{r}{3}, \ldots\right)$ (přičemž mocninná řada $\binom{r}{0} + \binom{r}{1}x + \binom{r}{2}x^2 + \cdots$ vždy konverguje pro $|x| < 1$).

Důkaz je opět záležitostí matematické analýzy, a udělá se snadno pomocí Taylorova rozvoje. Pro r celé záporné můžeme binomický koeficient $\binom{r}{k}$ upravit na $(-1)^k\binom{-r+k-1}{k} = (-1)^k\binom{-r+k-1}{-r-1}$ (což je „obyčejný“ binomický koeficient), takže pro celé záporné mocniny $(1-x)$ speciálně dostaneme

$$\frac{1}{(1-x)^n} = \binom{n-1}{n-1} + \binom{n}{n-1}x + \binom{n+1}{n-1}x^2 + \cdots + \binom{n+k-1}{n-1}x^k + \cdots.$$

Uvedeme jednoduchý příklad na použití vytvořujících funkcí, další jsou ve cvičeních. Pokročilejší příklady následují v samostatných oddílech.

12.2.6 Úloha. *V krabici je 30 červených, 40 modrých a 50 bílých míčků, míčky téže barvy se od sebe nepoznají. Kolik je různých možností, jak vybrat z takové krabice soubor 70 míčků?*

Poučeni úvahami z oddílu 12.1 zjistíme, že hledaný počet je roven koeficientu při x^{70} v součinu

$$(1 + x + x^2 + \cdots + x^{30})(1 + x + x^2 + \cdots + x^{40})(1 + x + x^2 + \cdots + x^{50}).$$

Toto není potřeba skutečně roznásobovat, místo toho přepíšeme

$$1 + x + x^2 + \cdots + x^{30} = \frac{1 - x^{31}}{1 - x}.$$

Abychom nahlédli tuto rovnost, můžeme se rozpomenout na vztah pro součet prvních n členů geometrické řady. Kdybychom se nerozpomněli, můžeme si pomoci takto: začneme s vytvořující funkcí posloupnosti $(1, 1, 1, \ldots)$, což je $1/(1-x)$, a od ní odečteme vytvořující funkci posloupnosti

$$(\underbrace{0, 0, \ldots, 0}_{31\times}, 1, 1, \ldots),$$

což je $x^{31}/(1-x)$ podle bodu C. Výsledkem je $(1-x^{31})/(1-x)$, což je vytvořující funkce pro posloupnost

$$(\underbrace{1, 1, \ldots, 1}_{31\times}, 0, 0, \ldots).$$

Celý součin tedy upravíme na

$$\frac{1-x^{31}}{1-x}\cdot\frac{1-x^{41}}{1-x}\cdot\frac{1-x^{51}}{1-x}=\frac{1}{(1-x)^3}(1-x^{31})(1-x^{41})(1-x^{51}).$$

Nyní podle zobecněné binomické věty rozvineme činitel $(1-x)^{-3}$, a v součinu zbývajících 3 činitelů spočteme koeficienty u mocnin až do x^{70}, což je velmi snadné. Vychází

$$\left(\binom{2}{2}+\binom{3}{2}x+\binom{4}{2}x^2+\cdots\right)(1-x^{31}-x^{41}-x^{51}+\cdots),$$

kde tečky $\cdots$ zastupují mocniny vyšší než x^{70}. Koeficient u x^{70} v tomto součinu bude tedy $\binom{70+2}{2}-\binom{70+2-31}{2}-\binom{70+2-41}{2}-\binom{70+2-51}{2}=1061$.

Cvičení

1. (a) Určete koeficient při x^{15} v $(x^2+x^3+x^4+\cdots)^4$.
   (b) Určete koeficient při x^{50} v $(x^7+x^8+x^9+x^{10}+\cdots)^6$.
   (c) Určete koeficient při x^5 v $(1-2x)^{-2}$.
   (d) Určete koeficient při x^4 v $\sqrt[3]{1+x}$.
   (e) Určete koeficient při x^3 v $(2+x)^{3/2}/(1-x)$.
   (f) Určete koeficient při x^4 v $(2+3x)^5\sqrt{1-x}$.
   (g) Určete koeficient při x^3 v $(1-x+2x^2)^9$.
2. Najděte vytvořující funkce pro následující posloupnosti (nepoužívejte v jejich zápisu nekonečné řady!)
   (a) $0,0,0,0,-6,6,-6,6,-6,\ldots$
   (b) $1,0,1,0,1,0\ldots$
   (c) $1,2,1,4,1,8,\ldots$
   (d) $1,1,0,1,1,0,1,1,0,\ldots$
3. Zjistěte, jaká je pravděpodobnost, že při hodu 12 hracími kostkami hodíme dohromady přesně 30 ok.
4. Buď a_n počet uspořádaných r-tic $(i_1,\ldots,i_r)$ celých nezáporných čísel takových, že $i_1+i_2+\cdots+i_r=n$; přitom r je nějaké pevné přirozené číslo.
   (a) Napište vytvořující funkci pro posloupnost $(a_0,a_1,a_2,\ldots)$.
   (b) Najděte vzorec pro a_n. (To jsme jiným způsobem řešili v části 3.3.)

5. Řešte úlohu 12.2.4 bez použití derivace – místo toho využijte zobecněnou binomickou větu.
6. Buď a_n počet způsobů, jímž lze zaplatit částku n korun pomocí korunových, dvoukorunových a pětikorunových mincí.
   (a) Napište vytvořující funkci pro posloupnost $(a_0,a_1,\ldots)$.
   (b)* Pomocí (a) najděte vzorec pro a_n (k odvození vzorce pomůže přečtení následujícího oddílu).
7. (a) Ověřte, že je-li $a(x)$ vytvořující funkce pro posloupnost $(a_0, a_1, a_2,\ldots)$, potom $a(x)/(1-x)$ je vytvořující funkce pro posloupnost částečných součtů $(a_0, a_0+a_1, a_0+a_1+a_2,\ldots)$.
   (b) Pomocí (a) a řešení úlohy 12.2.4 vypočítejte součet $\sum_{k=1}^n k^2$.
   (c) Podobnou metodou vyjádřete součet $\sum_{k=1}^n k^3$.
   (d) Podobnou metodou – a pomocí zobecněné binomické věty – spočítejte $\sum_{k=r}^n \binom{k}{r}$ (r,n jsou daná přirozená čísla).
   (e) Pro přirozená čísla n,m vypočítejte součet $\sum_{k=0}^m (-1)^k\binom{n}{k}$.
   (f) Teď by se mohlo zdát, že uvedenou metodou můžeme spočítat téměř jaké sumy se nám zachce, ale není to tak jednoduché. Co se stane, budeme-li takto počítat $\sum_{k=1}^n \frac{1}{k}$?
8.* Dokažte vzorec pro součin mocninných řad, tj. ukažte, že jsou-li $a(x)$, $b(x)$ mocninné řady vyhovující předpokladům tvrzení 12.2.1, potom funkce $a(x)b(x)$ je též mocninná řada, a její koeficienty jsou dány formulí (12.3).
9. Buď $a(x)=a_0+a_1x+a_2x^2+\cdots$ mocninná řada s nezápornými koeficienty, tj. $a_i\geq 0$ pro každé i. Definujme její *poloměr konvergence* jako

$$\rho=\sup\{x\geq 0;\ a(x)\text{ konverguje}\}.$$

   (a)* Dokažte, že $a(x)$ konverguje pro každé $x\in[0,\rho)$, a že funkce $a(x)$ je na intervalu $[0,\rho)$ spojitá.
   (b) Najděte příklad posloupnosti $(a_0,a_1,a_2,\ldots)$, pro niž $\rho=1$ a řada $a(\rho)$ diverguje.
   (c) Najděte příklad posloupnosti $(a_0,a_1,a_2,\ldots)$, pro niž $\rho=1$ a řada $a(\rho)$ konverguje.

10. (Varovný příklad) Definujme funkci f předpisem

$$f(x) = \begin{cases} e^{-1/x^2} & \text{pro } x \neq 0 \\ 0 & \text{pro } x = 0 \end{cases}$$

(a)* Ukažte, že všechny derivace funkce f v bodě 0 existují a rovnají se 0.

(b) Odvoďte, že funkce f není v žádném okolí 0 dána mocninnou řadou.

12.3 Fibonacciho čísla a zlatý řez

Budeme vyšetřovat posloupnost $(F_0, F_1, F_2, \ldots)$ danou předpisem

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n \quad \text{pro } n = 0, 1, 2, \ldots.$$

Tuto posloupnost studoval ve 13. století ve svém spise Leonardo z Pisy zvaný Fibonacci, a je známa pod jménem Fibonacciho čísla. Prvních několik členů je

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots.$$

V matematice i v teoretické informatice se tato čísla vynořují často a v rozličných souvislostech.

Ukážeme, jak se najde formule pro n-té Fibonacciho číslo použitím vytvořujících funkcí. Nechť tedy $F(x)$ značí vytvořující funkci této posloupnosti. Hlavní myšlenka je vyjádřit vytvořující funkci posloupnosti, jejíž k-tý člen je pro $k \geq 2$ roven $F_k - F_{k-1} - F_{k-2}$. Podle vztahu definujícího Fibonacciho čísla je tato posloupnost od druhého členu počínaje nulová. Na druhé straně lze takovou vytvořující funkci zkonstruovat z $F(x)$ pomocí operací probraných v oddílu 12.2, a tím vyjde rovnice určující $F(x)$.

Konkrétně, vezmeme funkci $F(x) - xF(x) - x^2F(x)$, odpovídající posloupnosti

$$(F_0, F_1 - F_0, F_2 - F_1 - F_0, F_3 - F_2 - F_1, \ldots) = (0, 1, 0, 0, \ldots).$$

V řeči vytvořujících funkcí to znamená $(1 - x - x^2)F(x) = x$, a odtud

$$F(x) = \frac{x}{1 - x - x^2}. \tag{12.4}$$

Kdybychom teď začali zjišťovat Taylorovu řadu této funkce derivováním, příliš neuspějeme. Musíme ještě uplatnit jeden obrat, který je dobře znám v integrálním počtu pod názvem *rozklad na částečné (parciální) zlomky*. V našem případě tato metoda zaručuje, že můžeme racionální funkci na pravé straně (12.4) přepsat do tvaru

$$\frac{x}{1 - x - x^2} = \frac{A}{x - x_1} + \frac{B}{x - x_2},$$

kde x_1, x_2 jsou kořeny kvadratického mnohočlenu $1 - x - x^2$ a A, B jsou vhodné konstanty. Pro naše účely se bude lépe hodit ještě trochu pozměněné vyjádření, totiž ve tvaru

$$\frac{x}{1 - x - x^2} = \frac{a}{1 - \lambda_1 x} + \frac{b}{1 - \lambda_2 x},$$

kde $\lambda_1 = 1/x_1$, $\lambda_2 = 1/x_2$ a a, b jsou jiné vhodné konstanty (toto vyjádření se dostane z výše uvedeného dělením čitatele i jmenovatele prvního zlomku číslem $-x_1$ a druhého zlomku $-x_2$). Z tohoto vyjádření je už snadné napsat vzorec pro F_n; jak čtenář může ověřit, vychází $F_n = a\lambda_1^n + b\lambda_2^n$.

Výpočet kořenů kvadratické rovnice jakož i stanovení konstant a, b vynecháme, a uvedeme jen výslednou formuli

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right].$$

Je pozoruhodné, že tento výraz plný iracionálních čísel dává pro každé přirozené n celé číslo.

S přibližnými numerickými hodnotami konstant vypadá tento vzorec takto:

$$F_n = (0.4472135\ldots)\,[(1.6180339\ldots)^n - (-0.6180339\ldots)^n]$$

Z toho vidíme, že pro velká n se čísla F_n chovají zhruba jako $\lambda_1^n/\sqrt{5}$. Také dostáváme, že poměr F_n/F_{n+1} má limitu $1/\lambda_1 = 0.6180339\ldots$. Tento poměr byl znám a ceněn již v antice; nazývá se *zlatý řez*. Obdélník s poměrem stran rovným zlatému řezu se považoval za nejuměřenější a nejkrásnější. Oddělíme-li od takového obdélníku čtverec, zbylý obdélník má opět poměr zlatého řezu. Podobně jako s Fibonacciho čísly, se zlatým řezem se v matematice setkáme překvapivě často.

Jiné odvození: schody. Uvažme schodiště s n stupni. Kolika způsoby je lze vyjít, když každým krokem vyjdeme jeden nebo dva schody? Jinak řečeno, kolika způsoby lze zapsat číslo n jako součet jedniček a dvojek, neboli kolik řešení má rovnice

$$s_1 + s_2 + \cdots + s_k = n,$$

kde $s_i \in \{1,2\}$, $i = 1,2,\ldots,k$, $k = 0,1,2,\ldots$? Označíme-li tento počet S_n, máme $S_1 = 1$, $S_2 = 2$, a není těžké ověřit, že pro $n \geq 1$ splňují čísla S_n rekurentní vztah $S_{n+2} = S_{n+1} + S_n$ (rozmyslete si to!). Z toho je indukcí vidět, že S_n je právě Fibonacciho číslo F_{n+1}. Odvodíme teď vytvořující funkci pro posloupnost $(S_0, S_1, S_2, \ldots)$ jiným způsobem. Podle návodu z části 12.1 dostaneme, že pro dané k je počet řešení rovnice $s_1 + s_2 + \cdots + s_k = n$, kde $s_i \in \{1,2\}$, roven koeficientu při x^n v součinu $(x + x^2)^k$. My ale můžeme zvolit k libovolně (není řečeno, kolika kroky máme schody vyjít), a proto S_n bude koeficient při x^n v součtu $\sum_{k=0}^{\infty}(x + x^2)^k$, takže tento součet je vytvořující funkcí pro čísla S_n. Tuto vytvořující funkci můžeme ještě dále upravit: uvedený součet je geometrická řada s kvocientem $x + x^2$ (tedy pro dost malé x konverguje), a její součet je $1/(1 - x - x^2)$. Vytvořující funkce pro Fibonacciho čísla je tudíž $x/(1 - x - x^2)$, jak jsme předtím nahlédli jinou metodou.

Recepty. Výše uvedenou metodou můžeme najít obecný tvar posloupnosti splňující vztah

$$y_{n+k} = a_{k-1}y_{n+k-1} + a_{k-2}y_{n+k-2} + \cdots + a_1 y_{n+1} + a_0 y_n \qquad (12.5)$$

pro $n = 0,1,2,\ldots$, kde k je konstanta, $a_0, a_1, \ldots, a_{k-1}$ jsou daná čísla (reálná nebo komplexní) a $(y_0, y_1, \ldots)$ je neznámá posloupnost reálných (nebo komplexních) čísel; tak například pro Fibonacciho čísla bychom měli $k = 2$, $a_0 = a_1 = 1$. Označme nyní písmenem $\mathcal{Y}$ množinu všech posloupností $(y_0, y_1, \ldots)$ splňujících vztah (12.5). V této množině bude obecně mnoho posloupností, protože prvních k členů posloupnosti $(y_0, y_1, \ldots)$ můžeme libovolně zvolit a ostatní členy postupně vypočítat ze vztahu (12.5). V dalším popíšeme, jak vypadají všechny posloupnosti z $\mathcal{Y}$, nejprve však terminologická odbočka.

Rovnice (12.5) se učeně nazývá *homogenní lineární diferenční rovnice k-tého stupně s konstantními koeficienty*. Pokusme se vysvětlit jednotlivé části názvu:

- *Homogenní* se v názvu objevuje proto, že je-li $(y_0, y_1, \ldots) \in \mathcal{Y}$, pak také pro každé reálné číslo α je $(\alpha y_0, \alpha y_1, \ldots) \in \mathcal{Y}$. Naproti tomu nehomogenní by byla třeba rovnice $y_{n+1} = y_n + 1$.
- Slovo *lineární* zde znamená, že hodnoty y_j se v rovnici objevují vždy v první mocnině. Nelineární diferenční rovnice by byla třeba $y_{n+2} = y_{n+1}y_n$.
- Fráze *s konstantními koeficienty* vyjadřuje, že $a_0, a_1, \ldots, a_{k-1}$ jsou pevná čísla nezávisející na n. Mohli bychom totiž také uvažovat např. rovnici tvaru $y_{n+1} = (n-1)y_n$, kde koeficient na pravé straně je funkcí n.
- Konečně *diferenční rovnice* se užívá jako obecného označení pro rovnice vyjadřující n-tý člen posloupnosti pomocí několika předchozích členů[3]. Název souvisí s tzv. *diferencemi* funkce, což je pojem trochu podobný derivacím. Jak známo, derivace funkce f v bodě x je limita podílu $(f(x+h) - f(x))/h$ pro $h \to 0$; je to tedy míra přírůstku funkce f při zvětšení x o „nekonečně malou" veličinu. Diference funkce f v bodě x je naproti tomu přírůstek funkce f při zvětšení argumentu o 1, tj. veličina $f(x+1) - f(x)$. Pro dostatečně hladké funkce je diference hrubou aproximací derivace. Čtenář se možná setkal s diferenciálními rovnicemi, což jsou vztahy mezi neznámou funkcí a jejími derivacemi, jako třeba $f'(x) = f(x) + 1$. Diferenční rovnice můžeme podobně chápat jako vztah mezi neznámou funkcí a jejími diferencemi (zde se ovšem můžeme omezit na celočíselné hodnoty x, a psát hodnotu neznámé funkce y v bodě n jako y_n). Analogií k právě zmíněnému příkladu diferenciální rovnice $f'(x) = f(x) + 1$ by byla diferenční rovnice $y_{n+1} - y_n = y_n + 1$, neboli $y_{n+1} = 2y_n + 1$. Takto název diferenční rovnice vznikl, a někdy může analogie mezi diferenčními a diferenciálními rovnicemi opravdu napomoci řešení jedněch pomocí druhých.

Tolik k onomu obšírnému názvu, teď zformulujeme obecný výsledek o řešení uvažovaných diferenčních rovnic. *Charakteristickým polynomem* diferenční rovnice (12.5) nazveme polynom

$$p(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0$$

(například charakteristický polynom vztahu pro Fibonacciho čísla je $x^2 - x - 1$). Připomeňme, že každý mnohočlen k-tého stupně s koefici-

[3] Jiný používaný název je *rekurence* nebo *rekurentní relace*.

entem 1 při x^k lze zapsat jako $(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_k)$, kde $\lambda_1,\ldots,\lambda_k$ jsou (obecně komplexní) čísla, zvaná *kořeny* daného mnohočlenu.

12.3.1 Tvrzení. *Nechť $p(x)$ je charakteristický polynom homogenní lineární diferenční rovnice (12.5).*

(i) (Jednoduché kořeny) *Předpokládejme, že $p(x)$ má k* navzájem různých *kořenů $\lambda_1,\ldots,\lambda_k$. Potom pro libovolnou posloupnost $y=(y_0,y_1,\ldots)\in\mathcal{Y}$ splňující (12.5) existují komplexní konstanty C_1, C_2, …, C_k takové, že pro každé n je*

$$y_n = C_1\lambda_1^n + C_2\lambda_2^n + \cdots + C_k\lambda_k^n.$$

(ii) (Obecný případ) *Nechť $\lambda_1,\ldots,\lambda_q$ jsou navzájem různá komplexní čísla a $k_1,\ldots,k_q$ přirozená čísla, $k_1+k_2+\cdots+k_q=k$, taková, že*

$$p(x) = (x-\lambda_1)^{k_1}(x-\lambda_2)^{k_2}\ldots(x-\lambda_q)^{k_q}.$$

Potom pro libovolnou posloupnost $y=(y_0,y_1,\ldots)\in\mathcal{Y}$ splňující (12.5) existují komplexní konstanty C_{ij} ($i=1,2,\ldots,q$, $j=0,1,\ldots,k_i-1$) takové, že pro každé n je

$$y_n = \sum_{i=1}^{q}\sum_{j=0}^{k_i-1} C_{ij}\binom{n}{j}\lambda_i^n.$$

Jak podle tohoto řešit diferenční rovnice? Uveďme dva stručné příklady. U rovnice $y_{n+2}=5y_{n+1}-6y_n$ je charakteristický polynom $p(x)$ roven $x^2-5x+6=(x-2)(x-3)$. Jeho kořeny jsou tedy $\lambda_1=2$, $\lambda_2=3$, a tvrzení 12.3.1 říká, že řešení máme hledat ve tvaru $C_1 2^n+C_2 3^n$. Máme-li předepsány počáteční podmínky, např. $y_0=2$, $y_1=5$, musíme dopočítat konstanty C_1, C_2 tak, aby uvedený vzorec dával tyto požadované hodnoty pro $n=0,1$; v našem případě bychom tudíž volili $C_1=C_2=1$.

A ještě dosti umělý příklad na násobné kořeny: rovnice

$$y_{n+5} = 8y_{n+4}+25y_{n+3}-38y_{n+2}+28y_{n+1}-8y_n$$

má charakteristický polynom[4] $p(x)=(x-1)^2(x-2)^3$, a tvrzení 12.3.1

[4]Samozřejmě autoři vybrali koeficienty tak, aby charakteristický polynom vyšel takhle pěkně. Uvedený návod na řešení (jakož i metoda pomocí vytvořujících funkcí) ponechává stranou otázku, jak v obecnosti najít kořeny. V příkladech z různých sbírek úloh a učebnic mají rekurence stupeň 1 nebo 2 nebo bývají koeficienty zvoleny tak, aby kořeny vyšly pěkně.

praví, že řešení bude tvaru

$$y_n = C_{10} + C_{11}n + C_{20}2^n + C_{21}n2^n + C_{22}\binom{n}{2}2^n.$$

Hodnoty konstant by se opět dopočítaly podle hodnot prvních 5 členů posloupnosti $(y_0,y_1,\ldots)$.

Právě uvedený postup řešení rekurence (12.5) se najde téměř ve všech učebnicích, a o vytvořujících funkcích zpravidla nepadne zmínka ani v důkaze tvrzení 12.3.1 – skutečně, toto tvrzení se dá dokázat dosti elegantně pomocí lineární algebry (naznačíme ve cvičeních), a pakliže odněkud víme, že řešení se má hledat ve zmíněném tvaru, vytvořující funkce už nepotřebujeme. Postup, který jsme uvedli pro Fibonacciho čísla, však ukazuje, jak správný tvar řešení opravdu odvodit. Navíc je to pěkný příklad na práci s vytvořujícími funkcemi, a podobný přístup se někdy dá s úspěchem použít i pro diferenční rovnice jiného tvaru, kde už obecný návod k řešení znám není (nebo je pracné ho v literatuře najít).

Cvičení

1.* Zjistěte, kolik existuje n-členných posloupností nul a jedniček, v nichž se nikde nevyskytují 2 nuly po sobě.

2. Vyjádřete obecný člen posloupností určených následovně (zobecněte postup použitý pro Fibonacciho čísla, příp. použijte výše uvedený obecný návod na řešení homogenních lineárních diferenčních rovnic s konstantními koeficienty):

   (a) $a_0=2,\ a_1=3,\ a_{n+2}=3a_n-2a_{n+1}\quad(n=0,1,2,\ldots)$

   (b) $a_0=0,\ a_1=1,\ a_{n+2}=2a_{n+1}-4a_n\quad(n=0,1,2,\ldots)$

   (c) $a_0=1, a_{n+1}=2a_n+3\quad(n=0,1,2,\ldots)$

3. V posloupnosti $(a_0,a_1,a_2,\ldots)$ je vždy následující člen aritmetickým průměrem předchozích dvou členů. Určete limitu $\lim_{n\to\infty}a_n$ (jako funkci a_0,a_1).

4. Řešte rekurenci $a_{n+2}=\sqrt{a_{n+1}a_n}$ s počátečními podmínkami $a_0=2$, $a_1=8$, najděte $\lim_{n\to\infty}a_n$.

5. (a) Řešte rekurenci $a_n = a_{n-1} + a_{n-2} + \ldots + a_1 + a_0$ s počáteční podmínkou $a_0 = 1$.

   (b) * Řešte rekurenci $a_n = a_{n-1} + a_{n-3} + a_{n-4} + a_{n-5} + \cdots + a_1 + a_0$ $(n \geq 3)$, pro $a_0 = a_1 = a_2 = 1$.

6.* Kolik existuje n-členných posloupností, tvořených písmeny a, b, c, d, v nichž a nikdy nesousedí s b?

7. Dokažte tvrzení 12.3.1 zobecněním postupu předvedeného pro Fibonacciho čísla (využijte obecný tvar věty o rozkladu racionální funkce na částečné zlomky z analýzy).

8. Dokažte tvrzení 12.3.1 přímo použitím lineární algebry, podle následujících bodů.

   (a) Ověřte, že množina $\mathcal{Y}$ všech řešení tvoří vektorový prostor vzhledem ke sčítání posloupností po složkách a násobení komplexním číslem po složkách.

   (b) Ukažte, že dimenze $\mathcal{Y}$ je rovna k.

   (c)* Ukažte, že v situaci části (i) tvrzení 12.3.1 posloupnosti $(\lambda_i^0, \lambda_i^1, \lambda_i^2, \ldots)$ pro $i = 1, 2, \ldots, k$ náleží do $\mathcal{Y}$, a jsou lineárně nezávislé, tj. podle (b) tvoří bázi vektorového prostoru $\mathcal{Y}$; tím dokážete část (i).

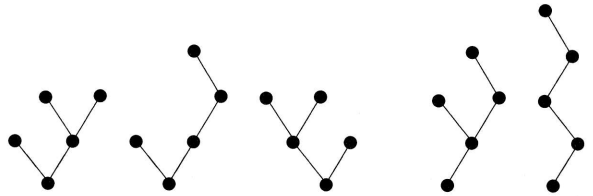
   (d) Ověřte, že v situaci části (ii) tvrzení 12.3.1 je každá z posloupností $(\binom{n}{j}\lambda_i^n)_{n=0}^{\infty}$ prvkem množiny řešení $\mathcal{Y}$.

   (e) ** Dokažte, že posloupnosti z předchozího bodu (d) jsou lineárně nezávislé v $\mathcal{Y}$, tj. tvoří bázi.

12.4 Binární stromy

Budeme uvažovat tzv. binární stromy, takové, jaké se často používají v datových strukturách. Na obr. 12.1 je nakresleno několik různých binárních stromů s 5 vrcholy. Pro naše účely můžeme binární strom definovat krátce takto: binární strom je buď prázdný (nemá žádný vrchol), nebo sestává z jednoho význačného vrcholu (zvaného *kořen*) plus z uspořádané dvojice binárních stromů[5] (levého a pravého podstromu).

[5] Toto je vlastně definice indukcí; nejdříve řekneme, co je binární strom s 0 vrcholy (prázdný strom), a potom definujeme binární strom s n vrcholy pomocí již definovaných binárních stromů s menším počtem vrcholů. Tím, že připouštíme prázdný strom, se vyhneme popisu různých speciálních případů, jako když kořen má jen levý či jen pravý podstrom.



Obrázek 12.1: Několik různých binárních stromů na 5 vrcholech.

Nechť b_n označuje počet binárních stromů s n vrcholy. Naším úkolem bude najít vzorec pro b_n. Probráním malých případů zjistíme $b_0 = 1$, $b_1 = 1$, $b_2 = 2$, $b_3 = 5$; to může sloužit jako kontrola správnosti výsledků v dalším.

Jako obvykle, $b(x) = b_0 + b_1 x + b_2 x^2 + \cdots$ bude příslušná vytvořující funkce. Pro $n \geq 1$, počet binárních stromů s n vrcholy je podle definice roven počtu uspořádaných dvojic tvaru (B, B'), kde B, B' jsou binární stromy s dohromady $n-1$ vrcholy, tj. má-li B k vrcholů, má B' $n-k-1$ vrcholů. Počet takových uspořádaných dvojic je

$$b_n = b_0 b_{n-1} + b_1 b_{n-2} + \cdots + b_{n-1} b_0. \tag{12.6}$$

To je ale podle definice násobení vytvořujících funkcí přesně koeficient při x^{n-1} v součinu $b(x).b(x) = b(x)^2$ (to je příklad na kombinatorický význam násobení vytvořujících funkcí, slíbený v oddílu 12.2), a tedy koeficient při x^n ve funkci $xb(x)^2$. Tím pádem je $xb(x)^2$ vytvořující funkce pro tutéž posloupnost jako funkce $b(x)$, až na to, že funkce $b(x)$ má absolutní člen b_0 rovný 1, zatímco ve funkci $xb(x)^2$ je absolutní člen 0 (to proto, že vzorec (12.6) je správný jen pro $n \geq 1$). Můžeme tudíž napsat následující rovnost mezi vytvořujícími funkcemi:

$$b(x) = 1 + xb(x)^2.$$

Na to se můžeme dívat jako na kvadratickou rovnici s neznámou $b(x)$ (přitom x si představujeme jako libovolné, ale pevné číslo). Podle

dobře známého vzorečku jsou její kořeny

$$b(x)_{1,2} = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

To vypadá, jako by byla dvě možná řešení, my však víme, že posloupnost $(b_0, b_1, b_2, \ldots)$ a tedy i její vytvořující funkce jsou určeny jednoznačně! Podíváme-li se však na řešení se znaménkem „+“, zjistíme, že pro $x \to 0+$ má limitu ∞, zatímco vytvořující funkce pro naši posloupnost musí mít limitu $b_0 = 1$. Toto řešení tedy vyloučíme. Řešení se znaménkem „−“ se ukazuje být hledané vyjádření vytvořující funkce, zbývá určit jeho koeficienty.

K tomu využijeme zobecněné binomické věty 12.2.5. Podle ní máme rozvoj

$$\sqrt{1-4x} = \sum_{k=0}^{\infty} (-4)^k \binom{1/2}{k} x^k.$$

Koeficient u x^0 je 1, takže $1 - \sqrt{1-4x}$ má po rozvinutí v řadu nulový absolutní člen, a tak můžeme tuto řadu vydělit $2x$ (posunutím o 1 člen doleva a dělením 2). Z toho dostáváme pro $n \geq 1$

$$b_n = -\frac{1}{2}(-4)^{n+1} \binom{1/2}{n+1}. \tag{12.7}$$

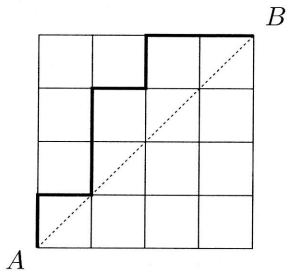
Dalšími úpravami (které ponecháváme do cvičení) lze získat pěknější tvar

$$b_n = \frac{1}{n+1} \binom{2n}{n}.$$

Takto definovaná čísla b_n jsou v literatuře známa pod jménem *Catalanova čísla*. Kromě toho, že udávají počet binárních stromů, mají i několik dalších kombinatorických významů.

Cvičení

1. Upravte pravou stranu rovnice (12.7) na tvar uvedený pod touto rovnicí.
2. Uvažme šachovnici $n \times n$ čtverečků:



Uvažujme cesty z bodu A do bodu B, které jdou po hranách čtverečků šachovnice a jsou nejkratší (tj. používají $2n$ hran).

(a) Kolik je všech takových cest?

(b)* Ukažte, že cest, které nikdy nejdou pod diagonálu šachovnice (tj. přímku AB) je právě b_n, tj. Catalanovo číslo. Jedna taková cesta je na obrázku vyznačena.

(c)** Dokažte vzorec $b_n = \frac{1}{n+1}\binom{2n}{n}$ elementárně, bez použití vytvořujících funkcí.

3. Uvažme součin 4 čísel, $abcd$. Ten lze „uzávorkovat“ 5 způsoby: $((ab)c)d$, $(a(bc))d$, $(ab)(cd)$, $a((bc)d)$ a $a(b(cd))$. Dokažte, že počet uzávorkování součinu n čísel je právě Catalanovo číslo b_{n-1}.
4. Ve frontě na lístky po 50 Kč kus je $2n$ lidí, každý kupuje 1 lístek, přitom n z nich má padesátikorunu a n stokorunu. Na začátku nemá pokladní žádné peníze.

   (a) Kolik je seřazení lidí do fronty, pro něž pokladní bude mít pro každého majitele 100 Kč bankovky nazpět padesátikorunu?

   (b) Jaká je pravděpodobnost toho, že při náhodném seřazení fronty bude mít pokladní pro každého nazpět?
5. *Uvažme pravidelný n-úhelník. Rozdělme jej na trojúhelníky zakreslením $n-3$ neprotínajících se úhlopříček. Ukažte, že takových triangulací existuje právě b_{n-2}.
6. V tomto a několika dalších cvičeních budeme používat pojmy *kořenový strom* a *pěstovaný strom* z části 5.2 (oba jsou stromy s kořenem, u pěstovaných stromů záleží na pořadí synů každého vrcholu, u kořenových stromů nikoli).

   (a) Označme c_n počet (navzájem neisomorfních) pěstovaných stromů s n vrcholy, kde každý vrchol je buď koncový, nebo má právě 2 syny

(příklady dvou takových neisomorfních stromů jsou první a třetí strom na obr. 12.1). Ukažte, že příslušná vytvořující funkce $c(x)$ splňuje rovnici $c(x) = x + xc(x)^2$, a vypočítejte výraz pro c_n.

(b)* Uměli byste odvodit hodnotu c_n ze znalosti b_n (počtu binárních stromů vyšetřovaných textu této části)?

(c) Najděte d_n, počet neisomorfních pěstovaných vrcholů s n vrcholy, kde každý nekoncový vrchol má jednoho nebo dva syny.

7. Nechť t_n značí počet neisomorfních pěstovaných stromů s n vrcholy.

(a) Ukažte, že příslušná vytvořující funkce $t(x)$ splňuje rovnici

$$t(x) = \frac{x}{1 - t(x)},$$

a vypočítejte výraz pro t_n.

(b)* Uměli byste odvodit hodnotu t_n ze znalosti b_n (počtu binárních stromů vyšetřovaných textu této části)?

8. Řekneme, že pěstovaný strom je *starý*, nemá-li žádný *mladý vrchol*, přičemž mladý vrchol je koncový vrchol přímo připojený ke kořeni. Nechť s_n je počet starých pěstovaných stromů s n vrcholy. Vyjádřete vytvořující funkci $s(x)$ pomocí vytvořující funkce $t(x)$ pro pěstované stromy z předchozího cvičení.

9.* Teď uvažme kořenové stromy, kde každý nekoncový vrchol má právě 2 syny (u kořenového stromu nezáleží na pořadí synů vrcholu, tj. první a třetí strom na obr. 12.1 budou nyní isomorfní). Nechť $\bar{b}(x)$ je příslušná vytvořující funkce. Odvoďte rovnici

$$\bar{b}(x) = 1 + \frac{x}{2}\left(\bar{b}(x)^2 + \bar{b}(x^2)\right).$$

10. Uvažme *alkanové radikály*, což jsou acyklické uhlovodíky, kde každý atom uhlíku má 4 jednoduché vazby, až na jeden, který má 3 jednoduché vazby a jednu „volnou" vazbu. Takové molekuly si můžeme představovat jako kořenové stromy (vrcholy odpovídají atomům uhlíku), kde každý nekoncový vrchol má 1,2 nebo 3 syny (přičemž pořadí synů jednoho vrcholu není důležité). Buď r_n počet takových stromů s n vrcholy (neboli alkanových radikálů s n uhlíky), a $r(x)$ příslušná vytvořující funkce.

(a)** Odvoďte rovnici $r(x) = 1 + \frac{x}{6}\left(r(x)^3 + 3r(x^2)r(x) + 2r(x^3)\right)$.

(b) Vypočítejte pomocí této rovnice tabulky r_n pro malá n. Srovnejte s hodnotami uvedenými v nějaké encyklopedii chemie.

Více o metodách počítání různých typů grafů, stromů atd. se najde např. v knize [14].

12.5 O házení kostkou

12.5.1 Úloha. *Budeme-li házet kostkou tak dlouho, až poprvé padne šestka, kolik hodů v průměru potřebujeme*[6]*?*

Pravděpodobnost, že v prvním hodu padne šestka, je $p = \frac{1}{6}$. Pravděpodobnost, že v prvním hodu šestka nepadne a v druhém padne, je $(1-p)p$, a obecně pravděpodobnost toho, že šestka padne poprvé v i-tém hodu je rovna číslu $q_i = (1-p)^{i-1}p$. Průměrný počet hodů (neboli střední hodnota počtu hodů) bude pak

$$S = \sum_{i=0}^{\infty} iq_i = \sum_{i=1}^{\infty} i(1-p)^{i-1}p\,.$$

Zavedeme vytvořující funkci $q(x) = q_1x + q_2x^2 + \cdots$. Derivujeme-li tuto řadu člen po členu, dostáváme $q'(x) = q_1 + 2q_2x + 3q_3x^2 + \cdots$, a hledaný průměrný počet hodů pak bude roven hodnotě $q'(1)$.

Po jistém úsilí spočítáme, že naše vytvořující funkce má vyjádření

$$q(x) = \frac{p}{1-p} \cdot \frac{1}{1-(1-p)x} - \frac{p}{1-p}.$$

Po malém cvičení v derivování vyjde $q'(x) = p/(1-(1-p)x)^2$, neboli $S = q'(1) = \frac{1}{p}$. Pro $p = \frac{1}{6}$ je tedy průměrný počet hodů 6.

Zde je způsob usuzování, který dává ještě mnohem kratší řešení: V každém případě hodíme kostkou aspoň jednou. S pravděpodobností $1-p$ nehodíme napoprvé šestku, a v tomto případě nás čeká v průměru ještě S dalších hodů (kostka nemá paměť). Odtud

$$S = 1 + (1-p)S,$$

a $S = \frac{1}{p}$ vyjde okamžitě.

[6] Po úvaze jsme dali přednost této formulaci před jinou, která se nabízí, totiž s tzv. ruskou ruletou.

Cvičení

1. Podobným postupem jako v textu této části najděte

   (a) průměrný počet líců, které padnou při n hodech mincí (se stejnou pravděpodobností rubu i líce),

   (b) průměrný počet šestek, které padnou při n hodech kostkou,

   (c)* průměrnou hodnotu výrazu $(i-6)^2$, kde i je počet hodů do první šestky (to je jakási míra „typické odchylky" od průměrného počtu hodů, tj. od 6).

12.6 Náhodná procházka

Představme si číselnou osu nakreslenou v rovině, na níž jsou celá čísla vyznačena kroužky. Po těchto kroužcích se bude pohybovat figurka podle následujících pravidel náhodné procházky:

- Na začátku (před prvním tahem) stojí figurka v čísle 1.
- V každém tahu se pohne z čísla, kde právě stojí, buď o 2 čísla doprava nebo o 1 číslo doleva. Jedna z těchto možností se vždy zvolí náhodně, a obě možnosti mají stejnou pravděpodobnost (tj. jako bychom hodili mincí a rozhodli se podle výsledku hlava/orel).

12.6.1 Úloha. *Jaká je pravděpodobnost, že figurka vůbec někdy dospěje do čísla 0?*

Nejdříve je potřeba vyjasnit, co se vůbec takovou pravděpodobností míní. Je celkem zřejmé, jak definovat pravděpodobnost, že se figurka aspoň jednou octne v 0 během prvních řekněme 7 tahů (označme ji P_7): Prvních 7 tahů náhodné procházky má 2^7 různých možných průběhů, protože v každém tahu se rozhodne mezi dvěma možnostmi, a tato rozhodnutí lze libovolně zkombinovat. Podle pravidla náhodné procházky v naší úloze jsou všechny tyto průběhy stejně pravděpodobné. Výše zmíněná pravděpodobnost P_7 bude potom rovna počtu takových průběhů, které projdou 0 (čtenář si může ověřit, že je jich 75), dělenému celkovým počtem průběhů, tj. 2^7.

Hledanou pravděpodobnost P v naší úloze potom můžeme definovat jako limitu $P = \lim_{i\to\infty} P_i$, kde definice P_i byla objasněna výše pro $i = 7$ (tato limita určitě existuje, protože zřejmě $P_1 \le P_2 \le \ldots$).

Nechť a_i značí počet průběhů prvních i tahů náhodné procházky takových, že figurka dorazí do 0 po i-tém tahu, a zároveň nikdy předtím (tj. před 1., 2.,..., i-tým tahem) v 0 nebyla. Platí tedy

$$P = \sum_{i=1}^{\infty} \frac{a_i}{2^i}.$$

Zavedeme-li vytvořující funkci $a(x) = a_1x + a_2x^2 + a_3x^3 + \cdots$, máme $P = a(\frac{1}{2})$.

Pro řešení úlohy bude užitečné podívat se i na procházky, které začínají v jiných číslech než 1 (ale pokračují podle stejného pravidla). Jaký bude například počet procházek začínajících v čísle 2, které dospějí poprvé do 0 v i-tém tahu (označme jej třeba b_i)? Aby taková procházka došla do 0, musí nejprve po nějakém j-tém tahu, $1 \le j < i$, poprvé dosáhnout čísla 1, a potom v dalších $i-j$ tazích poprvé vstoupit do 0. Pro dosažení čísla 1 poprvé v j-tém kroku je a_j možností, (jde totiž pouze o „posunutou kopii" procházky, která by začala v 1 a po j tazích došla do 0). Je-li figurka v j-tém kroku v 1, má ještě a_{i-j} možností dosažení 0 po $i-j$ dalších tazích. Celkem tedy dostaneme[7]

$$b_i = \sum_{j=1}^{i-1} a_j a_{i-j},$$

v řeči vytvořujících funkcí to znamená $b(x) = a(x)^2$.

Analogicky, c_i bude počet procházek začínajících v čísle 3, jež poprvé dorazí do 0 po i tazích. Podobně jako v předchozím nahlédneme že $c(x) = a(x)b(x) = a(x)^3$.

Zkoumejme teď procházky začínající v 1 z trochu jiného pohledu. Při prvním tahu můžeme rovnou dojít do 0 (což dává $a_1 = 1$), nebo se octneme v čísle 3, a potom máme c_{i-1} možností, jak poprvé vstoupit

[7] Všimněte si, že jsme podstatně využili toho, že doleva se chodí vždy jen o 1, takže se nelze dostat z 2 do 0 a přitom přeskočit 1.

do 0 po dalších $i-1$ tazích. Pro $i>1$ tedy $a_i = c_{i-1}$. Převedeno na vztah mezi vytvořujícími funkcemi

$$a(x) = x + xc(x) = x + xa(x)^3. \tag{12.8}$$

Speciálně pro $x = \frac{1}{2}$ odtud dostaneme pro $P = a(\frac{1}{2})$ rovnici

$$P = \frac{1}{2} + \frac{1}{2}P^3.$$

Ta má tři řešení, $1, (\sqrt{5}-1)/2$ a $-(\sqrt{5}+1)/2$. Záporné řešení můžeme vyloučit ihned, a ani 1 nemůže být odpovědí v naší úloze (řada pro $a(x)$ má nezáporné koeficienty a konverguje pro $x = \frac{1}{2}$, tedy definuje spojitou rostoucí funkci na intervalu $[0, \frac{1}{2}]$, a proto hodnota $a(\frac{1}{2})$ je nejmenší kladný kořen naší rovnice – rozmyslete si a případně nakreslete obrázek). Zbývá tedy $P = (\sqrt{5}-1)/2 = 0,618033988\ldots$ a jedině toto číslo může být hledaná hodnota P (zase zlatý řez!).

Z rovnice (12.8) bychom v principu mohli spočítat i funkci $a(x)$ a potom se snažit vyjádřit čísla a_i třeba pomocí jejího Taylorova rozvoje (což je ale dost pracné). Půvab výše uvedeného řešení je v tom, že jsme nic takového dělat nepotřebovali.

Cvičení

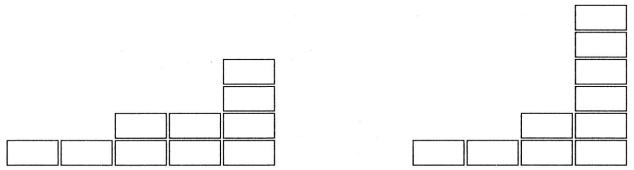
1. Uvažme náhodnou procházku začínající v 0, při níž se postupuje o 1 číslo doleva nebo o 1 číslo doprava, každá volba má pravděpodobnost $\frac{1}{2}$.
   (a)* Dokažte, že s pravděpodobností 1 se někdy vrátíme do 0.
   (b) Dokažte, že každé číslo k někdy navštívíme, s pravděpodobností 1.

12.7 Rozklady

Kolika způsoby můžeme napsat přirozené číslo n jako součet několika přirozených čísel? Odpověď není těžká, pokud počítáme *uspořádané rozklady*, což znamená, že zápisy $3 = 2+1$ a $3 = 1+2$ považujeme za dva různé rozklady čísla 3 (cvičení 1). Mnohem těžší a zajímavější otázku dostaneme, považujeme-li za stejné dva rozklady, jež se

liší pouze pořadím sčítanců (v tomto případě budeme v tomto oddílu mluvit prostě o *rozkladech čísla* n). Například pro $n = 5$ jsou všechny možné rozklady $5 = 1+1+1+1+1$, $5 = 1+1+1+2$, $5 = 1+2+2$, $5 = 1+1+3$, $5 = 2+3$, $5 = 1+4$ a $5 = 5$. Označme p_n počet rozkladů čísla n v tomto smyslu.

Abychom učinili zápis rozkladu jednoznačným, můžeme například požadovat, aby sčítance byly seřazeny vzestupně, jako jsme je psali v seznamu všech rozkladů čísla 5. Takže jiná formulace otázky o počtu rozkladů je: Kolika způsoby můžeme postavit z n cihel „neklesající zeď" jako na následujícím obrázku (který odpovídá rozkladům $10 = 1+1+2+2+4$ a $10 = 1+1+2+6$)?



(Takový obrázek se nazývá *Ferrersův diagram* daného rozkladu.)

Definice p_n vypadá jednoduše, takže čtenáře, ze středoškolských příkladů třeba zvyklého, že na všechno je vzoreček, může překvapit, že pro p_n žádný jednoduchý vzorec, něco jako třeba binomický koeficient, není. Problém odhadu čísla p_n se studoval v teorii čísel, a v roce 1918 ho s neuvěřitelnou přesností vyřešili Hardy a Ramanujan. (Tuto historii popisuje Littlewood v knížečce [20], již můžeme doporučit jako skvělé čtení o matematice.) Dokonce objevili přesný (ale komplikovaný) vzorec pro p_n. Porozumění tomuto výsledku, nemluvě o jeho důkazu, vyžaduje poměrně hluboké znalosti z teorie čísel (viz například Andrews [2]). Tady budeme mnohem skromnější: poměrně dobré asymptotické odhady pro p_n se dají dokázat jednoduše, i když rafinovaně, pomocí vytvořujících funkcí, a to zde předvedeme.

Už víme, jak vyjádřit počet řešení rovnice

$$i_1 + i_2 + \cdots + i_k = n,$$

s hodnotami každé proměnné i_j ležícími v nějaké předepsané množině, jako koeficient u x^n ve vhodném výrazu. Pro náš problém ale nezáleží na pořadí těch i_j, takže není vidět, jak to uvést do souvislosti s (neuspořádanými) rozklady čísla n. Trik je považovat i_j za *příspě-*

vek sčítanců rovných j v rozkladu n, nebo jinak řečeno, počet cihel ve sloupečcích výšky přesně j v naší neklesající zdi. Tudíž rozklady čísla n jsou ve vzájemně jednoznačné korespondenci s řešeními rovnice

$$i_1 + i_2 + \cdots + i_n = n,$$

kde

$$i_1 \in \{0,1,2,3,\ldots\},\quad i_2 \in \{0,2,4,6,\ldots\},\ \ldots,\quad i_j \in \{0,j,2j,3j,\ldots\}.$$

Třeba rozklad $5 = 1+2+2$ odpovídá řešení $i_1 = 1$, $i_2 = 4$, $i_3 = i_4 = i_5 = 0$.

Další krok je standardní. Z právě odvozené nové formulace hned dostáváme, že p_n je koeficient x^n v součinu

$$P_n(x) = (1+x+x^2+\cdots)(1+x^2+x^4+x^6+\cdots)\ldots(1+x^n+x^{2n}+\cdots)$$
$$= \prod_{k=1}^{n} \frac{1}{1-x^k}\,.$$

Tento konečný součin *není* vytvořující funkcí posloupnosti $(p_n)_{n=0}^{\infty}$. Abychom z něj opravdovou vytvořující funkci, která má u x^n koeficient p_n pro všechna n zároveň, museli bychom užít nekonečný součin

$$P(x) = \prod_{k=1}^{\infty} \frac{1}{1-x^k}\,.$$

Ale nekonečný součin by možná někoho mohl vystrašit, takže radši zůstaneme u konečného součinu $P_n(x)$.

Teď budeme p_n odhadovat shora metodou již předvedenou v důkazu věty 3.5.1 (odhad binomických koeficientů). Pro všechna $x \in (0,1)$ máme

$$p_n \le \frac{1}{x^n} P_n(x) = \frac{1}{x^n} \prod_{k=1}^{n} \frac{1}{1-x^k}.$$

Chceme x zvolit tak, aby pravá strana byla co nejmenší. Šikovný způsob odhadu $P_n(x)$ je další mazanou částí důkazu. Máme-li pracovat se součinem, často se vyplatí vše zlogaritmovat. V našem případě vychází

$$\ln p_n \le \ln\left(\frac{1}{x^n} P_n(x)\right) = -n\ln x - \sum_{k=1}^{n} \ln(1-x^k).$$

Připomeneme si mocninnou řadu pro logaritmus:

$$-\ln(1-y) = \frac{y}{1} + \frac{y^2}{2} + \frac{y^3}{3} + \frac{y^4}{4} + \cdots$$

pro všechna $y \in (-1,1)$. Tudíž můžeme přepsat

$$-\sum_{k=1}^{n} \ln(1-x^k) = \sum_{k=1}^{n}\sum_{j=1}^{\infty} \frac{x^{kj}}{j} = \sum_{j=1}^{\infty} \frac{1}{j} \sum_{k=1}^{n} x^{jk}$$
$$\le \sum_{j=1}^{\infty} \frac{1}{j} \sum_{k=1}^{\infty} x^{jk} = \sum_{j=1}^{\infty} \frac{1}{j} \frac{x^j}{1-x^j}.$$

Nyní se trochu neočekávaně použije vzorec pro součet geometrické řady „v obráceném směru“:

$$1 - x^j = (1-x)(1+x+x^2+\cdots+x^{j-1}) \ge (1-x)jx^{j-1}$$

(připomeňme, že $0 < x < 1$), a tedy

$$\sum_{j=1}^{\infty} \frac{1}{j} \frac{x^j}{1-x^j} \le \sum_{j=1}^{\infty} \frac{1}{j} \frac{x^j}{(1-x)jx^{j-1}} = \frac{x}{1-x} \sum_{j=1}^{\infty} \frac{1}{j^2}\,.$$

Teď potřebujeme následující podivuhodný

12.7.1 Fakt. $\displaystyle\sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}.$

Elementární důkaz této rovnosti je zařazen na konci tohoto oddílu jako matematický dezert. Nyní pokračujeme v odhadech $\ln p_n$ a dostáváme

$$\ln p_n \le -n\ln x + \frac{\pi^2}{6} \frac{x}{1-x}\,.$$

Pro následující výpočty je pohodlné zavést pomocnou proměnnou $u = x/(1-x)$ (takže u může být kterékoli číslo z $[0,\infty)$). Obráceně máme $x = u/(1+u)$. Uděláme tuto substituci a použijeme nerovnost

$\ln(1+\frac{1}{u}) \le \frac{1}{u}$ (která se snadno odvodí z faktu 3.4.3), a tím se dopracujeme k nerovnosti

$$\ln p_n < n \ln\left(1+\frac{1}{u}\right) + \frac{\pi^2}{6}u \le \frac{n}{u} + \frac{\pi^2}{6}u.$$

Do tohoto výrazu dosadíme $u = \sqrt{6n}/\pi$, čímž vyjde $\ln p_n \le \pi\sqrt{\frac{2}{3}n}$. (Proč je $u = \sqrt{6n}/\pi$ ta pravá hodnota? Trocha počítání s derivacemi ukazuje, že tato hodnota u minimalizuje odvozený horní odhad pro $\ln p_n$.) Takže jsme dokázali toto:

12.7.2 Věta. *Pro všechna $n \ge 1$ platí*

$$p_n < e^{\pi\sqrt{\frac{2}{3}n}} = e^{(2.5650\ldots)\sqrt{n}}.$$

Dolní odhad. Jak dobrý je právě odvozený horní odhad? Z výsledků Hardyho a Ramanujana vyplývá, že $p_n \sim \frac{1}{4\sqrt{3}\,n} e^{\pi\sqrt{\frac{2}{3}n}}$, tudíž jsme odvodili velmi dobrý odhad, dokonce se správnou konstantou v exponentu. Ale co kdybychom byli zrovna v divočině (v širokém významu, tj. odříznuti od matematických knihoven a od internetu), a chtěli vědět, jestli odhad ve větě 12.7.2 je přibližně správný? Ukážeme ještě krátké odvození dolního odhadu, který je samozřejmě mnohem slabší než zmíněné výsledky Hardyho a Ramanujana, ale aspoň je z něj jasné, že náš horní odhad není moc daleko od pravdy.

Začneme s výsledkem cvičení 1, v němž se řešitelé vyzývají k odvození vzorce $\binom{n-1}{k-1}$ pro počet uspořádaných rozkladů čísla n na k sčítanců. Poněvadž každý neuspořádaný rozklad s k sčítanci odpovídá maximálně $k!$ uspořádaným rozkladům, platí

$$p_n \ge \frac{\binom{n-1}{k-1}}{k!} \ge \frac{(n-1)(n-2)\ldots(n-k+1)}{(k!)^2}$$

pro libovolné $k \in \{1,2,\ldots,n\}$. Jaké k vzít, aby tento dolní odhad byl co nejsilnější? Zvětšíme-li k o 1, jmenovatel se vynásobí číslem $(k+1)^2$ a čitatel se vynásobí číslem $n-k$. Takže pro $(k+1)^2 < n-k$ je $k+1$ lepší než k, a abychom dostali co nejlepší k, $(k+1)^2$ by mělo být přibližně rovno $n-k$. Abychom si počítání příliš nekomplikovali, zvolíme $k = \lfloor\sqrt{n}\rfloor$.

Správná intuice potom říká, že $(n-1)(n-2)\cdots(n-k+1)$ se chová zhruba jako $n^{\sqrt{n}}$. Tuto intuici je ovšem nutné podložit korektním výpočtem:

$$(n-1)(n-2)\ldots(n-k+1) \ge (n-k)^{k-1} = n^{k-1}\left(1-\frac{k}{n}\right)^{k-1},$$

a protože $\frac{k}{n} = \lfloor\sqrt{n}\rfloor/n \le 1/\lfloor\sqrt{n}\rfloor = \frac{1}{k}$ a $(1-\frac{1}{k})^{k-1} > e^{-1}$, dostáváme

$$n^{k-1}\left(1-\frac{k}{n}\right)^{k-1} \ge n^{k-1}\left(1-\frac{1}{k}\right)^{k-1} \ge \frac{n^k}{en}.$$

Podle věty 3.4.4 odhadneme $k! \le ek(k/e)^k$, a odtud

$$p_n \ge \left(\frac{n}{k^2}\right)^k \frac{e^{2k-3}}{nk^2} \ge \frac{e^{2k-3}}{n^2} \ge \frac{1}{e^5 n^2} e^{2\sqrt{n}}.$$

Pro velká n je n^2 zanedbatelné proti $e^{\sqrt{n}}$, takže $n^{-2}e^{2\sqrt{n}} = \Omega(e^{\sqrt{n}})$. Ukázali jsme, že pro všechna dostatečně velká n leží číslo p_n mezi $e^{c_1\sqrt{n}}$ a $e^{c_2\sqrt{n}}$ pro vhodné konstanty $c_2 > c_1 > 0$. Taková informace už dává poměrně dobrou představu o rychlosti růstu funkce p_n, i když jak jsme viděli, u tak důležité funkce se matematici s tím nespokojili a pronikli mnohem dál.

Důkaz faktu 12.7.1. Začneme de Moivreovou větou (viz též cvičení 1.3.4): $(\cos\alpha + \mathrm{i}\sin\alpha)^n = \cos(n\alpha) + \mathrm{i}\sin(n\alpha)$, kde i je imaginární jednotka – kořen rovnice $\mathrm{i}^2 = -1$. Levou stranu rozvineme podle binomické věty. Imaginární části levé a pravé strany se musí rovnat, z čehož

$$\binom{n}{1}\sin\alpha\cos^{n-1}\alpha - \binom{n}{3}\sin^3\alpha\cos^{n-3}\alpha + \binom{n}{5}\sin^5\alpha\cos^{n-5}\alpha - \cdots = \sin(n\alpha).$$

S použitím funkce $\operatorname{cotg}\alpha = \frac{\cos\alpha}{\sin\alpha}$ přepíšeme levou stranu na

$$\sin^n\alpha\left[\binom{n}{1}\operatorname{cotg}^{n-1}\alpha - \binom{n}{3}\operatorname{cotg}^{n-3}\alpha + \binom{n}{5}\operatorname{cotg}^{n-5}\alpha - \cdots\right].$$

Odteď bude $n = 2m+1$ liché. Uzávorkovaný výraz se pak dá napsat jako $P(\operatorname{cotg}^2\alpha)$, kde $P(x)$ je mnohočlen $\binom{n}{1}x^m - \binom{n}{3}x^{m-1} + \binom{n}{5}x^{m-2} - \cdots$.

Každé čísel $r_k = \operatorname{cotg}^2\frac{k\pi}{n}$ pro $k = 1,2,\ldots,m$ je kořenem $P(x)$, protože pro $\alpha = \frac{k\pi}{n}$ je $\sin\alpha$ nenulový, zatímco $\sin(n\alpha) = 0$, a tedy $P(\operatorname{cotg}^2\alpha)$

je rovno 0. Protože čísla $r_1, \ldots, r_m$ jsou navzájem různá a $P(x)$ má stupeň m, známe nyní všechny kořeny. Tudíž

$$P(x) = n(x - r_1)(x - r_2)\cdots(x - r_m).$$

Porovnáním koeficientů u x^{m-1} na obou stranách této rovnosti zjistíme, že $n(r_1 + r_2 + \cdots + r_m) = \binom{n}{3}$. Odvodili jsme tedy identitu

$$\sum_{k=1}^{m} \operatorname{cotg}^2 \frac{k\pi}{2m+1} = \frac{m(2m-1)}{3}. \tag{12.9}$$

Pro $0 < \alpha < \frac{\pi}{2}$ máme $\operatorname{cotg}\alpha = 1/\operatorname{tg}\alpha < 1/\alpha$, a z (12.9) získáme nerovnost

$$\sum_{k=1}^{m} \frac{(2m+1)^2}{\pi^2 k^2} > \frac{m(2m-1)}{3}$$

neboli

$$\sum_{k=1}^{m} \frac{1}{k^2} > \frac{\pi^2}{6} \frac{2m(2m-1)}{(2m+1)^2}.$$

Pro $m \to \infty$ dostáváme $\sum_{k=1}^{\infty} 1/k^2 \geq \pi^2/6$. Odhad shora se dá dostat podobně. Použijeme rovnost $\operatorname{cotg}^2\alpha = \sin^{-2}\alpha - 1$ a nerovnost $\sin\alpha < \alpha$, která platí pro $0 < \alpha < \frac{\pi}{2}$, a z (12.9) obdržíme

$$\frac{m(2m-1)}{3} - m = \sum_{k=1}^{m} \frac{1}{\sin^2 \frac{k\pi}{2m+1}} > \sum_{k=1}^{m} \frac{(2m+1)^2}{\pi^2 k^2},$$

což pro $m \to \infty$ vede k $\sum_{k=1}^{\infty} 1/k^2 \leq \pi^2/6$. □

Cvičení

1. (a) Ověřte, že počet uspořádaných rozkladů čísla n s k sčítanci, neboli počet řešení rovnice $i_1 + i_2 + \cdots + i_k = n$ se všemi $i_j \geq 1$, se rovná $\binom{n-1}{k-1}$.

   (b) Spočítejte, kolik je všech uspořádaných rozkladů čísla n. Pro $n = 3$ například máme rozklady $3 = 1 + 1 + 1$, $3 = 1 + 2$, $3 = 2 + 1$ a $3 = 3$. Řešte třemi způsoby: přímo kombinatoricky, pomocí (a), a pomocí vytvořujících funkcí.

2. (a) (Pěkné cvičení z programování) Napište program, který vypíše všechny rozklady čísla n, každý právě jednou.

   (b) Naprogramujte (přesný) výpočet čísla p_n pro dané n. Nechcete-li používat násobnou aritmetiku, váš program by měl zvládnout výpočet p_n pro n nejméně do 5000 (kde $p_n < 10^{100}$) aspoň na 8 platných číslic. Může se uspořádat i soutěž o nejrychlejší správný program.

3. Zde uvažujeme počet $\bar{p}_n$ (neuspořádaných) rozkladů čísla n, které mají všechny sčítance navzájem různé. Kupříkladu pro $n = 5$ povolujeme jen rozklady $5 = 1 + 4$ a $5 = 2 + 3$.

   (a) Vyjádřete $\bar{p}_n$ jako koeficient u x^n ve vhodném výrazu.

   (b) Podle důvazu věty 12.7.2 odvoďte $\bar{p}_n \leq e^{2\sqrt{n}}$.

   (c) *Dokažte $\bar{p}_n \geq e^{c\sqrt{n}}$ pro všechna dost velká n pro nějakou kladnou konstantu c. Jaké největší c se vám povede dostat?

4. (a) Najděte vytvořující funkci pro čísla $\bar{p}_n$ ze cvičení 3 (je to nekonečný součin).

   (b) Najděte vytvořující funkci pro počet (neuspořádaných) rozkladů n na *liché* sčítance (taky nekonečný součin).

   (c) *Ověřte, že vytvořující funkce v (a) a (b) jsou tytéž, a tedy že počet rozkladů na různé sčítance se rovná počtu rozkladů na liché sčítance. **Podaří se vám najít přímý důkaz (bijekci)? (Řešení je např. v [19].)

5. Královská mincovna Středního Drobenska razí a_1 typů mincí v hodnotě 1 doublezon, a_2 typů mincí v hodnotě 2 doublezony atd. Ukažte, že částka n doublezonů se takovými mincemi dá zaplatit tolika způsoby, kolik udává koeficient u x^n ve výrazu

$$\prod_{i=1}^{n} \frac{1}{(1-x^i)^{a_i}}.$$

13

Aplikace lineární algebry

Několik pěkných použití lineární algebry v problémech diskrétní matematiky jsme ukázali už v předchozích kapitolách (obzvlášť v části 8.5). Zde předvedeme nejdříve dvě použití jednoduchých vlastností hodnosti matice pro úlohy, v nichž by lineární algebru na první pohled asi hledal málokdo: otázka existence blokových schémat a problém o pokrytí úplnými bipartitními grafy. O podobných důkazech se zájemce dočte mnohem více například ve svěží (ale bohužel dosud nedokončené) učebnici [3]. V dalších oddílech této kapitoly pak přiřadíme každému grafu několik vektorových prostorů, což vede k přehlednému popisu zdánlivě velmi složitých množin.

13.1 Bloková schémata

Nechť V je konečná množina a nechť $\mathcal{B}$ je systém podmnožin[1] množiny V. Abychom zdůraznili, že množinový systém $\mathcal{B}$ je na množině V, budeme jej zapisovat jako uspořádanou dvojici $(V, \mathcal{B})$. Na takovou dvojici se můžeme také dívat jako na zobecnění grafu (proto jiný termín pro takovou dvojici je *hypergraf*). Speciálně, mají-li všechny množiny $B \in \mathcal{B}$ stejnou velikost k, potom $(V, \mathcal{B})$ můžeme rovněž nazývat k-graf (2-graf tedy splývá s pojmem grafu).

[1] Volbu písmen V, $\mathcal{B}$ jsme podřídili dalším souvislostem této kapitoly.

S důležitým příkladem k-grafu jsme se setkali v kapitole 9 o konečných projektivních rovinách. Ukázali jsme tam, že jestliže V označuje množinu vrcholů projektivní roviny a $\mathcal{B}$ označuje množinu jejích přímek, potom množinový systém $(V, \mathcal{B})$ je $(k+1)$-graf pro vhodné k (a navíc $|V| = |\mathcal{B}| = k^2 + k + 1$). Tento příklad poslouží i ke snazšímu pochopení následující, na první pohled technické, definice. Nenechte se odradit.

13.1.1 Definice. *Nechť v, k, t a λ jsou celá čísla. Předpokládáme, že $v > k > t \geq 1$ a $\lambda \geq 1$. Blokové schéma typu t-(v, k, λ) je množinový systém $(V, \mathcal{B})$ splňující následující podmínky:*

(1) *V má v prvků.*

(2) *Každá množina $B \in \mathcal{B}$ má k prvků. Prvky $\mathcal{B}$ se nazývají* bloky.

(3) *Každá t prvková podmnožina V je obsažena právě v λ blocích $B \in \mathcal{B}$.*

Definici pochopíme uvážením několika případů.

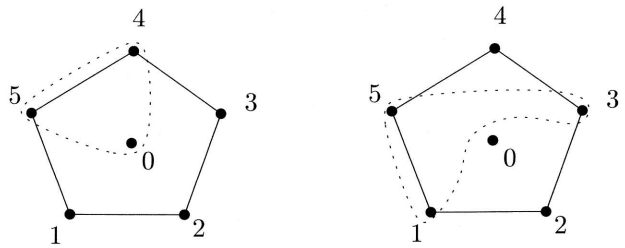
13.1.2 Příklad. *Nechť $\mathcal{B} = \binom{V}{k}$; $(V, \mathcal{B})$ se nazývá* triviální blokové schéma. *Snadno se přesvědčíme, že $(V, \mathcal{B})$ je t-(v, k, λ) blokové schéma pro $v = |V|$ a $\lambda = \binom{v-t}{k-t}$. (Zvolte libovolnou t-prvkovou podmnožinu T množiny V a přesvědčte se, že náleží právě $\binom{v-t}{k-t}$ blokům $B \in \mathcal{B}$.)*

13.1.3 Příklad. *Nechť $\mathcal{B} = \{B_1, \ldots, B_b\}$ označuje třídy rozkladu množiny V na stejně velké části. Položme $|B_i| = k$. Potom $(V, \mathcal{B})$ je blokové schéma typu 1-$(|V|, k, 1)$.*

13.1.4 Příklad. *Nechť V označuje body projektivní roviny řádu n, a pro tuto chvíli označme $\mathcal{B}$ množinu jejích přímek. Takové $(V, \mathcal{B})$ je blokové schéma typu 2-$(n^2+n+1, n+1, 1)$. Tuto netriviální skutečnost jsme ukázali v části 9.1.*

13.1.5 Příklad. *Nechť $V = \{0, 1, 2, 3, 4, 5\}$ a $\mathcal{B}$ tvoří následující trojice:* $\{0,1,2\}$, $\{0,2,3\}$, $\{0,3,4\}$, $\{0,4,5\}$, $\{0,1,5\}$, $\{1,2,4\}$, $\{2,3,5\}$, $\{1,3,4\}$, $\{2,4,5\}$, $\{1,3,5\}$.

Snadno se přesvědčíte, že $(V, \mathcal{B})$ je 2-$(6, 3, 2)$ blokové schéma. Toto schéma můžeme definovat také tak, že uvážíme kružnici s vrcholy 1, 2, 3, 4, 5 a jeden další vrchol 0. Systém $\mathcal{B}$ pak sestává ze všech trojic obsahujících právě jedinou hranu kružnice, viz obrázek:



Tyto příklady mají ve čtenáři vyvolat (správnou) představu, že bloková schémata představují jistý druh pravidelnosti, že představují příklad *pravidelných konfigurací*. Zpravidla není jednoduché blokové schéma sestrojit a základní otázkou v této celé oblasti je otázka existenční.

Základní problém. *Pro dané hodnoty v, k, λ, t rozhodněte, zda existuje blokové schéma typu t-(v, k, λ).*

Zde odvodíme některé nutné podmínky pomocí algebraických prostředků (teorie matic).

Na závěr tohoto úvodu zmiňme, že bloková schémata vznikla a dosud se používají v matematické statistice při návrhu experimentů. Tato motivace ovlivnila i standardní značení, které jsme výše zavedli.

Představme si, že chceme vyhodnotit účinnost několika způsobů ošetření určité rostliny. Porovnávaných způsobů ošetření je v (v od „variety"). Budeme je porovnávat sérií pokusů, a v každém z nich budeme vyhodnocovat k ošetření (to je dáno nějakými technickými podmínkami pokusů). Každý pokus bude tvořit *blok* příslušných ošetření. Mohli bychom samozřejmě vyšetřit všechny k-tice – všechny bloky – možných ošetření. V situaci polních pokusů je tento triviální způsob (odtud triviální blokové schéma) holou nemožností již pro malé hodnoty v a k. Proto začali statistikové používat návrhy experimentů, kde se nevyšetřují všechny k-tice, ale jen některé vybrané bloky. Tím samozřejmě může docházet k chybám, neboť návrh pokusu je neúplný, některé bloky nebyly uvažovány (a tedy

některá možná vzájemná působení ošetření byla zanedbána). Abychom alespoň částečně kompenzovali tuto (vynucenou) neúplnost návrhu experimentu, požadujeme, aby se každá dvojice ošetření vyskytovala ve stejném počtu pokusů-bloků. Schéma takového návrhu experimentu, tedy „blokové schéma", bude právě blokové schéma s parametry 2-(v, k, λ). Budeme-li požadovat, aby se každá trojice ošetření objevila ve stejném počtu λ pokusů, dostaneme blokové schéma typu 3-(v, k, λ), atd.

Pro rozlišení aplikace se bloková schémata vyskytují pod různými jmény: *Balanced Incomplete Block Design* (čili BIBD) pro schémata typu 2-(v, k, λ), *Steinerovy systémy* (pro $\lambda = 1$), *taktické konfigurace* (pro $t > 2$) atd.

Podmínky celočíselnosti. Je zřejmé, že blokové schéma typu t-(v, k, λ) nebude obecně existovat na každé množině, tedy pro každé v. Například 1-$(v, k, 1)$ schéma je rozklad, a tedy v musí být dělitelné k. Jiný, méně triviální příklad představovaly projektivní roviny, kde jsme určili velikost v jako funkci velikosti přímky. Následující věta popisuje nejdůležitější třídu nutných podmínek pro existenci blokového schématu typu t-(v, k, λ).

13.1.6 Věta (Podmínky celočíselnosti). *Nechť existuje blokové schéma s parametry t-(v, k, λ). Potom následující zlomky jsou celá čísla:*

$$\lambda\frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)},\ \lambda\frac{(v-1)\cdots(v-t+1)}{(k-1)\cdots(k-t+1)},\ \ldots,\ \lambda\frac{v-t+1}{k-t+1}.$$

Důkaz je snadnou aplikací počítání dvěma způsoby. Nechť $(V, \mathcal{B})$ je blokové schéma typu t-(v, k, λ). Zvolme pevné číslo s, kde $0 \le s \le t$, a s-prvkovou podmnožinu $S \subseteq V$. Počítejme dvěma způsoby počet dvojic (T, B), kde $S \subseteq T \in \binom{V}{t}$ a $T \subseteq B \in \mathcal{B}$.

Na jedné straně T lze zvolit $\binom{v-s}{t-s}$ způsoby, přičemž každé T je podmnožinou právě λ bloků B. Na druhé straně každý blok obsahující S obsahuje $\binom{k-s}{t-s}$ podmnožin $T \supseteq S$. Celkem tedy zlomek

$$\lambda\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} = \lambda\frac{(v-s)\cdots(v-t+1)}{(k-s)\cdots(k-t+1)}$$

vyjadřuje počet bloků B obsahujících množinu S, a tedy je to celé číslo. □

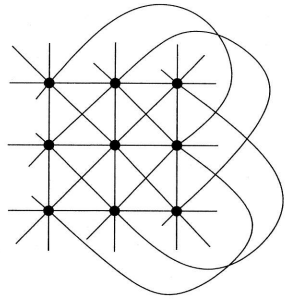
Poznámka. Použijeme-li uvedený důkaz pro $s = 0$ a $s = 1$, vidíme, že $\lambda\frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}$ určuje počet bloků a $\lambda\frac{(v-1)\cdots(v-t+1)}{(k-1)\cdots(k-t+1)}$ určuje počet bloků obsahujících daný prvek $x \in V$ (tedy „stupeň vrcholu x"). Ve statistické interpretaci, kterou jsme uvedli výše, toto číslo vyjadřuje, kolikrát se prvek x vyskytuje v různých pokusech (čili kolikrát byl x ošetřen). Proto se číslo $\lambda\frac{(v-1)\cdots(v-t+1)}{(k-1)\cdots(k-t+1)}$ zpravidla značí r („repetice").

13.1.7 Příklad (Steinerovy systémy trojic). *V jistém smyslu „první" netriviální případ blokového schématu typu t-(v, k, λ) dostaneme pro $t = 2$, $\lambda = 1$, $k = 3$. To je systém trojic kde každá dvojice bodů je obsažena v právě jedné trojici (jinými slovy, pokrytí množiny hran úplného grafu disjunktními trojúhelníky).*

V tomto případě podmínky celočíselnosti z věty 13.1.6 vyžadují, aby čísla

$$\frac{v(v-1)}{6} \quad \text{a} \quad \frac{v-1}{2}$$

byla celá, z čehož je snadné odvodit, že buď $v \equiv 1 \pmod 6$ nebo $v \equiv 3 \pmod 6$. Tedy v musí být prvkem posloupnosti 3, 7, 9, 13, 15, 19, 21, 25, 27, ... Pro všechny tyto hodnoty blokové schéma typu 2-$(v, 3, 1)$ existuje. Tato schémata se nazývají *Steinerovy systémy trojic* (viz cvičení 3). Pro $v = 7$ tvoří Steinerův systém projektivní rovinu řádu 2 (viz obr. 9.1(a)). Pro $v = 9$ máme takovýto Steinerův systém:



(což lze považovat za tzv. afinní rovinu – ta vznikne z projektivní roviny řádu 3 vypuštěním bodů ležících na jedné přímce).

13.1.8 Příklad (Bloková schémata). *Pro $t = 2$ (tj., požadujeme-li, aby každá dvojice byla právě v λ k-ticích z $\mathcal{B}$) vypadají podmínky celočíselnosti takto:*

$$\begin{aligned} \lambda v(v-1) &\equiv 0 \pmod{k(k-1)} \\ \lambda(v-1) &\equiv 0 \pmod{k-1}. \end{aligned} \tag{13.1}$$

Tyto podmínky již v obecnosti nejsou postačující. Platí ale základní (teoretický) výsledek, který uvádíme pro ilustraci:

13.1.9 Věta (Wilsonova věta). *Pro každou volbu čísel k, λ existuje takové číslo $v_0(k,\lambda)$, že pro všechny hodnoty $v \geq v_0(k,\lambda)$ splňující podmínky celočíselnosti (13.1) již existuje blokové schéma typu 2-(v,k,λ).*

Jinak řečeno, pro $t = 2$ jsou podmínky celočíselnosti postačující pro dostatečně velké množiny. Věta nic nesděluje o malých hodnotách v, jako například o existenci blokových schémat typu 2-$(k^2+k+1, k+1, 1)$ (neboli projektivních rovin).

Cvičení

1. (a) Ověřte, že projektivní rovina řádu p je blokové schéma typu 2-$(p^2+p+1, p+1, 1)$.
   (b)* Ukažte, že naopak blokové schéma typu 2-$(p^2+p+1, p+1, 1)$ je projektivní rovina řádu p.
2. Sestrojte Steinerův systém trojic s 15 prvky.
3.* Položme $n = 3m$, m je liché číslo. Definujme množinový systém $(X, \mathcal{M})$ následovně: $X = \{(x,i);\ i = 1,2,3, x = 0,1,\ldots,m-1\}$, a $\mathcal{M}$ obsahuje všechny trojice tvaru $\{(x,1),(x,2),(x,3)\}$, a pro každé $i = 1,2,3$ všechny trojice tvaru $\{(x,i),(y,i),(z,i+1)\}$, kde $x \neq y$ a $x + y \equiv 2z \pmod{m}$. Ukažte, že $(X, \mathcal{M})$ je Steinerův systém trojic.

13.2 Fisherova nerovnost

Jedním ze zakladatelů teorie blokových schémat byl anglický statistik R. A. Fisher. Ačkoliv dílčí příklady blokových schémat byly známy dlouhou dobu (např. Steinerovy systémy trojic již téměř 100 let), Fisher byl

první, kdo rozpoznal obecnou definici a její význam ve statistickém kontextu. Také našel další důležité omezující podmínky pro existenci blokových schémat.

13.2.1 Věta (Fisherova nerovnost). *Nechť $(V, \mathcal{B})$ je blokové schéma typu 2-(v,k,λ), kde $v > k$. Potom $|\mathcal{B}| \geq |V|$. (Tedy návrh experimentu pro v odrůd vyžaduje alespoň v pokusů.)*

Tato nerovnost se dá dokázat zajímavým využitím elementární lineární algebry, jak objevil indický matematik R. C. Bose. Než začneme s vlastním důkazem, zaveďme matici incidence množinového systému $(V, \mathcal{B})$. Označme prvky množiny V jako $x_1, \ldots, x_v$, a množiny z $\mathcal{B}$ jako $B_1, \ldots, B_b$. Definujme $b \times v$ matici $A = (a_{ij})$ předpisem

$$a_{ij} = \begin{cases} 1 & \text{jestliže } x_j \in B_i \\ 0 & \text{jinak.} \end{cases}$$

Matici A nazýváme *matice incidence* systému $(V, \mathcal{B})$. Řádky matice incidence jsou tedy charakteristické vektory množin $B_1, \ldots, B_b$.

Důkaz Fisherovy nerovnosti. Pro dané blokové schéma $(V, \mathcal{B})$ uvažme matici incidence $A = (a_{ij})$. Matice k ní transponovaná, A^T, má rozměr $v \times b$, a tedy součin $A^T A$ má rozměr $v \times v$. Ukážeme, že matice $B = A^T A$ má velmi jednoduchý tvar. Uvažme její člen b_{ij}; podle definice násobení matic máme

$$b_{ij} = \sum_{k=1}^{b} a_{ki} a_{kj}$$

(člen v i-tém řádku a k-tém sloupci matice A^T je a_{ki}). Člen b_{ij} tudíž vyjadřuje počet bloků B_k obsahujících zároveň x_i a x_j. Proto b_{ij} nabývá pouze dvou možných hodnot:

$$b_{ij} = \begin{cases} \lambda & \text{pro } i \neq j \\ \lambda \frac{v-1}{k-1} & \text{pro } i = j. \end{cases}$$

Číslo $\lambda \cdot \frac{v-1}{k-1}$ jsme výše označili r (počet opakování), a tedy matice B má tvar

$$\begin{pmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ & & \ddots & \\ \lambda & \lambda & \dots & r \end{pmatrix}.$$

Elementárními úpravami dostaneme

$$\begin{aligned} \det B &= \det \begin{pmatrix} r+(v-1)\lambda & r+(v-1)\lambda & \dots & r+(v-1)\lambda \\ \lambda & r & \dots & \lambda \\ \vdots & \vdots & \vdots & \\ \lambda & \lambda & \dots & r \end{pmatrix} \\ &= \Big(r+(v-1)\lambda\Big) \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda & r & & \lambda \\ \vdots & \vdots & & \\ \lambda & \lambda & & r \end{pmatrix} \\ &= \Big(r+(v-1)\lambda\Big) \cdot \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & r-\lambda & \dots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & & r-\lambda \end{pmatrix} \\ &= (r+(v-1)\lambda) \cdot (r-\lambda)^{v-1}. \end{aligned}$$

Připomeňme nyní, že $r = \lambda \cdot \frac{v-1}{k-1}$, a tedy $r + (v-1)\lambda = rk$. Protože $v > k$, máme i $r > \lambda$, a tak $\det B \neq 0$, čili matice B má hodnost[2] v. Kdyby ale $b < v$, potom hodnost matic A i A^T by byla ostře menší než v, a potom i $B = A^T A$ by měla hodnost $< v$ (zde používáme jednoduché vlastnosti hodnosti matice, viz cvičení 2). Tedy $b \geq v$. □

Jiný důkaz toho, že matice B má hodnost v, je naznačen ve cvičení 4.

[2]Připomeňme: *hodnost* nějaké matice M, označovaná zpravidla symbolem $r(M)$, je dimenze vektorového prostoru generovaného řádky této matice, nebo jinak řečeno je to maximální počet lineárně nezávislých řádků M (a totéž pro sloupce). Viz dodatek o algebře.

Toto použití hodnosti matice incidence se stalo základem mnoha podobných (a důležitých) důkazů.

Cvičení

1. Pro $\lambda = 1$ dokažte Fisherovu nerovnost přímo (bez použití lineární algebry).

2. Ukažte, že je-li A matice typu $n \times k$ a B matice typu $k \times m$, potom $r(AB) \leq \max(r(A), r(B))$.

3. Nechť F je nějaké těleso, a $G \subseteq F$ jeho podtěleso (představujte si např. pod F reálná čísla a pod G racionální čísla). Buď A matice s prvky z tělesa G. Hodnost matice A můžeme uvažovat nad tělesem G (lineární závislost s koeficienty v G) nebo nad tělesem F (lineární závislost s koeficienty v F). Zdůvodněte, proč v obou případech dostaneme tutéž hodnost.

4. Čtvercová $n \times n$ reálná matice B se nazývá *pozitivně definitní*, pokud platí $x^T B x > 0$ pro každý nenulový (sloupcový) vektor $x \in \mathbf{R}^n$.

   (a) Proč má pozitivně definitní $n \times n$ matice plnou hodnost n?

   (b) Ukažte, že matice B, použitá v důkazu v textu, je pozitivně definitní (a tedy B má hodnost v, bez počítání determinantu).

5. (a) Nechť $C_1, C_2, \dots, C_m$ jsou podmnožiny nějaké n-prvkové množiny X. Předpokládejme, že každá C_i má lichou velikost, a že velikost každého průniku $C_i \cap C_j$ (pro $i \neq j$) je sudá. Dokažte, že potom $m \leq n$. Podobně jako v textu, uvažte matici $A^T A$, kde A je matice incidence uvažovaného množinového systému, ale pracujte nad dvouprvkovým tělesem $GF(2)$.

   (b) Uvažme podobný problém jako v (a), ale tentokrát požadujeme, aby velikosti množin samotných byly *sudé*, zatímco velikosti průniků $|C_i \cap C_j|$ jsou všechny *liché*. Dokažte, že zase $m \leq n$.

   (c) A tentokrát požadujeme, aby všechny množiny C_i byly navzájem různé, a jejich velikosti i velikosti všech průniků byly *sudé*. Ukažte, že lze zkonstruovat $2^{\lfloor n/2 \rfloor}$ takových množin.

6. (Zobecněná Fisherova nerovnost) Buď X nějaká n-prvková množina, a q celé číslo, $1 \leq q < n$. Nechť $C_1, C_2, \dots, C_m$ jsou podmnožiny X, a předpokládejme, že všechny průniky $C_i \cap C_j$ (pro $i \neq j$) mají velikost přesně q.

(a)* Použitím metody z cvičení 4 dokažte, že platí $m \leq n$. (Zvlášť ošetřete případ, kdy $|C_i| = q$ pro některé i.)

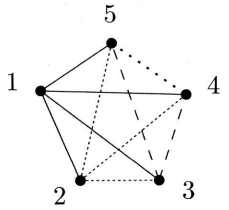
(b) Proč se tvrzení v (a) asi nazývá „zobecněná Fisherova nerovnost"? Odvoďte z něj Fisherovu nerovnost!

13.3 Pokrývání úplnými bipartitními grafy

R. L. Graham a H. O. Pollak, matematici v laboratořích firmy Bell, studovali následující otázku, motivovanou problémem z oblasti telekomunikací:

13.3.1 Úloha. *Množina hran úplného grafu K_n se má vyjádřit jako disjunktní sjednocení množin hran m úplných bipartitních grafů. Pro jakou minimální hodnotu $m = m(n)$ je to možné?*

Jedno možné vyjádření $E(K_n)$ pomocí $n-1$ úplných bipartitních grafů se snadno vyrobí z grafů typu K_{1,n_i} („hvězd"). Předpokládejme, že jsme již vyjádřili $E(K_{n-1})$ pomocí $n-2$ takových grafů. V grafu K_n uvážíme jeden vrchol, a hranami grafu $K_{1,n-1}$ pokryjeme všechny hrany z něj vycházející; pak zbývá pokrýt hrany K_{n-1}, což už umíme. Takhle vypadá vzniklé pokrytí pro $n = 5$:



Graham s Pollakem přišli na jednoduchý způsob, jak ukázat, že lepší pokrytí neexistuje:

13.3.2 Věta (Grahamova-Pollakova věta). *Platí $m(n) \geq n-1$.*

Důkaz. Předpokládejme, že úplné bipartitní grafy $B_1, \ldots, B_m$ disjunktně pokrývají všechny hrany K_n, tj.

$$V(B_k) \subseteq V(K_n) = \{1, 2, \ldots, n\},$$

$$E(K_n) = E(B_1) \dot\cup E(B_2) \dot\cup \ldots \dot\cup E(B_m).$$

Nechť (X_k, Y_k) je rozklad množiny vrcholů B_k na dvě části takové, že hrany B_k jdou jen mezi nimi.

Každému grafu B_k přiřadíme $n \times n$ matici A_k, jejíž prvek v i-tém řádku a j-tém sloupci je

$$a_{ij}^{(k)} = \begin{cases} 1 & \text{pokud } i \in X_k \text{ a } j \in Y_k \\ 0 & \text{jinak} \end{cases}$$

(definice A_k je trochu podobná matici sousednosti grafu B_k, až na to, že A_k není symetrická – každá hrana grafu B_k přispěje jenom jednou jedničkou). Tvrdíme, že každá z matic A_k má hodnost 1. To je proto, že všechny nenulové řádky matice A_k jsou rovny témuž vektoru, totiž vektoru s jedničkami v pozicích, jejichž indexy náležejí Y_k, a s nulami všude jinde.

Uvažme teď matici $A = A_1 + A_2 + \cdots + A_m$. Každá hrana $\{i, j\}$ náleží právě jednomu z grafů B_k, a proto pro každé $i \neq j$ platí buď $a_{ij} = 1$, $a_{ji} = 0$, anebo $a_{ij} = 0$, $a_{ji} = 1$, kde a_{ij} označuje prvek matice A v pozici (i, j) (přitom a_{ii}=0). Odtud plyne $A + A^T = J_n - I_n$, kde J_n je $n \times n$ matice samých jedniček a I_n je $n \times n$ jednotková matice (s jedničkami na hlavní diagonále a nulami jinde). Chceme teď ukázat, že hodnost takové matice A je aspoň $n-1$. Budeme-li to vědět, dostaneme $n-1 \leq r(A) \leq r(A_1) + \cdots + r(A_m) \leq m$, poněvadž pro hodnost libovolných dvou matic M_1 a M_2 platí $r(M_1 + M_1) \leq r(M_1) + r(M_2)$ – to je snadné ověřit z definice hodnosti.

Předpokládejme tedy $r(A) \leq n-2$. Připíšeme-li k matici A ještě jeden řádek ze samých jedniček, má vzniklá $(n+1) \times n$ matice pořád hodnost $\leq n-1$, a tedy existuje netriviální lineární kombinace jejích sloupců rovná nule. Jinými slovy, existuje (sloupcový) vektor $x \in \mathbf{R}^n$, $x \neq (0, 0, \ldots, 0)^T$ takový, že $Ax = 0$ a zároveň $\sum_{i=1}^n x_i = 0$.

Z posledně uvedeného vztahu plyne $J_n x = 0$. Spočítáme

$$x^T \left(A + A^T\right) x = x^T (J_n - I_n) x = x^T (J_n x) - x^T (I_n x) =$$

$$= 0 - x^T x = -\sum_{i=1}^n x_i^2 < 0.$$

Na druhé straně ale

$$x^T\left(A^T + A\right)x = \left(x^T A^T\right)x + x^T(Ax) = 0 \times x + x \times 0 = 0,$$

a to je spor. □

Cvičení

1. (a) Ukažte, že chceme-li pokrýt hrany K_n hranami bipartitních podgrafů K_n, a přitom netrváme na disjunktním pokrytí (tj., jedna hrana může být pokryta i mnohokrát), potom existuje pokrytí $\lceil \log_2 n \rceil$ bipartitními grafy.

   (b)* Dokažte, že pokrytí jako v (a) skutečně vyžaduje aspoň $\lceil \log_2 n \rceil$ bipartitních grafů.

2.* Tentokrát chceme pokrýt všechny hrany grafu K_n hranami bipartitních podgrafů tak, aby každá hrana byla pokryta lichým počtem bipartitních podgrafů. Dokažte, že potřebujeme aspoň $(n-1)/2$ bipartitních podgrafů. Postupujte podobně jako v důkazu v textu, ale pracujte s maticemi nad dvouprvkovým tělesem $GF(2)$. Místo matice A_k pak uvažte „skutečnou" matici sousednosti grafu B_k, jež má hodnost 2.

13.4 Prostor kružnic grafu

Nechť $G = (V, E)$ je neorientovaný graf. Označme symbolem $\mathcal{K}_G$ množinu všech kružnic (všech možných délek) v grafu G. Je vidět, že tato množina si zasluhuje složitější označení (kroucenými písmenkami), protože je značně veliká. Přesvědčte se, že např. pro úplný graf K_n platí

$$|\mathcal{K}_{K_n}| = \sum_{k=3}^{n} \binom{n}{k} \cdot \frac{(k-1)!}{2}, \tag{13.2}$$

a pro úplný bipartitní graf $K_{n,n}$ je

$$|\mathcal{K}_{K_{n,n}}| = \sum_{k=2}^{n} \binom{n}{k}^2 \cdot \frac{k!(k-1)!}{2}. \tag{13.3}$$

Na druhé straně $\mathcal{K}_G = \emptyset$ právě když G je les.

Zdálo by se, že struktura množiny $\mathcal{K}_G$ je nepřehledná a není možné ji nějak vhodně popsat. V této části zavedeme vhodné zobecnění pojmu kružnice, které souvisí s látku vyloženou v části 4.5, a které „doplní" množinu všech kružnic na větší množinu s velmi jednoduchou strukturou – strukturou vektorového prostoru. Myšlenky vyložené v dalším původně vznikly v souvislosti se studiem elektrických obvodů.

13.4.1 Definice (Eulerovská množina hran). *Nechť $G = (V, E)$ je (neorientovaný) graf. Množina $E' \subseteq E$ se nazývá* eulerovská, *jestliže graf (V, E') má všechny stupně sudé.*

Tedy prázdná množina a množina hran libovolné kružnice jsou eulerovské množiny.

V dalším bude pro nás výhodné ztotožňovat kružnici s její množinou hran.

13.4.2 Lemma. *Množina E' je eulerovská právě když existují kružnice $E_1, \ldots, E_t$ tak, že E_i jsou navzájem disjunktní množiny a E' je jejich sjednocením.*

Důkaz. Je-li E' neprázdná eulerovská množina, potom (V, E') není les a tedy obsahuje kružnici E_1. Množina $E' \setminus E_1$ je opět eulerovská, a lze tedy postupovat indukcí. □

Popíšeme strukturu všech eulerovských množin v daném grafu $G = (V, E)$ algebraicky. Hrany grafu G očíslujeme $e_1, e_2, \ldots, e_m$ a každé podmnožině $A \subseteq E$ přiřadíme charakteristický vektor $\mathbf{v}_A = (v_1, \ldots, v_m)$ definovaný předpisem

$$v_i = \begin{cases} 1 & \text{jestliže } e_i \in A \\ 0 & \text{jinak.} \end{cases}$$

Vektory budeme sčítat a násobit ve dvojkové soustavě (kde $1+1 = 0$). Snadno potom sami nahlédnete, že

$$\mathbf{v}_A + \mathbf{v}_B = \mathbf{v}_C,$$

kde $C = (A \setminus B) \cup (B \setminus A)$ je *symetrický rozdíl* množin A a B.

Symbolem $\mathcal{C}$ označme množinu všech charakteristických vektorů eulerovských množin v G. Kvůli snadné formulaci zobecněme trochu pojem kostry grafu: kostra libovolného grafu G je každý jeho podgraf neobsahující kružnice a maximální vzhledem k této vlastnosti (tj. přidáním libovolné další hrany z $E(G)$ kružnice vznikne). Pro souvislý graf toto splývá s definicí z části 5.3, pro nesouvislý graf dostáváme les, sestávající z koster všech komponent.

13.4.3 Věta (O prostoru kružnic).

(1) Pro každý graf G tvoří množina $\mathcal{C}$ vektorový prostor nad dvouprvkovým tělesem[3] *$GF(2)$ dimenze $|E| - |V| + k$, kde k je počet komponent grafu G.*

(2) Zvolme libovolnou kostru (V, E') grafu G, a pro každou hranu $e \in E \setminus E'$ označme K_e jedinou kružnici obsaženou v grafu $(V, E' \cup \{e\})$. Charakteristické vektory kružnic K_e (vzhledem ke zvolené kostře G) potom tvoří bázi $\mathcal{C}$.

Kružnici K_e nazýváme *elementární kružnice* (určená hranou e, vzhledem k dané kostře).

Důkaz. Nejprve ukážeme, že $\mathcal{C}$ je vektorový prostor. K tomu musíme zkontrolovat, že sčítáním vektorů z $\mathcal{C}$ i jejich násobením prvky tělesa $GF(2)$ dostaneme zase vektory z $\mathcal{C}$. Protože $0\mathbf{v}_A = \mathbf{v}_\emptyset$, $1\mathbf{v}_A = \mathbf{v}_A$, stačí ověřit, že množina $\mathcal{C}$ je uzavřena na sčítání vektorů. Vzhledem k poznámce před touto větou stačí ukázat, že pro eulerovské množiny A a B je i jejich symetrický rozdíl eulerovská množina. Zvolme tedy libovolný vrchol $v \in V$. Nechť k_A hran vycházejících z v náleží do A, k_B do B a k do obou těchto množin (kde k_A, k_B jsou sudá čísla). Potom do symetrického rozdílu $(A \setminus B) \cup (B \setminus A)$ patří zřejmě $k_A + k_B - 2k$ hran vycházejících z vrcholu v, a tedy stupeň v v symetrickém rozdílu množin A a B je sudý. Proto tento symetrický rozdíl je také eulerovská množina.

[3] GF je zkratka Galois Field, neboli Galoisovo těleso. Viz dodatek o algebře.

Nechť (V, E') je libovolná kostra grafu G. Potom $|E'| = |V| - k$, kde k je počet komponent grafu G. Stačí tedy ukázat, že charakteristické vektory všech elementárních kružnic tvoří bázi vektorového prostoru $\mathcal{C}$.

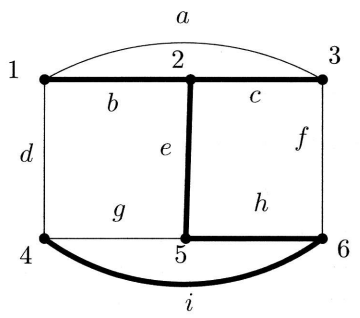
Můžeme předpokládat, že $E' = \{e_1, \ldots, e_t\}$, kde $t = |V| - k$ (případně přeznačíme hrany z E tak, aby hrany z E' byly na začátku). Ukážeme nejprve, že elementární kružnice jsou lineárně nezávislé. Uvážíme-li libovolnou hranu $e_i \notin E'$ (tj. $i > t$), pak vektor odpovídající elementární kružnici K_{e_i} je jediný mezi vektory elementárních kružnic, jenž má 1 v pozici i. Z tohoto důvodu nemůže být žádný z vektorů elementárních kružnic lineární kombinací jiných.

Dokažme teď, že elementární kružnice generují $\mathcal{C}$. Zvolme eulerovskou množinu A a definujme množinu B předpisem

$$\mathbf{v}_B = \sum_{e \in A \setminus E'} \mathbf{v}_{K_e}.$$

Jaké prvky množina B obsahuje? Právě ty hrany, které náleží lichému počtu elementárních kružnic (vzhledem k E'). Zajisté tedy B obsahuje množinu $A \setminus E'$ (každá její hrana náleží jediné elementární kružnici). Označme C symetrický rozdíl množin A a B. To je eulerovská množina, a přitom je obsažena v E', a E' neobsahuje kružnici – proto $C = \emptyset$. Odtud $A = B$, takže jsme (libovolně zvolený) vektor $\mathbf{v}_A \in \mathcal{C}$ vyjádřili jako lineární kombinaci elementárních kružnic. □

Příklad. Uvažme následující graf $G = (V, E)$:



Dimenze prostoru kružnic je $9 - 6 + 1 = 4$. Zvolíme-li silně vytaženou kostru, potom odpovídající báze prostoru kružnic je tvořena vektory elementárních kružnic

$$\begin{aligned} K_a &= \{a, b, c\} \\ K_d &= \{b, e, h, i, d\} \\ K_g &= \{g, h, i\} \\ K_f &= \{c, f, h, e\}. \end{aligned}$$

Například pro kružnici $K = \{a, f, i, d\}$ máme vyjádření

$$\mathbf{v}_K = \mathbf{v}_{K_a} + \mathbf{v}_{K_d} + \mathbf{v}_{K_f}.$$

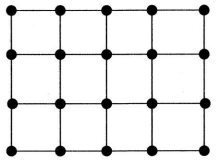
Z věty 13.4.3 snadno plyne toto:

13.4.4 Důsledek. *Počet eulerovských množin grafu $G = (V, E)$ je roven $2^{|E|-|V|+k}$, kde k je počet komponent G.*

Přes obrovský počet eulerovských podmnožin je jejich struktura jednoduchá a lze je rovněž snadno generovat (z mnohem menší báze). To byla rovněž jedna z původních motivací. Číslo $|E| - |V| + k$ se nazývá *cyklomatické číslo* grafu $G = (V, E)$.

Cvičení

1. Ověřte vzorce (13.2) a (13.3).
2. Dokažte důsledek 13.4.4.
3. Určete cyklomatické číslo (=dimenzi prostoru kružnic) $m \times n$ mřížky, například:



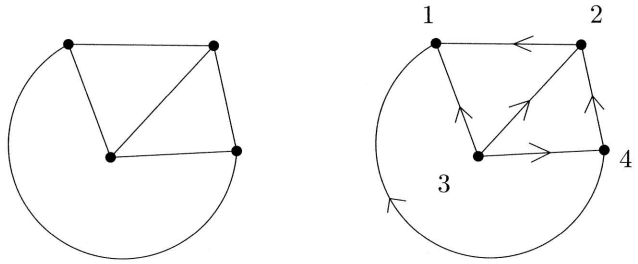
3×4

4. Dokažte, že pro každý topologický rovinný 2-souvislý graf (tj. 2-souvislý graf s daným rovinným nakreslením) tvoří bázi prostoru $\mathcal{C}$ kružnice ohraničující omezené stěny.

13.5 Cirkulace a řezy: prostor kružnic podruhé

V tomto článku vyložíme látku předchozího odstavce v poněkud jiném světle, za pomoci základů teorie matic. Budeme rovněž pracovat jak s grafy, tak s jejich orientacemi. Při tomto zesložitění se dostane věta 13.4.3 do nových souvislostí.

Z části 8.5 si připomeňme pojem *orientace*: Orientace grafu $G = (V, E)$ je orientovaný graf tvaru $\vec{G} = (V, \vec{E})$, kde množina $\vec{E}$ obsahuje pro každou hranu $\{x, y\} \in E$ právě jednu ze šipek (x, y) a (y, x). Následující obrázek ukazuje příklad grafu a jednu z jeho možných orientací:



G $\vec{G}$

(Všech možných orientací grafu G je $2^{|E|}$, mnoho jich však může být isomorfních.)

Orientaci $\vec{G} = (V, \vec{E})$ budeme pokládat za pevně zvolenou. Reálná funkce $f : \vec{E} \to \mathbf{R}$ se nazývá *cirkulace*, jestliže pro každý vrchol v grafu G platí

$$\sum_{x \in V;\, (v,x) \in \vec{E}} f(v, x) = \sum_{x \in V;\, (x,v) \in \vec{E}} f(x, v). \tag{13.4}$$

(Poznamenejme, že cirkulace může nabývat záporných hodnot.)

Pojem cirkulace má různé názorné interpretace. Například, je-li $\vec{G}$ schéma elektrického obvodu a $f(e)$ vyjadřuje proud tekoucí hranou e, potom (13.4) říká, že do každého vrcholu vtéká stejně, jako z něj vytéká – což je první Kirchhoffův zákon. Tato interpretace byla jednou z původních motivací pro teorii vyloženou v tomto článku.

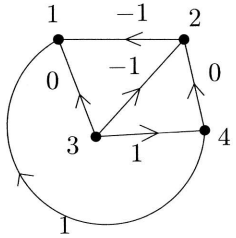
Jeden příklad cirkulace se dostane následovně. Buď

$$K = (v_1, v_2, \ldots, v_{k+1} = v_1)$$

kružnice (neorientovaná) v grafu G. Definujeme cirkulaci f (v orientaci $\vec{G}$) předpisem

$$\begin{array}{rcll} f(v_i, v_{i+1}) & = & 1 & \text{jestliže } (v_i, v_{i+1}) \in \vec{E} \\ f(v_{i+1}, v_i) & = & -1 & \text{jestliže } (v_{i+1}, v_i) \in \vec{E} \\ f(x, y) & = & 0 & \text{pokud } \{x, y\} \text{ není hrana kružnice } K. \end{array}$$

Cirkulace tedy závisí na směru, v němž jsme (neorientovanou) kružnici zapsali. O takto definované cirkulaci říkáme, že přísluší kružnici K. Pro graf na předchozím obrázku a kružnici s pořadím vrcholů 1 2 3 4 vypadá cirkulace takto:



Snadno nahlédneme, že jsou-li f_1 a f_2 cirkulace, je rovněž funkce $f_1 + f_2$ cirkulace na G. Pro reálné číslo c je také cf_1 cirkulace. (V obou případech stačí ověřit podmínku (13.4).) Odtud dostáváme, že každá eulerovská množina dává vzniknout přirozeným způsobem cirkulaci. Definujeme *nosič* dané cirkulace jako množinu

$$\big\{\{x, y\} \in E;\ \text{aspoň jedna z hodnot } f(x, y),\ f(y, x) \text{ je nenulová}\big\}.$$

S trochou nepřesnosti označíme $\mathcal{C}$ množinu všech cirkulací. Množina $\mathcal{C}$ tvoří vektorový prostor, který nazýváme prostor cirkulací a nebo rovněž *prostor kružnic* (stejný název jako v předchozím článku). Oba pojmy jsou si velmi příbuzné. Hlavní rozdíl mezi tímto a předcházejícím článkem spočívá v tom, že zde pracujeme nad tělesem reálných čísel, zatímco v předcházejícím článku nad tělesem $GF(2)$.

Nechť nyní $p : V \to \mathbf{R}$ je libovolná funkce (p od slova potenciál). Definujme funkci δp na šipkách $\vec{G}$ předpisem

$$\delta p(x, y) = p(x) - p(y) \tag{13.5}$$

pro každou šipku $(x, y) \in \vec{E}$.

Funkce $\delta p : \vec{E} \to \mathbf{R}$ se nazývá *potenciálový rozdíl* (kdo si pamatuje trochu fyziky, vidí jistě souvislost s elektrickými obvody). Každá funkce

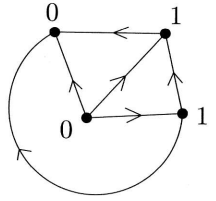
$g : \vec{E} \to \mathbf{R}$, pro niž existuje potenciál p splňující $g = \delta p$, se také nazývá *potenciálový rozdíl*.

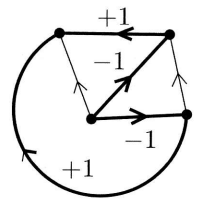
Snadno se opět přesvědčíme (ověřením podmínky (13.5)), že součet potenciálových rozdílů je opět potenciálový rozdíl, stejně tak číselný násobek. Množinu všech potenciálových rozdílů označíme $\mathcal{R}$ a nazýváme ji *prostor řezů*.

Proč jsme zvolili tento název? Uvažme následující situaci: Nechť potenciál p nabývá pouze hodnot 0 a 1. Položme $A = \{v \in V;\ p(v) = 1\}$, $B = V \setminus A$. Potom potenciálový rozdíl $g = \delta p$ nabývá nenulové hodnoty pouze pro šipky s jedním vrcholem v A a druhým v B:

$$\begin{array}{rcll} g(x, y) & = & 1 & \text{pro } x \in A,\ y \in B \\ g(x, y) & = & -1 & \text{pro } x \in B,\ y \in A \\ g(x, y) & = & 0 & \text{jinak.} \end{array}$$

Je přitom přirozené množinu všech hran mezi množinami A a B nazývat *řezem*, protože po jejím odejmutí bude mít vzniklý graf více komponent (samozřejmě pokud existuje alespoň jedna hrana mezi A a B). Na obrázku jsme znázornili potenciál p





a příslušný potenciálový rozdíl, hrany řezu jsou vyznačeny silněji.

Nyní celou situaci popíšeme pomocí matice incidence. Očíslujeme proto vrcholy $V = \{v_1, \ldots, v_n\}$ a hrany $E = \{e_1, \ldots, e_m\}$. Symbol $\vec{e}_i$ bude označovat šipku příslušející hraně e_i. Jako v části 8.5 zavedeme *matici incidence* orientace $\vec{G}$. Tato matice, D, je typu $n \times m$ a má prvky d_{ik} definované předpisem

$$d_{ik} = \begin{cases} -1 & \text{je-li } v_i \text{ začátek šipky } \vec{e}_k \\ 1 & \text{je-li } v_i \text{ konec šipky } \vec{e}_k \\ 0 & \text{jinak.} \end{cases}$$

Platí následující elegantní popis prostoru cyklů a prostoru řezů:

13.5.1 Věta. *Pro každý graf G je prostor řezů $\mathcal{R}$ generován řádky matice incidence D a prostor cirkulací $\mathcal{C}$ je ortogonální doplněk prostoru $\mathcal{R}$ (tj. $\mathcal{C} = \{x \in \mathbf{R}^m;\ x^T y = 0$ pro všechna $y \in \mathcal{R}\}$).*

Důkaz. Nechť $D = (d_{ij})$ je $n \times m$ matice incidence. Nejprve uvažme libovolný potenciálový rozdíl $g = \delta p$. Podle definice potenciálového rozdílu pro každou šipku $(v_r, v_s) = \vec{e}_j$ platí $g(\vec{e}_j) = p(v_r) - p(v_s) = \sum_{i=1}^{n} d_{ij} p(v_i)$ (porovnáním (13.5) s definicí matice incidence). Funkce g (chápaná jako řádkový vektor) je tedy lineární kombinací řádků matice incidence. Obrácením postupu vidíme, že řádky matice generují prostor $\mathcal{R}$.

Přepišme nyní podmínku (13.4) pro cirkulaci f pomocí matice incidence. Ze vztahu

$$\sum_{x \in V;\, (x,v) \in \vec{E}} f(x,v) = \sum_{x \in V;\, (v,x) \in \vec{E}} f(v,x)$$

plyne

$$\sum_{(x,v) \in \vec{E}} f(x,v) - \sum_{(v,x) \in \vec{E}} f(v,x) = 0,$$

což pro $v = v_i$ můžeme jinak zapsat

$$\sum_{j=1}^{m} f(\vec{e}_j) d_{ij} = 0.$$

Funkce f, chápaná jako m-členný řádkový vektor, má tedy s i-tým řádkem matice D nulový skalární součin. Tudíž f je kolmá na každý řádek D, a proto prostor $\mathcal{C}$ tvoří ortogonální doplněk $\mathcal{R}$ (v prostoru všech m-členných reálných vektorů). □

Jakou má prostor $\mathcal{R}$ dimenzi? Podle předchozí věty stejnou jako prostor generovaný řádky matice incidence D. Nyní přijde častý a užitečný trik: protože hodnost matice je stejná jako hodnost matice transponované, uvažme lineární nezávislost sloupců matice D. Symbolem d_j označme j-tý sloupec matice D (odpovídající šipce $\vec{e}_j$).

Uvažme nějakou množinu $J \subseteq \{1, 2, \ldots, m\}$ indexů sloupců, a ptejme se, kdy je množina sloupců $\{d_j;\ j \in J\}$ lineárně závislá. Lineární závislost znamená, že existují čísla c_j, $j \in J$, z nichž alespoň jedno je nenulové, tak, že $\sum_{j \in J} c_j d_j$ je nulový sloupcový n-členný vektor. Rozepišme to po složkách: i-tá složka, odpovídající vrcholu v_i, má tvar

$$\sum_{j \in J} c_j d_{ij} = 0.$$

Definujeme-li $c_t = 0$ pro $t \notin J$, dostáváme podmínku (13.4), a tedy $c = (c_1, \ldots, c_m)$ je nenulová cirkulace. Tím pádem nosič c obsahuje kružnici.

Na druhé straně, jak již víme, pro každou kružnici K existuje nenulová cirkulace s nosičem K. Celkem dostáváme, že množina sloupců $\{d_j;\ j \in J\}$ je lineárně nezávislá právě když množina hran $\{e_j;\ j \in J\}$ grafu G neobsahuje kružnici. Tedy hodnost matice D je $n - k$, kde k je počet komponent grafu G. Touto úvahou jsme tedy dokázali:

13.5.2 Věta. *Pro graf G s n vrcholy, m hranami a k komponentami má prostor řezů $\mathcal{R}$ dimenzi $n - k$, a prostor cirkulací $\mathcal{C}$ dimenzi $m - n + k$.*

Toto je jakási verze věty 13.4.3 pro vektorový prostor nad tělesem reálných čísel.

Vztah mezi eulerovskými množinami (nebo cirkulacemi) a řezy má povahu duality. Uvedené úvahy lze rozšířit na další struktury (nejenom grafy). Tímto se zabývá tzv. teorie matroidů.

Cvičení

1. Podejte definici „elementární cirkulace vzhledem k dané kostře".

Dodatek: opakování algebry

V této kapitolce zopakujeme základní skutečnosti o maticích, tělesech, vektorových prostorech a několika dalších algebraických objektech, které potřebujeme na některých místech knížky. Narozdíl od ostatních kapitol, tato část není míněna jako úvod do problematiky, nýbrž jako stručné shrnutí, v němž si může čtenář osvěžit své případně již zasuté znalosti.

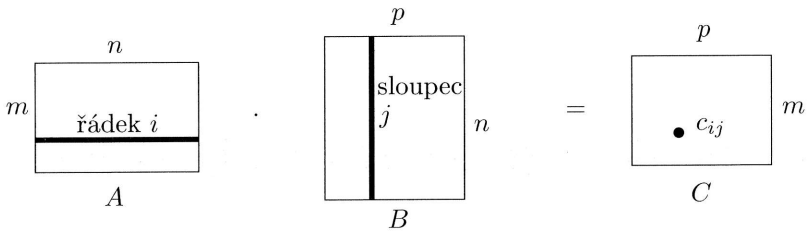
Matice. Matice je obdélníková tabulka čísel. Její položky mohou být reálná nebo komplexní čísla, případně i prvky dalších algebraických struktur. Matice typu $m \times n$ má m řádků n sloupců. Prvek v i-tém řádku a j-tém sloupci matice zvané A se obvykle označuje a_{ij}. Takže například matice A typu 3×2 má obecný tvar

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}.$$

Matice se sčítají po složkách, a sčítané matice musejí mít týž typ. Jsou-li tedy A a B matice typu $m \times n$ a $C = A + B$, pak $c_{ij} = a_{ij} + b_{ij}$. Podobně pro násobení číslem α: matice αA má v pozici (i, j) prvek αa_{ij}. Složitější a na první pohled nečekaná je však definice *násobení matic*. Součin AB je definován jen když počet sloupců matice A souhlasí s počtem řádků matice B. Je-li A typu $m \times n$ a B typu $n \times p$, pak součin $C = AB$ je matice typu $m \times p$ daná vzorcem

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Obrázkově:



Buď $x = (x_1, x_2, \ldots, x_n)$ vektor. V souvislosti s maticemi, takový vektor se zpravidla považuje za matici typu $n \times 1$ (představujeme si jej napsaný ve sloupečku), a je-li A matice typu $m \times n$, výraz Ax čteme jako součin dvou matic.

Zápis A^T, kde A je matice typu $m \times n$, znamená *matici transponovanou* k A, což je matice typu $n \times m$, která má v i-tém řádku a v j-tém sloupci prvek a_{ji}. Je snadné ověřit vzoreček pro transpozici součinu: $(AB)^T = B^T A^T$.

Skalární součin dvou n-složkových vektorů x a y je číslo $\sum_{i=1}^{n} x_i y_i$. Skalární součin x a y se mnohdy zapisuje $x^T y$. Přísně vzato, součin $1 \times n$ matice x^T a $n \times 1$ matice y je matice typu 1×1, jejíž jediný prvek je skalární součin definovaný výše, ale mezi maticí 1×1 a jejím prvkem se většinou nerozlišuje. Vektory x a y jsou *kolmé* pokud $x^T y = 0$.

Čtvercová matice je typu $n \times n$ pro nějaké $n \geq 1$. Její *diagonála* (někdy zvaná *hlavní diagonála*) sestává z prvků $a_{11}, a_{22}, a_{33}, \ldots, a_{nn}$. *Horní trojúhelníková matice* má nuly všude pod diagonálou; jinak řečeno $a_{ij} = 0$ pro $i > j$. *Diagonální matice* smí mít nenulové prvky jen na diagonále. *Jednotková matice* typu $n \times n$, označovaná zpravidla I_n, má jedničky na diagonále a všude jinde nuly.

Determinanty. Každé čtvercové matici A je přiřazeno číslo $\det(A)$ zvané *determinant* A. Definuje se formulí

$$\det(A) = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, a_{1,\pi(1)} a_{2,\pi(2)} \cdots a_{n,\pi(n)},$$

kde se sčítá přes všechny permutace π množiny $\{1, 2, \ldots, n\}$, a kde $\operatorname{sgn}(\pi)$ značí *znaménko* permutace π. Znaménko permutace je vždycky

buď $+1$ nebo -1, a krátce se dá definovat jako

$$\operatorname{sgn}(\pi) = \prod_{1 \leq i < j \leq n} \frac{\pi(j) - \pi(i)}{j - i}.$$

Kupříkladu determinant matice A typu 2×2 je roven $a_{11}a_{22} - a_{12}a_{21}$. Determinanty větších matic se málokdy počítají podle definice. Účinnější metody vyčíslení determinantu jsou zpravidla založeny na následujících pravidlech:

1. Determinant horní trojúhelníkové matice (a speciálně diagonální matice) je roven součinu všech prvků diagonály.

2. („Elementární řádková operace I“) Vynásobíme-li všechny prvky nějakého řádku matice A nějakým číslem α, determinant se také násobí α. Speciálně má-li A řádek ze samých nul, pak $\det(A) = 0$. Podobně pro sloupec.

3. („Elementární řádková operace II“) Determinant se nezmění, přičteme-li násobek nějakého řádku k jinému řádku. Jinými slovy, máme-li indexy $i \neq k$ a nahradíme-li prvek a_{ij} prvkem $a_{ij} + \alpha a_{kj}$ pro každé $j = 1, 2, \ldots, n$, kde α je nějaké pevné číslo, determinant zůstane stejný. Podobně pro sloupce.

4. Prohozením dvou řádků (nebo dvou sloupců) změní determinant znaménko. (To se dá odvodit z předchozích dvou pravidel.)

5. Pro libovolné čtvercové matice A, B téhož typu platí

$$\det(AB) = \det(A) \det(B).$$

6. („Rozvoj determinantu podle řádku“) Pro každý řádkový index i platí vztah

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}),$$

kde A_{ij} je matice, která vznikne z A vypuštěním i-tého řádku a j-tého sloupce.

Čtvercová matice A je *regulární* pokud $\det(A) \neq 0$ a *singulární* pokud $\det(A) = 0$. *Podmaticí* rozumíme každou matici vzniklou z A vymazáním některých řádků nebo sloupců. Důležitý pojem *hodnosti matice* bude připomenut později v souvislosti s lineární nezávislostí vektorů.

Grupy a tělesa. *Binární operace* na nějaké množině X je libovolné zobrazení $X \times X \to X$; to znamená, že každým dvěma prvkům $a, b \in X$ je přiřazen nějaký prvek X, což je „výsledek" uvažované binární operace. Například sčítání a násobení jsou binární operace na množině všech přirozených čísel, zatímco odčítání není binární operací na této množině. Binární operace se obvykle zapisují symboly jako $*$, $\circ$, $+$, $\cdot$ a podobně. Je-li tedy $*$ nějaká binární operace, zápis $a * b$ označuje prvek přiřazený operací $*$ uspořádané dvojici (a, b).

Binární operaci $*$ nazveme *asociativní*, pokud $a*(b*c) = (a*b)*c$ pro všechna $a, b, c \in X$. *Komutativita* operace $*$ znamená $a * b = b * a$ pro všechna $a, b \in X$. Prakticky veškeré binární operace, s nimiž se v matematice běžně setkáme, bývají asociativní, ale mnohé důležité a často se vyskytující operace jsou nekomutativní, jako třeba násobení matic typu $n \times n$ (pro $n \geq 2$) nebo skládání zobrazení nějaké množiny.

Grupa je množina G s asociativní binární operací $*$ splňující následující podmínky (existuje mnoho různých ekvivalentních verzí těchto podmínek):

(i) Existuje prvek $e \in G$, zvaný *jednotkový prvek* (případně *neutrální prvek*), takový že pro všechna $a \in G$ platí $a * e = e * a = a$. (Je snadno vidět, že pokud takové e existuje, je jen jedno.)

(ii) Pro každé $a \in G$ existuje $b \in G$, pro něž $a * b = b * a = e$, kde e je jednotkový prvek. Takové b se jmenuje *inverzní prvek* k prvku a, a obvykle se označuje a^{-1}. Inverzní prvek je také určen pro každé $a \in G$ jednoznačně[4].

[4]Někdy se grupa definuje jako algebraická struktura se třemi operacemi: binární operací $*$ jako výše, unární operací inverzního prvku ($a \mapsto a^{-1}$) a nulární operací, čili konstantou, e (zatímco v uvedené definici jsou operace inverzního prvku a e odvozené definicí z $*$). To má jisté výhody z hlediska obecné algebry, například podgrupa je pak prostě podmnožina uzavřená na tyto tři operace.

Některé z důležitých příkladů grup jsou celá čísla s operací sčítání, kladná reálná čísla s násobením, množina všech regulárních matic typu $n \times n$ s operací násobení, množina všech permutací dané množiny X s operací skládání permutací a množina všech rotací třídimenzionálního euklidovského prostoru kolem počátku s operací skládání (provedení nejprve jedné rotace a pak druhé dá opět nějakou rotaci). Na druhé straně, přirozená čísla se sčítáním ani reálná čísla s násobením grupu netvoří.

Grupa je komutativní pokud její binární operace je komutativní. Komutativním grupám se někdy říká *abelovské*.

Těleso je množina K se dvěma binárními operacemi$+$ a $\times$ (tyto symboly zde nemusí nutně znamenat obvyklé operace s čísly!), pro něž platí takovéto axiomy:

1. Množina K s operací $+$ je komutativní grupa. Její jednotkový prvek se značí 0.

2. Množina $K \setminus \{0\}$ s operací $\times$ je komutativní grupa. Její jednotkový prvek se značí 1.

3. Platí *distributivita*: $a \times (b + c) = (a \times b) + (a \times c)$ pro každé $a, b, c \in K$.

Podobně jako u grup, v literatuře se najde mnoho ekvivalentních verzí axiomů tělesa. Násobení $a \times b$ se často zkráceně zapisuje ab. Nejběžnější tělesa jsou racionální čísla, reálná čísla a komplexní čísla (s obvyklým násobením a sčítáním jako operacemi). Naproti tomu celá čísla se sčítáním a násobením tělesem nejsou.

Buď K těleso. Jeho podmnožina L je jeho *podtěleso* pokud je L tělesem s binárními operacemi a prvky 0 a 1 zděděnými z K. Například těleso racionálních čísel je podtělesem tělesa reálných čísel.

V kombinatorice se mnohdy potřebují konečná tělesa. Konečné těleso s q prvky, pokud takové existuje, se často označuje $GF(q)$. Nejjednodušší konečné těleso je $GF(2)$, což je prostě množina $\{0, 1\}$ s obvyklým násobením (jako v celých číslech) a se sčítáním daným rovnostmi $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$. Je známo, že konečné těleso

$GF(q)$ existuje právě když je q mocnina prvočísla. V takovém případě je vždy jen jediné q-prvkové těleso (až na přejmenování prvků). Je-li q prvočíslo, těleso $GF(q)$ se popíše velmi snadno. Je to množina $\{0, 1, 2, \ldots, q-1\}$, kde sčítání a násobení se provádějí jako pro celá čísla, ale po sečtení nebo vynásobení dvou čísel vezmeme zbytek při dělení výsledku číslem q (tomu se říká *aritmetika modulo q*). Výše uvedený popis $GF(2)$ je speciálním případem této konstrukce. Zdůrazněme ale, že pro $q = p^k$, kde p je prvočíslo a $k > 1$, množina $\{0, 1, \ldots, q-1\}$ s aritmetikou modulo q *není* tělesem, a konstrukce tělesa $GF(q)$ je jiná a složitější.

Vektorové prostory. Nechť K je nějaké těleso (nejčastěji uvažujeme těleso všech reálných čísel). *Vektorový prostor* nad K je komutativní grupa V s grupovou operací $+$ a s neutrálním prvkem 0, plus zobrazení $K \times V \to V$. To znamená, že každé dvojici (α, v), kde $\alpha \in K$ a $v \in V$, je přiřazen prvek z V, a tedy každý prvek z V můžeme „vynásobit" libovolným prvkem z K. Tohle násobení se zpravidla zapisuje bez nějakého zvláštního znaménka pro násobení, takže píšeme prostě αv a míníme v vynásobené α. Pro vektorový prostor musí být dále splněný takovéto požadavky, pro libovolná $u, v \in V$ a jakákoli $\alpha, \beta \in K$: $\alpha(u+v) = \alpha u + \alpha v$, $(\alpha+\beta)v = \alpha v + \beta v$ (jakási distributivita), $\alpha(\beta v) = (\alpha\beta)v$ (něco jako asociativita), a $1v = v$. Z těchto axiomů lze už dokázat všelijaké další vlastnosti, jako třeba $0v = 0$ (ta 0 nalevo je v tělese K, zatímco ta napravo je ve vektorovém prostoru V). Prvky V se jmenují *vektory*.

Nejobvyklejší a nejdůležitější příklad vektorového prostoru je tvořen množinou všech uspořádaných n-tic reálných čísel (pro nějaké přirozené číslo n). Tyto n-tice se sčítají a násobí reálným číslem po složkách. Tak dostaneme vektorový prostor nad reálnými čísly, ale podobně můžeme uvažovat vektorový prostor všech uspořádaných n-tic prvků jakéhokoli tělesa K, čímž dostaneme vektorový prostor nad K. Ten se zpravidla označuje K^n.

Množina $A \subset V$ ve vektorovém prostoru V je *lineárně závislá*, pokud existují vektory $v_1, v_2, \ldots, v_n \in A$, $n \geq 1$, a čísla $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, ne všechna najednou rovná 0, tak, že

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0.$$

Není-li A lineárně závislá, nazývá se *lineárně nezávislá*.

Největší mohutnost lineárně nezávislé množiny v daném vektorovém prostoru V se jmenuje *dimenze* V, a každá lineárně nezávislá množina této mohutnosti se nazývá *báze* vektorového prostoru V. Vektorový prostor K^n má dimenzi n, jak by každý čekal.

Každý vektorový prostor má nějakou bázi, a každá lineárně nezávislá množina maximální vzhledem k inkluzi (tj., nelze přidat žádný vektor bez pokažení lineární nezávislosti) je bází. V kombinatorice se skoro vždy setkáváme jen s vektorovými prostory konečné dimenze.

Je-li $(e_1, e_2, \ldots, e_n)$ báze nějakého n-dimenzionálního vektorového prostoru V, pak každý vektor $v \in V$ se dá právě jedním způsobem vyjádřit ve tvaru $v = \sum_{i=1}^{n} \alpha_i e_i$ pro nějaká $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$. Tato jednoznačně určená $\alpha_1, \ldots, \alpha_n$ jsou *souřadnice* vektoru v vzhledem k bázi $(e_1, \ldots, e_n)$. Každému vektoru $v \in V$ je tudíž jednoznačně přiřazen vektor z K^n, totiž n-tice jeho souřadnic. Tím dostaneme bijekci mezi V a K^n (pro daný V je mnoho takových bijekcí, jedna pro každou volbu báze ve V). Všechny n-dimenzionální vektorové prostory nad daným tělesem jsou „stejné", tj. jsou ve vhodně definovaném smyslu isomorfní. Takže na K^n můžeme pohlížet jako na „jediný" n-dimenzionální vektorový prostor nad K, a vektory si obvykle můžeme představovat jako n-tice čísel. Na druhé straně, často je užitečné pracovat i s jinými konkrétními verzemi n-dimenzionálních vektorových prostorů. V kombinatorických použitích lineární algebry je často rozhodujícím krokem šikovná a nečekaná konstrukce nějakého pomocného vektorového prostoru, a hlavní část důkazu pak spočívá v odhadu jeho dimenze.

Podprostor vektorového prostoru V je podmnožina $W \subseteq V$ uzavřená na sčítání vektorů a na násobení prvky z tělesa K. Je-li $X \subseteq V$ libovolná množina vektorů, definujeme *podprostor generovaný* X jako nejmenší podprostor prostoru V obsahující X. Explicitní popis tohoto podprostoru je $\{\sum_{i=1}^{n} \alpha_i v_i;\ n \in \mathbf{N},\ \alpha_1, \ldots, \alpha_n \in K,\ v_1, \ldots, v_n \in X\}$.

Hodnost matice A typu $m \times n$, jejíž prvky jsou z tělesa K, je definována jako dimenze podprostoru generovaného řádky matice A (chápanými jako n-složkové vektory) v prostoru K^n. Hodnost A se zpravidla označuje $r(A)$. Tato hodnost je také rovna dimenzi podprostoru generovaného sloupci matice A v prostoru K^m, tedy $r(A) = r(A^T)$. Pro hodnost součinu a součtu matic platí nerovnosti

$$r(AB) \leq \min(r(A), r(B)) \quad \text{a} \quad r(A+B) \leq r(A) + r(B).$$

Čtvercová matice typu $n \times n$ je regulární (má nenulový determinant), právě když má hodnost n – to je významné kriterium lineární nezávislosti pomocí determinantu. Obecněji, platí následující charakterizace hodnosti: $r(A)$ je největší celé číslo k takové, že A (ne nutně čtvercová) má aspoň jednu regulární podmatici typu $k \times k$.

Jsou-li V a W vektorové prostory nad stejným tělesem K, definujeme *lineární zobrazení* prostoru V do prostoru W jako zobrazení $f: V \to W$ splňující

$$f(\alpha u) = \alpha f(u) \quad \text{a} \quad f(u+v) = f(u) + f(v)$$

pro všechna $\alpha \in K$ a $u, v \in V$. *Jádro* lineárního zobrazení f je množina $\ker(f) = \{v \in V;\ f(v) = 0\}$. Jádro f je podprostor V, a množina $f(V)$ je podprostor W. Dimenze $f(V)$ je *hodnost* zobrazení f. Pro každé lineární zobrazení $f : V \to W$ je pravda

$$\dim \ker(f) + \dim f(V) = \dim V.$$

Buď $(e_1, e_2, \ldots, e_n)$ nějaká báze V a $(f_1, f_2, \ldots, f_m)$ nějaká báze W. Volbou těchto bází získáme bijekci mezi všemi lineárními zobrazeními $f: V \to W$ a všemi maticemi typu $m \times n$ s prvky z tělesa K. Jak víme, každý vektor $v \in V$ můžeme jednoznačně napsat ve tvaru $v = \sum_{i=1}^{n} \alpha_i e_i$. Lineární zobrazení $f: V \to W$ se dá vyjádřit takto:

$$f(v) = f\Big(\sum_{i=1}^{n} \alpha_i v_i\Big) = \sum_{j=1}^{m} \Big(\sum_{i=1}^{n} a_{ji}\alpha_i\Big) f_j,$$

kde a_{ij} jsou prvky $m \times n$ matice A odpovídající f. Jinými slovy, je-li α sloupcový vektor souřadnic vektoru v vzhledem k bázi $(e_1, \ldots, e_n)$ a β je sloupcový vektor souřadnic $f(v)$ vzhledem k bázi $(f_1, \ldots, f_m)$, potom máme $\beta = A\alpha$.

Takže lineární zobrazení můžeme chápat jako abstraktní verzi matic, nebo matice jako „souřadnicový zápis“ lineárních zobrazení. Násobení matic pak odpovídá skládání lineárních zobrazení. Hodnost lineárního zobrazení je ovšem totéž jako hodnost jeho matice (vzhledem k libovolným bázím).

Geometrická interpretace. Mnohdy je užitečné si některé objekty z lineární algebry představovat geometricky, a naopak lineární algebra samozřejmě pomáhá pracovat s objekty geometrickými.

Nedá se říct, které geometrické interpretace lineárně-algebraických pojmů jsou nejlepší, to vždy závisí na situaci. Zde uvedeme několik jednoduchých možností. Budeme se držet vektorového prostoru $\mathbf{R}^3$, i když geometrické představy mohou při určitém cviku pomoci i pro vyšší dimenze.

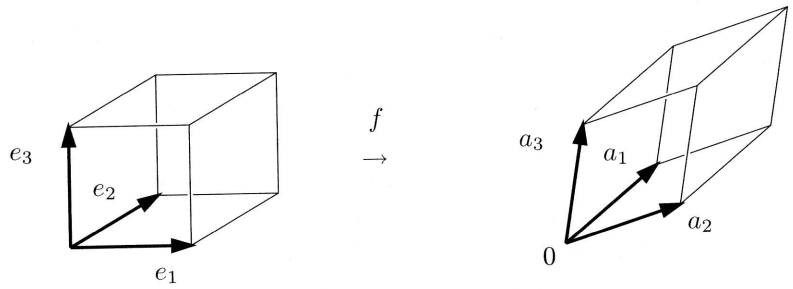
Podprostory $\mathbf{R}^3$ (jako vektorového prostoru nad $\mathbf{R}$) jsou: bod 0 (počátek), všechny přímky a roviny procházející počátkem, a $\mathbf{R}^3$ sám. Lineární závislost 3 vektorů $a_1, a_2, a_3 \in \mathbf{R}^3$ znamená, že body a_1, a_2, a_3 leží na společné rovině procházející počátkem.

Rovina neprocházející počátkem není (vektorovým) podprostorem. Můžeme ji vyjádřit jako posun nějakého podprostoru o vhodný vektor, nebo též jako řešení jedné lineární rovnice, tj. jako množinu všech $x = (x_1, x_2, x_3) \in \mathbf{R}^3$, pro něž $a^T x = a_1x_1 + a_2x_2 + a_3x_3 = b_0$, pro nějaké $b_0 \in \mathbf{R}$ a nějaké nenulové $a \in \mathbf{R}^3$.

Je-li A matice typu $m \times 3$ a $b \in \mathbf{R}^m$ je sloupcový m-složkový vektor, $Ax = b$ je soustava m lineárních rovnic pro neznámý vektor $x \in \mathbf{R}^3$. Každý řádek A dává jednu lineární rovnici. S výjimkou patologického případu nulového řádku, taková rovnice určuje rovinu, a geometricky je množina řešení soustavy $Ax = b$ průnikem m rovin (nemá-li A nulové řádky). Pro $m = 2$, příslušné 2 roviny mohou být totožné (řešením jsou všechny body této roviny), rovnoběžné (žádné řešení), nebo různoběžné (řešením jsou body přímky). V prvních dvou případech má A hodnost 1, a ve třetím případě hodnost 2. Podobně můžeme diskutovat případ $m = 3$: matice A hodnosti 3 odpovídá třem rovinám protínajícím se v jediném bodě, a menší hodnosti odpovídají

několika možným „degenerovaným“ situacím (některé z rovin splývají nebo jsou rovnoběžné, případně průnik dvou rovin je rovnoběžný s rovinou třetí).

Nechť $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$ je standardní báze prostoru $\mathbf{R}^3$. Lineární zobrazení $f : \mathbf{R}^3 \to \mathbf{R}^3$ je určeno obrazy $a_i = f(e_i)$ bázových vektorů. Vektoru $x \in \mathbf{R}^3$ je přiřazen vektor $f(x) = Ax \in \mathbf{R}^3$, kde A je matice typu 3×3 s a_1, a_2, a_3 jako sloupci (přesněji řečeno, A je matice zobrazení f vzhledem ke dvojici bází (e_1, e_2, e_3) a (e_1, e_2, e_3)). Zobrazení f převádí jednotkovou krychli na rovnoběžnostěn určený vektory a_1, a_2, a_3:



Absolutní hodnota determinantu A je přesně objem tohoto rovnoběžnostěnu! Jako speciální případ, je-li $\det A = 0$, má A hodnost ≤ 2, tudíž a_1, a_2, a_3 leží ve společné rovině procházející počátkem, a místo rovnoběžnostěnu máme placku nulového objemu. Obecněji, je-li $K \subset \mathbf{R}^3$ množina objemu v, potom $f(K)$ má objem $v|\det A|$. Podobný význam má absolutní hodnota determinantu i pro vyšší dimenze. Znaménko determinantu je pak dáno orientací trojice (a_1, a_2, a_3): příkladem trojice s kladnou orientací je (e_1, e_2, e_3), a příkladem trojice se zápornou orientací je $(e_1, e_2, -e_3)$.

Literatura

[1] A. Aho, J. Hopcroft, J. Ullman: *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, Massachusetts, 1983.

[2] G. E. Andrews: *The Theory of Partitions* (Encyclopedia of mathematics and its applications, vol. 2), Addison-Wesley, Reading, Massachusetts, 1976.

[3] L. Babai, P. Frankl: *Linear algebra methods in combinatorics* (Preliminary version 2), Department of Computer Science, The University of Chicago, 1992.

[4] B. Balcar, P. Štěpánek: *Teorie množin*, Academia Praha 1986.

[5] O. Borůvka: Několik vzpomínek na matematický život v Brně, *Pokroky mat. fyz. a astr.* 22(1977) 91–99.

[6] J. M. Borwein, P. B. Borwein: *Pi and the AGM*, John Wiley & Sons, New York 1987.

[7] K. Chandrasekhar: *Introduction to Analytic Number Theory*, Springer-Verlag 1968.

[8] D. Cox, J. Little, and D. O' Shea: *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 2nd edition, Springer-Verlag, Berlin, 1996.

[9] R. Diestel: *Graph Theory*, Graduate Texts in Mathematics 173, Springer-Verlag, Berlin etc., 3. vydání 2005. Volně dostupné též elektronicky.

[10] P. Flajolet, R. Sedgewick: *Analytic Combinatorics*, Cambridge University Press, Cambridge 2009. Předběžná verze dostupná na webové stránce Philippa Flajoleta.

[11] G. Gonthier: Formal proof—the four-color theorem. *Notices Amer. Math. Soc.* 55(2008) 1382–1393.

[12] T. Gowers: Matematika. Průvodce pro každého. Dokořán Praha 2006.

[13] R. Graham, D. Knuth, O. Patashnik: *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, Reading, Massachusetts, 1989.

[14] F. Harary, E. M. Palmer: *Graphical Enumeration*, Academic Press, New York and London, 1973.

[15] K. Havlíček a kol.: *Cesty moderní matematiky*, Horizont Praha 1976.

[16] G. Kant: Drawing planar graphs using the canonical ordering, *Algorithmica* 16(1996), 4–32.

[17] D. Karger, P. Klein, R. Tarjan: A Randomized Linear-Time Algorithm to Find Minimum Spanning Trees, *Journal of the ACM* 42(1995), 321–328.

[18] D. Knuth: *The Art of Computer Programming*, Volume I: Fundamental Algorithms, Addison-Wesley, Reading, MA 1968.

[19] J. H. van Lint, R. M. Wilson: *A Course in Combinatorics*, Cambridge University Press, Cambridge 1992.

[20] J. Littlewood: *A Mathematician's Miscellany*, London, Methuen, 1953.

[21] L. Lovász: *Combinatorial Problems and Exercises*, 2. vydání, Akadémiai Kiadó Budapest and North-Holland, Amsterdam 1993.

[22] B. Mohar and C. Thomassen: *Graphs on Surfaces*, Johns Hopkins University Press, Baltimore, Maryland, 1997.

[23] J. Nešetřil: *Teorie grafů*, SNTL Praha 1979.

[24] J. Nešetřil: Kombinatorika a teorie grafů I, skripta, Universita Karlova Praha 1981.

[25] N. Robertson, D. P. Sanders, P. D. Seymour, and R. Thomas: The Four Color Theorem, *Journal of Combinatorial Theory* Ser. B 70(1997), 2–44.

[26] N. Robertson, P. D. Seymour, and R. Thomas: Permanents, Pfaffian orientations, and even directed circuits, *Ann. Math.* 150(1999), 929–975.

[27] A. de Saint-Exupéry: *Malý princ*, SNDK Praha 1966.

[28] J. Stillwell: *Classical Topology and Combinatorial Group Theory* (Graduate Texts in Mathematics 72), Springer-Verlag 1980.

[29] C. Thomassen: The Jordan–Schoenflies theorem and the classification of surfaces, *American Mathematical Monthly* 99(1992), No. 2, 116–130.

[30] N. J. Vilenkin: *Kombinatorika*, SNTL Praha 1977.

[31] G. M. Ziegler: *Lectures on Polytopes*, Revised edition, Graduate Texts in Mathematics 152, Springer-Verlag, Berlin, 1998.

Rejstřík

$\binom{n}{k}$, 76
$\binom{n}{k_1,\ldots,k_m}$, 81
$\binom{V}{2}$, 112
$\binom{X}{k}$, 76(3.3.1)
$\prec$, 52
$\preceq$, 51
$a \mid b$, 53(2.1.2)
$\sum$, 25, 28
$\prod$, 25
(a, b), 24
(m, n), 107
$[a, b]$, 24
$[x]$, 24
$\lfloor x \rfloor$, 24
$\lceil x \rceil$, 24
$\{\ldots\}$, 26
(x, y), 35
$\{x, y\}$, 34
$\emptyset$, 27
2^X, 27
$\subseteq$, 28
$\subseteq$ (uspořádání), 54(2.1.3)
$\subset$, 28
$\in$, 26
$|X|$, 27
$X \setminus Y$, 29
X^2, 36
$X \cap Y$, 28
$X \cup Y$, 28
$X \dot\cup Y$, 29
$X \times Y$, 35(1.4.1)
$R[x]$, 47
$R \circ S$, 38
xRy, 36
$f(x)$, 41
$f(X)$, 41
$f : x \mapsto y$, 40
$f : X \to Y$, 40
$f : X \hookrightarrow Y$, 43
$f : X \twoheadrightarrow Y$, 43
$f : X \hookrightarrow\!\!\!\!\!\!\twoheadrightarrow Y$, 43
$f \sim g$, 87
$g \circ f$, 42
A^T, 272, 400
$G + \bar{e}$, 148(4.7.2)
$G\%e$, 149(4.7.2)
$G - e$, 148(4.7.2)
$G - v$, 148(4.7.2)
$G.e$, 227(4.7.2)
$G \cong H$, 114(4.1.2)
$\overline{ab}$, 282
$\alpha(n)$, 177
$\alpha(G)$, 324(10.4.2)
$\alpha(P)$, 64

δp, 394
$\delta(.)$, 229(cv. 2)
Δ_X, 46
$\chi(.)$, 222(6.8.2)
$\kappa(.)$, 259
$\Omega(.)$, 87
$\omega(G)$, 332
$\omega(P)$, 65
π, viz Ludolfovo číslo
$\Theta(.)$, 87

A_G, 121(4.2.3)
abelovská grupa, 403
acyklická relace, 56(cv. 2)
algebra lineární (aplikace), 268–277, 290–293, 377–397
algoritmus
— Borůvkův, 182(5.4.3)
— Dijkstrův, 124–129
— — s heuristikou, 128
— hladový, 172(5.3.3), 177, 179(cv. 10), 179(cv. 11), 179(cv. 12)
— Jarníkův, 180(5.4.1)
— Kruskalův, 172(5.3.3)
— Primův, viz Jarníkův algoritmus
— prohledávání do šířky, 129(cv. 5)
— QUICKSORT, 327–329
— třídicí, 75(cv. 4), 327–329
antiřetězec, 64, 246
antisymetrická relace, 44(1.6.1)
anuloid, 231
aritmetický průměr, 87
asociativní (operace), 29, 402
asymetrický graf, 117(cv. 4)
asymetrický strom, 169(cv. 1)
automorfismus
— grafu, 117(cv. 4)
— uspořádané množiny, 249, 252(cv. 6)
axiom, výměnný, 178(cv. 5)

$\mathcal{B}_n$, 63
barevnost grafu, 222(6.8.2), 229(cv. 2)
— výběrová, 230(cv. 10)
báze, 405
Bellovo číslo, 109(cv. 7)
Bernoulliho nerovnost, 93
Bertrandův postulát, 98
bezprostřední předchůdce, 54
bijekce, 42
binární operace, 402
binární strom, 360–362
Binetova-Cauchyho věta, 274(8.5.4)
binomická věta, 79
— kombinatorický význam, 343
— zobecněná, 350(12.2.5), 362
binomický koeficient, viz kombinační číslo
bipartitní graf, 114, 124(cv. 3), 278(cv. 3), 322(10.4.1)
— úplný, 114
blokové schéma, 377–385
bod
— projektivní roviny, 282(9.1.1)
— v nekonečnu, 282
Bonferroniho nerovnosti, 104
booleovská funkce, 302, 307(cv. 2)
Borůvkův algoritmus, 182(5.4.3)
Brouwerova věta, 240(7.1.3), 244(cv. 2)

$\mathcal{C}$, 390, 394
C_n, 113
$C(G)$, 168
$\mathcal{C}_n$, 310(10.2.2)

Catalanovo číslo, 362–363
Cauchyho-Schwarzova nerovnost, 254(7.3.2), 256(cv. 4)
celá čísla, 24
centroid (stromu), 170(cv. 6)
centrum grafu, viz střed grafu
cesta, 113, 118
— jednoznačnost pro strom, 162(5.1.4)
— nejkratší, 124–129
cirkulace, 393
cyklomatické číslo, 392
cyklus, 143
— permutace, 74, 322

časová složitost, 175
částečné uspořádání, 52, 246
částečné zlomky, 355
číslo
— Bellovo, 109(cv. 7)
— Catalanovo, 362–363
— celé, 24
— cyklomatické, 392
— dokonalé, 110(cv. 10)
— Eulerovo, 89
— Fibonacciho, 354–356
— harmonické, 94(cv. 12)
— kombinační, 76–85, 343, 345, 345(cv. 5)
— — odhad, 94–98
— — zobecněné, 350(12.2.5)
— Ludolfovo, 92
— — výpočet, 93(cv. 7)
— přirozené, 24
— racionální, 24
— Ramseyovo, 335
— reálné, 24
čtvercová matice, 400
čtverec latinský, 294–298

$d_G(.,.)$, 121
$d_{G,w}(.,.)$, 125
De Bruijnův graf, 146
de Moivreova věta, 33(cv. 4), 373
de Morganovy vzorce, 30
$\deg_G(.)$, 129
$\deg^+_G(.)$, 144
$\deg^-_G(.)$, 144
dělení
— grafu, 149(4.7.2)
— hrany, 149(4.7.2)
determinant, 400
— rozvoj, 401
diagonála, 46, 400
diagonální matice, 400
diagram
— Ferrersův, 369
— Hasseův, 55
diference (funkce), 357
diferenční rovnice, 356–359
Dijkstrův algoritmus, 124–129
— s heuristikou, 128
Dilworthova věta, 68(cv. 7)
dimenze, 405
— uspořádané množiny, 67
Dirichletův princip, 333(11.1.2)
disjunktní množiny, 28
distributivní (operace), 29, 403
dobré uspořádání, 32
dokonalé číslo, 110(cv. 10)
dominující množina, 179(cv. 12)
duál (geometrický), 223(6.8.3)
dualita, 287, 293
duální množinový systém, 287
Dushnikova-Millerova dimenze, 67
2-obarvení, 299(9.4.1), 304–306, 307(cv. 3)
dvojice

— neuspořádaná, 34
— uspořádaná, 35
2-souvislý graf, 148–153
— kritický, 153(cv. 2)

e, 89
E, 318(10.3.6)
$E(G)$, 112
ekvivalence, 46(1.6.2)
— počet, 109(cv. 7)
— třída, 47
— udržování, 176(5.3.6), 179(cv. 9)
elementární jev, 309
elementární kružnice, 390
elementární řádková operace, 401
Erdősovo-Szekeresovo lemma, 66(2.4.6)
Erdős, Paul, 331
Eulerova funkce, 107–108, 109(cv. 8)
Eulerovo číslo, 89
eulerovská množina, 389(13.4.1)
— počet, 392(13.4.4)
eulerovský graf, 135–147, 189(cv. 2)
eulerovský tah, 135
Eulerův vzorec, 203(6.4.1)
— pro strom, 162(5.1.4)
excentricita, viz výstřednost
$\mathrm{ex}_G(.)$, 168
extremální teorie, 156, 253, 323

faktoriál, 74
— dělitelnost, 75(cv. 5)
— odhad, 87–92, 93(cv. 8)
Fanova rovina, 283, 298(cv. 1)
Ferrersův diagram, 369
Fibonacciho čísla, 354–356
Fisherova nerovnost, 383(13.2.1)
formule
— Leibnizova, 83(cv. 11)
— logická, 302, 307(cv. 2)
— Stirlingova, 92
funkce, 40(1.5.1)
— bijektivní, 42
— booleovská, 302, 307(cv. 2)
— Eulerova, 107–108, 109(cv. 8)
— graf (orientovaný), 264, 264(cv. 1), 264(cv. 3)
— charakteristická, 71
— identická, 44(cv. 3)
— injektivní, 42
— konvexní, 256(cv. 5)
— monotonní, 82(cv. 6)
— na, 42(1.5.3)
— — počet, 109(cv. 6)
— perioda, 264(cv. 3)
— počet, 69(3.1.1)
— prostá, 42(1.5.3)
— — počet, 71(3.1.4)
— skládání, 41
— spojitá, 240
— surjektivní, 42
— vytvořující, 341–375
— — operace s, 347–350
— — posloupnosti, 347(12.2.2)
— vzájemně jednoznačná, 42(1.5.3)

$GF(q)$, 403
$\mathcal{G}_n$, 312(10.2.6)
geometrický průměr, 87
graf, 111(4.1.1)
— barevnost, 222(6.8.2), 229(cv. 2)
— bez $K_{2,2}$, 253, 299
— bez $K_{2,t}$, 256(cv. 1)
— bez $K_{3,3}$, 257(cv. 6)
— bez trojúhelníků, 154–157, 329(cv. 1)
— bipartitní, 114, 124(cv. 3), 278(cv. 3), 322(10.4.1)
— De Bruijnův, 146
— duální, 223(6.8.3)
— 2-souvislý, 148–153
— — kritický, 153(cv. 2)
— eulerovský, 135–147, 189(cv. 2)
— funkce (orientovaný), 264, 264(cv. 1), 264(cv. 3)
— Heawoodův, 287
— incidence, 287, 299
— isomorfismus, 114(4.1.2)
— k-souvislý
— — hranově, 147
— — vrcholově, 147
— náhodně eulerovský, 141(cv. 6)
— náhodný, 312(10.2.6), 316(cv. 1), 316(cv. 2)
— nakreslení, 191(6.2.2)
— obarvení, 222(6.8.2)
— orientace, 272
— orientovaný, 143(4.6.1)
— počet, 110(cv. 12), 115
— poloměr, 124(cv. 6)
— pravidelný, viz regulární graf
— průměr, 124(cv. 6)
— regulární, 134(cv. 10)
— rovinný, 187–231, 238, 244(cv. 1)
— — maximální, 208
— — počet hran, 204(6.5.1)
— — skóre, 212(cv. 7)
— s násobnými hranami, 139
— se smyčkami, 139
— silně souvislý, 144(4.6.2)
— slabě souvislý, 144(4.6.2)
— souvislý, 119
— strnulý, viz asymetrický graf
— úplný, 113
— úplný bipartitní, 114
— úplný k-partitní, 158(cv. 4)
— vnějškově rovinný, 229(cv. 3)
— výběrové obarvení, 230(cv. 10)
— vyvážený, 144
— znázornění, 112
Grahamova-Pollakova věta, 386(13.3.2)
Grötschova věta, 229(cv. 4)
grupa, 402

hamiltonovská kružnice, 138, 141(cv. 5)
harmonické číslo, 94(cv. 12)
harmonický průměr, 93(cv. 5)
Hasseův diagram, 55
Heawoodův graf, 287
Heawoodův vzorec, 236
heuristika, 128
HEX (hra), 242
hladový algoritmus, 172(5.3.3), 177, 179(cv. 10), 179(cv. 11), 179(cv. 12)
hodnost matice, 384, 406
hodnota střední, 318
horní trojúhelníková matice, 400
hrana, 111(4.1.1)
— násobná, 139
— orientovaná, 143(4.6.1)
hranice, 195(6.3.1)
hranově k-souvislý graf, 147
hypergraf, 377

charakteristická funkce, 71
charakteristický polynom, 357

I_n, 124(cv. 7), 387, 400
identita, 44(cv. 3)
indikátor, 319(10.3.7)

indukce
— matematická, 31
— úplná, viz matematická indukce
indukční krok, 32
indukční předpoklad, 32
indukovaný podgraf, 118(4.2.1)
infimum, 61(cv. 9)
injektivní funkce, 42
inkluze a exkluze, 99–105
— aplikace, 105–110
inverze permutace, 75(cv. 4)
inverzní relace, 46
isomorfismus
— grafů, 114(4.1.2)
— relací, 50(cv. 8)
— stromů, 164–169
— uspořádaných množin, 57(cv. 4), 249

J_n, 387
jádro, 406
Jarníkův algoritmus, 180(5.4.1)
jednotková matice, 400
jev, 309
— elementární, 309
jevy nezávislé, 314–315
Jordanova věta, 195(6.3.1)

$\mathcal{K}_G$, 388
K_n, 113
$K_{n,m}$, 114
k-graf, 377
kartézský součin, 35
k-souvislost, 147
Kleinova láhev, 232
kód stromu, 164
— Prüferův, 265
koeficient
— binomický, viz kombinační číslo
— multinomický, 81
kolmé vektory, 400
kombinační číslo, 76–85, 343, 345, 345(cv. 5)
— odhad, 94–98
— zobecněné, 350(12.2.5)
kompaktnost, 241
komponenta
— obloukové souvislosti, 195
komponenta grafu, 120
komutativní (operace), 29, 402
koncový vrchol, 160(5.1.2)
konečná projektivní rovina, 281–300, 381
— definice, 281(9.1.1), 288(cv. 2), 289(cv. 5), 382(cv. 1)
— existence, 289–290
— řád, 285(9.1.4)
konečný pravděpodobnostní prostor, 308(10.2.1)
konfigurace taktická, 380
kontrakce hrany, 227
konvexní
— funkce, 256(cv. 5)
— těleso, 214
kořen stromu, 164
kostra, 390
— maximální, 178(cv. 2)
— minimální, 170–185
— počet, 259–280
kritický 2-souvislý graf, 153(cv. 2)
krok indukční, 32
Kruskalův algoritmus, 172(5.3.3)
kružnice, 113
— elementární, 390
— hamiltonovská, 138, 141(cv. 5)
— topologická, 195
— v grafu, 119

Kuratowského věta, 219(6.7.1)

láhev Kleinova, 232
Laplaceova matice, 268, 277(cv. 1)
latinské čtverce, ortogonální, 295
latinský čtverec, 294–298
latinský obdélník, 298(cv. 6)
Leibnizova formule, 83(cv. 11)
lemma
— Erdősovo-Szekeresovo, 66(2.4.6)
— Spernerovo, 238(7.1.1), 244(cv. 2)
levé maximum, 318(10.3.4), 321
lexikografické uspořádání, 52, 167
linearita střední hodnoty, 320(10.3.9)
lineární algebra (aplikace), 268–277, 290–293, 360(cv. 8), 377–397
lineární rozšíření, 57
lineární uspořádání, 46(1.6.2)
lineární závislost, 404
lineární zobrazení, 406
list, viz koncový vrchol
— Möbiův, 231
Littlewoodův-Offordův problém, 252(cv. 7)
logická formule, 302, 307(cv. 2)
lomenice, 193
Ludolfovo číslo, 92
— výpočet, 93(cv. 7)

mapa (obarvení), 220–231
matematická indukce, 31
matice, 399
— diagonální, 400
— incidence, 272, 278(cv. 3), 383
— jednotková, 400
— Laplaceova, 268, 277(cv. 1)
— násobení, 123(4.2.5), 399
— permutační, 124(cv. 8)
— pozitivně definitní, 385(cv. 4)
— regulární, 402
— singulární, 402
— sousednosti
— — grafu, 121(4.2.3)
— — relace, 37
— transponovaná, 272, 400
— trojúhelníková, 400
— unimodulární, 278(cv. 3)
matroid, 177, 397
maximální kostra, 178(cv. 2)
maximální prvek, 57(2.2.2)
maximum levé, 318(10.3.4), 321
metrika grafu, 121, 124(cv. 5)
minimální kostra, 170–185
minimální prvek, 57(2.2.2)
minor, 219, 230(cv. 9)
mnohočlen charakteristický, 357
mnohostěn pravidelný, 214
množina
— částečně uspořádaná, 52
— dominující, 179(cv. 12)
— nezávislá, 64(2.4.1), 323, 333
— prázdná, 27
— uspořádaná, 51
množinový systém, 27
— 2-obarvitelný, 299(9.4.1), 304–306, 307(cv. 3)
— duální, 287
Möbiův list, 231
mocninná řada, 345–347, 354(cv. 10)
monotonní funkce (počet), 82
monotonní posloupnost, 66
multigraf, 139
multinomická věta, 81(3.3.4),

262, 345(cv. 3)
multinomický koeficient, 81

N, 24
náhodná permutace, 310(10.2.3), 314, 322, 324, 328
náhodná procházka, 366–368
náhodná veličina, 317(10.3.1)
náhodně eulerovský graf, 141(cv. 6)
náhodný graf, 312(10.2.6), 316(cv. 1), 316(cv. 2)
nakreslení grafu, 191(6.2.2)
násobení matic, 123(4.2.5), 399
násobné hrany, 139
nejkratší cesta, 124–129
nejmenší prvek, 59(2.2.4)
největší prvek, 59(2.2.4)
neomezená stěna, 202
nerovnost
— Bernoulliho, 93
— Bonferroniho, 104
— Cauchyho-Schwarzova, 254(7.3.2), 256(cv. 4)
— Fisherova, 383(13.2.1)
neuspořádaná dvojice, 34
nezávislá množina, 64(2.4.1), 323, 333
nezávislé jevy, 314–315
nezávislost, lineární, 405
nezávislý systém množin, 245
nosič, 394

$o(.)$, 87
$O(.)$, 86
obarvení
— grafu, 222(6.8.2)
— mapy, 220–231
obdélník latinský, 298(cv. 6)
oblouk, 191(6.2.1)
oblouková souvislost, 195
obratlovec, 262
odhad
— faktoriálu, 87–92, 93(cv. 8)
— kombinačního čísla, 94–98
omezená stěna, 202
operace, binární, 402
orientace grafu, 147(cv. 4), 272
orientovaná hrana, 143(4.6.1)
orientovaný graf, 143(4.6.1)
orientovaný tah, 143
ortogonální latinské čtverce, 295
otec (v kořenovém stromu), 164

$P(.)$, 308(10.2.1)
p_n, 369
P_n, 113
$\mathcal{P}(X)$, 27
parciální zlomky, 355
párování, 179(cv. 10)
Pascalův trojúhelník, 79
perioda funkce, 264(cv. 3)
permutace, 72–75
— cyklus, 74, 322
— inverze, 75(cv. 4)
— levé maximum, 318(10.3.4), 321
— náhodná, 310(10.2.3), 314, 322, 324, 328
— pevný bod, 105, 109(cv. 4), 109(cv. 5), 322(cv. 3)
— rostoucí úseky, 74(cv. 3)
— řád, 74(cv. 2)
— znaménko, 275, 400
permutační matice, 124(cv. 8)
pěstovaný strom, 164
pevný bod permutace, 105, 109(cv. 4), 109(cv. 5), 322(cv. 3)
platónská tělesa, 214
počet

— binárních stromů, 360–362
— dělitelů, 110(cv. 10)
— ekvivalencí, 109(cv. 7)
— eulerovských množin, 392(13.4.4)
— funkcí, 69(3.1.1)
— funkcí na, 109(cv. 6)
— grafů, 110(cv. 12), 115
— — neisomorfních, 116
— hran rovinného grafu, 204(6.5.1)
— koster, 259–280
— — obecného grafu, 268(8.5.1)
— — s daným skóre, 260(8.2.1)
— — úplného grafu, viz počet stromů
— latinských obdélníků, 298(cv. 6)
— monotonních funkcí, 82(cv. 6)
— neuspořádaných k-tic, 83(cv. 14)
— podmnožin, 70(3.1.2), 76(3.3.2), 83(cv. 13)
— — liché velikosti, 71(3.1.3), 80
— prostých funkcí, 71(3.1.4)
— rozkladů čísla n, 368–375
— rozmístění kuliček, 77, 84(cv. 15)
— řešení rovnice, 77, 342
— seřazení, 81
— stromů, 259(8.1.1)
— — neisomorfních, 170(cv. 5), 260(cv. 1)
— triangulací mnohoúhelníka, 84(cv. 19), 363(cv. 5)
— uspořádaných k-tic, 83(cv. 14)
počítání dvěma způsoby, 77, 237–257, 289(cv. 5), 329, 380
podgraf, 118(4.2.1)
— indukovaný, 118(4.2.1)
podmatice, 402
podmínky celočíselnosti, 380(13.1.6)
podmnožiny, počet, 70(3.1.2), 76(3.3.2), 83(cv. 13)
podposloupnost, 66
podprostor, 405
podtěleso, 403
poloměr grafu, 124(cv. 6)
polynom charakteristický, 357
posloupnost
— monotonní, 66
— stupňů, viz skóre grafu
postulát Bertrandův, 98
potenciál, 147(cv. 5), 394
potenciálový rozdíl, 394
pozitivně definitní matice, 385(cv. 4)
pravděpodobnost, 75(cv. 3), 88, 105, 110(cv. 11), 301–330, 337–339, 365–368
pravděpodobnostní prostor
— konečný, 308(10.2.1)
— nekonečný, 310
pravidelný graf, viz regulární graf
pravidelný mnohostěn, 214
prázdná množina, 27
prázdná suma, 28
prázdný součin, 28
Primův algoritmus, viz Jarníkův algoritmus
princip
— Dirichletův, 333(11.1.2)
— duality, 287
— inkluze a exkluze, 99–105
— — aplikace, 105–110
— sudosti, 130
— — aplikace, 238–244,

244(cv. 1)
problém
— čtyř barev, 221
— Littlewoodův-Offordův, 252(cv. 7)
— maximální kostry, 178(cv. 2)
— minimální kostry, 172(5.3.2)
— Sylvesterův, 213(cv. 10)
— šatnářky, 105–106
— — rekurence, 108(cv. 1), 109(cv. 2)
prohledávání do šířky, 129(cv. 5)
procházka náhodná, 366–368
projekce stereografická, 215
projektivní rovina
— dualita, 287, 293
— konečná, 281–300, 381
— — definice, 281(9.1.1), 288(cv. 2), 289(cv. 5), 382(cv. 1)
— — existence, 289–290
— — řád, 285(9.1.4)
— konstrukce, 290–293, 296–297
— reálná, 282, 290
prostá funkce, 42(1.5.3)
— počet, 71(3.1.4)
prostor
— cyklů, viz prostor kružnic
— kružnic, 390(13.4.3), 394
— pravděpodobnostní
— — konečný, 308(10.2.1)
— — nekonečný, 310
— řezů, 395
— vektorový, 404
průměr
— aritmetický, 87
— geometrický, 87
— grafu, 124(cv. 6)
— harmonický, 93(cv. 5)
průnik, 28
průsečík úrovně k, 325–327, 330(cv. 4)
prvek
— maximální, 57(2.2.2)
— minimální, 57(2.2.2)
— nejmenší, 59(2.2.4)
— největší, 59(2.2.4)
prvočíselná věta, 98(3.5.3)
Prüferův kód, 265
předchůdce bezprostřední, 54
předpoklad indukční, 32
přímka
— projektivní roviny, 282(9.1.1)
— v nekonečnu, 282
přirozená čísla, 24

QUICKSORT, 327–329

$\mathcal{R}$, 395
$\mathbf{R}$, 24
$r(A)$, 384, 406
$r(k, \ell)$, 335
racionální čísla, 24
Ramseyova věta, 334(11.2.1)
— pro p-tice, 336(cv. 6)
Ramseyovo číslo, 335
reálná čísla, 24
reálná projektivní rovina, 282, 290
reflexivní relace, 44(1.6.1)
regulární graf, 134(cv. 10)
regulární matice, 402
rekurence, 357
relace, 36(1.4.2)
— acyklická, 56(cv. 2)
— antisymetrická, 44(1.6.1)
— inverzní, 46
— reflexivní, 44(1.6.1)
— rekurentní, 357

— skládání, 38
— symetrická, 44(1.6.1)
— transitivní, 44(1.6.1), 75(cv. 4)
rod grafu, 236(6.9.2)
rostoucí úseky permutace, 74(cv. 3)
rovina
— Fanova, 283
— projektivní, viz projektivní rovina
rovinné nakreslení, 192(6.2.2)
rovinný graf, 187–231, 238, 244(cv. 1)
— maximální, 208
— počet hran, 204(6.5.1)
— skóre, 212(cv. 7)
rovnice diferenční, 356–359
rozdíl symetrický, 389
rozklad
— čísla n, 368–375
— — uspořádaný, 368, 374(cv. 1)
rozklad (množiny), 49
rozšíření, lineární, 57
rozvoj determinantu, 401

řád
— latinského čtverce, 294
— permutace, 74(cv. 2)
— projektivní roviny, 285(9.1.4)
řada mocninná, 345–347, 354(cv. 10)
řádková operace, elementární, 401
řetězec, 60(cv. 2), 65(2.4.4), 246
— symetrický, 248
řez, 395
— zlatý, 355, 368

S_n, 106
$\mathcal{S}_n$, 310(10.2.3)
sféra s ušima, 232
$\operatorname{sgn}(\pi)$, 275, 400
schéma blokové, 377–385
silně souvislý graf, 144(4.6.2)
singulární matice, 402
síť, 171
sjednocení, 28
skalární součin, 400
skládání
— funkcí, 41
— relací, 38
skóre
— grafu, 129–133
— rovinného grafu, 212(cv. 7)
— stromu, 164(cv. 6)
slabě souvislý graf, 144(4.6.2)
sled, 122
složitost časová, 175
smyčka, 139
součin
— kartézský, 35
— prázdný, 28
— skalární, 400
souvislost
— silná, 144(4.6.2)
— slabá, 144(4.6.2)
souvislý graf, 119
Spernerova věta, 245(7.2.1)
Spernerovo lemma, 238(7.1.1), 244(cv. 2)
spojitá funkce, 240
Steinerův strom, 171
Steinerův systém, 378(13.1.5), 381(13.1.7), 382(cv. 3)
Steinitzova věta, 218
stěna (mnohostěnu), 216
stěna (rovinného grafu), 202
stereografická projekce, 215
Stirlingova formule, 92
strnulý graf, viz asymetrický graf

strom, 160(5.1.1)
— asymetrický, 169(cv. 1)
— binární, 360–362
— kód, 164
— kořenový, 164
— pěstovaný, 164
— počet, 170(cv. 5), 259(8.1.1), 260(cv. 1)
— Steinerův, 171
střed grafu, 168
střední hodnota, 317–330, 365
— definice, 318(10.3.6)
— linearita, 320(10.3.9)
stupeň vrcholu, 129
— vstupní, 144
— výstupní, 144
suma prázdná, 28
supremum, 61(cv. 9)
surjektivní funkce, 42
Sylvesterův problém, 213(cv. 10)
sym(.), 144
symetrická relace, 44(1.6.1)
symetrický rozdíl, 389
symetrický řetězec, 248
symetrizace, 144
syn (v kořenovém stromu), 164
systém množin, 27
— 2-obarvení, 299(9.4.1), 304–306, 307(cv. 3)
— duální, 287
— nezávislý, 245
systém Steinerův, 378(13.1.5), 381(13.1.7), 382(cv. 3)

šatnářka, 105
šipka (v grafu), 143(4.6.1)

tah, 135
— eulerovský, 135
— orientovaný, 143
taktická konfigurace, 380
těleso, 403
těleso platónské, 214
topologické třídění, 59
torus, 231
transitivní relace, 44(1.6.1), 75(cv. 4)
transponovaná matice, 272, 400
triangulace, 208
triangulace mnohoúhelníka (počet), 84(cv. 19), 363(cv. 5)
trojúhelníková matice, 400
třída ekvivalence, 47
třídění topologické, 59
třídicí algoritmus, 75(cv. 4), 327–329
Turánova věta, 158(cv. 5), 324(10.4.2)
turnaj, 315

udržování ekvivalence, 176(5.3.6), 179(cv. 9)
unimodulární matice, 278(cv. 3)
UNION-FIND, 176(5.3.6), 179(cv. 9)
úplná indukce, viz matematická indukce
úplné uspořádání, viz lineární uspořádání
úplný bipartitní graf, 114
úplný graf, 113
úplný k-partitní graf, 158(cv. 4)
uspořádaná dvojice, 35
uspořádaná množina, 51
— automorfismus, 249, 252(cv. 6)
— isomorfismus, 57(cv. 4), 249
uspořádání, 46(1.6.2)
— částečné, 52, 246
— dobré, 32
— lexikografické, 52, 167

— lineární, 46(1.6.2)
— úplné, viz lineární uspořádání
uzel (grafu), viz vrchol

$V(G)$, 112
váha hrany, 171
variace bez opakování, 72
vektorový prostor, 404
vektory, kolmé, 400
veličina náhodná, 317(10.3.1)
věta
— Binetova-Cauchyho, 274(8.5.4)
— binomická, 79
— — kombinatorický význam, 343
— — zobecněná, 350(12.2.5), 362
— Brouwerova, 240(7.1.3), 244(cv. 2)
— de Moivreova, 33(cv. 4), 373
— Dilworthova, 68(cv. 7)
— Grötschova, 229(cv. 4)
— Grahamova-Pollakova, 386(13.3.2)
— Jordanova, 195(6.3.1)
— Kuratowského, 219(6.7.1)
— multinomická, 81(3.3.4), 262, 345(cv. 3)
— o čtyřech barvách, 221
— o pěti barvách, 225(6.8.5)
— o pevném bodě, 239(7.1.2), 240(7.1.3), 244(cv. 3)
— o skóre, 131(4.4.3)
— prvočíselná, 98(3.5.3)
— Ramseyova, 334(11.2.1)
— — pro p-tice, 336(cv. 6)
— Spernerova, 245(7.2.1)
— Steinitzova, 218
— Turánova, 158(cv. 5), 324(10.4.2)
— Wilsonova, 382(13.1.9)
vnější stěna, 202
vnějškově rovinný graf, 229(cv. 3)
vnitřní stěna, 202
vnoření uspořádaných množin, 61(2.3.1)
vrchol, 111(4.1.1)
— koncový, 160(5.1.2)
vrcholově k-souvislý graf, 147
vstupní stupeň, 144
výběrová barevnost, 230(cv. 10)
výměnný axiom, 178(cv. 5)
výstřednost, 168
výstupní stupeň, 144
vytvořující funkce, 341–375
— operace s, 347–350
— posloupnosti, 347(12.2.2)
vyvážený graf, 144
vzájemně jednoznačná funkce, 42(1.5.3)
vzdálenost v grafu, 121
vzorec
— de Morganův, 30
— Eulerův, 203(6.4.1)
— — pro strom, 162(5.1.4)
— Heawoodův, 236

Wilsonova věta, 382(13.1.9)

Z, 24
závislost, lineární, 404
zlatý řez, 355, 368
zlomky parciální, 355
znaménko permutace, 275, 400
zobecněná binomická věta, 350(12.2.5), 362
zobrazení, viz funkce
— lineární, 406



Návody ke cvičením

1.2.2(b). $\lfloor \log_{10} n \rfloor + 1$.

1.2.3. Označíme-li pravou stranu m, je celé číslo m určeno vztahy $m^2 \leq \lfloor x \rfloor < (m+1)^2$. To platí, právě když $m = \lfloor \sqrt{x} \rfloor$.

1.2.5(d). Viz část 12.4, cvičení 3.

1.3.3(a). Přidáním další přímky k n přímkám bude právě $n+1$ oblastí rozříznuto na 2.

1.3.3(b). V indukčním kroku použijte (a). Vyjde $(n^3 + 5n + 6)/6$.

1.3.5. Definujte $x_1 = \min(M)$, $x_{i+1} = \min(M \setminus \{x_1, \ldots, x_i\})$. Kdyby M byla nekonečná, nemá podmnožina $\{x_1, x_2, \ldots\}$ největší prvek.

1.3.7. Ukažte, že čitatel se každým krokem zmenší.

1.4.3(a). Existuje jen konečně mnoho relací na X.

1.4.3(c). Vezměte $(\mathbf{N}, <)$.

2.1.2. Definujte relaci $S = \{(x,x);\, x \in X\} \cup R \cup R \circ R \cup R \circ R \circ R \cup \ldots$, dokažte že je to uspořádání.

2.1.3. Např. pro množinu všech racionálních čísel je relace bezprostředního předchůdce prázdná.

2.1.4(b). Konečná lineárně uspořádaná množina má největší prvek. Zobrazte největší prvek na největší prvek, a pokračujte indukcí.

2.1.4(d). Nespočetně: Rozdělte $\mathbf{N}$ na spočetně mnoho disjunktních podmnožin $A_1, A_2, \ldots$. Každou A_i uspořádejte buď jako přirozená čísla, nebo jako záporná celá čísla; potom dejte tyto množiny za sebe v pořadí $A_1, A_2, \ldots$.

2.2.9(c). Ukažte, že pro $A \subseteq X$ je $\inf A = \sup\{x \in X;\, x \leq a \,\forall a \in A\}$.

2.4.7. Indukcí dle $|X|$. Nechť x je minimální prvek a y maximální prvek s $x \prec y$ (neexistují-li, je X nezávislá množina). Buď A největší nezávislá množina v $X \setminus \{x, y\}$. Pokud $|A| < \alpha$, použijeme indukční předpoklad. Jinak

rozložíme množiny $\{t \in X;\ \exists a \in A : t \le a\}$ a $\{t \in X;\ \exists a \in A : t \ge a\}$ každou na α řetězců a tyto řetězce napojíme přes prvky z A.

3.1.1. Kódujte dvojici (A, B) zobrazením do množiny $\{0, 1, 2\}$: prvek $x \in A$ dostane 2, $x \in B \setminus A$ dostane 1, a $x \notin B$ 0.

3.1.2(b). První sloupec zvolme jako libovolný nenulový vektor. Druhý sloupec nesmí být násobkem prvního, tím se vylučuje q vektorů. Třetí sloupec nesmí být lineární kombinací prvních dvou, tím se pro něj vylučuje q^2 možností (žádné 2 různé lineární kombinace prvních dvou sloupců nedají týž vektor – ověřte!); obecně pro i-tý sloupec je $q^n - q^i$ možností.

3.2.1. $(n-1)!$.

3.2.2. Uvažte cykly permutace. Jaký je řád permutace s jediným cyklem délky k? S dvěma cykly délky k_1 a k_2?

3.2.3(a). Ukažte, že napíšeme-li permutaci s k úseky pozpátku, dostaneme permutaci s $n+1-k$ úseky.

3.2.3(b). Uvažte permutaci čísel $\{1, 2, \ldots, n-1\}$ s k úseky (v jednořádkovém zápisu), a vložte do ní číslo n na některou z možných $n+1$ pozic. Pro kolik pozic bude mít výsledná permutace $k+1$ úseků, a pro kolik k?

3.2.3(c). Obecný vzorec, odvozený Eulerem, je
$f(n,k) = \sum_{j=0}^{k} (-1)^j (k-j)^n \binom{n+1}{j}$.

3.2.3(d). Rozdělte permutace do tříd podle množiny čísel na prvních $k+1$ místech. Všechna pořadí prvních $k+1$ čísel jsou stejně pravděpodobná. Která z možných rozestavení prvních $k+1$ čísel dávají počáteční úsek délky k? Pravděpodobnost vyjde $k/(k+1)!$.

3.2.4(b). Jsou-li na počátku čísla srovnána podle permutace π, jednou výměnou sousedů ubude nanejvýš 1 inverze.

3.2.5(b). Kolik z čísel $1, 2, \ldots, n$ je dělitelných p^j pro dané j? Vyjde $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$.

3.3.2(b). Pravá strana je počet $(r+2)$-tic nezáporných celých čísel řešících rovnici $X_1 + X_2 + \cdots + X_{r+2} = n - r$. Rozdělte tyto $(r+2)$-tice na $n-r$ skupin podle hodnoty X_{r+2} a spočítejte počet řešení v každé skupině zvlášť, tím se dostane levá strana.

3.3.3. Upravte k-tý člen na $\binom{n}{m}\binom{n-m}{n-k}$, $\binom{n}{m}$ vytkněte. Vyjde $\binom{n}{m}2^{n-m}$.

3.3.4(a). Užijte $\frac{1}{k}\binom{k}{m} = \frac{1}{m}\binom{k-1}{m-1}$ a vzorec (3.9).

3.3.4(b). Tentokrát $k\binom{k}{m} = (k+1)\binom{k}{m} - \binom{k}{m} = (m+1)\binom{k+1}{m+1} - \binom{k}{m}$.

3.3.5. Buď M nějaká m-prvková množina, N n-prvková. Obě strany počítají počet uspořádaných dvojic (X, Y), kde $X \subseteq M$, $Y \subseteq N \cup X$, $|Y| = m$. Pro levou stranu vybereme napřed X, pak Y, pro pravou nejdřív $Y \cap M$, pak $Y \cap N$, nakonec X.

3.3.6. Položme $k_i = f(i+1) - f(i)$, $i = 0, 1, \ldots, n$, kde uměle dodefinujeme $f(0) = 1$, $f(n+1) = n$. Hledaný počet je počet celých nezáporných řešení rovnice $k_0 + \cdots + k_n = n - 1$.

3.3.8. Uvažme k-tici $\{a_1, \ldots, a_k\}$, $a_1 < \cdots < a_k$. Přiřaďme jí k-tici $\{a_1, a_2 - 1, a_3 - 2, \ldots, a_k - k + 1\}$. To je bijekce na $\binom{\{1,2,\ldots,n-k+1\}}{k}$.

3.3.9(c). Počítejte plochu velkého čtverce dvěma způsoby. Jeho strana je $2(1 + 2 + 3 + \cdots + n)$. Přitom k-tá "vrstva" (od středu) má $4k$ čtverečků $k \times k$.

3.3.11. Postupujte třeba indukcí podle n.

3.3.12(b). Ve vzorci pro binomický koeficient, právě 1 z činitelů v čitateli je dělitelný p. Tedy $\binom{n}{p}$ je dělitelné p právě když tento činitel je dělitelný i p^2.

3.3.13(a). Dosaďte postupně do binomické věty $x = 1$, $x = -1$, $x = \mathrm{i}$ a $x = -\mathrm{i}$ (i značí imaginární jednotku) a výsledné rovnice sečtěte. Upravte n-té mocniny pomocí de Moivreova vzorce. Pro hledaný počet vyjde podivuhodná formule $2^{n-2} + 2^{n/2-1} \cos \frac{\pi n}{4}$. Ověřte správnost pro malé hodnoty n.

3.3.13(b). Postupujte podobně jako v (a), ale do binomické věty dosazujte za x všechny 3 kořeny rovnice $x^3 = 1$.

3.3.16. Nejdřív rozestavte čarodějnice, tím je určeno 8 možných pozic pro vodníky, vyberte 5 z nich, a nakonec určete pořadí vodníků.

3.3.18. Nejprve zvolte zastoupené státy, pak pro každý určete jednoho ze 2 senátorů.

3.3.19. Vyjděte z trojúhelníku T_0 který má 2 strany na obvodu n-úhelníka, zvolte k němu přiléhající trojúhelník T_1, T_2 přiléhající k T_1, ... Pro T_0 je n možností, v každém dalším kroku jsou 2 možnosti. Přitom každou triangulaci dostaneme $2\times$ (pro T_0 jsou 2 možnosti). Vyjde $n2^{n-5}$ (pro $n \ge 4$).

3.3.21(a). Levá strana je počet seřazení n předmětů, k_i předmětů i-tého druhu. Pravá strana: nejdříve zvolíme druh předmětu na první pozici, pak rozestavíme zbývající předměty.

3.4.3. Napřed upravte všechny funkce na tvar $e^{f(n)}$.

3.4.4. Přímka $y = x + 1$ je tečnou ke grafu funkce e^x v bodě $(0, 1)$. Dále funkce e^x je konvexní, poněvadž má nezápornou druhou derivaci, a proto nemůže svoji tečnu protínat jinde než v bodě dotyku.

3.4.6(b). Označme $A = (x_1 + x_2 + \cdots + x_{n-1})/(n-1)$. Podle $AG(n)$ aplikovaného na čísla $x_1, \ldots, x_{n-1}$ a A máme $A^n = ((x_1 + x_2 + \cdots + x_{n-1} + A)/n)^n \ge x_1 x_2 \cdots x_{n-1} A$, a odtud po úpravě $A \ge (x_1 \cdots x_{n-1})^{1/(n-1)}$.

3.4.9. Funkce $\ln x$ je konkávní, speciálně každý trojúhelníček s vrcholy v bodech $(i, \ln i)$, $(i+1, \ln i)$ a $(i+1, \ln(i+1))$ leží celý pod jejím grafem (nakreslete si). Jeho plocha je $(\ln(i+1) - \ln i)/2$. Proto $\ln n! \le \ln n + \int_1^n \ln x \,\mathrm{d}x - \frac{1}{2}\sum_{i=1}^{n-1}(\ln(i+1) - \ln i)$; upravte.

3.4.10. Indukcí podle n.

3.4.11. Dolní odhad: indukcí, dokazujte $2(\sqrt{n} - \sqrt{n-1}) \le 1/\sqrt{n+1}$, levou stranu upravte na zlomek se jmenovatelem $\sqrt{n} + \sqrt{n-1}$. Horní odhad podobně.

3.4.12(a). Aproximujte každý zlomek $1/i$ shora a zdola nejbližším zlomkem tvaru $1/2^k$.

3.5.3(a). Taková prvočísla všechna dělí $\binom{2m}{m}$.

3.5.3(b). Je-li P součin prvočísel jako v (a), máme $\log_2 P \le 2m$, ale na druhé straně $P \ge m^{\pi(2m)-\pi(m)}$. Odtud $\pi(2m) \le \pi(m) + O(m/\ln m)$.

3.5.3(c). Maximální mocnina p dělící $n!$ je $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots$. Použijte vyjádření $\binom{2m}{m} = (2m)!/(m!)^2$ a vyjádřete rozdíl max. mocnin p pro čitatele i jmenovatele.

3.5.3(d). Podle (c) je $2^{2n}/(n+1) \le \binom{2n}{n} \le (2n)^{\pi(2n)}$.

3.6.2. Postupujte jako ve druhém důkazu principu inkluze a exkluze. tj. uvažte příspěvek jednoho prvku.

3.7.1. Rozdělte všechny permutace do tříd podle počtu pevných bodů, vyjádřete počet permutací v každé třídě pomocí funkce $š(k)$.

3.7.2(a). První pán si vymění klobouk, který dostal, za svůj klobouk, a odejde. Buď má ten, s nímž první pán měnil, taky svůj klobouk – a odjede – nebo nemá svůj klobouk, a máme situaci s $n-1$ pány.

3.7.4. Zvolte pevný bod, zbytek je permutace bez pevného bodu, užijte výsledek problému šatnářky.

3.7.6(c). Zobrazujte na množinu $\{1, 2, \ldots, m\}$; nechť A_i je množina zobrazení, která nic nezobrazí na prvek i. Použijte princip inkluze a exkluze na určení $|A_1 \cup \ldots \cup A_m|$, tj. počtu špatných zobrazení. Pro $m = n$ musíme dostat $n!$.

3.7.6(d). Zobrazení f množiny N na m-prvkovou množinu definuje ekvivalenci na N s m třídami. Ukažte, že každá z ekvivalencí na N s m třídami je definována právě $m!$ takovými zobrazeními.

3.7.7(a). Můžete použít návodu k (d) předchozího cvičení a výsledku (c) onoho cvičení.

3.7.7(b). Výsledek (a) sčítáme přes všechna k; vyjde $\sum_{k=0}^{n} \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n$.

3.7.7(c). Ve vyjádření z (b) pište i místo $k-j$, nechte k formálně probíhat do ∞, a zaměňte pořadí sčítání podle k a j.

3.7.10(b). Každý člen součinu rozepište jako $1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}$.

3.7.10(c). Buď $n = 2^q \prod_{i=1}^{r} p_i^{\alpha_i}$, p_i lichá prvočísla. Podle (b) musí být $2n = t \prod (p_i^{\alpha_i} + p_i^{\alpha_i - 1} + \cdots + 1)$, $t = 2^{q+1} - 1$. Po vydělení výrazem $t \prod p_i^{\alpha_i}$ máme $1 + 1/t = \prod (1 + 1/p_i + \cdots + 1/p_i^{\alpha_i})$. Přitom některé p_i dělí t. Aby pravá strana nebyla větší než levá, musí být $r = 1$, $t = p_1$.

3.7.11(a). Pro každé prvočíslo $p_i \le N$, nechť A_i je množina dvojic (m, n) takových, že $p_i | n$ a $p_i | m$. Použijte princip inkluze a exkluze na určení počtu špatných dvojic.

3.7.12(a). Definujte A_i jako množinu všech grafů, v nichž vrchol i je izolovaný, počítejte $|A_1 \cup \ldots \cup A_n|$.

3.7.12(b). Zvolte izolované vrcholy, na zbytek užijte (a).

3.7.13. Definujte A_i jako množinu těch rozsazení, kdy i-tý pár sedí vedle sebe.

4.1.6(a). Protipříklad je třeba graf vpravo na druhém obrázku sekce 4.4.

4.1.7. Jak sestrojit $2^{n^2/2 - O(n \log n)}$ neisomorfních (téměř tolik jako se dostane počítáním uvedeným v textu): Buď n dost velké, a buď m nejmenší splňující $2^m \ge n$. Pojmenujme vrcholy $a, b, c, d, u_0, u_1, \ldots, u_{m-1}$ a $v_0, v_1, \ldots, v_{n-m-5}$; pišme $U = \{u_0, \ldots, u_{m-1}\}$, $V = \{v_0, \ldots, v_{n-m-5}\}$. Spojme a s b, a b spojíme s c, s d a se všemi vrcholy z U. Na U zvolme nějaký asymetrický graf, např. cestu $u_0, u_1, \ldots, u_{m-1}$ kde u_0 je ještě propojen s u_3. Vrcholy c, d spojme se všemi vrcholy V (takže teď a je jediný vrchol stupně 1). Na V zvolme libovolný graf, a konečně každý vrchol $v_i \in V$ spojme s vrcholy $u_{j_1}, \ldots, u_{j_k}$, kde $0 \le j_1 < j_2 < \ldots < j_k \le m-1$ jsou (jednoznačně určená) čísla pro něž platí $2^{j_1} + 2^{j_2} + \cdots + 2^{j_k} = i$ (to odpovídá dvojkovému zápisu čísla i). Lze snadno ukázat, že pro dva různé grafy na V jsou výsledné grafy neisomorfní, a máme tedy aspoň $2^{\binom{n-m-5}{2}}$ neisomorfních grafů na n vrcholech.

4.2.1. Nejvíce hran zřejmě dostaneme pro sjednocení k úplných grafů; jsou-li jejich velikosti $n_1, \ldots, n_k$, $\sum n_i = k$, potřebujeme maximalizovat výraz $\binom{n_1}{2} + \cdots + \binom{n_k}{2}$. Ukažte, že pokud např. $n_1 \ge n_2 > 1$, zmenšením n_1 a zvětšením n_2 o 1 hodnota neklesne; maximum je tedy pro $n_1 = n - k + 1$ a ostatní $n_i = 1$.

4.2.3. Neobsahuje-li lichou kružnici, předpokládejte, že je souvislý, a označujte vrcholy následujícím algoritmem: libovolný vrchol označte +1; dále

kdykoli je v vrchol sousedící s vrcholem označeným x, označte v $-x$. Ukažte, že takto se postupně označí všechny vrcholy a žádné 2 stejně označené vrcholy nesousedí.

4.2.4(a). Je-li v vrchol stupně > 1, musí být spojen se všemi vrcholy své komponenty. Každá komponenta musí být buď K_3, nebo $K_{1,n}$.

4.2.4(b). Uvažme jen souvislé grafy G. Případ kdy max. stupeň je ≤ 2 je snadný; předpokládejme že max. stupeň ≥ 3, a uvažme vrchol v max. stupně. Podle předchozího cvičení musí být graf G_v indukovaný na sousedech v být disjunktním sjednocením trojúhelníků a hvězd (=grafů tvaru $K_{1,n}$). Diskusí možných případů vyjdou následující možnosti pro G: libovolný graf na ≤ 4 vrcholech, dvě hvězdy spojené hranou za středy, trojúhelník s několika hranami přivěšenými k jednomu vrcholu, a $K_{1,n}$ jehož všechny vrcholy jsou spojeny s jedním dalším vrcholem.

4.2.6. Průměr: $\max\{d_G(u,v);\ u,v \in V(G)\}$.
Poloměr: $\min_{v\in V(G)} \max_{u\in V(G)} d_G(u,v)$.

4.3.2. Graf zadejte seznamem sousedů pro každý vrchol. Uchovávejte vrcholy množiny A spolu s hodnotami $d(v)$ ve vhodné datové struktuře, která umožňuje rychle najít a vymazat vrchol s minimálním $d(v)$ – takovou strukturou je např. tzv. halda (heap).

4.3.4. Pro každý vrchol v uchovávejte vrchol $p(v)$, z nějž se do v přišlo.

4.3.5(b). Algoritmus je totožný s Dijkstrovým algoritmem (v naší formulaci) pro ohodnocení $w = 1$.

4.3.6. Jako v textu se ukáže, že vždy platí $d(v) \geq d_{G,w}(s,v)$. Pro spor, nechť existuje v pro nějž $d(v) > d_{G,w}(s,v)$ v okamžiku, kdy opustil A. V tomto okamžiku uvažte poslední vrchol u na nejkratší cestě z s do v, který není v A, a vrchol u_1 následující na této cestě po u (ve směru od s). Protože $u \notin A$, je $d(u) = d_{G,w}(s,u)$, a $d(u_1) \leq d(u) + w(\{u,u_1\}) = d_{G,w}(s,u_1)$. Dále $d(u_1) + h(u_1) \geq d(v) + h(v) > d_{G,w}(s,v) + h(v)$ (protože u_1 je ještě v A), odtud $d_{G,w}(s,v) - d_{G,w}(s,u_1) < h(u) - h(v)$, a to dává spor s podmínkou pro h.

4.4.1. Např.: první graf neobsahuje žádnou kružnici délky 4, druhý 2 takové kružnice, třetí 5 kružnic délky 4.

4.4.7(a). Ne; musel by mít skóre $(0,1,\ldots,n-1)$, ale má-li vrchol spojený se všemi ostatními nemůže mít zároveň vrchol stupně 0.

4.4.7(b). Pro všechna $n \geq 2$. Indukcí konstruujeme grafy G_n se skóre obsahujícím čísla $0,1,\ldots,n-2$, v němž se opakuje $\lfloor (n-1)/2 \rfloor$: G_2 jsou 2 izolované vrcholy, G_{n+1} vznikne přidáním izolovaného vrcholu k doplňku grafu G_n (*doplněk* grafu $G = (V,E)$ je graf $(V, \binom{V}{2} \setminus E)$).

4.4.8. Uvažte obarvení s nejmenším možným počtem jednobarevných hran.

4.4.9. Uvažte cestu maximální možné délky v G. Její koncový vrchol je spojen aspoň se dvěma dalšími vrcholy této cesty; to dá hledaný podgraf.

4.4.10. Zřejmě musí platit $k \leq n-1$, kn sudé. To je taky postačující; např. $V = \{0,\ldots,n-1\}$, $E = \{\{i,j\};\ i-j \pmod n \in S\}$, kde $S = \{1,-1,2,-2,\ldots,k/2,-k/2\}$ pro k sudé, $S = \{1,-1,\ldots,(k-1)/2,-(k-1)/2,n/2\}$ pro k liché, n sudé.

4.4.13. Stačí ukázat, že je-li $\{u,v\} \in E(G)$, pak $\deg_G(u) = \deg_G(v)$. Buď U množina všech sousedů u mimo v, a V množina všech sousedů v mimo u. Každý vrchol z U musí mít 4 sousedy ve V, a každý vrchol z V má 4 sousedy v U. Proto $|U| = |V|$ (počítání hran mezi U a V dvěma způsoby).

4.4.14. Sporem, nechť žádné 2 takové vrcholy nejsou. Pro libovolný vrchol v se podíváme na podgraf indukovaný jeho sousedy; v něm musí být všechny stupně liché, a proto má v sudý stupeň. Počítejme sledy délky 2 začínající ve v. Celkem je jich sudý počet. Přitom sudý počet se jich vrací zpátky do v, ale každý jiný vrchol dosáhneme lichým počtem sledů, proto je počet vrcholů různých od v sudý – spor.

4.4.15(b). Uvažte trojúhelník xyz (existující podle (a)), a vyjádřete pomocí principu inkluze a exkluze počet vrcholů spojených aspoň s jedním z vrcholů x,y,z.

4.7.2(b). Např. v K_{n+1} podrozdělte každou hranu.

4.7.2(c). Vezměte strom T, v němž každý vrchol mimo listů má stupeň n, a kde všechny listy mají od kořene vzdálenost n (úplný n-ární strom). Udělejte jeho kopii T_1, a ztotožněte každý list s jeho vzorem v T.

4.7.3(a). Ano.

4.7.3(b). Ano.

4.7.4. Např. indukcí pomocí lemmatu o vytváření 2-souvislých grafů přilepováním uší.

5.1.5. Máme $2n-2 = 2|E(T)| = \sum_{v\in V(T)} \deg_T(v) = \sum_{i=1}^{n-1} ip_i$. Úpravou plyne žádaná rovnost.

5.1.6. (ii)⇒(ii): indukcí podle n; buď $n \geq 3$, $(d_1,\ldots,d_n)$ splňují (ii); pak existuje nějaké $d_i = 1$ a nějaké $d_j > 1$ (např. $d_n = 1$, $d_{n-1} > 1$). Aplikujeme indukční předpoklad na $(d_1,\ldots,d_{n-2},d_{n-1}-1)$ a připojíme koncový vrchol za vrchol číslo $n-1$.

5.2.4. Rozdělte posloupnosti do dvou skupin: začínající 0 a začínající 1, a obě skupiny setřiďte rekurzivně. Při skutečném programování algoritmu se

posloupnosti ve skutečnosti nepřemisťují, pracuje se jen s vhodnými ukazateli na ně.

5.2.5. Kód stromu na n vrcholech má délku $2n$. Existuje tedy nejvýš 4^n kódů.

5.2.6. Indukcí podle $|V|$.

5.3.2. Důkaz správnosti Kruskalova algoritmu nevyužívá nikde nezápornosti ohodnocení w. Proto jej lze použít na ohodnocení $-w$, a tím se najde maximální kostra.

5.3.7(a). Pro vrchol v stupně ≥ 7 existují hrany $\{v,u_1\}$ a $\{v,u_2\}$ svírající úhel $< 60°$. Jednu z nich lze nahradit hranou $\{u_1,u_2\}$.

5.3.8. Jedno řešení: rozdělte jednotkový čtverec na síť $\sqrt{n} \times \sqrt{n}$ čtverečků. Očíslujte čtverečky $1,2,\ldots,n$ tak, že po sobě jdoucí čtverečky vždy sousedí (např. jako když se oře pole). Spojte cestou nejdřív všechny body z V ve čtverečku 1, potom ve čtverečku 2, atd. Jiné řešení: Dokažte, že existují 2 body se vzdáleností $O(n^{-1/2})$. Vymažte jeden z nich, sestrojte kostru indukcí, a připojte vymazaný bod.

5.3.9. Dokažte, že jeden vrchol se přeznačuje nejvýš $(\log_2 n)$-krát.

5.3.10(a). Buď E_M maximální párování, E_H párování nalezené hladovým algoritmem, a každé hraně $e \in E_M$ přiřaďme první z hran E_H, která ji protíná. Každá $\check{e} \in E_H$ je tak přiřazena nejvýš 2 hranám $e_1, e_2 \in E_M$, $w(e_1), w(e_2) \leq w(\check{e})$.

5.3.11(b). Buďte $e_1,\ldots,e_k$ hrany vybrané hladovým algoritmem, $\check{e}_1,\ldots,\check{e}_t$ hrany nějakého optimálního pokrytí, a buď $k_1 = |\{i;\ e_i \cap (e_1 \cup \ldots \cup e_{i-1}) = \emptyset\}|$, a podobně $t_1 = |\{i;\ \check{e}_i \cap (\check{e}_1 \cup \ldots \cup \check{e}_{i-1}) = \emptyset\}|$. Máme $|V| = k + k_1 = t + t_1$. Klíčové pozorování: v krocích hladového algoritmu pro $i > k_1$ už musel být aspoň 1 bod z každé hrany $\check{e}_j$ přispívající k t_1 pokryt, takže $k_1 \geq t_1/2$. Odtud $k = t + t_1 - k_1 \leq t + t_1/2 \leq \frac{3}{2}t$.

5.3.12. Buď $V = \{1,2,\ldots,2^{k+2}-2\} \cup \{a_1,a_2,b_1,b_2,\ldots,b_k\}$. Vrchol a_1 je spojen s $1,3,5,\ldots$, a_2 s $2,4,6,\ldots$, b_i s $2^i-1, 2^i, \ldots, 2^{i+1}-2$, a a_1, a_2 jsou navíc spojeny se všemi b_i. Hladový algoritmus vybere všechny b_i, optimální je $\{a_1,a_2\}$.

5.4.5(a). Ukažte, že každá komponenta po i-tém kroku má $\geq 2^i$ vrcholů.

5.4.5(b). Pro každou komponentu udržujte seznam hran z ní vycházejících. V každé fázi můžete každý seznam projít a najít v něm hranu minimální váhy.

6.1.1(a). Obr. 6.1.

6.1.1(b). Grafy G_1, G_2 jako v (a) se dají slepit dohromady. Například se dá odstranit hrana $\{a,b\}$ sousedící s vnější stěnou v G_1 a hrana $\{c,d\}$ sousedící s vnější stěnou v G_2 a přidat hrany $\{a,c\}$ a $\{b,d\}$.

6.1.2. Indukcí podle počtu hran. Uvažme v nakreslení nějaký vrchol v stupně aspoň 4, a 2 sousední hrany z něj vycházející, a pokud možno zasahující do různých komponent grafu $G-v$. Nahraďte je jedinou hranou spojující jejich druhé konce. (Je výhodné připustit i grafy s násobnými hranami.)

6.5.6. Nejprve je potřeba vyřešit případ, kdy G není 2-souvislý. Pro 2-souvislý G dokažte, že do stěny s ≥ 6 stranami lze přidat diagonálu. Přitom je třeba dávat pozor, aby nevznikl trojúhelník. Asi bude potřeba rozebrat několik případů.

6.5.9(a). Řekneme, že puntík, z něhož vychází $k \leq 3$ hran, přispívá $3-k$ stupni volnosti. Na začátku je $3n$ stupňů volnosti, na konci aspoň 1, každým tahem 1 ubude.

6.5.9(c). Ukažte, že na konci hry čouhá do každé stěny přesně jedno rameno křížku (nevyužité). Počet volných ramen se libovolném tahem zachovává, takže na konci je $4n$ stěn. Přitom $n-1$ tahů spojí dvě komponenty do nové, a zbývající tahy každý zvyšuje počet stěn o 1. Na začátku byla 1 stěna, celkem tedy $5n-2$ tahů.

6.5.10(a). Platí $e = v + s - 1$ – dokazujte indukcí dle n, při vkládání nové přímky rozlišujte nově vytvořené průsečíky a již existující průsečíky.

6.5.10(c). Z (b) odvoďte $e \geq 3s - n$. Je-li d_i počet přímek procházejících i-tým vrcholem, spočítá se $\sum d_i = e - n$ (každá hrana přispěje dvěma konci až na $2n$ nekonečných hran). Dosazením za s z (a) vyjde $\sum d_i \leq 3v - 3$.

6.5.11. Předpokládejme souvislost. Nechť červenomodrý roh je dvojice (S,v), kde S je stěna a v vrchol na její hranici takový, že obcházíme-li hranici stěny S po směru hodinových ručiček (pro neomezenou stěnu proti směru), vrcholu v předchází červená hrana a následuje po něm modrá hrana. Počítáním dvěma způsoby a pomocí Eulerova vzorce ukažte, že existuje vrchol s nejvýš jedním červenomodrým rohem.

6.7.2. Na každé pětici vrcholů je indukován K_5, a nějaké 2 jeho hrany se musí protínat; tím dostáváme $\binom{n}{5}$ protínajících se dvojic. Přitom dané 2 protínající se hrany se účastní v $n-4$ pěticích, takže celkem je aspoň $\binom{n}{5}/(n-4)$ křížících se dvojic.

6.8.2. Postupujte indukcí podle počtu vrcholů. V daném grafu odstraňte vrchol s nejmenším stupněm, obarvěte zbytek a vrchol vraťte zpět.

6.8.3. Podgraf vnějškově rovinného grafu je zase vnějškově rovinný. Podle cvičení 2 stačí tedy ukázat, že vnějškově rovinný graf má vždycky vrchol

stupně ≤ 2. To jde z Eulerova vzorce s využitím toho, že 1 stěna sousedí s aspoň n hranami.

6.8.4. Ukažte, že $\delta(G) \leq 3$ a použijte cvičení 2.

6.8.6(b). Dokonce stačí vzít i strom.

6.8.6(c). Přidejte dostatečně mnoho listů a upravte stupně.

6.8.8(a). Indukcí podle počtu hran. Uvažte stěnu S a množinu hran E_S, které leží na její hranici. Ukažte, že stupně všech vrcholů grafu (V, E_F) jsou sudé. Vymažte hrany E_S, obarvěte graf podle indukčního předpokladu, vraťte E_S zpět a přebarvěte stěnu S druhou barvou.

6.8.8(b). Obarvěte stěny 2 barvami. Počet hran se dá počítat jako součet obvodů stěn jedné barvy i jako součet obvodů stěn druhé barvy. Jeden způsob počítání ale dá číslo dělitelné 3, druhý ne.

6.8.10(b). Za jednu podmnožinu vrcholů zvolte k vrcholů $v_1, \ldots, v_k$, kde pro v_i je dán seznam $L(v_i) = \{k(i-1)+1, k(i-1)+2, \ldots, ki\}$. Za každou množinu S obsahující právě jeden prvek z každého $L(v_i)$ dosaďte do druhé podmnožiny vrchol v_S se seznamem $L(v_S) = S$.

6.8.11. Při indukčním kroku je třeba rozlišit dva případy. Pokud existuje hrana $\{v_i, v_j\}$ s v_i a v_j na kružnici C, ale nikoli sousedícími, rozdělte G podél této hrany. Jinak odstraňte v_k a vhodně upravte seznamy jeho sousedů.

7.1.1. Definujte graf na stěnách přesně jako v důkazu Spernerova lemmatu.

7.1.2(a). Napodobte důkaz rovinné verze. Spojujte hranou malé čtyřstěny přes stěnu očíslovanou 1,2,3, a užijte rovinné verze na důkaz toho, že stupeň vnějšího vrcholu je lichý.

7.1.3. Názorné řešení – představte si 2 turisty v týž den, jeden vystupuje, druhý sestupuje.

7.1.4(b). Zařiďte, aby z a do c bylo podstatně dále než z b do d.

7.1.4(c). Sporem. Kdyby měl B vyhrávající strategii, A bude ignorovat svůj první tah, tím se octne v situaci B (jedno zabrané políčko navíc z prvního tahu může jen pomoci) a použije jeho vyhrávající strategii.

7.2.4. Nezávislý množinový systém $\mathcal{M}$ splňuje $\sum_{M\in\mathcal{M}} \binom{n}{|M|}^{-1} = 1$, proto množiny největšího systému mají všechny velikost $\lfloor n/2 \rfloor$ nebo $\lceil n/2 \rceil$ (pro n sudé jsme tím hotovi). Ukažte, že obsahuje-li $\mathcal{M}$ t množin velikosti $\lfloor n/2 \rfloor$ a $0 < t < \binom{n}{\lfloor n/2 \rfloor}$, potom má $< \binom{n}{\lfloor n/2 \rfloor} - t$ množin velikosti $\lceil n/2 \rceil$.

7.2.5. Pro automorfismus h definujte zobrazení $f : X \to X$, $f(x)$ je y takové, že $h(\{x\}) = \{y\}$. Ukažte $h = f^{\#}$ (z toho je vidět, že je $n!$ automorfismů).

7.2.7. Aplikujte Spernerovu větu na množinový systém $\{\{i;\, \varepsilon_i = 1\};\, \sum \varepsilon_i a_i \in (-1, 1)\}$.

7.2.8. Buď $n = p_1 p_2 \ldots p_n$ rozklad na prvočinitele. Děliteli $d = p_{i_1} p_{i_2} \ldots p_{i_k}$ přiřaďte podmnožinu $M_d = \{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$; pak $d_1 | d_2 \Leftrightarrow M_{d_1} \subseteq M_{d_2}$. Užijte Spernerovy věty.

7.3.1. Napodobte důkaz pro $K_{2,2}$, jediný rozdíl je, že jeden vrchol v přispěje do M nejvýš $t-1$ prvky.

7.3.2. Uvažte graf incidence s množinou vrcholů $X \cup \{1, 2, \ldots, n\}$, kde vrcholy $x \in X$ a $i \in \{1, 2, \ldots, n\}$ jsou spojeny, právě když $x \in S_i$. Ten neobsahuje $K_{2,2}$, tedy má $O(n^{3/2})$ hran.

7.3.6. Uvažte funkci $f(x)$, rovnou 0 pro $x \leq 2$ a $x(x-1)(x-2)$ pro $x > 2$, ta je konvexní.

8.1.1. Jako pro neisomorfní grafy v 4.1; využijte odhad $n!$ z věty 3.4.4.

8.1.2. Počítejte kostry, obsahující danou hranu; tento počet je pro všechny hrany stejný, přitom každá kostra obsahuje $n-1$ hran.

8.1.3. Z každé kostry K_n můžeme $n-1$ způsoby vyjmout hranu, tím dostaneme dvojici stromů. Obráceně, z kostry na k-bodové podmnožině a kostry na doplňku této podmnožiny můžeme udělat kostru celého K_n přidáním hrany, právě $k(n-k)$ způsoby.

8.1.4. Vyjde $n^{m-1} m^{n-1}$, nejsnáze možná pomocí determinantu.

8.2.1(a). Pro liché n 0. Pro n sudé je $n/2+1$ listů a $n/2-1$ vrcholů stupně 3 (indukcí). Sčítáme tedy výraz $(n-2)!/2^{n/2-1}$ přes všechny volby $(d_1, \ldots, d_n)$, $d_i \in \{1, 3\}$, $\sum d_i = 2n-2$. Substitucí $k_i = (d_i - 1)/2$ vidíme, že počet sčítanců je roven počtu $(n/2-1)$-prvkových podmnožin n-prvkové množiny, takže odpověď je $(n-2)!\binom{n}{n/2-1} 2^{-n/2+1}$.

8.2.1(b). Asi nejlépe přes vytvořující funkce (viz kapitola 12). Odpověď je koeficient při x^{2n-2} ve výrazu $(n-2)!(x + x^2 + x^3/2)^n$, který se najde podle multinomické věty (podobně se dá řešit i (a)).

8.3.3. Představte si, že na grafu zobrazení vyšlete z bodu i dva chodce – jeden projde jednu šipku za minutu, druhý dvě šipky. Rozmyslete, kdy se budou potkávat.

8.5.1(a). Q má nulový součet řádek.

8.5.1(b). $\kappa(G) > 0$, proto $\det Q_{11} \neq 0$ podle věty o počtu koster.

8.5.1(c). Součet řádků matice Q přes každou komponentu je nulový, tedy prostor generovaný řádky má dimenzi $< n-1$.

8.5.1(d). Jádro obsahuje $(1, 1, \ldots, 1)$, protože součet řádků je nulový, a podle (b) je jádro Q jednodimenzionální.

8.5.1(e). Součin i-tého řádku Q a i-tého sloupce Q^* je rozvoj $\det Q$ podle i-tého řádku, užijte $\det Q = 0$. Ostatní pozice součinu jsou rozvojem determinantu matice, v níž se 1 řádek opakuje dvakrát, tedy také 0.

8.5.3. Na jednu implikaci stačí spočítat determinant matice incidence pro kružnici liché délky (protože každý ne-bipartitní graf obsahuje kružnici liché délky). Pro bipartitní G se požadovaná vlastnost M dá dokázat indukcí, podobně jako jsme dokazovali lemma 8.5.3.

9.1.1. Viz cvičení 3.

9.1.2. Ukažte, že 2 body z $P_1 \setminus P_2$ a 2 body z $P_2 \setminus P_1$ tvoří dohromady konfiguraci $\check{C}$ jako v (P0).

9.1.3. Možnosti: $\mathcal{P} = \{X\}$, $\mathcal{P} = \{X, \{a\}\}$, $\mathcal{P} = \{X \setminus \{a\}\} \cup \{\{a, x\};\ x \in X \setminus \{a\}\}$, kde $a \in X$ je nějaký bod (při důkazu se dá využít cvičení 2).

9.1.5(a). Jedna dvojice je nejvýš v jedné množině. Jedna množina pokrývá $\binom{n+1}{2}$ dvojic, celkový počet pokrytých dvojic vyjde shodný jako počet všech dvojic, každá dvojice je tedy pokryta nějakou množinou.

9.1.5(b). Kdyby jich bylo více, mají dohromady více než $n^2 + n + 1$ bodů.

9.1.5(c). Počítejte dvěma způsoby dvojice (x, P), $x \in P$. Sčítáním napřed přes množiny je vidět, že jich je $(n+1)|\mathcal{P}|$, kdyby nějaký bod byl v méně než $n + 1$ množinách, vzhledem k (b) dostaneme méně než $(n + 1)|X|$ dvojic.

9.1.5(d). Uvažme nějakou množinu P, v každém z jejích $n + 1$ bodů ji protíná n dalších přímek, celkem $n^2 + n + 1$ přímek, žádná neprotínající P už nezbývá.

9.3.4(a). K daným t ortogonálním latinským čtvercům můžeme přidat jeden čtverec mající v i-tém řádku všude i, a jeden čtverec mající v i-tém sloupci všude i.

9.3.4(b). Aby byl osvobozený čtverec ortogonální k jinému, musí obsahovat každé $i \in \{1, 2, \ldots, n\}$ právě $n\times$. Permutujte políčka daných $t+2$ ortogonálních osvobozených čtverců (všechny čtverce touž permutací) tak, aby první čtverec měl v i-tém řádku samá i, $i = 1, \ldots, n$. Potom ještě permutujte uvnitř každého řádku (zase všechny čtverce stejně) tak, aby druhý čtverec měl v j-tém sloupci samá j. Ověřte, že ortogonalita se neporušila a zbývajících t čtverců je latinských.

9.3.6. Hledaný počet je $n!\times$ počet permutací bez pevného bodu.

10.1.1. Kódujte možné průjezdy vagónů kolejištěm, např. „vagón z A na I, vagón z A na C, vagón z C na II,...“ (stačí vždy uvést z které koleje na kterou se v daném kroku přesunuje, který vagón je jasné z momentální pozice). Existuje tedy nanejvýš C^n možných kódů (pro vhodnou konstantu C), takže vznikne nejvýš C^n různých pořadí na koleji B, což je pro velká n méně než $n!$.

10.1.2(a). Např. indukcí podle n – funkce n proměnných definuje dvě funkce $n - 1$ proměnných, jednu pro $x_n = 0$ a jednu pro $x_n = 1$.

10.1.4. Každé vážení má 3 možné výsledky, 3 váženími lze tedy rozlišit maximálně 3^3 možností.

10.2.2. Pro nesouvislý graf existuje vlastní podmnožina A vrcholů taková, že mezi A a jejím doplňkem nejsou hrany. Spočtěte pravděpodobnost tohoto jevu pro pevnou A, pak sčítejte přes všechny A.

10.2.5(b). Nahradíme-li některé z A_i jejich doplňky, máme pořád soubor nezávislých jevů, a průnik těchto jevů má nenulovou pravděpodobnost. Takto se vyrobí 2^n disjunktních neprázdných jevů.

10.2.7. Je to $\frac{1}{3}$ (nechť děti jsou A a B; 3 stejně pravděpodobné možné případy: A=kluk, B=kluk; A=kluk, B=holka A=holka, B=kluk).

10.3.2. Ukažte $0 \leq \mathbf{E}((f - \mathbf{E}f)^2) = \mathbf{E}(f^2) - (\mathbf{E}f)^2$.

10.3.3. Použijte indikátorů; nechť A_i je jev "$\pi(i) = i$". Vyjde $\mathbf{E}f = 1$.

10.3.4(a). Definujte X_i jako indikátor jevu „jednička je v cyklu délky i“; ukažte že $P(X_i = 1) = \frac{1}{n}$.

10.3.4(b). Hledaný počet je roven $\sum_{i,j=1}^{n} X_{ij}$, kde X_{ij} je indikátor „j je v cyklu délky i“.

10.3.5. Počítejte raději rozhraní mezi sériemi. Pravděpodobnost, že na daném místě bude rozhraní, je $\frac{1}{2}$.

10.4.4. Na úrovni 0 jsou jen 2 špice. Počítejte dvěma způsoby střední hodnotu počtu špic na úrovni 0 pro náhodnou podmnožinu $R \subseteq L$.

12.1.3. Abychom dostali člen $x_1^{k_1} \ldots x_m^{k_m}$ při roznásobování n závorek, musíme zvolit k_1 závorek z nichž vybereme x_1, ..., k_m závorek z nichž vybereme x_m. Počet možností je právě multinomický koeficient.

12.1.5. Vyjděte z rovnosti $(1 - x)^n(1 + x)^n = (1 - x^2)^n$.

12.2.6(a). Vytvořující funkce je $1/((1 - x)(1 - x^2)(1 - x^5))$.

12.2.7(d). Výsledek: $(-1)^m\binom{n-1}{m}$.

12.2.9(a). Pro spojitost potřebujeme dokázat, že pro $x_0 \in [0, \rho)$ je $\lim_{x \to x_0} |a(x) - a(x_0)| = 0$. Užijte

$$|x_0^i - x^i| \leq |x_0 - x|(x_0^{i-1} + x_0^{i-2}x + \cdots + x^{i-1}) \leq |x - x_0| i m^{i-1},$$

kde $m = \max(x, x_0)$.

12.2.9(c). Třeba $a_i = 1/i^2$.

12.2.10(a). Napřed indukcí ukažte, že každá derivace funkce f v bodě $x \neq 0$ je tvaru $R(x)e^{-1/x^2}$, kde $R(x)$ je podíl dvou mnohočlenů. Pak indukcí odvoďte podle definice derivace, že všechny derivace v 0 jsou 0.

12.2.10(b). Koeficienty mocninné řady se dají vyjádřit pomocí derivací, musely by tedy být všechny nulové.

12.3.1. Nechť a_n, resp. b_n je počet takových posloupností končících 1, resp. 0. Odvoďte rekurentní vzorce pro a_n a b_n. Vyjdou Fibonacciho čísla.

12.3.4. Uvažte posloupnost $b_n = \log_2 a_n$.

12.3.6. Označme u_n počet takových posloupností začínajících a nebo b, a v_n počet takových posloupností začínajících c nebo d. Vyjdou rekurence $u_n = u_{n-1} + 2v_{n-1}$, $v_n = 2u_{n-1} + 2v_{n-1}$. Napište odpovídající rovnice pro vytvořující funkce $u(x)$ a $v(x)$, vyřešte a spočítejte koeficienty. Vyjde $u_n + v_n = ((\sqrt{17}+1)/4\sqrt{17})((3+\sqrt{17})/2)^{n+1} + ((\sqrt{17}-1)/4\sqrt{17})((3-\sqrt{17})/2)^{n+1}$.

12.3.8(b). Ukažte, že posloupnosti, jejichž j-tý člen je 1 a ostatní členy mezi $y_0, \ldots, y_{k-1}$ jsou nulové, pro $j = 0, 1, \ldots, k-1$ tvoří bázi.

12.3.8(c). Aby se ukázala lineární nezávislost, stačí např. dokázat, že vektory tvořené prvními k členy jsou lineárně nezávislé. Na to se dá použít kritérium pomocí determinantu, a vede to na tzv. Vandermondův determinant probíraný v lineární algebře.

12.3.8(e). Asi nejjednodušší metoda zde je pomocí rychlosti růstu jednotlivých posloupností. Kdyby byly posloupnosti lineárně závislé, šlo by nejrychleji rostoucí z nich vyjádřit jako lineární kombinaci pomaleji rostoucích, což není možné. Potíž v tomto přístupu nastane, má-li několik různých komplexních kořenů stejnou absolutní hodnotu; tento případ se dá řešit zvlášť např. pomocí determinantu jako v návodu k (c).

12.4.2(a). $\binom{2n}{n}$.

12.4.2(b). Cesta, která nikdy nejde pod diagonálu, kóduje binární strom s n vrcholy např. takto: rozdělte cestu na 2 části v bodě, kde poprvé dosáhne diagonály. Od první části odeberte první a poslední úsek, druhou nechte beze změny. Obě části pak rekurzivně kódují levý a pravý podstrom (přitom cesta s 0 úseky kóduje prázdný strom.

12.4.2(c). Zaveďme souřadnice: A je $(0,0)$, B je (n,n). Nastavíme šachovnici o jeden sloupec vpravo. Ukažte, že cesty, které *zasahují* pod diagonálu, se dají vzájemně jednoznačně přiřadit cestám z A do bodu $B_1 = (n+1, n-1)$ –

dojděte po cestě až na konec prvního úseku po prvním překročení diagonály, a zbytek cesty překlopte symetricky podle přímky $y = x - 1$.

12.4.3. Najděte korespondenci s cestami nejdoucími pod diagonálu.

12.4.6(b). $c_{2n+1} = b_n$; bijekce mezi pěstovanými stromy jako ve cvičení a binárními stromy uvažovanými v textu se dostane smazáním všech koncových vrcholů pěstovaného stromu.

12.4.7(a). Vyjde $t_n = b_{n-1}$.

12.4.8. Starý strom je buď samotný kořen, nebo vznikne připojením nějakých k pěstovaných stromů, každý aspoň se dvěma vrcholy, ke kořeni. Odtud $s(x) = x + x/(1 - t(x) + x)$.

12.6.1(a). Buď a_i počet cest začínajících v 1 a vstupujících poprvé do 0 po i tazích. Hledaná pravděpodobnost je $a(\frac{1}{2})$. Odvoďte vztah $a(x) = x + xa(x)^2$. Hodnotu a_i lze též explicitně spočítat, např. pomocí Catalanových čísel.

12.7.1(a). Takový uspořádaný rozklad můžeme zakódovat rozdělením čísel $1, 2, \ldots, n$ do k souvislých úseků. Vyrobte $(k-1)$-prvkovou podmnožinu množiny $\{1, 2, \ldots, n-1\}$ z čísel, která jsou poslední ve svém úseku (přitom se ignoruje poslední úsek).

12.7.3(a). $(1+x)(1+x^2)\ldots(1+x^n)$.

13.1.1(b). V podstatě duální úloha ke cvičení 9.1.5.

13.2.2. Každý řádek matice AB je lineární kombinací řádků matice B (koeficienty jsou dány odpovídajícím řádkem A), proto $r(AB) \leq r(B)$.

13.2.3. Regularita čtvercové matice znamená totéž jako nenulovost determinantu, a definice determinantu nezávisí na tom, nad jakým tělesem pracujeme. Hodnost se dá vyjádřit pomocí existence regulárních podmatic.

13.2.4(a). Kdyby měla hodnost $< n$, má soustava $Bx = 0$ nenulové řešení, a takové řešení dá $x^T Bx = 0$.

13.2.4(b). B je součtem diagonální matice D s kladnými prvky na diagonále a matice L ze samých $\lambda > 0$. Pro každé nenulové $x \in \mathbf{R}^v$ platí $x^T Dx > 0$ a $x^T Lx \geq 0$.

13.2.6(a). Je-li A matice incidence systému, potom $A^T A$ je součtem matice Q ze samých q a diagonální matice D, jejíž diagonální prvky jsou $|C_i| - q > 0$ (za předpokladu $|C_i| > q$ který můžeme udělat). Proto je $A^T A$ pozitivně definitní a tudíž regulární.

13.2.6(b). V situaci Fisherovy nerovnosti, uvažte množinový systém duální k $(V, \mathcal{B})$, a aplikujte na něj část (a).

13.3.1(b). Dokažte indukcí podle k, že je-li E sjednocení množin hran k bipartitních grafů na množině vrcholů $\{1, 2, \ldots, n\}$, potom existuje podmnožina aspoň $\lceil n/2^k \rceil$ vrcholů, na níž není žádná hrana z E.

POZNÁMKY

Kapitoly z diskrétní matematiky

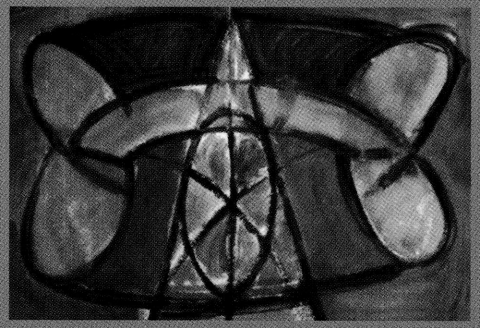
prof. RNDr. Jiří Matoušek, DrSc.
prof. RNDr. Jaroslav Nešetřil, DrSc.

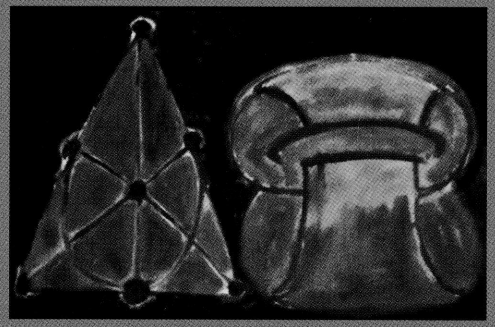
Vydala Univerzita Karlova v Praze
Nakladatelství Karolinum, Ovocný trh 3, Praha 1
Praha 2009
Prorektor-editor prof. PhDr. Mojmír Horyna
Obálku s použitím obrazů Jiřího Načeradského
a Jaroslava Nešetřila navrhla Kateřina Řezáčová
Z předloh připravených autory v systému LaTeX
vytiskla tiskárna PB tisk, Příbram
Čtvrté, upravené a doplněné vydání
ISBN 978-80-246-1740-4

MORAVSKÁ ZEMSKÁ
BRNO
KNIHOVNA

KAPITOLY Z DISKRÉTNÍ MATEMATIKY jsou úvodní učebnicí kombinatoriky a teorie grafů určenou zejména posluchačům úvodních přednášek z diskrétní matematiky. Některé části je možno použít i v navazujících a pokročilejších kurzech. Kniha je napsána s cílem podpořit zájem o matematiku a zdůrazňuje aktivní a problémově orientovaný přístup k látce. Je doprovázena 373 cvičeními rozličné obtížnosti, z nichž mnoho je opatřeno stručnými návody k řešení.

Text předpokládá pouze znalosti na úrovni střední školy. Rozsáhlá úvodní kapitola zavádí či připomíná obecné matematické pojmy a postupy uvažování. Hlavní témata: uspořádání, kombinatorické počítání, asymptotické odhady, teorie grafů, pravděpodobnostní metoda, souvislosti kombinatoriky s lineární algebrou a geometrií.





Kniha vznikla z přednášek autorů na Matematicko-fyzikální fakultě UK. Toto je čtvrté, rozšířené a doplněné vydání. Kniha vyšla též anglicky (Oxford University Press), německy, japonsky, francouzsky (Springer Verlag), španělsky (Editorial Reverte) a další cizojazyčná vydání se připravují. Autoři jsou zaměstnáni na Katedře aplikované matematiky Matematicko-fyzikální fakulty Univerzity Karlovy v Praze a pracují v oblasti matematiky a teoretické informatiky.

JIŘÍ MATOUŠEK je profesorem informatiky a dosud publikoval pět učebnic a přes 100 vědeckých článků, převážně v kombinatorice, kombinatorické geometrii a složitosti geometrických algoritmů.

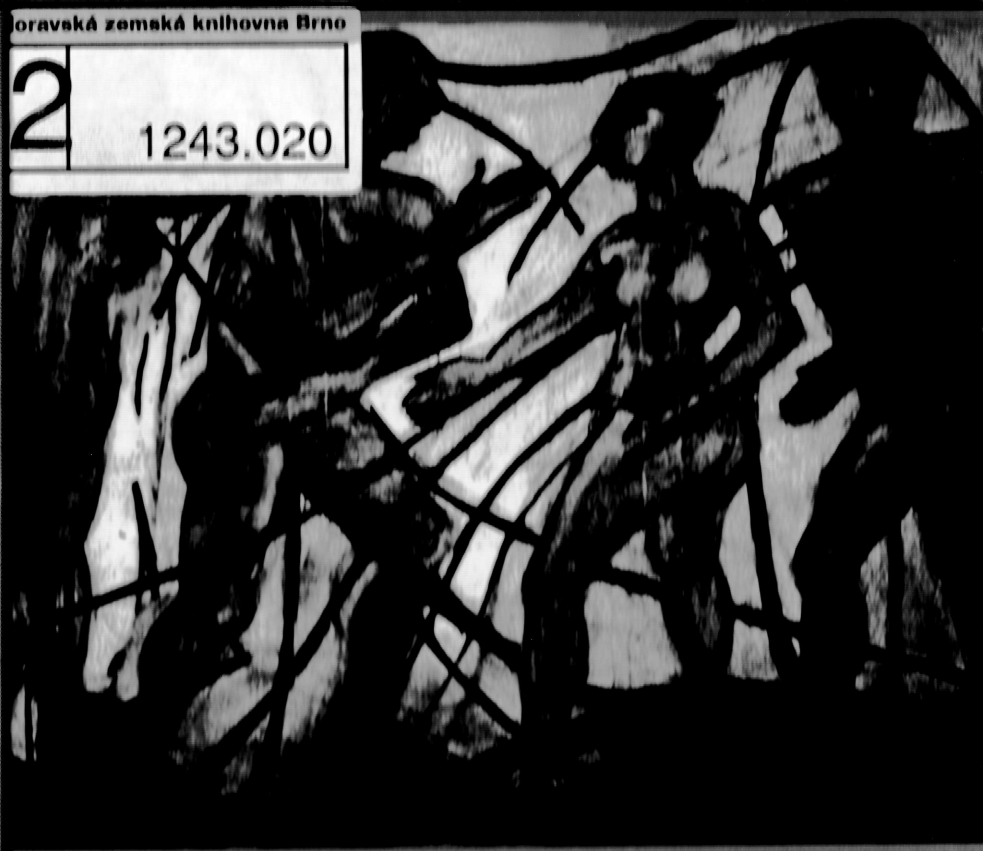
JAROSLAV NEŠETŘIL je profesorem matematiky. Napsal několik knih a přes 250 vědeckých článků, hlavně v kombinatorice, teorii grafů a algebře.

http://cupress.cuni.cz
ISBN 978-80-246-1740-4

MZK – UK Brno
2610434082

Jiří Matoušek ● Jaroslav Nešetřil
Kapitoly z diskrétní matematiky

oravská zemská knihovna Brno
2
1243.020



Jiří Matoušek ● Jaroslav Nešetřil

Kapitoly z diskrétní matematiky