

PV109: Historie a vývojové trendy ve VT

Historie teoretických základů informatiky a výpočetní techniky

Eva Hladká

Fakulta informatiky Masarykovy univerzity

podzim 2014



CZ.1.07/2.2.00/28.0041

Centrum interaktivních a multimediálních studijních opor pro inovaci výuky a efektivní učení



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

- Seznámení s historií výpočetní techniky a informatiky
- Lepší porozumění:
historie → vývojové trendy → predikce budoucího vývoje
- Poučení z chyb minulých může zabránit jejich opakování

- Od matematiky k informatice
- Základní kameny výpočetní techniky:
 - logika,
 - teorie jazyků,
 - teorie komunikace.

- Teoretická informatika
 - Vyčíslitelnost a složitost
 - Teorie informací a kódování
 - Algoritmy a datové struktury
 - Teorie jazyků – automaty a gramatiky
 - Paralelismus a distribuované systémy
 - Databáze a dolování dat
 - ...
- Aplikovaná informatika
 - Umělá inteligence
 - Architektura a návrh počítačů
 - Počítačová grafika a vizualizace
 - Bezpečnost
 - Softwarové inženýrství
 - ...

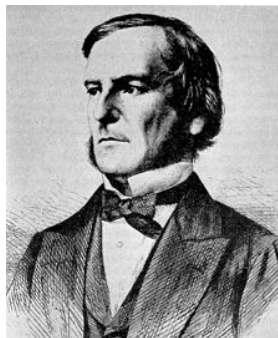
Od matematiky k informatice

- Počítat museli i lovci mamutů (ať už na prstech, nebo na stěnu jeskyně)
- Starověké Řecko
 - Mnoho významných matematiků a filosofů, v matematice se rozvíjela zejména geometrie.
 - Aristoteles ze Stageiry (4. stol. p. n. l.)
 - Položil základy *logiky* – aristotelovská logika
 - a formálního *dokazování* pravdivosti formulí – důkaz sporem, náznaky důkazu indukcí
- Blízký východ
 - Kupci a obchodníci, přinesli arabská čísla do Evropy.
 - První počítadla se objevila již v 11. stol. p. n. l.)
 - Muhamad ibn Músa al Chwárizmí (8./9. stol. n. l.)
 - shrnul znalosti arabské matematiky v knize *Al-džabr wa-b-maǧábala* (odtud *algebra*)
 - z jeho jména vznikl pojem *algoritmus*

- Z řeckého slova *logos* – slovo, smysl, rozum
 - výroková logika
 - predikátová logika
- Úplné systémy logických spojek
 - Booleova algebra (operace AND, OR, negace)
 - Shefferova algebra (operace NAND)
 - Piercova algebra (operace NOR)
 - Tyto operace tvoří základní členy v logických obvodech

George Boole (1815 – 1864)

- Pocházel z rodiny obchodníka, otec jej vedl k matematice již od raného dětství
- Učil se z Newtonových *Principií*, ve 24 letech vydal první matematický článek
- Ve 32 letech vydal knihu *The Mathematical Analysis of Logic*, která umožnila exaktně vyjádřit logické operace a formule.
- Vycházel ze dvou poznatků:
 - 1 Logika je počítání na dvouprvkové množině {True, False}.
 - 2 Logické operátory jsou v podstatě „početní“ operace nad touto množinou.



Zdroj: <http://en.wikipedia.org>

Kurt Friedrich Gödel (1906 – 1978)

- Brněnský rodák rakouské národnosti, nikdy neuměl česky. S rodinou emigrovali po anšlusu Rakouska do USA, kde se usadil v Princetonu.
- Zcela rozvrátil dosavadní úvahy o axiomatizaci matematiky a její formální úplnosti.
 - První a druhá Gödelova věta o neúplnosti.
 - Těmito větami tak Gödel položil, skrze teorii množin, pevné základy mj. pro teorii výpočetní složitosti či programování počítačů.
 - Více v předmětu MA015 – Matematická logika (prof. Kučera)



Zdroj: <http://en.wikipedia.org>

- Množina konečných slov nad určitou abecedou.
- Pojem **formální jazyk** poprvé zmínil Gottlob Frege v knize *Begriffsschrift* v roce 1879.
- Využití:
 - Programovací jazyky
 - Lexikální analýza
 - Syntaktická analýza

Alan Mathison Turing (1912 – 1954)

- Britský matematik, logik a kryptoanalytik, který se podílel na prolomení Enigmy
- Ovlivnil obor vyčíslitelnosti, definoval Turingův stroj
- Během 2. světové války působil jako Člen týmu v Bletchley Park, UK.
- Podílel se na prolomení Enigmy (jeden z důsledků bylo i významné zkrácení války).
- 1950: Turingův test (opačný přístup je hojně využíván jako CAPTCHA)
- Turingova cena – ocenění pro informatiky



Zdroj: <http://en.wikipedia.org>

Turingův stroj, RAM a problém zastavení

- Turingův stroj
 - teoretický model – tvoří jej konečný automat, program ve formě pravidel přechodové funkce a nekonečná páska (různé varianty)
- Problém zastavení (1936)
 - Úloha z teorie vyčíslitelnosti
 - *Lze rozhodnout, zda výpočet libovolného programu skončí v konečném čase, nebo nikoliv?*
- Random-Access Machine
 - další teoretický model, ekvivalentní s turingovým strojem (nezaměňovat s Random Access Memory)
 - RAM je tvořen speciálním registrem a potenciálně neomezenou pamětí, instrukční sada obsahuje základní aritmetické operace a metody přímé a nepřímé adresace paměti.
- Dalším teoretickým turingovsky úplným modelem jsou např. WHILE-programy používané v teorii vyčíslitelnosti.

Alonzo Church (1903 – 1995)

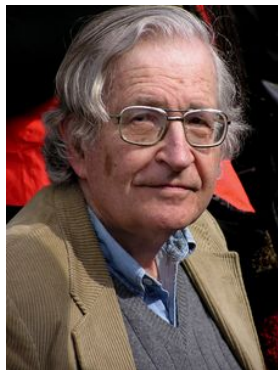
- Americký matematik a logik, který významně přispěl v oblasti teorie vyčíslitelnosti a formálních jazyků.
- Churchova-Turingova teze – původně dvě nezávislé teze, jejichž ekvivalenci dokázal v roce 1952 S. C. Kleene.
 - Teze: *Ke každému algoritmu existuje ekvivalentní Turingův stroj*
- 1936: publikoval λ -kalkul (spolu s Kleenem)
 - Základ funkcionálních programovacích jazyků (např. LISP, Haskell)
 - Formální systém a výpočetní model, jež slouží pro studium funkcí a rekurze
 - Výpočetní silou je ekvivalentní Turingovu stroji



Zdroj: <http://en.wikipedia.org>

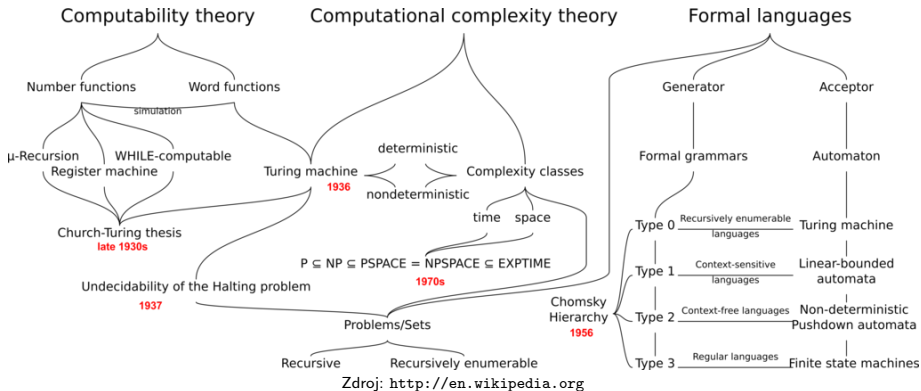
Avram Noam Chomsky (*1928)

- Lingvista, filosof, logik původem z USA
- V lingvistice se zabývá formálními jazyky, emeritní profesor, stále působí na MIT
- 1956: Definoval **Chomského hierarchii jazyků**
 - Zdefinoval formální jazyky a vztahy mezi nimi
 - Chomského hierarchie jazyků patří k základním stavebním kamenům informatiky
 - regulární \subset bezkontextové \subset kontextové \subset rekursivně spočetné jazyky



Zdroj: <http://en.wikipedia.org>

Vztahy mezi vyčíslitelností, složitostí a formálními jazyky



- Součást teorie vyčíslitelnosti a složitosti
- Využívá se pro určení zdrojů (čas, prostor) potřebných pro běh algoritmu.
- Asymptotická složitost (*Big O notation*)
 - Součást rozsáhlejší Bachmann-Landau notace, která vznikla již na počátku 19. století.
 - Původně určena pro zjišťování chování funkcí.

Donald Ervin Knuth (*1938)

- Emeritní profesor na Stanford University
- Bývá označován jako otec analýzy algoritmů
- Zasadil se o využití asymptotické notace v analýze algoritmů, významně také přispěl v oblasti výpočetní složitosti.
- Vedle teoretické informatiky je také autorem sázecího systému $\text{T}_{\text{E}}\text{X}$ a autorem „programátorské bible“ *The Art of Computer Programming*



Zdroj: <http://en.wikipedia.org>

Edsger Wybe Dijkstra (1930 – 2002)

- Holandský informatik, který významně ovlivnil mnoho oblastí informatiky.
- Za významný přínos v rozvoji programovacích jazyků získal v roce 1972 Turingovu cenu.
- 1968: V článku *A Case against the GO TO Statement* prezentoval problémy používání příkazu GO TO.
- Patřil mezi průkopníky distribuovaného počítání, zavedl pojem **semaforu**.
- V teorii grafů je známý díky algoritmu pro hledání nejkratší cesty.



Zdroj: <http://en.wikipedia.org>

- Odvětví informatiky, které se zabývá měřením, přenosem, kódováním, ukládáním a následným zpracováním informací.
- Spojuje aplikovanou matematiku a elektrotechniku.
- Praktickými výsledky jsou algoritmy pro ztrátovou a bezztrátovou kompresi dat a modulační techniky signálu.
- Zakladatelem tohoto oboru je Claude Shannon.
- Klíčovým pojmem je **entropie** (míra neurčitosti informace).

Claude Elwood Shannon (1916 – 2001)

- Americký matematik, elektrotechnik a kryptograf
- 1938: Využil poznatků booleovy algebry pro návrh přepínacích okruhů (založených na relé)
- Během 2.SV se podílel jako kryptoanalytik i na rozluštění šifer používaných německými ponorkami.
- 1948: Po válce ve svém článku *A Mathematical Theory of Communication* položil základy teorie informace. Dále se zaměřil na způsoby, jak co nejefektivněji zakódovat informace.
- Claude E. Shannon Award (IEEE) – ocenění pro významné osobnosti v teorii informace



Zdroj: <http://en.wikipedia.org>

- Věda, která se zabývá principy řízení a přenosu informací v komplexních systémech (strojích, živých organismech a společnostech).
- K popisu procesů je použit matematický aparát.
- **Norbert Wiener** (1894 – 1964) – matematik, profesor na MIT, považován za zakladatele kybernetiky
- 1948: kniha *Kybernetika aneb Řízení a sdělování u organismů a strojů*



Zdroj: <http://www.nap.edu>

Nositelé titulu Doctor honoris Causa na MU

- Donald E. Knuth
 - viz výše
- Niklaus Wirth
 - navrhl několik programovacích jazyků (např. Pascal); nositel Turingovy ceny
- Charles Bennett
 - jeden ze zakladatelů moderní teorie kvantové informace
- Dines Bjørner
 - Zabýval se oblastí formálních metod pro vývoj počítačových systémů, jeho stěžejním dílem je trojdílná publikace Software Engineering.
- Javier Esparza
 - Zabývá se verifikací a formálními modely distribuovaných systémů
- http://www.fi.muni.cz/about/cestne_doktoraty.xhtml

- Významných osobností informatiky a výpočetní techniky je mnohem více a s dalšími jmény se zcela jistě potkáme ještě později v semestru či v jiných kurzech.
- Žádná z uvedených osobností nepůsobila jen v rámci jedné podoblasti informatiky, ale měli daleko širší záběr i do jiných oborů (např. Gödel).
- Mnohé myšlenky byly natolik převratné, že zcela změnily další směřování výzkumu a vývoje v této oblasti.