# *Profinite semigroups and applications in Computer Science*

Jorge Almeida

Departamento Matemática, CMUP
Faculdade de Ciências, Universidade do Porto
Porto, Portugal
http://www.fc.up.pt/cmup/jalmeida/

October, 2011
Ústav matematiky a statistiky
Přírodovědecká fakulta
Masarykova univerzita

# Abstract

Finite semigroups appear naturally in Computer Science, namely as syntactic semigroups of regular languages, transition semigroups of finite automata, or as finite recognizing devices on their own. Eilenberg's correspondence theorem gives a general framework for the classification of regular languages through algebraic properties of their syntactic semigroups. Here is the resulting typical problem on the algebraic side: a recursively enumerable set R of finite semigroups is given and one wishes to decide whether a given finite semigroup is a homomorphic image of a subsemigroup of a finite product of members of R. Since such a problem is often undecidable, special techniques have been devised to handle special cases. Relatively free profinite semigroups turn out to be quite useful in this context. They play the role of free algebras in Universal Algebra, capturing in their algebraic-topological/metric structure combinatorial properties of the corresponding classes of languages.
The aim of this short course is to introduce reltively free profinite semigroups and to explore two topics in which there have been significant recent developments, namely the separation of a given word from a given regular language by a regular language of a special type (for instance, a group language), and connections with symbolic dynamics.
Tentative syllabus and preliminary references:

Part 1 Relatively free profinite semigroups. (1 lecture)
Reference:
[1] J. Almeida, Profinite semigroups and applications, in "Structural Theory of Automata, Semigroups, and Universal Algebra", V. B. Kudryavtsev and I. G. Rosenberg (eds.), Proceedings of the NATO Advanced Study Institute on Structural Theory of Automata, Semigroups and Universal Algebra (Montréal, Québec, Canada, 7-18 July 2003), Springer, New York, 2005, pp. 1-45.

Part 2 Separating words and regular languages. (2 lectures)
Reference:
[2] S. Margolis, M. Sapir, and P. Weil, Closed subgroups in pro-V topologies and the extension problem for inverse automata, Int. J. Algebra and Comput. 11 (2001) 405-455.

Part 3 Relatively free profinite semigroups and Symbolic Dynamics. (2 lectures)
Reference:
[1] (see above).

# Part I

## *Relatively free profinite semigroups*

# Outline

- A regular language is a subset of the free monoid $A^*$ on an alphabet $A$ admitting a regular expression, i.e., a formal expression describing it in terms of the empty set $\emptyset$ and the letters $a \in A$ using the following operations:
  - $(K, L) \mapsto K \cup L$ (union)
  - $(K, L) \mapsto KL$ (concatenation)
  - $L \mapsto L^*$ (Kleene star)
- The syntactic congruence of the language $L \subseteq A^*$ is the binary relation $\sigma_L$ on $A^*$ defined by:

$$u \, \sigma_L \, v \quad \text{if } \forall \, x, y \in A^* \ (xuy \in L \Leftrightarrow xvy \in L).$$

- The syntactic monoid $M(L)$ of the language $L \subseteq A^*$ is the quotient monoid $A^*/\sigma_L$.

## Theorem 1.1

*The following conditions are equivalent for a language $L$ over a finite alphabet $A$:*

(1) *$L$ is regular;*

(2) *$L$ is recognized by some finite automaton;*

(3) *$L$ is recognized by some finite complete deterministic automaton;*

(4) *the syntactic monoid $A^*/\sigma_L$ on $A^*$ is finite;*

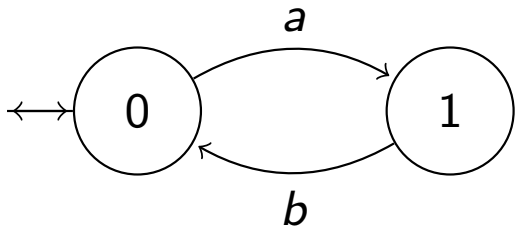
(5) *$L$ is recognized by some homomorphism $\varphi : A^* \to M$ into a finite monoid, in the sense that $L = \varphi^{-1}\varphi L$.*

## Corollary 1.2

*The set $\mathrm{Reg}(A^*)$ of all regular languages over the alphabet $A$ is a Boolean subalgebra of the Boolean algebra of all subsets of $A^*$.*

# Example: (restricted) Dyck languages

- Regular expression: $L_1 = (ab)^*$
- Minimal (incomplete) automaton:




- Transition monoid ($M(L_1)$):

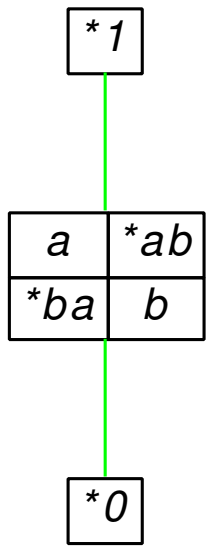
| | 0 | 1 |
|---|---|---|
| $a$ | 1 | - |
| $b$ | - | 0 |
| $ab$ | 0 | - |
| $ba$ | - | 1 |
| 0 | - | - |

| | $a$ | $b$ | $ab$ | $ba$ | 0 |
|---|---|---|---|---|---|
| $a$ | 0 | $ab$ | 0 | $a$ | 0 |
| $b$ | $ba$ | 0 | $b$ | 0 | 0 |
| $ab$ | $a$ | 0 | $ab$ | 0 | 0 |
| $ba$ | 0 | $b$ | 0 | $ba$ | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 |

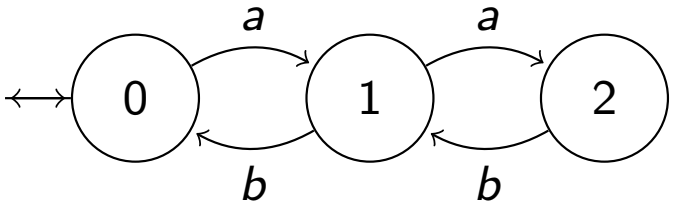
- Presentation: $\langle a, b;\ aba = a,\ bab = b,\ a^2 = b^2 = 0 \rangle$.

One may then compute Green's relations, which are summarized in the following eggbox picture:

- same row: elements generate the same right ideal ($\mathcal{R}$)
- same column: elements generate the same left ideal ($\mathcal{L}$)
- elements above are factors of elements below ($\geq_{\mathcal{J}}$)
- $^*e$ marks an idempotent ($e^2 = e$)
- the "eggboxes" are the $\mathcal{J}$-classes ($\mathcal{J} = \geq_{\mathcal{J}} \cap \leq_{\mathcal{J}}$)
- $\mathcal{D} = \mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$
- in a finite monoid, $\mathcal{D} = \mathcal{J}$



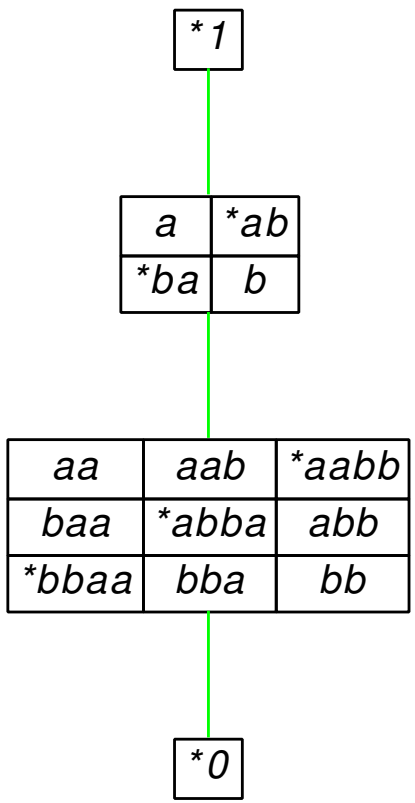
- Regular expression: $L_2 = (a(ab)^*b)^*$
- Minimal (incomplete) automaton:



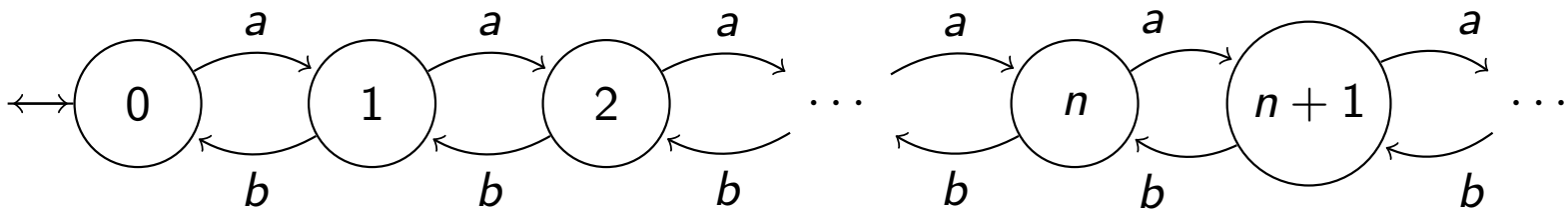

- Presentation of syntactic monoid $M(L_2)$:

$$\langle a, b;\ aba = a, bab = b, a^2b^2a^2 = a^2, b^2a^2b^2 = b^2,$$
$$ab^2a = ba^2b, a^3 = b^3 = 0\rangle$$

- Eggbox picture:



- Dyck language: $L_\infty = \bigcup_{n\geq 0} L_n$, where $L_0 = \{1\}$, $L_{n+1} = (aL_nb)^*$.
- Recognition by infinite automaton:

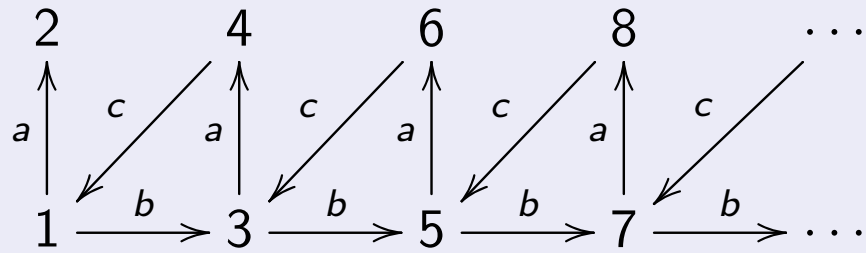



- Syntactic monoid: $M(L_\infty) = \langle a, b; ab = 1\rangle$.
- Eggbox picture:

| | | | | | | |
|---|---|---|---|---|---|---|
| $^*1$ | $a$ | $a^2$ | $\cdots$ | $a^n$ | $a^{n+1}$ | $\cdots$ |
| $b$ | $^*ba$ | $ba^2$ | $\cdots$ | $ba^n$ | $ba^{n+1}$ | $\cdots$ |
| $b^2$ | $b^2a$ | $^*b^2a^2$ | $\cdots$ | $b^2a^n$ | $b^2a^{n+1}$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ | $\vdots$ | $\vdots$ | |
| $b^n$ | $b^na$ | $b^na^2$ | $\cdots$ | $^*b^na^n$ | $b^na^{n+1}$ | $\cdots$ |
| $b^{n+1}$ | $b^{n+1}a$ | $b^{n+1}a^2$ | $\cdots$ | $b^{n+1}a^n$ | $^*b^{n+1}a^{n+1}$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ | $\ddots$ |

# Exercise 1.3

Consider the transition semigroup $S$ of the following infinite automaton:




1. Note that, in $S$, $aca$ is a factor of $a$ but $a$ is not regular.
2. Verify that $S$ admits the following presentation:

$$\langle a, b, c;\ baca = a, bacb = b^2ac = b, cbac = c,$$
$$a^2 = ab = bc = c^2 = 0\rangle.$$

3. Show that $S$ has two $\mathcal{J}$-classes, one of which is reduced to zero.
4. Show that the non-trivial $\mathcal{J}$-class of $S$ consists of two infinite $\mathcal{D}$-classes, one of which is regular and a bicyclic monoid, while the other is not regular and has only one $\mathcal{L}$-class. All $\mathcal{H}$-classes of $S$ are trivial.

# Outline

- A variety of languages is a correspondence $\mathcal{V}$ associating with each finitely generated free monoid $A^*$ a set $\mathcal{V}(A^*)$ of languages over the finite alphabet $A$ such that the following conditions hold:
  1. $\mathcal{V}(A^*)$ is a Boolean subalgebra of $\mathrm{Reg}(A^*)$;
  2. if $L \in \mathcal{V}(A^*)$ and $a \in A$, then the following languages also belong to $\mathcal{V}(A^*)$:

$$a^{-1}L = \{w \in A^* : aw \in L\}$$
$$La^{-1} = \{w \in A^* : wa \in L\};$$

  3. if $\varphi : A^* \to B^*$ is a homomorphism and $L \in \mathcal{V}(B^*)$, then $\varphi^{-1}(L) \in \mathcal{V}(A^*)$.
- A pseudovariety of monoids is a nonempty class $\mathbf{V}$ of finite monoids which is closed under taking homomorphic images, submonoids, and finite direct products.

## Theorem 2.1 (Eilenberg [Eil76])

*The complete lattices of varieties of languages and of pseudovarieties of monoids are isomorphic. More precisely, the following correspondences are mutually inverse isomorphisms between the two lattices:*

- *to a variety $\mathcal{V}$ of languages, associate the pseudovariety $\mathbf{V}$ generated by all syntactic monoids $M(L)$ with $L \in \mathcal{V}(A^*)$ for some finite alphabet $A$;*
- *to a pseudovariety $\mathbf{V}$, associate the variety of languages $\mathcal{V}$ such that, for each finite alphabet $A$, $\mathcal{V}(A^*)$ consists of the languages $L \subseteq A^*$ such that $M(L) \in \mathbf{V}$.*

- Thus, problems about varieties of languages admit a translation into problems about pseudovarieties of monoids.
- For instance, to determine if a language $L \subseteq A^*$ belongs to smallest variety of languages containing two given varieties of languages $\mathcal{V}$ and $\mathcal{W}$ is equivalent to determine if $M(L)$ belongs to the pseudovariety join $\mathbf{V} \vee \mathbf{W}$.
- Typically, we are given a recursively enumerable set $\mathcal{R}$ of finite monoids and we want to determine an algorithm to decide whether a given finite monoid $M$ belongs to the pseudovariety $\mathbf{V}(\mathcal{R})$ generated by $\mathcal{R}$.

*Mutatis mutandis*, we have

- languages $L \subseteq A^+$ without the empty word 1;
- syntactic congruence $\sigma_L$ of $L$ over $A^+$:

$$u \,\sigma_L\, v \quad \text{if } \forall\, x, y \in A^* \ (xuy \in L \Leftrightarrow xvy \in L).$$

- syntactic semigroup $A^+/\sigma_L$;
- varieties of languages without the empty word;
- pseudovarieties of semigroups;
- Eilenberg's correspondence in this setting.

Examples of pseudovarieties:

- **S**: all finite semigroups
- **I**: all singleton (trivial) semigroups
- **G**: all finite groups
- $\mathbf{G}_p$: all finite $p$-groups
- **A**: all finite aperiodic semigroups
- **Com**: all finite commutative semigroups
- **J**: all finite $\mathcal{J}$-trivial semigroups
- **R**: all finite $\mathcal{R}$-trivial semigroups
- **L**: all finite $\mathcal{L}$-trivial semigroups
- **Sl**: all finite semilattices
- **RZ**: all finite right-zero semigroups
- **B**: all finite bands
- **N**: all finite nilpotent semigroups
- **K**: all finite semigroups in which idempotents are left zeros
- **D**: all finite semigroups in which idempotents are right zeros

# Important examples of instances of Eilenberg's correspondence

- A language $L \subseteq A^+$ is said to be star free if it admits an expression in terms of the languages $\{a\}$ ($a \in A$) using only the operations: $\_ \cup \_$, $A^+ \setminus \_$, and concatenation.

**Theorem 2.2 ([Sch65])**

*A language over a finite alphabet is star free if and only if its syntactic semigroup is finite and aperiodic.*

- A language $L \subseteq A^*$ is piecewise testable if it is a Boolean combination of languages of the form $A^* a_1 A^* a_2 A^* \cdots a_n A^*$, with the $a_i \in A$.

**Theorem 2.3 ([Sim75])**

*A language over a finite alphabet is piecewise testable if and only if its syntactic semigroup is finite and $\mathcal{J}$-trivial.*

- A language $L \subseteq A^*$ is locally testable if it is a Boolean combination of languages of the forms $A^* u$, $A^* v A^*$, and $w A^*$, where $u, v, w \in A^+$.

**Theorem 2.4 ([BS73, MP71])**

*A language $L$ over a finite alphabet is locally testable if and only if its syntactic semigroup $S$ is finite and a local semilattice (i.e., $eSe$ is a semilattice for every idempotent $e \in S$).*

# Outline

## Definition 3.1

We say that a pseudovariety $\mathbf{V}$ is decidable if there is an algorithm which, given a finite semigroup $S$ as input, produces as output, in finite time, YES or NO according to whether or not $S \in \mathbf{V}$.

The semigroup $S$ may be given in various ways:

- extensively, meaning the complete list of its elements together with its multiplication table;
- as the transformation semigroup on a finite set $Q$ generated by a finite set $A$ of transformations of $Q$ ;
  $\rightarrow$ transition semigroup of a finite automaton $(Q, A, \delta, I, F)$;
- by means of a presentation.
- Different ways of describing $S$ may lead to different complexity results, when such an algorithm exists.

Of course, not all pseudovarieties are decidable.

For instance, if $P$ is a non-recursive set of primes, then the pseudovariety $\mathbf{Ab}_P$, generated by all groups $\mathbb{Z}/p\mathbb{Z}$ with $p \in P$, contains a group $\mathbb{Z}/q\mathbb{Z}$ of prime order $q$ if and only if $q \in P$.

Since there are non-recursive sets of primes $P$, there are pseudovarieties of the form $\mathbf{Ab}_P$ which are not decidable.

**Question 3.2 (Very imprecise!!)**

Are all "natural" pseudovarieties decidable?

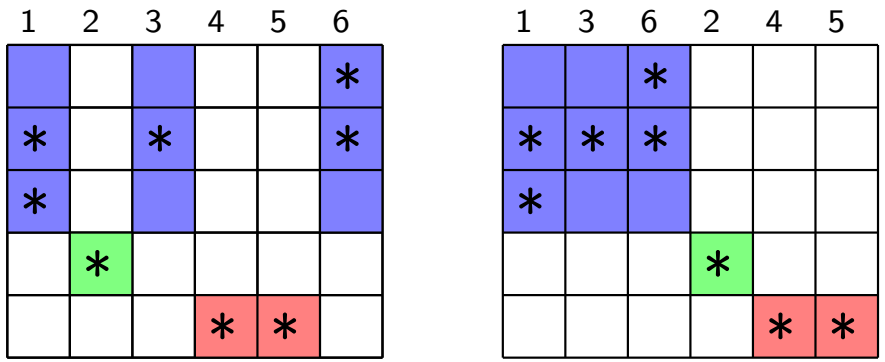
There are many ways to construct new pseudovarieties from known ones, that is by applying operators to pseudovarieties.
We proceed to introduce some natural operators.

## Definition 3.3

Given a pseudovariety $\mathbf{V}$, consider the classes of all finite semigroups $S$ such that, respectively:

- **LV**: $eSe \in \mathbf{V}$ for every idempotent $e \in S$;
- **EV**: $\langle E(S) \rangle \in \mathbf{V}$, where $\langle E(S) \rangle$ is the subsemigroup generated by the set $E(S)$ of all idempotents of $S$;
- **DV**: the regular $\mathcal{J}$-classes of $S$ (are subsemigroups which) belong to $\mathbf{V}$;
- $\overline{\mathbf{V}}$: the subgroups of $S$ belong to $\mathbf{V}$;

- Let $S$ be a finite semigroup and let $D$ be one of its regular $\mathcal{D}$-classes.
- Let $\sim$ be the equivalence relation on the set of group elements of $D$ generated by the identification of elements which are either $\mathcal{R}$ or $\mathcal{L}$-equivalent.
- A block of $D$ is the Rees quotient of the subsemigroup of $S$ generated by a $\sim$-class modulo the ideal consisting of the elements which do not lie in $D$.




- The blocks of $S$ are the blocks of its regular $\mathcal{D}$-classes.

## Definition 3.4

For a pseudovariety **V**, let **BV** be the class of all finite semigroups whose blocks lie in **V**.

## Proposition 3.5

*For a pseudovariety* $\mathbf{V}$*, the classes* $\mathbf{BV}$, $\mathbf{DV}$, $\mathbf{EV}$, $\mathbf{LV}$, $\overline{\mathbf{V}}$ *are pseudovarieties.*
*Moreover, if* $\mathbf{V}$ *is decidable then so are those pseudovarieties.*

## Proof.

We consider only the case of $\mathbf{LV}$, leaving all other cases as exercises.

- If $\varphi : S \to T$ is an onto homomorphism, with $S \in \mathbf{S}$, and $f \in E(T)$, then $\exists e \in \varphi^{-1}(f) \cap E(S)$ and $\varphi|_{eSe} : eSe \to fTf$ is an onto homomorphism
  $\therefore$ $\mathbf{LV}$ is closed under taking homomorphic images.
- If $S \leq T$ and $e \in E(S)$, then $eSe \leq eTe$
  $\therefore$ $\mathbf{LV}$ is closed under taking subsemigroups.
- If $S, T$ are semigroups, $e \in E(S)$, and $f \in E(T)$, then $(e, f)(S \times T)(e, f) \simeq eSe \times fTf$
  $\therefore$ $\mathbf{LV}$ is closed under taking finite direct products.

Given a finite semigroup, one can compute its set of idempotents $E(S)$ and, for each $e \in E(S)$, the monoid $eSe$.
Provided $\mathbf{V}$ is decidable, one can then effectively check whether $eSe \in \mathbf{V}$.
Hence one can effectively check whether $S \in \mathbf{LV}$. □

But, the most interesting operators are defined not in structural terms but rather by describing generators: the resulting pseudovariety is given as the smallest pseudovariety containing certain semigroups which are constructed from those in the argument pseudovarieties.

### Definition 3.6

We say that a semigroup $S$ divides a semigroup $T$, or that $S$ is a divisor of $T$, and we write $S \prec T$, if $S$ is a homomorphic image of a subsemigroup of $T$.

### Proposition 3.7

*Let $\mathcal{C}$ be a class of finite semigroups. Then the smallest pseudovariety $\mathbf{V}(\mathcal{C})$ containing $\mathcal{C}$ consists of all divisors of products of the form $S_1 \times \cdots \times S_n$ with $S_1, \ldots, S_n \in \mathcal{C}$.*
*In particular, if $\mathcal{C}$ is closed under finite direct product, then $\mathbf{V}(\mathcal{C})$ consists of all divisors of elements of $\mathcal{C}$.*

Let $S$ and $T$ be semigroups and let $\varphi : T^1 \to \operatorname{End} S$ be a homomorphism of monoids, with endomorphisms acting on the left. For $s \in S$ and $t \in T^1$, let ${}^t s = \varphi(t)(s)$.
The semidirect product $S *_\varphi T$ is the set $S \times T$ under the multiplication

$$(s_1, t_1) \cdot (s_2, t_2) = (s_1 \, {}^{t_1} s_2, t_1 t_2).$$

## Definition 3.8

The semidirect product $\mathbf{V} * \mathbf{W}$ of the pseudovarieties $\mathbf{V}$ and $\mathbf{W}$ is the smallest pseudovariety containing all semidirect products $S * T$ with $S \in \mathbf{V}$ and $T \in \mathbf{W}$.

## Proposition 3.9

*The pseudovariety $\mathbf{V} * \mathbf{W}$ consists of all divisors of semidirect products of the form $S * T$ with $S \in \mathbf{V}$ and $T \in \mathbf{W}$.*

## Proposition 3.10

*The semidirect product of pseudovarieties is associative.*

## Definition 3.11

The Mal'cev product $\mathbf{V} \textcircled{m} \mathbf{W}$ of two pseudovarieties $\mathbf{V}$ and $\mathbf{W}$ is the smallest pseudovariety containing all finite semigroups $S$ for which there exists a homomorphism $\varphi : S \to T$ such that $T \in \mathbf{W}$ and $\varphi^{-1}(e) \in \mathbf{V}$ for all $e \in E(T)$.

Given two semigroups $S$ and $T$, a relational morphism $S \to T$ is a relation $\mu : S \to T$ with domain $S$ such that $\mu$ is a subsemigroup of $S \times T$.

## Proposition 3.12

*The pseudovariety $\mathbf{V} \textcircled{m} \mathbf{W}$ consists of all finite semigroups $S$ such that there is a relational morphism $\mu : S \to T$ such that $T \in \mathbf{W}$ and $\mu^{-1}(e) \in \mathbf{V}$ for all $e \in E(T)$.*

For a semigroup $S$, denote by $\mathcal{P}(S)$ the semigroup of subsets of $S$ under the product operation

$$X \cdot Y = \{xy : \ x \in X, \ y \in Y\}.$$

Note that the empty set $\emptyset$ is a zero and $\mathcal{P}'(S) = \mathcal{P}(S) \setminus \{\emptyset\}$ is a subsemigroup.

## Definition 3.13

For a pseudovariety $\mathbf{V}$, denote by

**PV**: the pseudovariety generated by all semigroups of the form $\mathcal{P}(S)$, with $S \in \mathbf{V}$;

**P′V**: the pseudovariety generated by all semigroups of the form $\mathcal{P}'(S)$, with $S \in \mathbf{V}$.

## Proposition 3.14

*The pseudovariety* $\mathbf{PV}$ *consists of all divisors of semigroups of the form* $\mathcal{P}(S)$ *with* $S \in \mathbf{V}$.
*Similar statement for* $\mathbf{P}'$.

Some examples of results on finite semigroups formulated in terms of these operators:

1. $\mathbf{J} = \mathbf{N} \mathbin{ⓜ} \mathbf{Sl}$
2. $\mathbf{DA} = \mathbf{LI} \mathbin{ⓜ} \mathbf{Sl}$, $\mathbf{DS} = \mathbf{LG} \mathbin{ⓜ} \mathbf{Sl}$
3. $\mathbf{R} = \mathbf{Sl} * \mathbf{J}$ [Sti73]
4. $\mathbf{G} \vee \mathbf{Com} = \mathbf{ZE}$ (the pseudovariety of all finite semigroups in which idempotents are central) [Alm95]
5. $\mathbf{ESl} = \mathbf{Sl} * \mathbf{G} = \mathbf{Sl} \mathbin{ⓜ} \mathbf{G} = \mathbf{Inv}$ (the pseudovariety generated by all finite inverse semigroups) [MP87, Ash87, Pin95],
   $\mathbf{ER} = \mathbf{R} * \mathbf{G}$ [Eil76], $\mathbf{EDS} = \mathbf{DS} * \mathbf{G}$ [AE03]
6. $\mathbf{PG} = \mathbf{J} * \mathbf{G} = \mathbf{J} \mathbin{ⓜ} \mathbf{G} = \mathbf{EJ} = \mathbf{BG}$
   [MP84, HR91, Ash91, HMPR91, Pin95],
   $\mathbf{PJ} = \mathbf{PV}(Y)$ [PS85, Alm95] where $Y = \mathrm{Synt}(a^* bc^*)$
7. $\mathbf{S} = \bigcup_{n \geq 0} (\mathbf{A} * \mathbf{G})^n * \mathbf{A}$ [KR65]

$$\mathbf{S} = \bigcup_{n \geq 0} (\mathbf{A} * \mathbf{G})^n * \mathbf{A}$$

The (Krohn-Rhodes) hierarchy $\left((\mathbf{A} * \mathbf{G})^n * \mathbf{A}\right)_{n \geq 0}$ is strict.

The smallest $n$ such that a given finite semigroup $S$ belongs to $(\mathbf{A} * \mathbf{G})^n * \mathbf{A}$ is called the complexity of $S$, denoted $c(S)$.

Let $T_n$ denote the full transformation semigroup of an $n$-element set It is known that $c(T_n) = n - 1$ [Eil76] and so certainly $c(S) \leq |S|$ (since $S \hookrightarrow T_{S^1}$).

## Note 3.15

To know an algorithm to compute the complexity function is equivalent to know algorithms to decide the membership problem for each pseudovariety in the Krohn-Rhodes hierarchy.

This brings us to the following basic question:

### Question 3.16

For the operators which were defined above in terms of generators, do they preserve decidability?

### Theorem 3.17 (Albert, Baldinger & Rhodes'1992 [ABR92])

*There exists a finite set $\Sigma$ of identities such that* $\mathbf{Com} \vee [\![\Sigma]\!]$ *is undecidable.*

Let $C_{2,1} = \langle a; a^2 = 0 \rangle^1$.

### Theorem 3.18 (Auinger & Steinberg'2003 [AS03])

*There exists a decidable pseudovariety of groups* $\mathbf{U}$ *such that the following pseudovarieties are all undecidable:*
$\mathbf{Sl} * \mathbf{U}$ *(*$= \mathbf{Sl} \circledcirc{m} \mathbf{U}$*),* $\mathbf{V}(C_{2,1}) \vee \mathbf{U}$*,* $\mathbf{PU}$ *(*$= \mathbf{P}'\mathbf{U}$*).*

The pseudovariety $\mathbf{U}$ is defined to be

$$\mathbf{U} = \bigvee_{p \in A} \mathbf{G}_p * (\mathbf{G}_{f(p)} \cap \mathbf{Com}) \vee \bigvee_{p \in D} (\mathbf{G}_p \cap \mathbf{Com})$$

where:

- $A$ and $B$ constitute a computable partition of the set of primes into two infinite sets;
- $f : A \to B$ is an injective recursive function whose range $C = f(A)$ is recursively enumerable but not recursive;
- $D = B \setminus C$ is not recursively enumerable.

## Exercise 3.19

Show that $\mathbf{U}$ is decidable.

# Outline

- Let $\mathbf{V}$ be a pseudovariety of semigroups.
- For two words $u, v \in A^+$, and $T \in \mathbf{V}$, let

$T \models u = v$ if, for every homomorphism $\varphi : A^+ \to T$, $\varphi(u) = \varphi(v)$,

$$r_{\mathbf{V}}(u, v) = \min\{|S| : S \in \mathbf{V} \text{ and } S \not\models u = v\},$$

$$d_{\mathbf{V}}(u, v) = 2^{-r_{\mathbf{V}}(u,v)}$$

where we take $\min \emptyset = \infty$ and $2^{-\infty} = 0$.

## Note 4.1

The following hold for $u, v, w, t \in A^+$ and a positive integer $n$:

(1) $r_{\mathbf{V}}(u, v) \geq n$ if and only if, for every $S \in \mathbf{V}$ with $|S| < n$, $S \models u = v$;
(2) $d_{\mathbf{V}}(u, v) \leq 2^{-n}$ if and only if, for every $S \in \mathbf{V}$ with $|S| < n$, $S \models u = v$;
(3) $d_{\mathbf{V}}(u, v) = 0$ if and only if, for every $S \in \mathbf{V}$, $S \models u = v$;
(4) $\min\{r_{\mathbf{V}}(u, v), r_{\mathbf{V}}(v, w)\} \leq r_{\mathbf{V}}(u, w)$;
(5) $\min\{r_{\mathbf{V}}(u, v), r_{\mathbf{V}}(w, z)\} \leq r_{\mathbf{V}}(uw, vz)$.

## Definition 4.2

A function $d : X \times X \to \mathbb{R}_{\geq 0}$ is said to be a pseudo-ultrametric on the set $X$ if the following properties hold for all $u, v, w \in X$:

1. $d(u, u) = 0$;
2. $d(u, v) = d(v, u)$;
3. $d(u, w) \leq \max\{d(u, v), d(v, w)\}$.

We then also say that $X$ is a pseudo-ultrametric space.
If instead of Condition 3, the following weaker condition holds

4. $d(u, w) \leq d(u, v) + d(v, w)$ (triangle inequality).

then $d$ is said to be a pseudo-metric on $X$, and $X$ is said to be a pseudo-metric space. If the following condition holds

5. $d(u, v) = 0$ if and only if $u = v$,

then we drop the prefix "pseudo".

- A function $f : X \to Y$ between two pseudo-metric spaces is said to be uniformly continuous if the following condition holds:

$$\forall\, \epsilon > 0\ \exists\, \delta > 0\ \forall\, x_1, x_2 \in X\ \big(d(x_1, x_2) < \delta \Rightarrow d(f(u), f(v)) < \epsilon\big).$$

## Proposition 4.3

1. *The function $d_{\mathbf{V}}$ is a pseudo-ultrametric on $A^+$.*
2. *The multiplication is contractive:*

$$d_{\mathbf{V}}(u_1 u_2, v_1 v_2) \leq \max\{d_{\mathbf{V}}(u_1, v_1), d_{\mathbf{V}}(u_2, v_2)\}.$$

*In particular, the multiplication on $A^+$ is uniformly continuous.*

- For a (pseudo-ultra)metric $d$, $u \in X$, and a positive real number $\epsilon$, consider the open ball

$$B_\epsilon(u) = \{v \in X : d(u, v) < \epsilon\}.$$

The point $u$ is the center and $\epsilon$ is the radius of the ball.

- A metric space that can be covered by a finite number of balls of any given positive radius is said to be totally bounded.

## Proposition 4.4

*The metric space $(A^+, d_{\mathbf{V}})$ is totally bounded.*

## Proof.

Let $n$ be a positive integer such that $2^{-n} < \epsilon$. Note that, up to isomorphism, there are only finitely many semigroups of cardinality at most $n$ in $\mathbf{V}$. For such a semigroup $S_i$ consider all possible homomorphisms $\varphi_{i,j} : A^+ \to S_i$, let $S = \prod_{i,j} S_i$ and

$$\begin{aligned} \varphi : A^+ &\to S \\ u &\mapsto (\varphi_{i,j}(u))_{i,j}. \end{aligned}$$

Then $S \in \mathbf{V}$ and $d_{\mathbf{V}}(u, v) < 2^{-n}$ if and only if $\varphi(u) = \varphi(v)$.

For each $s \in S$, choose $u_s \in A^+$ such that $\varphi(u_s) = s$.

For $v \in A^+$ and $s = \varphi(v)$, we have $\varphi(v) = \varphi(u_s)$, and so $v \in B_\epsilon(u_s)$.

We have thus shown that $A^+ = \bigcup_{s \in S} B_\epsilon(u_s)$. □

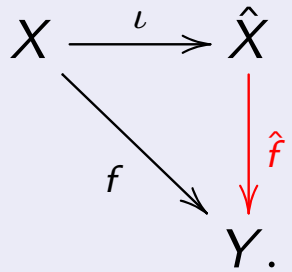
- A sequence $(u_n)_n$ in a (pseudo-ultra)metric space $X$ is said to be a Cauchy sequence if

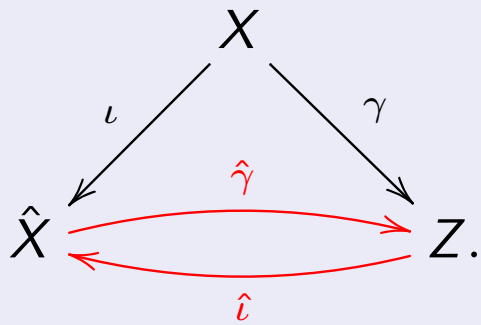
$$\forall\, \epsilon > 0\ \exists\, N\ \big(m, n \geq N \Rightarrow d(u_m, u_n) < \epsilon\big).$$

- Note that every convergent sequence is a Cauchy sequence.
- The space $X$ is complete if every Cauchy sequence in $X$ converges in $X$.

## Theorem 4.5

*Let $X$ be a pseudo-(ultra)metric space. Then there exists a complete metric space $\hat{X}$ and a uniformly continuous function $\iota : X \to \hat{X}$ with the following universal property: for every uniformly continuous function $f : X \to Y$ into a complete metric space $Y$, there exists a unique uniformly continuous function $\hat{f} : \hat{X} \to Y$ such that $\hat{f} \circ \iota = f$.*




*In particular, if $\gamma : X \to Z$ is another uniformly continuous function into another complete metric space with the above universal property then the induced unique uniformly continuous mappings $\hat{\iota} : \hat{X} \to Z$ and $\hat{\gamma} : Z \to \hat{X}$ are mutually inverse.*

- The "unique" space $\hat{X}$ of Theorem 4.5 is called the Hausdorff completion of $X$.

- It may be constructed in the same way that the real numbers are obtained by completion of the rational numbers. Here is a sketch:
  - (A) consider the set $C \subseteq X^{\mathbb{N}}$ of all Cauchy sequences of elements of $X$;
  - (B) note that, for $s = (u_n)_n$ and $t(v_n)_n$ in $C$, the sequence of real numbers $\big(d(u_n, v_n)\big)_n$ is a Cauchy sequence and, therefore, it converges; its limit is denoted $d(s, t)$;

$$\begin{aligned} &|d(u_n, v_n) - d(u_m, v_m)| \\ &\quad \leq |d(u_n, v_n) - d(u_n, v_m)| + |d(u_n, v_m) - d(u_m, v_m)| \\ &\quad \leq d(u_n, u_m) + d(v_n, v_m) \end{aligned}$$

  - (C) Step (B) defines a pseudo-(ultra)metric on $C$;
  - (D) for $s = (u_n)_n$ and $t(v_n)_n$ in $C$, let $s \sim t$ if $d(s, t) = 0$; this is an equivalence relation on $C$; the class of $s$ is denoted $s/\!\sim$;
  - (E) let $\hat{X} = C/\!\sim$ and put $d(s/\!\sim, t/\!\sim) = d(s, t)$, which can be easily checked to be defined;
  - (F) finally, let $\iota : X \to \hat{X}$ map each $u \in X$ to the $\sim$-class of the constant sequence $(u)_n$, and check that this mapping is uniformly continuous and has the appropriate universal property.

- Note that $\iota(X)$ is dense in $\hat{X}$.
- In particular, we may consider the Hausdorff completion of the pseudo-ultrametric space $(A^+, d_{\mathbf{V}})$, which is denoted $\overline{\Omega}_A\mathbf{V}$.
- Since the multiplication of $A^+$ is uniformly continuous with respect to $d_{\mathbf{V}}$, it induces a uniformly continuous multiplication in $\overline{\Omega}_A\mathbf{V}$:

$$\begin{array}{ccc} A^+ \times A^+ & \xrightarrow[(\text{mult.})]{\mu} & A^+ \\ \downarrow{\scriptstyle \iota\times\iota} & & \downarrow{\scriptstyle \iota} \\ \overline{\Omega}_A\mathbf{V} \times \overline{\Omega}_A\mathbf{V} & \xrightarrow{\hat{\mu}} & \overline{\Omega}_A\mathbf{V} \end{array}$$

- We endow each finite semigroup $S$ with the discrete metric:

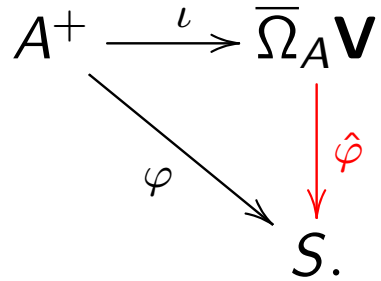
$$d(s,t) = \begin{cases} 0 & \text{if } s = t \\ 1 & \text{otherwise} \end{cases}$$

- Since $\iota(A^+)$ is dense in $\overline{\Omega}_A\mathbf{V}$, multiplication in $\overline{\Omega}_A\mathbf{V}$ is associative, and thus $\overline{\Omega}_A\mathbf{V}$ is naturally a semigroup.
- From hereon, we write $d$ for $d_{\mathbf{V}}$. The context should leave clear which pseudovariety is involved.

- Note that, for $S \in \mathbf{V}$, every homomorphism $\varphi : A^+ \to S$ is uniformly continuous with respect to $d$.

$$d(u, v) < 2^{-|S|} \Rightarrow d(\varphi(u), \varphi(v)) = 0.$$

Thus, $\varphi$ induces a unique uniformly continuous mapping $\hat{\varphi} : \overline{\Omega}_A\mathbf{V} \to S$ such that the following diagram commutes:




One can easily check that $\hat{\varphi}$ is a homomorphism:

$$\begin{aligned}\hat{\varphi}(uv) &= \lim \varphi(\iota(u_n v_n)) = \lim \varphi(\iota(u_n))\varphi(\iota(v_n)) \\ &= \lim \varphi(\iota(u_n)) \cdot \lim \varphi(\iota(v_n)) = \hat{\varphi}(u)\hat{\varphi}(v).\end{aligned}$$

- Given $u, v \in \overline{\Omega}_A\mathbf{V}$ and $S \in \mathbf{V}$, we write $S \models u = v$ if, for every homomorphism $\varphi : A^+ \to S$ (which is determined by $\varphi|_A$), the equality $\hat{\varphi}(u) = \hat{\varphi}(v)$ holds.
  We call the formal equality $u = v$ a **V**-pseudoidentity.
- Note that, if $u = \lim u_n$, $v = \lim v_n$, and $S \in \mathbf{V}$, then $S \models u = v$ if and only if $S \models u_n = v_n$ for all sufficiently large $n$.
- Given distinct elements $u, v \in \overline{\Omega}_A\mathbf{V}$, there exists a positive integer $m$ such that $d(u, v) \geq 2^{-m}$.

  Consider sequences of words $(u_n)_n$ and $(v_n)_n$ such that $u = \lim \iota(u_n)$ and $v = \lim \iota(v_n)$.

  Then, for sufficiently large $n$, $d(u, \iota(u_n)) < 2^{-m}$ and $d(v, \iota(v_n)) < 2^{-m}$.

  Hence $d(u_n, v_n) = d(\iota(u_n), \iota(v_n)) \geq 2^{-m}$ for all sufficiently large $n$.

  It follows that every $S \in \mathbf{V}$ with $|S| < m$ fails the identity $u_n = v_n$ and, therefore, also the pseudoidentity $u = v$.

## Proposition 4.6

*For $u, v \in \overline{\Omega}_A\mathbf{V}$, we have $d(u,v) = 2^{-r(u,v)}$, where*

$$r(u,v) = \min\{|S| : S \in \mathbf{V} \text{ and } S \not\models u = v\}.$$

## Proof.

We have already shown that $d(u,v) \geq 2^{-m}$ implies $r(u,v) \leq m$. The converse, as well as how the equivalence gives the proposition are left as an exercise. □

- Recall that a metric space is compact if every sequence admits some convergent subsequence. Equivalently, every covering by open subsets contains a finite covering.

## Proposition 4.7

1. *If $X$ is a totally bounded pseudo-metric space, then $\hat{X}$ is also totally bounded.*
2. *If $X$ is a totally bounded complete metric space, then $X$ is compact.*

## Proof.

1. Given $\epsilon > 0$, let $u_1, \ldots, u_m \in X$ be such that $X = \bigcup_{i=1}^m B_{\epsilon/2}(u_i)$. Then $\hat{X} = \bigcup_{i=1}^m B_\epsilon(\iota(u_i))$ since every element of $\hat{X}$ is at distance at most $\epsilon/2$ of some element of $\iota(X)$.

2. For each positive integer $m$, let $F_m$ be a finite subset of $X$ such that $X = \bigcup_{x \in F_m} B_{2^{-m}}(x)$ and consider an arbitrary sequence $(u_n)_n$ in $X$.

For infinitely many indices $n$, the $u_n$ belong to the same $B_{2^{-1}}(x_1)$. Let $k_1$ be the first of these indices. Similarly, among the remaining such indices, there are infinitely many $n$ such that the $u_n$ belong to the same $B_{2^{-2}}(x_2)$. We let $k_2$ be the first of them. And so on.

We thus construct a subsequence $(u_{k_n})_n$ with the property that $d(u_{k_m}, u_{k_n}) \leq 2^{-\min\{m,n\}+1}$,

*if* $p = \min\{m, n\}$, *then* $u_{k_m}, u_{k_n} \in B_{2^{-p}}(x_p)$, *which yields*

$$d(u_{k_m}, u_{k_n}) \leq d(u_{k_m}, x_p) + d(x_p, u_{k_n}) \leq 2^{-p} + 2^{-p}$$

whence a Cauchy sequence and, therefore, convergent. □

# Outline

- By a pro-**V** semigroup we mean a semigroup $S$ endowed with a metric such that the following properties hold:
  1. $S$ is compact;
  2. the multiplication is uniformly continuous (metric semigroup);
  3. for every pair $u, v$ of distinct elements of $S$, there is a uniform continuous homomorphism $\varphi : S \to T$ into a semigroup from **V** such that $\varphi(u) \neq \varphi(v)$ ($S$ residually in **V**).
- By a profinite semigroup we mean a pro-**S** semigroup.

## Proposition 5.1

*Let $S$ be a pro-$\mathbf{V}$ semigroup. Then there is a sequence $(S_n)_{n\in\mathbb{N}}$ of semigroups from $\mathbf{V}$ and an injective homomorphism $\varphi : S \to \prod_{n\in\mathbb{N}} S_n$ such that, for each component projection $\pi_m : \prod_{n\in\mathbb{N}} S_n \to S_m$, the homomorphism $\pi_m \circ \varphi$ is uniformly continuous.*

*We may define in $\prod_{n\in\mathbb{N}} S_n$ a metric structure by letting*

$$d(u,v) = \sum_{n\in\mathbb{N}} 2^{-n} d_n(\pi_n(u), \pi_n(v))$$

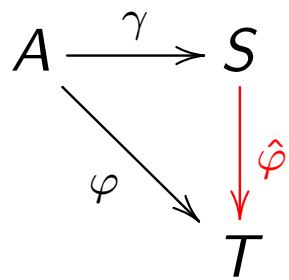
*where $d_n$ is the discrete metric on $S_n$. Then $\varphi$ is uniformly continuous. In particular, the image $T$ of $\varphi$ is closed in $\prod_{n\in\mathbb{N}} S_n$, being a compact subset.*

- Note that the sequence $(S_n)_{n\in\mathbb{N}}$ may be chosen so that there is a finite bound on the number of generators of the $S_n$ if and only if $S$ is finitely generated in the sense that there is a finite subset which generates a dense subsemigroup.
- On the other hand, if there is no such bound, one can show that $S$ cannot have a countable dense subset, while it is easy to see that a compact metric space always admits a countable dense subset.

### Proposition 5.2

*Every pro-**V** metric semigroup is finitely generated.*

- For a finite set $A$, we say that the pro-$\mathbf{V}$ semigroup $S$ is freely generated by $A$ if there is a mapping $\gamma : A \to S$ such that $\gamma(A)$ generates a dense subsemigroup of $S$ and the following universal property is satisfied, where $\varphi : A \to T$ is an arbitrary mapping into a pro-$\mathbf{V}$ semigroup $T$, and $\hat{\varphi}$ is a unique continuous homomorphism:

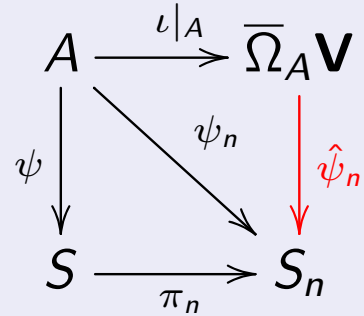



## Theorem 5.3

*For a pseudovariety of semigroups* $\mathbf{V}$ *and a finite set* $A$*, the metric semigroup* $\overline{\Omega}_A\mathbf{V}$ *is a pro-*$\mathbf{V}$ *semigroup freely generated by* $A$ *via the mapping* $\iota|_A$*.*

## Proof.

Let $S$ be a pro-$\mathbf{V}$ semigroup and let $(S_n)_{n\in\mathbb{N}}$ be a countable family of semigroups from $\mathbf{V}$ as given by Proposition 5.1, so that there is an embedding $\varphi : S \to \prod_{n\in\mathbb{N}} S_n$ with each composite function $\pi_n \circ \varphi : S \to S_n$ uniformly continuous.
Given a mapping $\psi : A \to S$, let $\psi_n = \pi_n \circ \psi$.




The family $(\hat{\psi}_n)_{n\in\mathbb{N}}$ induces a homomorphism $\hat{\psi} : \overline{\Omega}_A\mathbf{V} \to \prod_{n\in\mathbb{N}} S_n$. Its image lies in the closed subsemigroup $T$, whence it lifts to the required continuous homomorphism $\overline{\Omega}_A\mathbf{V} \to S$. It is uniformly continuous because every continuous mapping from a compact metric space into another metric space is uniformly continuous. □

- A subset of a metric space is said to be clopen if it is both closed and open.
- A metric space is said to be zero-dimensional if every open set is a union of clopen subsets.

## Proposition 5.4

*Every pro-**V** semigroup is zero-dimensional.*

## Proof.

Let $u$ be an element of the pro-**V** semigroup $S$. It suffices to show that the open ball $B_\epsilon(u)$ contains some clopen set which contains $u$.
For each $v \in S \setminus B_\epsilon(u)$, let $\varphi_v : S \to T_v$ be a uniformly continuous homomorphism into a semigroup from **V** such that $\varphi_v(u) \neq \varphi_v(v)$. Then $K_v = \varphi_v^{-1}\varphi_v(v)$ is a clopen set which contains $v$ but not $u$. In particular, the $K_v$ form a clopen covering of the closed set $S \setminus B_\epsilon(u)$, from which a finite covering $\mathcal{F}$ can be extracted.
The union of the clopen sets in $\mathcal{F}$ is itself a clopen set $K$. Note that $S \setminus K$ is also clopen, contains $u$, and is contained in $B_\epsilon(u)$. □

- For a mapping $\varphi : S \to T$, let $\ker \varphi = \{(u, v) : \varphi(u) = \varphi(v)\}$ be the kernel of $\varphi$.

## Theorem 5.5

*An $A$-generated profinite semigroup $S$ is a continuous homomorphic image of $\overline{\Omega}_A\mathbf{V}$ if and only if it is a pro-$\mathbf{V}$ semigroup.*

## Corollary 5.6

*Let $S$ be a pro-$\mathbf{V}$ semigroup and suppose that $\varphi : S \to T$ is a continuous homomorphism onto a finite semigroup. Then $T \in \mathbf{V}$.* □

## Proof of Theorem 5.5.

($\Leftarrow$) Apply Theorem 5.3.

($\Rightarrow$) Let $\varphi : \overline{\Omega}_A\mathbf{V} \to S$ be an onto continuous homomorphism. We need to show that $S$ is residually in $\mathbf{V}$.
Given distinct points $s_1, s_2 \in S$, since $S$ is residually in $\mathbf{S}$, there is an onto uniformly continuous homomorphism $\psi : S \to T$ such that $T \in \mathbf{S}$ and $\psi(s_1) \neq \psi(s_2)$. Note that $T$ is a finite continuous homomorphic image of $\overline{\Omega}_A\mathbf{V}$. If we can show that $S \in \mathbf{V}$, we will be done. In other words, it suffices to consider the case where $S$ is finite.
Since $\varphi$ is continuous and $\overline{\Omega}_A\mathbf{V}$ is compact, $\varphi$ is uniformly continuous. Hence, there is a positive integer $n$ such that, for all $u, v \in \overline{\Omega}_A\mathbf{V}$,

$$d(u, v) < 2^{-n} \Rightarrow \varphi(u) = \varphi(v).$$

In view of Proposition 4.6, it follows that the intersection $\rho$ of the kernels of the uniformly continuous homomorphisms $\overline{\Omega}_A\mathbf{V} \to V$ with $V \in \mathbf{V}$ and $|V| \leq n$ is contained in $\ker\varphi$. Hence, $\varphi$ factors through the natural homomorphism $\overline{\Omega}_A\mathbf{V} \to \overline{\Omega}_A\mathbf{V}/\rho$. Since $\overline{\Omega}_A\mathbf{V}/\rho$ belongs to $\mathbf{V}$, so does $S$. □

## Lemma 5.7 ([Num57, Hun88])

*Let $K$ be a clopen subset of a compact zero-dimensional metric semigroup $S$. Then there is a continuous homomorphism $\varphi : S \to T$ into a finite semigroup $T$ such that $K = \varphi^{-1}\varphi(K)$.*

## Proof.

We may define on $S$ a syntactic congruence of $K$ by

$$u \,\sigma_K\, v \quad \text{if } \forall\, x, y \in S^1 \ (xuy \in K \Leftrightarrow xvy \in K).$$

It suffices to show that the classes of this congruence are open: then there are only finitely many of them, so that $S/\sigma_K$ is a finite semigroup, and the natural mapping $S \to S/\sigma_K$ is a continuous homomorphism.
We show that, if $\lim u_n = u$, then all but finitely many terms in the sequence are $\sigma_K$-equivalent to $u$. Arguing by contradiction, otherwise, there is a subsequence consisting of terms which fail this property. We may as well assume that so does the original sequence.
For each $n$ there are $x_n, y_n \in S^1$ such that one, but not both, of the products $x_n u_n y_n$ and $x_n u y_n$ lies in $K$. Again, by taking subsequences we may assume that $\lim x_n = x$, $\lim y_n = y$ (in $S^1$), and $x_n u y_n \notin K$. Then
$xuy = \lim x_n u_n y_n = \lim x_n u y_n$ must belong to both $K$ and its complement. □

- A useful application of Lemma 5.7 is the following result, which completes that of Proposition 5.4.

## Theorem 5.8

*A compact metric semigroup is profinite if and only if it is zero-dimensional.*

## Proof.

($\Rightarrow$) This follows from Proposition 5.4.

($\Leftarrow$) Let $S$ be a compact metric semigroup which is zero-dimensional. We need to show that it is residually in $\mathbf{S}$, that is that, for every pair $s, t$ of distinct points of $S$, there is a continuous homomorphism $\varphi : S \to T$ in to a finite semigroup $T$ such that $\varphi(s) \neq \varphi(t)$.
Since $S$ is a zero-dimensional metric space, there is some clopen subset $K$ such that $s \in K$ and $t \notin K$. By Lemma 5.7, there is a continuous homomorphism $\varphi : S \to T$ into a finite semigroup $T$ such that $K = \varphi^{-1}\varphi(K)$. In particular, we have $\varphi(s) \neq \varphi(t)$, as required. □

- A language $L \subseteq A^+$ is **V**-recognizable if its syntactic semigroup belongs to **V**.

## Theorem 5.9

*A language $L \subseteq A^+$ is **V**-recognizable if and only if the closure $K = \overline{\iota(L)}$ is open in $\overline{\Omega}_A\mathbf{V}$ and $\iota^{-1}(K) = L$. The latter condition is superfluous if $\iota$ is injective and $\iota(A^+)$ is a discrete subset of $\overline{\Omega}_A\mathbf{V}$.*

## Proof.

($\Rightarrow$) Use the universal property of $\overline{\Omega}_A\mathbf{V}$ (Theorem 5.3).

($\Leftarrow$) By Lemma 5.7, there is a continuous homomorphism $\varphi : \overline{\Omega}_A\mathbf{V} \to S$ such that $S \in \mathbf{V}$ and $K = \varphi^{-1}\varphi(K)$. Then $\psi = \varphi \circ \iota$ is a homomorphism $A^+ \to S$ such that $\psi^{-1}\varphi(K) = \iota^{-1}(K) = L$ and so $L$ is **V**-recognizable. □

- Theorem 5.9 implies that, as a topological space, $\overline{\Omega}_A\mathbf{V}$ is the Stone dual of the Boolean algebra of **V**-recognizable languages of $A^+$.

## Theorem 5.10

*A set $\mathcal{S}$ of $\mathbf{V}$-recognizable languages over a finite alphabet $A$ generates the Boolean algebra of all such languages if and only if the clopen sets of the form $\overline{\iota(L)}$ ($L \in \mathcal{S}$) suffice to separate points of $\overline{\Omega}_A\mathbf{V}$.*

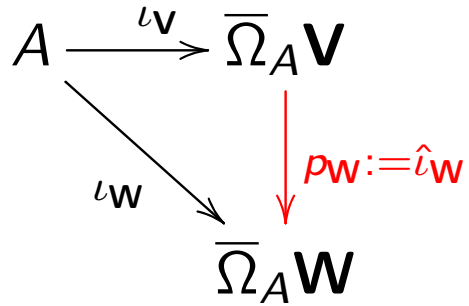
## Proof.

($\Rightarrow$) Let $u, v \in \overline{\Omega}_A\mathbf{V}$ be distinct points. Then $\epsilon = d(u, v)$ is positive. Since $\overline{\Omega}_A\mathbf{V}$ is zero-dimensional (Proposition 5.4), there is a clopen subset $K$ containing $u$ and contained in $B_\epsilon(u)$, whence not containing $v$. By Theorem 5.9, $L = \iota^{-1}(K)$ is $\mathbf{V}$-recognizable. From the hypothesis, it follows that $L$ is a Boolean combination $f(L_1, \ldots, L_n)$ of languages $L_i$ from $\mathcal{S}$. By Theorem 5.9 again, each set $\overline{\iota(L_i)}$ is clopen. Since $\overline{\iota(X_1 \cup X_2)} = \overline{\iota(X_1)} \cup \overline{\iota(X_2)}$ and $\overline{\Omega}_A\mathbf{V} \setminus \overline{\iota(X)} = \overline{\iota(A^+ \setminus X)}$ for $\mathbf{V}$-recognizable languages $X, X_1, X_2 \subseteq A^+$, we have $K = \overline{\iota(L)} = f(\overline{\iota(L_1)}, \ldots, \overline{\iota(L_n)})$. Hence at least one of the sets $\overline{\iota(L_i)}$ must contain exactly one of the points $u$ and $v$.

($\Leftarrow$) By Theorem 5.9, it suffices to show that the clopen sets of the form $\overline{\iota(L)}$, with $L \subseteq A^+$ $\mathbf{V}$-recognizable, generate the Boolean algebra of all clopen subsets of $\overline{\Omega}_A\mathbf{V}$. This is a nice exercise on compactness. □

# Outline

- Recall that a $\mathbf{V}$-pseudoidentity is a formal equality $u = v$ with $u, v \in \overline{\Omega}_A\mathbf{V}$ for some finite set $A$.
- Recall also that, for $S \in \mathbf{V}$, we write $S \models u = v$ if $\varphi(u) = \varphi(v)$ for every continuous homomorphism $\varphi : \overline{\Omega}_A\mathbf{V} \to S$. In this case, we also say that $u = v$ holds in $S$.
- For a set $\Sigma$ of $\mathbf{V}$-pseudoidentities, let $[\![\Sigma]\!]$ denote the class of all $S \in \mathbf{V}$ such that $S \models u = v$ for every pseudoidentity $u = v$ from $\Sigma$.
- For a subpseudovariety $\mathbf{W}$ of $\mathbf{V}$, let $p_{\mathbf{W}} : \overline{\Omega}_A\mathbf{V} \to \overline{\Omega}_A\mathbf{W}$ be the natural continuous homomorphism:



## Lemma 6.1

*A pseudoidentity $u = v$, with $u, v \in \overline{\Omega}_A \mathbf{V}$, holds in every member of a subpseudovariety $\mathbf{W}$ of $\mathbf{V}$ if and only if $p_{\mathbf{W}}(u) = p_{\mathbf{W}}(v)$.*

## Theorem 6.2 ([Rei82])

*A subclass $\mathbf{W}$ of $\mathbf{V}$ is a subpseudovariety if and only if it is of the form $[\![\Sigma]\!]$ for some set $\Sigma$ of $\mathbf{V}$-pseudoidentities.*

- Usually, one takes $\mathbf{V} = \mathbf{S}$.

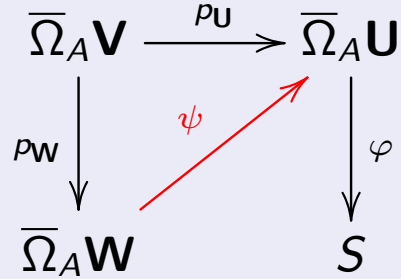
## Proof of Theorem 6.2.

($\Leftarrow$) This amounts to verifying that the property $S \models u = v$ is preserved under taking homomorphic images, subsemigroups and finite direct products, which follows easily from the definitions.

($\Rightarrow$) Fix a countably infinite set $X$ and let $\Sigma$ be the set of all pseudoidentities $u = v$ such that $u, v \in \overline{\Omega}_A\mathbf{V}$ for some finite subset $A$ of $X$ and $S \models u = v$ for all $S \in \mathbf{W}$. Then $\mathbf{U} = [\![\Sigma]\!]$ is a subpseudovariety of $\mathbf{V}$ by the first part of the proof, and it clearly contains $\mathbf{W}$. We claim that $\mathbf{U} = \mathbf{W}$.

Let $S \in \mathbf{U}$ and choose an onto continuous homomorphism $\varphi : \overline{\Omega}_A\mathbf{U} \to S$ for some finite subset $A$ of $X$ (cf. Theorem 5.3).

Consider the natural continuous homomorphisms $p_{\mathbf{U}}$ and $p_{\mathbf{W}}$. By Lemma 6.1 and the choice of $\Sigma$, we have $\ker p_{\mathbf{W}} \subseteq \ker p_{\mathbf{U}}$ and so there is a factorization $p_{\mathbf{U}} = \psi \circ p_{\mathbf{W}}$ for some onto continuous homomorphism $\psi : \overline{\Omega}_A\mathbf{W} \to \overline{\Omega}_A\mathbf{U}$. Hence $\varphi \circ \psi : \overline{\Omega}_A\mathbf{W} \to S$ is an onto continuous homomorphism. Corollary 5.6 then implies that $S \in \mathbf{W}$ since $\overline{\Omega}_A\mathbf{W}$ is a pro-$\mathbf{W}$ semigroup by Theorem 5.3.




□

- To write pseudoidentities that are not identities, one needs to construct some elements of $\overline{\Omega}_A\mathbf{S} \setminus A^+$.

## Lemma 6.3

*Let $S$ be a profinite semigroup, let $s$ be an element of $S$, and let $k \in \mathbb{Z}$. Then the sequence of powers $(s^{n!+k})_{n \geq |k|}$ converges. For $k = 0$ the limit is an idempotent.*

## Proof.

Using Proposition 5.1, it suffices to consider the case where $S$ is finite, which is left as an exercise. □

- The limit $\lim s^{n!+k}$ is denoted $s^{\omega+k}$.
- Note that $s^{\omega+k}s^{\omega+\ell} = s^{\omega+k+\ell}$.
  In particular, $s^{\omega} := s^{\omega+0}$ is an idempotent and $s^{\omega-k}$ and $s^{\omega+k}$ are mutual inverses in the maximal subgroup containing the idempotent $s^{\omega}$.

# Examples I

$$\mathbf{S} = [\![x = x]\!]$$
$$\mathbf{I} = [\![x = y]\!]$$
$$\mathbf{G} = [\![x^\omega = 1]\!]$$
$$\mathbf{G}_p = ?$$
$$\mathbf{A} = [\![x^{\omega+1} = x^\omega]\!]$$
$$\mathbf{Com} = [\![xy = yx]\!]$$
$$\mathbf{J} = [\![(xy)^\omega = (yx)^\omega, x^{\omega+1} = x^\omega]\!]$$
$$\mathbf{R} = [\![(xy)^\omega x = (xy)^\omega]\!]$$
$$\mathbf{L} = [\![y(xy)^\omega = (xy)^\omega]\!]$$

$$\mathbf{Sl} = [\![xy = yx, x^2 = x]\!]$$
$$\mathbf{RZ} = [\![xy = y]\!]$$
$$\mathbf{B} = [\![x^2 = x]\!]$$
$$\mathbf{N} = [\![x^\omega = 0]\!]$$
$$\mathbf{K} = [\![x^\omega y = x^\omega]\!]$$
$$\mathbf{D} = [\![yx^\omega = x^\omega]\!]$$

# Examples II

- Since there are uncountably many pseudovarieties of the form $\mathbf{Ab}_P$, where $P$ is a set of primes, and one can show that all of them admit a description of the form $[\![xy = yx, u = 1]\!]$ [Alm95, Corollary 3.7.8], for some $u \in \overline{\Omega}_{\{x\}}\mathbf{S}$, we conclude that $\overline{\Omega}_{\{x\}}\mathbf{S}$ is uncountable.
- Let $P$ be an infinite set of primes and let $p_1, p_2, \ldots$ be an enumeration of its elements, without repetitions.
  Let $u_P$ be an accumulation point in $\overline{\Omega}_{\{x\}}\mathbf{S}$ of the sequence $(x^{p_1 \cdots p_n})_n$.

$$\mathbf{Ab}_P = [\![xy = yx, u_P = 1]\!].$$

- *Does the sequence $(x^{p_1 \cdots p_n})_n$ converge?*

# Examples III

- To describe the pseudovariety $\mathbf{G}_p$ of all finite $p$-groups, we use the following result, whose proof is similar to that of Lemma 6.3.

## Lemma 6.4

*Let $S$ be a profinite semigroup and $s \in S$. Then the sequence $(s^{p^{n!}})_n$ converges.*

- We let $s^{p^\omega} = \lim s^{p^{n!}}$.

$$\mathbf{G}_p = [\![x^{p^\omega} = 1]\!].$$

# Examples IV

## Exercise 6.5 (For those that know some group theory)

Find, for each of the following pseudovarieties of groups, a single pseudoidentity defining them:

(1) the pseudovariety $\mathbf{G}_{p'}$ of all finite groups which have no elements of order $p$ ($p$ being a fixed prime number);
(2) the pseudovariety $\mathbf{G}_{\mathrm{nil}}$ of all finite nilpotent groups;
(3) the pseudovariety $\mathbf{G}_{\mathrm{sol}}$ of all finite solvable groups.

# Outline

- Recall that $\mathbf{N} = [\![x^\omega = 0]\!] = \bigcup_{n\geq 1}[\![x_1 \cdots x_n = 0]\!]$.
  The proof depends on the following key result.

## LEMMA 7.1

*Let $S$ be a finite semigroup with $n$ elements. Then, for every choice of elements $s_1, \ldots, s_n \in S$, there exist indices $i, j$ such that $0 \leq i < j \leq n$ and the following equality holds for all $k \geq 1$:*

$$s_1 \cdots s_n = s_1 \cdots s_i (s_{i+1} \cdots s_j)^k s_{j+1} \cdots s_n.$$

## PROOF.

Consider the $n$ products $p_r = s_1 \cdots s_r$ $(r = 1, \ldots, n)$. If they are all distinct, then at least one of them, say $p_r$, is idempotent and we may take $i = 0$, $j = r$. Otherwise, there are indices $i, j$ such that $1 \leq i < j \leq n$ and $p_i = p_j$, in which case $p_i = p_j = p_i s_{i+1} \cdots s_j = p_i (s_{i+1} \cdots s_j)^k$. □

- Let $\varphi : A^+ \to S$ be a homomorphism into a semigroup $S \in \mathbf{N}$, say satisfying $x_1 \cdots x_n = 0$. Then, all words of length at least $n$ belong to $\varphi^{-1}(0)$ and for $s \in S \setminus \{0\}$, the words in the language $L = \varphi^{-1}(s)$ have length less than $n$, and so $L$ is a finite set.

  Thus, every **N**-recognizable language is either finite or cofinite.

- To show that these are precisely the **N**-recognizable languages, it suffices to show that every singleton language $\{w\} \subseteq A^+$ is **N**-recognizable.

  Let $n = |w|$ be the length of the word $w$. Consider the semigroup $S$ consisting of the words of $A^+$ of length at most $n$ together with a zero element 0. The product of two words is the word resulting from their concatenation if that word has length at most $n$ and is 0 otherwise.[1] Then $S$ satisfies the identity $x_1 \cdots x_n = 0$, for the natural homomorphism $\varphi : A^+ \to S$, that sends each letter to itself, we have $\varphi^{-1}(w) = \{w\}$.

[1] This amounts to "killing" the ideal of the semigroup $A^+$ consisting of the words of length greater than $n$, identifying all the elements in the ideal to a zero. In semigroup theory, such a construction is called a Rees quotient.

## Proposition 7.2

*A language over a finite alphabet $A$ is* $\mathbf{N}$*-recognizable if and only if it is finite or its complement in $A^+$ is finite.*

- In view of Theorem 5.9, we deduce the following result:

## Proposition 7.3

*Let* $\mathbf{V}$ *be a pseudovariety of semigroups containing* $\mathbf{N}$*. Then the completion homomorphism $\iota : A^+ \to \overline{\Omega}_A\mathbf{V}$ is injective and $A^+$ is a discrete subspace of $\overline{\Omega}_A\mathbf{V}$. In particular, a language $L \subseteq A^+$ is* $\mathbf{V}$*-recognizable if and only if its closure $\overline{L}$ in $\overline{\Omega}_A\mathbf{V}$ is a clopen subset.*

## Proof.

The injectivity of $\iota$ amounts to $\mathbf{V}$ satisfying no identity $u = v$ with $u, v \in A^+$ distinct words. Indeed, $\mathrm{Synt}(\{u\})$ is nilpotent, whence it belongs to $\mathbf{V}$. Since $1u1 \in \{u\}$ while $1v1 \notin \{u\}$, we deduce that $u$ and $v$ are not $\sigma_{\{u\}}$-equivalent and so $\mathrm{Synt}(\{u\}) \not\models u = v$.
We may therefore identify each $w \in A^+$ with $\iota(w) \in \overline{\Omega}_A\mathbf{V}$.
For $w \in A^+$, we have $\overline{\{w\}} = \{w\}$, because $\overline{\Omega}_A\mathbf{V}$ is a metric space. Since $\{w\}$ is $\mathbf{V}$-recognizable, its closure $\overline{\{w\}}$ is an open subset of $\overline{\Omega}_A\mathbf{V}$ by Theorem 5.9. Hence $A^+$ is a discrete subset of $\overline{\Omega}_A\mathbf{V}$. □

## Proposition 7.4

*The semigroup $\overline{\Omega}_A\mathbf{N}$ is obtained by adding to $A^+$ a zero element. The open sets containing zero consist of zero together with a cofinite subset of $A^+$.*[2]

## Proof.

It suffices to observe that a non-eventually constant sequence $(w_n)_n$ of words of $A^+$ is a Cauchy sequence with respect to the metric $d_{\mathbf{N}}$ if and only if $\lim |w_n| = \infty$. In the affirmative case, for every homomorphism $\varphi : A^+ \to S$ into $S \in \mathbf{N}$, we have $\lim \varphi(w_n) = 0$. Thus, all non-eventually constant Cauchy sequences converge to the same point of $\overline{\Omega}_A\mathbf{N}$, which is a zero.

The open subsets of $\overline{\Omega}_A\mathbf{N}$ containing 0 have complement which is a closed, whence compact, subset of $A^+$. Since $A^+$ is a discrete subset of $\overline{\Omega}_A\mathbf{N}$, that complement must be finite. The converse is clear. □

[2] This is known as the Alexandroff or one-point compactification, which in general is obtained by adding one point and declaring the open sets containing it to consist also of the complement of a compact subset of the original space.

# K: FINITE SEMIGROUPS SATISFYING $es = e$

- Recall that $\mathbf{K} = [\![x^\omega y = x^\omega]\!]$. Note that

$$\mathbf{K} = \bigcup_{n \geq 1} \mathbf{K}_n \text{ where } \mathbf{K}_n = [\![x_1 \cdots x_n y = x_1 \cdots x_n]\!].$$

- Let $A^{\mathbb{N}}$ denote the set of all right infinite words over $A$, i.e., sequences of letters.
- Endow the set $S = A^+ \cup A^{\mathbb{N}}$ with the operation

$$u \cdot v = \begin{cases} uv & \text{if } u \in A^+ \\ u & \text{otherwise} \end{cases}$$

and the function $d : S \times S \to \mathbb{R}_{\geq 0}$ defined by $d(u, v) = 2^{-r(u,v)}$, where $r(u, v)$ is the length of the longest common prefix of $u$ and $v$.

## Proposition 7.5

*The set $S$ is a pro-$\mathbf{K}$ semigroup for the above operation and distance function $d$. The unique continuous homomorphism $\overline{\Omega}_A\mathbf{K} \to S$ that sends each letter $a \in A$ to itself is an isomorphism.*

## Proof.

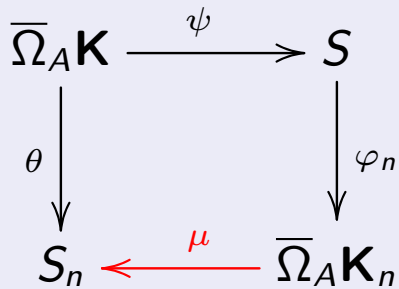
It is easy to check that the multiplication defined on $S$ is associative and that $d$ is an totally bounded complete ultrametric.
Consider the set $S_n$ consisting of all words of $A^+$ of length at most $n$, endowed with the operation

$$u \cdot v = \begin{cases} uv & \text{if } |uv| \leq n \\ \mathrm{i}_n(u) & \text{otherwise} \end{cases}$$

where $\mathrm{i}_n(w)$ denotes the longest prefix of length at most $n$ of the word $w$. This operation is associative and $S_n \in \mathbf{K}_n$. Moreover, every $n$-generated semigroup from $\mathbf{K}_n$ is a homomorphic image of $S_n$. Hence $S_n \simeq \overline{\Omega}_A\mathbf{K}_n$.
Note also that the mapping $\varphi_n : S \to S_n$ which sends each $w \in S$ to $\mathrm{i}_n(w)$ is a continuous homomorphism.
Hence, given two distinct points $u$ and $v$ from $S$, for $n = r(u, v) + 1$, the mapping $\varphi_n$ is a continuous homomorphism into a semigroup from $\mathbf{K}$ which distinguishes $u$ from $v$. Thus, $S$ is a pro-$\mathbf{K}$ semigroup.

## $(\ldots)$

Consider next the unique continuous homomorphism $\psi : \overline{\Omega}_A\mathbf{K} \to S$ which maps each letter $a \in A$ to itself. Since $\mathbf{K} = \bigcup_{n\geq 1} \mathbf{K}_n$, given distinct $u, v \in \overline{\Omega}_A\mathbf{K}$, there exists a continuous homomorphism $\theta : \overline{\Omega}_A\mathbf{K} \to S_n$ such that $\theta(u) \neq \theta(v)$.




The fact that the above diagram can always be completed by a homomorphism $\mu$ shows that $\psi(u) \neq \psi(v)$. Hence $\psi$ is injective. □

# Outline

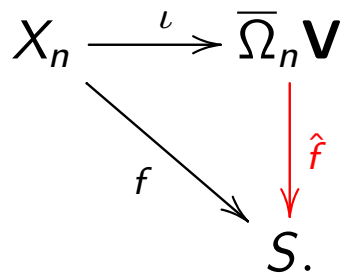
# Implicit operations

- Let $n$ be a positive integer.
- An *$n$-ary implicit operation* on pro-$\mathbf{V}$ semigroups is a correspondence $\pi$ associating to each pro-$\mathbf{V}$ semigroup $S$ an $n$-ary operation $\pi_S : S^n \to S$ such that , for every continuous homomorphism $\varphi : S \to T$ between pro-$\mathbf{V}$ semigroups, the following diagram commutes:

$$\begin{array}{ccc} S^n & \xrightarrow{\pi_S} & S \\ \downarrow{\scriptstyle \varphi^n} & & \downarrow{\scriptstyle \varphi} \\ T^n & \xrightarrow{\pi_T} & T, \end{array}$$

  i.e., $\varphi\big(\pi_S(s_1, \ldots, s_n)\big) = \pi_T\big(\varphi(s_1), \ldots, \varphi(s_n)\big)$ for all $s_1, \ldots, s_n \in S$.
- Examples: the binary multiplication $(s_1, s_2) \mapsto s_1 s_2$ and the component projections $(s_1, \ldots, s_n) \mapsto s_i$ are implicit operations. Composing implicit operations we also obtain implicit operations.

- If $A$ and $B$ are finite sets with the same cardinality $n$, then $\overline{\Omega}_A\mathbf{V} \simeq \overline{\Omega}_B\mathbf{V}$. We denote by $\overline{\Omega}_n\mathbf{V}$ any of them. Usually, we identify $\overline{\Omega}_n\mathbf{V}$ with $\overline{\Omega}_{X_n}\mathbf{V}$, where $X_n = \{x_1, \ldots, x_n\}$ has cardinality $n$.
- To each $w \in \overline{\Omega}_n\mathbf{V}$, we may associate an $n$-ary implicit operation $\pi_w$ on pro-$\mathbf{V}$ semigroups as follows:
  - for a pro-$\mathbf{V}$ semigroup $S$, given $s_1, \ldots, s_n \in S$, let $f : X_n \to S$ be the function defined by $f(x_i) = s_i$ $(i = 1, \ldots, n)$;
  - let $(\pi_w)_S(s_1, \ldots, s_n) = \hat{f}(w)$ where $\hat{f}$ is a continuous homomorphism completing the following diagram:

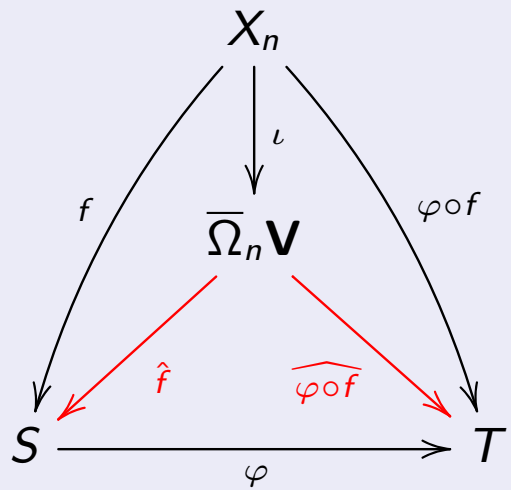


## Proposition 8.1

1. *For each $w \in \overline{\Omega}_n\mathbf{V}$, $\pi_w$ is indeed an $n$-ary implicit operation on pro-$\mathbf{V}$ semigroups.*
2. *The correspondence $w \in \overline{\Omega}_n\mathbf{V} \mapsto \pi_w$ is injective and in fact $\pi_w$ is completely characterized by the operations $(\pi_w)_S$ with $S \in \mathbf{V}$.*

## Proof.

1. Let $\varphi : S \to T$ be a continuous homomorphism between two pro-$\mathbf{V}$ semigroups and let $s_1, \ldots, s_n$ be elements of $S$. Let $f : X_n \to S$ be defined by $f(x_i) = s_i$ $(i = 1, \ldots, n)$. Then we have the following commutative diagram:




which shows that

$$\begin{aligned}\varphi\big((\pi_w)_S(f(s_1), \ldots, f(s_n))\big) &= \varphi\big(\hat{f}(w)\big) = \widehat{\varphi \circ f}(w) \\ &= (\pi_w)_T\big(\varphi(f(s_1)), \ldots, \varphi(f(s_n))\big).\end{aligned}$$

$(\ldots)$

2. Let $u, v \in \overline{\Omega}_n\mathbf{V}$ be two distinct elements. Then there exists a continuous homomorphism $\varphi : \overline{\Omega}_n\mathbf{V} \to S$ into a semigroup $S \in \mathbf{V}$ such that $\varphi(u) \neq \varphi(v)$. Let $s_i = \varphi(x_i)$ $(i = 1, \ldots, n)$. For $w \in \overline{\Omega}_n\mathbf{V}$, by definition of $\pi_w$ we have

$$(\pi_w)_S(s_1, \ldots, s_n) = \varphi(w).$$

Since $\varphi(u) \neq \varphi(v)$, we deduce that

$$(\pi_u)_S(s_1, \ldots, s_n) \neq (\pi_v)_S(s_1, \ldots, s_n)$$

and so, certainly $\pi_u \neq \pi_v$. □

- We identify $w$ with $\pi_w$.
- Note that $S \in \mathbf{V}$ satisfies the $\mathbf{V}$-pseudoidentity $u = v$ if and only if $u_S = v_S$.
- We say that a pro-$\mathbf{V}$ semigroup $S$ satisfies the $\mathbf{V}$-pseudoidentity $u = v$ if $u_S = v_S$.

# Outline

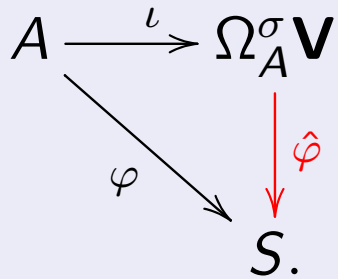
- By an implicit signature we mean a set $\sigma$ of implicit operations (on $\mathbf{S}$) which includes the binary operation of multiplication.
- Example: $\kappa = \{\_ \cdot \_,\ \_^{\omega-1}\}$.
- Given an implicit signature $\sigma$, each profinite semigroup $S$ becomes a natural $\sigma$-algebra in which each operation $w \in \sigma$ is interpreted as $w_S$.
- In particular, each $\overline{\Omega}_A\mathbf{V}$ becomes a $\sigma$-algebra. The $\sigma$-subalgebra generated by $\iota(A)$ is denoted $\Omega_A^\sigma\mathbf{V}$.
- For the minimum implicit signature $\sigma$, consisting only of multiplication, we denote $\Omega_A^\sigma\mathbf{V}$ simply by $\Omega_A\mathbf{V}$.[3]
- A formal term constructed from the letters $a \in A$ using the operations from the implicit signature $\sigma$ is called a $\sigma$-term over $A$. Such a $\sigma$-term $w$ determines an element $w_{\mathbf{V}}$ of $\Omega_A^\sigma\mathbf{V}$ by evaluating the operations within $\Omega_A^\sigma\mathbf{V}$.

[3] The bar in the notation $\overline{\Omega}_A\mathbf{V}$ comes from the fact $\Omega_A\mathbf{V} = \iota(A^+)$ is dense in $\overline{\Omega}_A\mathbf{V}$. This notation (without reference to $\mathbf{V}$) was introduced by Reiterman [Rei82].

- The following result is an immediate consequence of Theorem 5.3.

## Proposition 9.1

*The $\sigma$-algebra $\Omega_A^\sigma \mathbf{V}$ is a $\mathbf{V}$-free $\sigma$-algebra freely generated by $A$ in the sense of the following universal property: for every mapping $\varphi : A \to S$ into a semigroup $S \in \mathbf{V}$, there is a unique homomorphism $\hat{\varphi}$ of $\sigma$-algebras such that the following diagram commutes:*



Examples:

- $\Omega_A^\kappa \mathbf{N} = \overline{\Omega}_A \mathbf{N}$;
- for $|A| \geq 2$, since $\overline{\Omega}_A \mathbf{K}$ is uncountable, we have $\Omega_A^\sigma \mathbf{K} \subsetneqq \overline{\Omega}_A \mathbf{K}$ for every countable implicit signature $\sigma$;
- $\Omega_A^\kappa \mathbf{J} = \overline{\Omega}_A \mathbf{J}$ [Alm95, Section 8.1];
- $\Omega_A^\kappa \mathbf{G}$ is the free group freely generated by $\iota(A) = A$;
- $\Omega_A^\kappa \mathbf{CR}$ is the free completely regular (union of groups) semigroup freely generated by $\iota(A) = A$.

- A key problem for the applications is to be able to solve the word problem in the free $\sigma$-algebra $\Omega_A^\sigma \mathbf{V}$: to find an algorithm, if one exists, that given two $\sigma$-terms over $A$, determines whether $u_{\mathbf{V}} = v_{\mathbf{V}}$.
  If such an algorithm exists, then we say that the word problem is decidable; otherwise, we say that it is undecidable.

## Examples:

- The word problem for $\Omega_A^\kappa \mathbf{N}$: two $\kappa$-terms coincide in $\Omega_A^\kappa \mathbf{N}$ if and only if they are equal or they both involve the operation $\_^{\omega-1}$.
- The word problem for $\Omega_A^\kappa \mathbf{G}$ is well known: the operation $\_^{\omega-1}$ is inversion in profinite groups, so all $\kappa$-terms can be effectively reduced (over $\mathbf{G}$) to $\kappa$-terms in which that operation is only applied to letters; then use, in any order, the reduction rules $aa^{\omega-1} \to 1$ and $a^{\omega-1}a \to 1$ ($a \in A$) to obtain a canonical form for $\kappa$-terms over $\mathbf{G}$; two $\kappa$-terms are equal over $\mathbf{G}$ if and only if they have the same canonical form.
- Word problem for $\Omega_A^\kappa \mathbf{K}$: exercise.
- The solution of the word problem for $\Omega_A^\kappa \mathbf{J} = \overline{\Omega}_A \mathbf{J}$ gives the structure of $\overline{\Omega}_A \mathbf{J}$ [Alm95, Section 8.1].
- The word problem for $\Omega_A^\kappa \mathbf{CR}$ has been solved by Kad'ourek and Polák [KP86].
- The word problem for $\Omega_A^\kappa \mathbf{A}$ has been solved by McCammond [McC01].

# Part II

## *Separating words and regular languages*

# Outline

# A separation problem

- Let $\mathbf{V}$ be a pseudovariety of semigroups.
- Suppose that a regular language $L \subseteq A^+$ and a word $w \in A^+$ are given. How do we find out whether a proof that $w \notin L$ exists using $\mathbf{V}$-recognizable languages?
- More precisely, we wish to decide whether, given such $L$ and $w$, there exists a $\mathbf{V}$-recognizable language $K \subseteq A^+$ such that $L \subseteq K$ and $w \notin K$.
- For instance, how do we determine whether there exists a finite permutation automaton such that no word from $L$ ends in the same state as $w$ does?
- Another example of the same type of problem: is there some integer $n$ such that no word from $L$ has the same subwords of length at most $n$ as $w$ does?

- Our problem sounds like a topological separation problem, and indeed it admits such a formulation in the profinite world.

## Proposition 10.1

*Let $\mathbf{V}$ be a pseudovariety of semigroups, $L \subseteq A^+$ a regular language and $w$ a word in $A^+$. Then there is a $\mathbf{V}$-recognizable language $K \subseteq A^+$ such that $L \subseteq K$ and $w \notin K$ if and only if $\iota_{\mathbf{V}}(w)$ does not belong to the closure of $\iota_{\mathbf{V}}(L)$ in $\overline{\Omega}_A\mathbf{V}$.*

## Proof.

By Proposition 5.4, the condition $\iota_{\mathbf{V}}(w)$ belongs to the closure $\overline{\iota_{\mathbf{V}}(L)}$ in $\overline{\Omega}_A\mathbf{V}$ holds if and only if every clopen subset of $\overline{\Omega}_A\mathbf{V}$ which contains $\iota_{\mathbf{V}}(w)$ has nontrivial intersection with $\iota_{\mathbf{V}}(L)$. By Theorem 5.9, such clopen subsets are precisely the sets of the form $\overline{\iota_{\mathbf{V}}(K)}$ where $K$ is a $\mathbf{V}$-recognizable subset of $A^+$. It remains to observe that, $\iota_{\mathbf{V}}(w) \in \overline{\iota_{\mathbf{V}}(K)}$ and $\overline{\iota_{\mathbf{V}}(K)} \cap \iota_{\mathbf{V}}(L) = \emptyset$ if and only if $w \in K$ and $K \cap L = \emptyset$, which follows from the facts that $K = \iota_{\mathbf{V}}^{-1}(\overline{\iota_{\mathbf{V}}(K)})$ and $L \subseteq \iota_{\mathbf{V}}^{-1}(\iota_{\mathbf{V}}(L))$. □

## Corollary 10.2

*Let* $\mathbf{V}$ *be a pseudovariety containing* $\mathbf{N}$*. If* $w$ *is a word in* $A^+$ *and* $L \subseteq A^+$ *is a regular language, then* $w$ *and* $L$ *can be separated by a* $\mathbf{V}$*-recognizable language if and only if* $w \notin L$*.*

## Proof.

By Proposition 7.3, $\iota$ embeds $A^+$ in $\overline{\Omega}_A\mathbf{V}$ as a discrete subspace, meaning that every subset is open. Hence, if $w$ belongs to the closure $\overline{L}$ of $L$ in $\overline{\Omega}_A\mathbf{V}$, then $w \in L$. □

- More directly, in case $\mathbf{N} \subseteq \mathbf{V}$, the language $\{w\}$ is $\mathbf{V}$-recognizable and therefore there is a $\mathbf{V}$-recognizable language containing $w$ and disjoint from $L$ if and only if $w \notin L$.
- Note that the condition $\mathbf{N} \subseteq \mathbf{V}$ is equivalent to $\mathbf{V}$ satisfying some pseudoidentity of the form $x^{\omega+n} = x^n$, where $n$ is a positive integer.

- Even for pseudovarieties $\mathbf{V}$ containing $\mathbf{N}$, the separation problem becomes nontrivial if we wish instead to separate two regular languages by a $\mathbf{V}$-recognizable language.
- The following result can be proved basically by the same argument as presented for the proof of Proposition 10.1, taking additionally into account that $\overline{\Omega}_A\mathbf{V}$ is compact. The details are left as an exercise.

**Proposition 10.3**

*Let $\mathbf{V}$ be a pseudovariety of semigroups and $L_1, L_2 \subseteq A^+$ regular languages. Then there is a $\mathbf{V}$-recognizable language $K \subseteq A^+$ such that $L_1 \subseteq K$ and $L_2 \cap K = \emptyset$ if and only if the closures of $\iota_{\mathbf{V}}(L_1)$ and $\iota_{\mathbf{V}}(L_2)$ in $\overline{\Omega}_A\mathbf{V}$ are disjoint sets.*

- In the case of **A**, Henckell has constructed an algorithm, working directly in a finite semigroup which recognizes simultaneously two given regular languages, which decides whether they may be separated by a star-free language [Hen88].
- An idea due to Pin and Reutenauer [PR91] in the case of the pseudovariety **G** of all finite groups is to somehow "compute" the closure of $\iota_{\mathbf{V}}(L)$ not in $\overline{\Omega}_A\mathbf{G}$ but in the free group $\Omega_A^\kappa\mathbf{G}$, or even in $A^+$.
- Under the assumption of a conjectured property for the pseudovariety **G**, they produced an algorithm for computing the required closure, which solves our problem for **G**.
- We proceed to introduce the required property in general, returning later to their algorithm.

- For a subset $L$ of $A^+$, denote by $\mathrm{cl}_{\sigma,\mathbf{V}}(L)$ and $\mathrm{cl}_{\mathbf{V}}(L)$ respectively the closure of $\iota_{\mathbf{V}}(L)$ in $\Omega_A^\sigma\mathbf{V}$ and in $\overline{\Omega}_A\mathbf{V}$.
- Note that $\mathrm{cl}_{\sigma,\mathbf{V}}(L) = \mathrm{cl}_{\mathbf{V}}(L) \cap \Omega_A^\sigma\mathbf{V}$.
- In particular, for $w \in A^+$, we have $\iota(w) \in \mathrm{cl}_{\mathbf{V}}(L)$ if and only if $\iota(w) \in \mathrm{cl}_{\sigma,\mathbf{V}}(L)$.
- Denote by $p_{\mathbf{V}}$ the natural continuous homomorphism $\overline{\Omega}_A\mathbf{S} \to \overline{\Omega}_A\mathbf{V}$.
- Since $\overline{\Omega}_A\mathbf{S}$ is compact and $p_{\mathbf{V}}$ is an onto continuous mapping, we always have the equality $\mathrm{cl}_{\mathbf{V}}(L) = p_{\mathbf{V}}(\mathrm{cl}_{\mathbf{S}}(L))$.
  - In general, for a continuous function $f : S \to T$, and a subset $X$ of $S$, we have $f(\overline{X}) \subseteq \overline{f(X)}$. The reverse inclusion also holds if $f$ is onto and $S$ is compact.

- We say that the pseudovariety $\mathbf{V}$ is $\sigma$-full if, for every regular language $L \subseteq A^+$, the following equality holds:

$$\mathrm{cl}_{\sigma,\mathbf{V}}(L) = p_{\mathbf{V}}(\mathrm{cl}_{\sigma,\mathbf{S}}(L)).$$

  In other words, membership of $w \in \Omega_A^\sigma \mathbf{V}$ in $\mathrm{cl}_{\sigma,\mathbf{V}}(L)$ is witnessed by some $w' \in \mathrm{cl}_{\sigma,\mathbf{S}}(L)$ such that $p_{\mathbf{V}}(w') = w$.

## Theorem 10.4 ([AS00a])

*Let* $\mathbf{V}$ *be a pseudovariety,* $A$ *a finite alphabet and* $\sigma$ *an implicit signature such that the following conditions hold:*

(1) $\mathbf{V}$ *is* $\sigma$*-full;*

(2) *the word problem for* $\Omega_A^\sigma \mathbf{V}$ *is decidable;*

(3) $\sigma$ *is recursively enumerable;*

(4) $\mathbf{V}$ *is recursively enumerable;*

(5) *for each operation in* $\sigma$*, there is an algorithm to compute it in any given finite semigroup.*

*Then it is decidable whether, given a regular language* $L \subseteq A^+$ *and a pseudoword* $w \in \Omega_A^\sigma \mathbf{V}$*, we have* $w \in \mathrm{cl}_{\sigma,\mathbf{V}}(L)$*.*

## Proof sketch.

Enumerate the pairs $(w, L)$ for which $w \in \mathrm{cl}_{\sigma,\mathbf{V}}(L)$ holds using the assumptions (1)–(3). To enumerate those for which the condition fails, enumerate 4-tuples $(\varphi, \psi, X, w)$ where $\varphi : \overline{\Omega}_A \mathbf{S} \to S$ and $\psi : \overline{\Omega}_A \mathbf{S} \to T$ are onto continuous homomorphisms with $S \in \mathbf{S}$ and $T \in \mathbf{V}$, $X \subseteq S$, and $w \in \Omega_A^\sigma \mathbf{S}$ are such that $X \times \{\psi(w)\} \cap \mathrm{Im}(\varphi \times \psi) = \emptyset$ and output the corresponding pairs $(w, \varphi^{-1}(L) \cap A^+)$. This requires the assumptions (4) and (5). □

Examples:

- The pseudovariety **N** is $\kappa$-full: for a regular language $L \subseteq A^+$ and a $\kappa$-term $w$, $w_{\mathbf{N}} \in \mathrm{cl}_{\kappa,\mathbf{N}}(L)$ if and only if $w$ is a word from $L$ or $w$ involves the operation $\_^{\omega-1}$ and $L$ is infinite; in the latter case, by compactness there is some $\kappa$-term $v$ such that $v_{\mathbf{S}} \in \mathrm{cl}_{\kappa,\mathbf{S}}(L) \setminus A^+$ and so $w_{\mathbf{N}} = 0 = p_{\mathbf{N}}(v_{\mathbf{S}})$.
- That the pseudovariety **J** is $\kappa$-full follows from the structure theorem for $\overline{\Omega}_A\mathbf{J}$ [Alm95, Section 8.2].
- The pseudovariety **G** is $\kappa$-full: the essential ingredient is a seminal theorem of Ash [Ash91]; the details follow from [AS00a] and [Del01].
- The pseudovariety **Ab** is $\kappa$-full [Del01].

- The pseudovariety $\mathbf{G}_p$ is not $\kappa$-full: this follows from a weak version of Ash's theorem proved by Steinberg [Ste01] for $\mathbf{G}_p$ together with the fact that the conjunction of this weaker property with $\kappa$-fullness implies that the pseudovariety is defined by pseudoidentities in which both sides are given by $\kappa$-terms [AS00a] (cf. Proposition 11.1); however, such a definition does not exist since, by a theorem of Baumslag [Bau65], the free group is residually a finite $p$-group.
- That the pseudovarieties $\mathbf{A}$ and $\mathbf{R}$ are $\kappa$-full has been proved by JA-JCCosta-MZeitoun using the solution of the word problems for $\Omega_A^\kappa\mathbf{A}$ [McC01][4] and $\Omega_A^\kappa\mathbf{R}$ [AZ07].

[4] plus refinements from an alternative proof obtained by the same authors including the fact that $\Omega_A^\kappa\mathbf{A}$ is closed for taking factors in $\overline{\Omega}_A\mathbf{A}$.

# Outline

# Separation in $\sigma$-algebras

- Let $\sigma$ be an implicit signature.
- Let $\mathbf{V}$ be a pseudovariety of semigroups.
- Note that, if two regular languages $K, L \subseteq A^+$ have disjoint closures in $\overline{\Omega}_A\mathbf{V}$ then they also have disjoint closures in $\Omega_A^\sigma\mathbf{V}$.
- If the converse also holds, then we say that $\mathbf{V}$ is weakly $\sigma$-reducible for the separation problem.
- This is a special case of a more general weak reducibility property introduced in [AS00a]. The property is considered in general for an arbitrary system of equations, the present case being that of the equation $x = y$.
  Naturally, there is also a stronger form of that property, which we are not considering in these lectures. For a $\sigma$-full pseudovariety, the two versions of the property are equivalent [AS00a, AS00b].

Among others, the following pseudovarieties are known to be weakly $\kappa$-reducible for the separation problem:

- **G** [Ash91];
- **CR** [AT01];
- $\mathbf{G}_p$, with $p$ prime [Ste01];
- **A** [JA-JCCosta-MZeitoun];
- **R** [AS01];
- **J** (follows from the solution of the word problem for $\overline{\Omega}_A\mathbf{J}$ [Alm95, Section 8.2]);
- **LSI** [CT04].

- Say that a pseudovariety $\mathbf{V}$ is $\sigma$-equational if it admits a definition by pseudoidentities involving only $\sigma$-operations. Such pseudoidentities are also called $\sigma$-identities.

**Proposition 11.1 ([AS00a])**

*If a pseudovariety $\mathbf{V}$ is weakly $\sigma$-reducible for the separation problem and $\sigma$-full, then $\mathbf{V}$ is $\sigma$-equational.*

## Proof.

Let $\Sigma$ be the set of all $\sigma$-identities which are valid in $\mathbf{V}$. Clearly $\mathbf{V} \subseteq [\![\Sigma]\!]$.

Let $S$ be a finite semigroup $S$ that satisfies $\Sigma$. By Reiterman's Theorem 6.2, to show that $S \in \mathbf{V}$, it suffices to establish that $S$ satisfies every pseudoidentity which is valid in $\mathbf{V}$. Consider such a pseudoidentity $u = v$, say with $u, v \in \overline{\Omega}_A\mathbf{S}$, and let $\varphi : \overline{\Omega}_A\mathbf{S} \to S$ be a continuous homomorphism. We claim that $\varphi(u) = \varphi(v)$.

Let $K = \varphi^{-1}(\varphi(u)) \cap A^+$ and $L = \varphi^{-1}(\varphi(v)) \cap A^+$. Note that, since $u \in \mathrm{cl}_{\mathbf{S}}(K)$, $v \in \mathrm{cl}_{\mathbf{S}}(L)$, and $p_{\mathbf{V}}(u) = p_{\mathbf{V}}(v)$, we have $\mathrm{cl}_{\mathbf{V}}(K) \cap \mathrm{cl}_{\mathbf{V}}(L) \neq \emptyset$. Since $\mathbf{V}$ is weakly $\sigma$-reducible for the separation problem, there is some $w \in \mathrm{cl}_{\sigma,\mathbf{V}}(K) \cap \mathrm{cl}_{\sigma,\mathbf{V}}(L)$. Since $\mathbf{V}$ is $\sigma$-full, there are $w_1 \in \mathrm{cl}_{\sigma,\mathbf{S}}(K)$ and $w_2 \in \mathrm{cl}_{\sigma,\mathbf{S}}(L)$ such that $p_{\mathbf{V}}(w_1) = w = p_{\mathbf{V}}(w_2)$. Hence $w_1 = w_2$ is a pseudoidentity from $\Sigma$, which therefore is valid in $S$. Hence, we have $\varphi(u) = \varphi(w_1) = \varphi(w_2) = \varphi(v)$, which establishes the claim. □

## Theorem 11.2 ([AS00a])

*Let* $\mathbf{V}$ *be a pseudovariety,* $A$ *a finite alphabet and* $\sigma$ *an implicit signature such that the following conditions hold:*

(1) $\mathbf{V}$ *is* $\sigma$*-full;*

(2) $\mathbf{V}$ *is weakly* $\sigma$*-reducible for the separation problem;*

(3) *the word problem for* $\Omega_A^\sigma \mathbf{V}$ *is decidable;*

(4) $\sigma$ *is recursively enumerable;*

(5) $\mathbf{V}$ *is recursively enumerable;*

(6) *for each operation in* $\sigma$*, there is an algorithm to compute it in any given finite semigroup.*

*Then it is decidable whether two given regular languages* $L_1, L_2 \subseteq A^+$ *may be separated by a* $\mathbf{V}$*-recognizable language* $K \subseteq A^+$*.*

## Proof.

Using property (5), we may enumerate the pairs $(L_1, L_2)$ of regular languages over $A^+$ that may be separated by $\mathbf{V}$-recognizable languages, by simply enumerating triples $(L_1, L_2, \varphi)$, with $\varphi : A^+ \to S$ a homomorphism onto an arbitrary semigroup from $\mathbf{V}$, and test whether $\varphi$ separates $L_1$ and $L_2$. In the affirmative case, output $(L_1, L_2)$.

To enumerate the pairs that may not be separated, we use the assumption (2) plus Proposition 10.3, which guarantees that, if $L_1$ and $L_2$ cannot be separated by a $\mathbf{V}$-recognizable language, then there is some $w \in \mathrm{cl}_{\sigma,\mathbf{V}}(L_1) \cap \mathrm{cl}_{\sigma,\mathbf{V}}(L_2)$ which witnesses the non-separability. Each condition $w \in \mathrm{cl}_{\sigma,\mathbf{V}}(L_i)$ may be effectively tested by Theorem 10.4 and the candidates for witnesses may be recursively enumerated by (4). We may thus proceed as follows:

- enumerate all triples $(L_1, L_2, w)$ with $L_1, L_2 \in A^+$ regular languages and $w \in \Omega^\sigma_A \mathbf{V}$;
- for each such triple, test whether $w \in \mathrm{cl}_{\sigma,\mathbf{V}}(L_i)$ $(i = 1, 2)$;
- output the pairs $(L_1, L_2)$ which pass the test as non-separable by $\mathbf{V}$-recognizable languages.

□

- The algorithms described in Theorems 10.4 and 11.2 are purely theoretical, being unusable in practice.
- Thus, it is worth, particularly in cases where the decidability of the separation property is already guaranteed by Theorem 11.2, to find efficient algorithms to test separability.

# Outline

- The same way we defined a pseudo-ultrametric on the free semigroup $A^+$ associated with a pseudovariety $\mathbf{V}$, we may define a pseudo-ultrametric on an arbitrary semigroup $S$: let

$$d(s_1, s_2) = 2^{-r(s_1,s_2)},$$

  where $r(s_1, s_2)$ is the smallest cardinality of a semigroup $T \in \mathbf{V}$ for which there is a homomorphism $\varphi : S \to T$ such that $\varphi(s_1) \neq \varphi(s_2)$.
- Similar arguments show that $d$ is indeed a pseudo-ultrametric on $S$, with respect to which the multiplication in $S$ is uniformly continuous. If $S$ is finitely generated, then the completion $\hat{S}$ is again a pro-$\mathbf{V}$ semigroup, but it may not be a free pro-$\mathbf{V}$ semigroup.
- The pseudo-ultrametric $d$ is an ultrametric if and only if $S$ is residually in $\mathbf{V}$.
- Every homomorphism $S \to T$ into $T \in \mathbf{V}$ is uniformly continuous.

- Let $\mathbf{V}$ be a pseudovariety of semigroups, and let $\sigma$ be an implicit signature.
- Considering the members of $\mathbf{V}$ as $\sigma$-algebras under the natural interpretation of the operations from $\sigma$, since the homomorphisms are the same, $\mathbf{V}$ is still a pseudovariety of $\sigma$-algebras.
- We may define a pseudo-ultrametric on a $\sigma$-algebra $S$ similarly to the semigroup case: let

$$d^\sigma(s_1, s_2) = 2^{-r^\sigma(s_1, s_2)}$$

where $r^\sigma(s_1, s_2)$ is the smallest cardinality of a member $T \in \mathbf{V}$ for which there is a homomorphism $\varphi : S \to T$ of $\sigma$-algebras such that $\varphi(s_1) \neq \varphi(s_2)$.

- The delicate point here is that, while continuous semigroup homomorphisms between profinite semigroups respect implicit operations, and in particular so do semigroup homomorphisms between finite semigroups, semigroup homomorphisms between arbitrary $\sigma$-algebras may not be homomorphisms of $\sigma$-algebras.
- Example: let $U_1$ be two-element semilattice, which the multiplicative subsemigroup of $\mathbb{Z}$ consisting of $0, 1$; consider the mapping $\varphi : \overline{\Omega}_A\mathbf{N} \to U_1$ that maps $A^+$ to 1 and everything else to 0. Then $\varphi$ is a semigroup homomorphism but not a homomorphism of $\kappa$-algebras.

## Proposition 12.1

*For a pseudovariety* $\mathbf{V}$ *and an implicit signature* $\sigma$*, the completion of* $\Omega_A^\sigma \mathbf{V}$ *with respect to the pseudo-ultrametric* $d^\sigma$ *is* $\overline{\Omega}_A \mathbf{V}$*, both metrically and algebraically.*

## Proof.

Since the algebraic structure is inherited by extension of uniformly continuous operations, it suffices to show that, for $u, v \in \Omega_A^\sigma \mathbf{V}$, $d^\sigma(u, v) = d(u, v)$, where $d$ is the completion metric on $\overline{\Omega}_A \mathbf{V}$.
By Proposition 4.6, $d(u, v) = 2^{-r}$, where $r$ is the smallest cardinality of a member $T \in \mathbf{V}$ for which there exists a continuous homomorphism $\varphi : \overline{\Omega}_A \mathbf{V} \to T$ such that $\varphi(u) \neq \varphi(v)$. Since the restriction of $\varphi$ to $\Omega_A^\sigma \mathbf{V}$ is a homomorphism of $\sigma$-algebras which separates $u$ from $v$, it follows that $r^\sigma(u, v) \leq r$. On the other hand, by the universal property of $\overline{\Omega}_A \mathbf{V}$ and since we interpret $\sigma$-operations naturally, every homomorphism of $\sigma$-algebras $\Omega_A^\sigma \mathbf{V} \to T \in \mathbf{V}$ extends uniquely to a continuous homomorphism $\overline{\Omega}_A \mathbf{V} \to T$. Hence $r^\sigma(u, v) = r$. □

# Pro-**H** metric on groups

- Traditionally, one denotes by **H** an arbitrary pseudovariety of groups.
- Because a group is highly symmetrical, the pro-**H** metric structure looks similar everywhere.

## Lemma 12.2

*Let $G$ be a group and consider the pro-**H** metric on $G$. Then, for every $u, v, w \in G$, the equalities $d(uw, vw) = d(u, v) = d(wu, wv)$ hold. In particular, for $\epsilon > 0$, we have $B_\varepsilon(u) = uB_\varepsilon(1) = B_\varepsilon(1)u$ and a subset $X$ is open (respectively closed) if and only if so is $Xw$. Moreover, for $\epsilon > 0$, the ball $B_\epsilon(1)$ is a clopen normal subgroup of $G$ such that $G/B_\epsilon(1) \in \mathbf{H}$. A subgroup $H$ is open if and only if it contains some open ball $B_\epsilon(1)$.*

## Proof.

This is a simple exercise. □

- For a subgroup $H$ of a group $G$, denote by $H_G$ the largest normal subgroup of $G$ which is contained in $H$. It is given by the formula
$$H_G = \bigcap_{g \in G} g^{-1} H g.$$
- If we let $G$ act on the set of right cosets of $H$ in $G$ by right translation, then we obtain a homomorphism $\varphi : G \to S_{G/H}$ into the full symmetric group $S_{G/H}$ (of all permutations of the set $G/H$) such that $\varphi^{-1}(\mathrm{id}) = H_G$.
- It follows that, if the index $(G : H)$ of the subgroup $H$ in $G$ is finite, then so is $(G : H_G)$ and $(G : H_G)$ is a divisor of $(G : H)!$.

## Lemma 12.3

*A subgroup $H$ of $G$ is (cl)open in the pro-$\mathbf{H}$ metric if and only if $G/H_G \in \mathbf{H}$.*

## Proof.

Suppose first that $H$ is open. By Lemma 12.2, $H$ contains a normal subgroup $K$ of $G$ such that $G/K \in \mathbf{H}$. Then $K \subseteq H_G$ and so $G/H_G \simeq (G/K)/(H_G/K)$ belongs to $\mathbf{H}$. Conversely, if $G/H_G \in \mathbf{H}$ then $H_G$ is an open set, because the natural homomorphism $G \to G/H_G$ is (uniformly) continuous. Since $H$ contains $H_G$, $H$ is a union of cosets of $H_G$, and so is its complement. Hence $H$ is clopen. □

- Another natural question is whether, for a subgroup $H$ of $G$, the intersection with $H$ of an open subset of $G$ in the pro-**H** metric of $G$ is also open in the pro-**H** metric of $H$.
- In general, the answer is negative, but there are important situations in which it is affirmative.

### Example 12.4

Let $G$ be the free group on two free generators $a, b$ and consider the homomorphism $\varphi : G \to S_3$ defined by $\varphi(a) = (12)$ and $\varphi(b) = (13)$. Let $K = \varphi^{-1}(1)$ and let $H = \varphi^{-1}\langle(123)\rangle$ be the inverse image of the subgroup of index 2. Then $H$ is clopen in the pro-**Ab** metric of $G$ and $K$ is clopen in the pro-**Ab** metric of $H$ but $K$ is not clopen in the pro-**Ab** metric of $G$.

- Note that, for pseudovarieties of groups $\mathbf{K}$ and $\mathbf{H}$, $\mathbf{K} * \mathbf{H}$ consists of all groups $G$ which have a normal subgroup $K$ such that both $K \in \mathbf{K}$ and $G/K \in \mathbf{H}$.[5]
- If $\mathbf{H} * \mathbf{H} = \mathbf{H}$, then we say that $\mathbf{H}$ is closed under extension.
- A condition for the answer to the above question to be affirmative is drawn from the following result.

### Lemma 12.5

*Let $H$ be a clopen subgroup of $G$ in the pro-$\mathbf{H}$ metric of $G$ and suppose that $U$ is a normal subgroup of $H$ such that $H/U \in \mathbf{H}$. Then the normal subgroup $U_G$ of $G$ is such that $G/U_G \in \mathbf{H} * \mathbf{H}$.*

[5] For those unfamiliar with semidirect products, take this as the definition of $\mathbf{K} * \mathbf{H}$ and show that it is a pseudovariety of groups.

## Proof.

Consider also the normal subgroup $H_G$ and let $g \in G$. By Lemma 12.3, $G/H_G$ belongs to $\mathbf{H}$. For each $x \in H_G$, the conjugate $gxg^{-1}$ belongs to $H$ and so the mapping $\varphi_g : H_G \to H/U$ which sends $x$ to $gxg^{-1}U$ is a group homomorphism. Moreover, for $x \in H_G$, we have

$$\begin{aligned} x \in U_G &\Leftrightarrow x \in g^{-1}Ug \text{ for all } g \in G \\ &\Leftrightarrow gxg^{-1} \in U \text{ for all } g \in G \\ &\Leftrightarrow \varphi_g(x) = 1 \text{ for all } g \in G. \end{aligned}$$

It follows that $H_G/U_G$ embeds in a finite power of $H/U$ and so $H_G/U_G \in \mathbf{H}$. The result now follows from the observation that $G/H_G \simeq (G/U_G)/(H_G/U_G)$. □

- A first application of the preceding lemma is the following answer to the above question.

## Proposition 12.6

*Suppose that* $\mathbf{H}$ *is closed under extension. Let* $H$ *be a clopen subgroup of* $G$ *in the pro-*$\mathbf{H}$ *metric of* $G$*. Then a subset of* $H$ *is open in the pro-*$\mathbf{H}$ *metric of* $H$ *if and only if it is open in the pro-*$\mathbf{H}$ *metric of* $G$*.*

## Proof.

By Lemma 12.2, a subgroup $L$ of $H$ is open in the pro-$\mathbf{H}$ metric of $H$ if and only if it contains a normal subgroup $U$ of $H$ such that $H/U \in \mathbf{H}$. By Lemma 12.5, the normal subgroup $U_G$ of $G$ is such that $U/U_G \in \mathbf{H} * \mathbf{H} = \mathbf{H}$. Hence $U$ is open in the pro-$\mathbf{H}$ metric of $G$ by Lemma 12.3. Since $L$ is a union of cosets of $U$, $L$ is also open in the pro-$\mathbf{H}$ metric of $G$. □

- In terms of pro-**H** metrics, we obtain the following more precise result.

## Proposition 12.7

*Suppose that* **H** *is closed under extension and* $G$ *is a group residually in* **H**. *Let* $H$ *be a clopen subgroup of* $G$ *in the pro-***H** *metric of* $G$. *Then the pro-***H** *metric* $d_H$ *of* $H$ *and the restriction to* $H$ *of the pro-***H** *metric* $d_G$ *of* $G$ *have the same Cauchy sequences.*

## Proof.

Let $d$ be the restriction of $d_G$ to $H$ and let $r$ be the corresponding partial function $H \times H \to \mathbb{N}$. Denote by $d'$ the pseudo-metric $d_H$ and by $r'$ the corresponding partial function. We start by establishing the following function inequalities:

$$r' \leq r \leq \big((G : H) \cdot r'\big)!. \tag{1}$$

The first inequality in (1) follows from the observation that, if a homomorphism from $G$ into a member of $\mathbf{H}$ distinguishes two elements of $H$ then its restriction to $H$ also distinguishes them. Suppose next that $u, v \in H$ and the homomorphism $\varphi : H \to K$ with $K \in \mathbf{H}$ are such that $\varphi(u) \neq \varphi(v)$. Let $U = \varphi^{-1}(1)$. Then $H/U$ embeds in $K$ and, therefore, it belongs to $\mathbf{H}$. By Lemma 12.5, $U_G$ is a normal subgroup of $G$ of finite index such that $G/U_G \in \mathbf{H} * \mathbf{H} = \mathbf{H}$ and, by an earlier observation, $(G : U_G)$ divides $(G : U)!$. If we choose above $K$ so that $|K|$ is minimum, then $(H : U) = r'(u, v)$ and so, since $uU_G \neq vU_G$,

$$r(u, v) \leq (G : U_G) \leq (G : U)! = \big((G : H) \cdot (H : U)\big)! = \big((G : H) \cdot r'(u, v)\big)!$$

which proves (1).

## $(\ldots)$

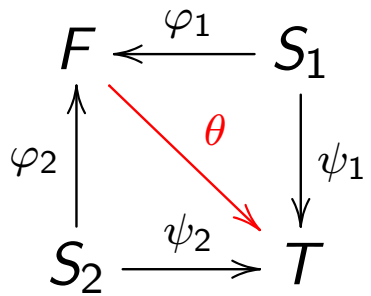
From the first inequality in (1) we deduce that every Cauchy sequence with respect to $d'$ is also a Cauchy sequence with respect to $d$. For the converse, let $f(n) = \big((G : H) \cdot n\big)!$. Then $f$ is an increasing sequence and a simple calculation shows that, for every $\varepsilon > 0$,

$$d \leq 2^{-f(\lceil -\log_2 \varepsilon \rceil)} \implies d' \leq \varepsilon.$$

This implies that Cauchy sequences for $d$ are also Cauchy sequences for $d'$. □

# Free products

- A free product in a variety $\mathcal{V}$ of semigroups is given by two homomorphisms $\varphi_i : S_i \to F$ $(i = 1, 2)$, with $S_1, S_2, F \in \mathcal{V}$ such that, given any other pair of homomorphisms $\psi_i : S_i \to T$, with $T \in \mathcal{V}$, there exists a unique homomorphism $\theta : F \to T$ such that the following diagram commutes:




- By the usual argument, if the free product exists, then it is unique up to isomorphism.

## Exercise 12.8

Show that, for every variety $\mathcal{V}$ and semigroups $S_1, S_2 \in \mathcal{V}$, the free product of $S_1$ and $S_2$ in $\mathcal{V}$ exists.

- For semigroups $S$ and $T$ in a variety $\mathcal{V}$, we say that $S$ is a free factor of $T$ if there exists $U \in \mathcal{V}$ such that $T$ is a free product of $S$ and $U$ in $\mathcal{V}$. Note that every semigroup is a free factor of itself.

## Exercise 12.9

Suppose that $S$ is a free factor of $T$ in the variety $\mathcal{V}$ generated by a pseudovariety $\mathbf{V}$. Show that:

1. the pseudo-metric $d_{\mathbf{V}}^S$ and the restriction of the pseudo-metric $d_{\mathbf{V}}^T$ to $S$ coincide;
2. the open sets in pro-$\mathbf{V}$ metric of $S$ are the intersection with $S$ of the open sets of $T$ in the pro-$\mathbf{V}$ metric of $T$.

## Theorem 12.10

*Let $H$ be a finitely generated subgroup of a finitely generated free group $G$ in the variety generated by the extension-closed pseudovariety* **H** *and suppose that $H$ is a free factor of a clopen subgroup of $G$ in the pro-***H** *metric. Then the following hold:*

1. *the pro-***H** *metric $d_H$ of $H$ has the same Cauchy sequences as the restriction of the pro-***H** *metric $d_G$;*
2. *the completion of $H$ with respect to $d_G$ is a free pro-***H** *group.*

## Proof.

We may as well assume that $\mathbf{H}$ is not the trivial pseudovariety for, otherwise, the result is obvious. Hence $\mathbf{H}$ contains some cyclic group of prime order $\mathbb{Z}/p\mathbb{Z}$. Since $\mathbf{H}$ is closed under extension, it follows that $\mathbf{G}_p \subseteq \mathbf{H}$ for some prime $p$. Since the free group is residually a finite $p$-group by a result of Baumslag [Bau65], we may therefore assume that $G$ is an absolutely free group. By the Nielsen-Schreier Theorem, the subgroup $H$ is also an absolutely free group. By Proposition 12.1, the completion of $H$ with respect to the metric $d_H$ is a free pro-$\mathbf{H}$ group. Since, by Proposition 12.7 and Exercise 12.9, the Cauchy sequences of $H$ are the same with respect to both metrics $d_H$ and $d_G$, the completion of $H$ with respect to both metrics is the same metric group and so it is a free pro-$\mathbf{H}$ group. □

The following corollaries will be useful later.

### Corollary 12.11

*Let* **H** *be an extension-closed pseudovariety of groups and let* $G$ *be a finitely generated free group in the variety generated by* **H**. *If the finitely generated subgroup* $H$ *is a free factor of a clopen subgroup of* $G$ *in the pro-***H** *metric, then* $H$ *is closed in that metric.*

The following result is known as the subgroup theorem in the theory of profinite groups. For simplicity, it is presented here only in the finitely generated case, although the proof could be extended to the general case.

### Corollary 12.12

*Let* $H$ *be a clopen subgroup of a finitely generated free pro-***H** *group* $G$, *where* **H** *is an extension-closed pseudovariety of groups. Then* $H$ *is itself a free pro-***H** *group.*

## Proof of Corollary 12.11.

Since the pro-**H** metric of a clopen subgroup is the induced metric, we may as well assume that $H$ is a free factor of $G$. Let $(h_n)_n$ be a sequence of elements of $H$ and suppose that it converges in $G$ to an element $g$. Suppose $H'$ is another subgroup of $G$ such that $G$ is the free product of $H$ and $H'$. Then, by considering the identity mapping on $H$ and sending $H'$ to 1 we obtain an onto homomorphism $\varphi : G \to H$ which is obviously continuous with respect to the pro-**H** metrics of $G$ and $H$. Hence $(h_n)_n$ already converges in $H$, namely to $\varphi(g)$. Since the metrics $d_H$ and $d_G$ have the same Cauchy sequences in $H$ by Theorem 12.10, the limit must be the same in both cases, and so $g \in H$. This shows that $H$ is closed in the pro-**H** metric of $G$. □

## Proof of Corollary 12.12.

Let $A$ be a finite free generating set for $G$. Let $G'$ be the subgroup of $G$ discretely generated by $A$. Then $G'$ is a free group over $A$ in the variety generated by **H** and it is a dense subgroup of $G$. Let $H' = H \cap G'$. Then $H'$ is a clopen subgroup of $G'$ in the pro-**H** topology of $G'$. Since $H$ is open, $H'$ is dense in $H$. Hence $H$ is the completion of $H'$ with respect to the metric $d_G$. Applying Theorem 12.10 to the free factor $H'$ of itself, it follows that $H$ is a free pro-**H** group. □

# Outline

# The free group and inverse automata

Let now $G$ be a free group on a finite set $A$. To each finite subset $X$ of $G$ we associate a finite inverse automaton as follows.[6]

- For each reduced group word representative $w$ of an element of $X$, consider a linear graph with directed edges labeled by the successive letters of $w$, the edge appearing in the direction of left-to-right reading of $w$ if the corresponding generator appears with exponent 1 and in the opposite direction if the exponent is $-1$. Thus the label of the undirected path which traverses the graph in the direction of left-to-right reading of $w$ is $w$.
- Glue these graphs together by identifying their ends to a single vertex $v_0$ which is the unique initial and final state of the automaton.
- Fold edges so that the resulting automaton becomes inverse in the sense that the transformations defined by the labels are partial bijections. This can be done by applying the following procedure, in an arbitrary order, until it no longer applies: whenever we encounter two edges with the same label leaving from the same state or arriving at the same state, we identify them.

[6] See [Sta83, MSW01, KM02] for details and further references.

# Example 1

Let $G$ be the free group on the free generators $a, b, c$ and let $X = \{ab^{-1}c^{-1}a, a^{-1}b^{-1}ac^{-1}a, bc^{-1}a\}$. Then the sequence of pictures in Figure 1 describes the construction of the folded inverse automaton associated with $X$.

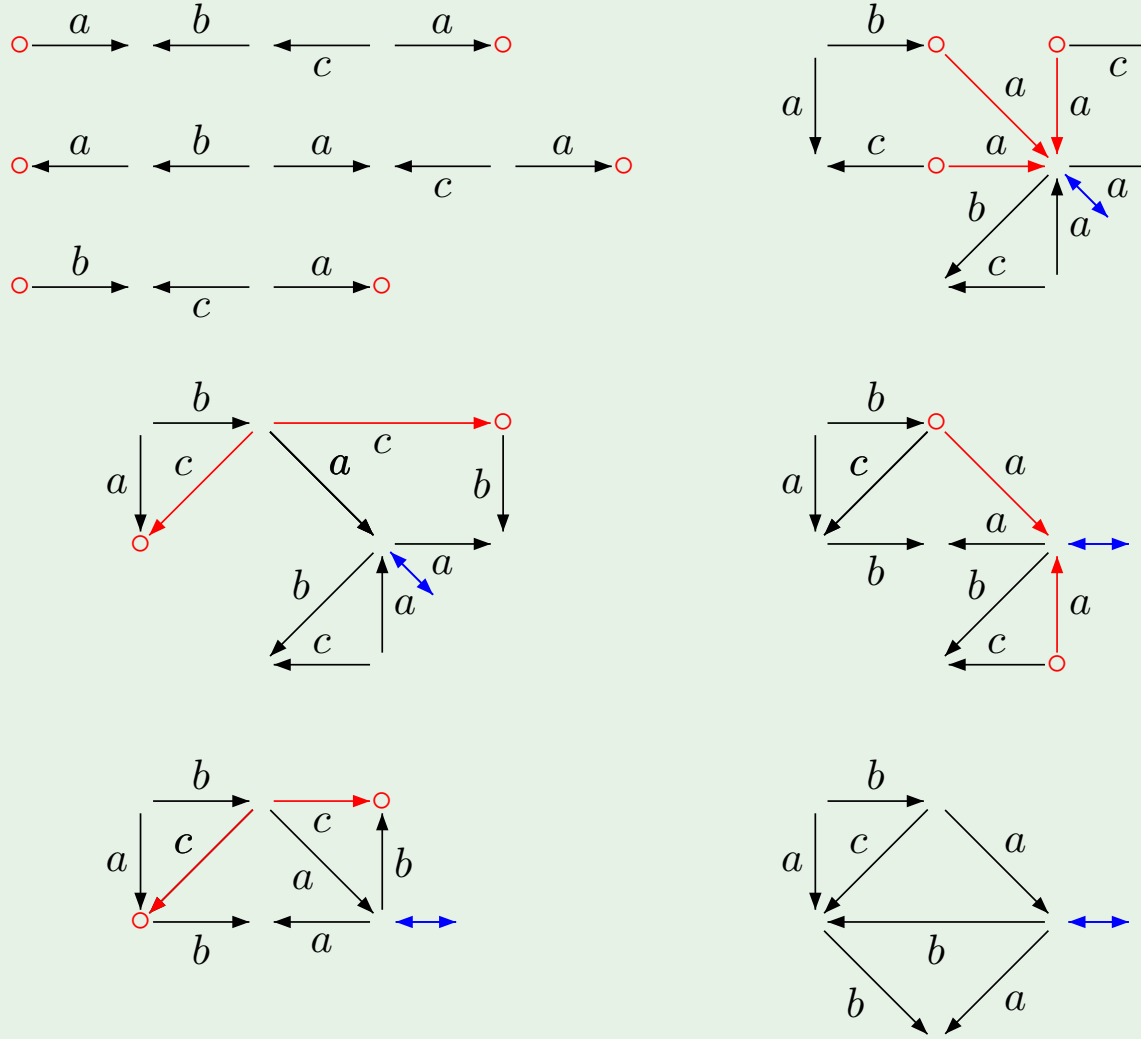


Figure: The folding procedure

- The automaton resulting from the above procedure is reduced in the sense that it has a unique initial state which is simultaneously the unique final state, every state is accessible from it (through an undirected path), and there is no state of degree 1 other than possibly the initial and final state.
- The set of reduced group words recognized by the automaton is precisely the subgroup $\langle X \rangle$ generated by $X$.
- Moreover, this automaton is unique up to isomorphism and it depends only on the subgroup $\langle X \rangle$ and not on the specific generating set $X$. Thus, for a finitely generated subgroup $H$ of the free group $G$ on a set $A$, we will denote its automaton by $\mathcal{A}(H)$.
- Conversely, a given finite reduced inverse automaton $\mathcal{A}$ over the alphabet $A$ recognizes a finitely generated subgroup of the free group on $A$ whose associated automaton is $\mathcal{A}$. This subgroup is the fundamental group of the underlying graph.

The following result summarizes the properties of the construction of the automaton associated with a finitely generated subgroup of a free group.

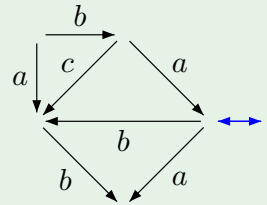
### Theorem 13.1

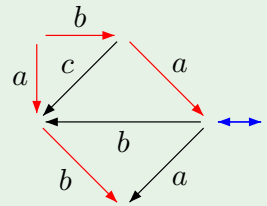
*The correspondence which maps each finitely generated subgroup $H$ of the free group $G$ on the set $A$ to its automaton $\mathcal{A}(H)$, constructed from a finite generating set of $H$, has the following properties:*

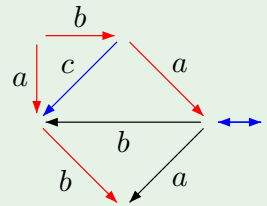
1. *the automaton $\mathcal{A}(H)$ is effectively constructible and does not depend on the generating set but only on $H$;*
2. *the correspondence defines a bijection between the set of all finitely generated subgroups of $G$ and the set of all finite reduced inverse automata with input alphabet $A$.*

# Example 2

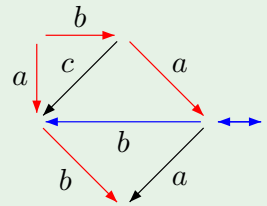
We recall the procedure to compute the fundamental group of a connected labeled directed graph with a root vertex, namely to exhibit a finite generating set for that subgroup. First, choose a generating tree, that is a maximal subgraph whose underlying undirected graph is a tree. Note that every vertex of the original graph is on the tree. To each edge $e$ which is not on the chosen tree, associate the group word which is obtained by reading the label of the (undirected) path which goes from the root along the tree to the beginning vertex of $e$, then follows $e$, and then returns to the root along the tree. The set of all words associated in this way to the edges which are not on the tree generates a subgroup of the free group on the labels which is called the fundamental group of the labeled graph. This procedure is shown here for the inverse automaton obtained in the preceding example. The resulting generating set for the same subgroup, namely the subgroup recognized by the inverse automaton, is $\{a^{-1}ca^{-1}ba, ba^{-1}ba, ab^{-1}a^{-1}ba\}$. The set thus obtained freely generates the subgroup. This also gives a procedure to compute free generators for the subgroup of a free group generated by a given finite set of group words.



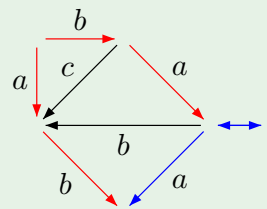




$a^{-1} \cdot c \cdot a^{-1}ba$




$b \cdot a^{-1}ba$




$a \cdot b^{-1}a^{-1}ba$

We proceed to explore some other relationships between inverse automata and finitely generated subgroups of free groups.
Let $\mathcal{A}$ and $\mathcal{B}$ be two reduced inverse automata with the same input alphabet $A$. A morphism $f : \mathcal{A} \to \mathcal{B}$ is a function which maps states of $\mathcal{A}$ to states of $\mathcal{B}$, sending the initial state of $\mathcal{A}$ to that of $\mathcal{B}$, in such a way that the action of $A$ is respected:

- if $q$ is a state of $\mathcal{A}$, $a \in A \cup A^{-1}$, and $qa$ is defined, then $f(q)a$ is also defined and $f(q)a = f(qa)$.

Note that if such a morphism exists then it is unique.

## Proposition 13.2

*Let $G$ be a free group and let $H$ and $K$ be finitely generated subgroups of $G$. Then $H \subseteq K$ if and only if there is an automaton morphism from $\mathcal{A}(H)$ into $\mathcal{A}(K)$. Moreover, if the morphism is injective then $H$ is a free factor of $K$.*

## Proof.

Suppose first that there exists an automaton morphism $\mathcal{A}(H) \to \mathcal{A}(K)$. A reduced group word $w$ representing an element of $H$ labels a successful path in $\mathcal{A}(H)$. By transforming this path by the morphism, we obtain a successful path in $\mathcal{A}(K)$, which shows that $w$ also represents an element from $K$. Hence $H \subseteq K$.

Conversely, suppose that $H \subseteq K$. We may choose finite sets $X$ and $Y$ of reduced words such that $\langle X \rangle = H$ and $\langle X \cup Y \rangle = K$. Then, the construction of $\mathcal{A}(H)$ and $\mathcal{A}(K)$ proceeds from sets of linear automata in which the first is contained in the second. This implies that every identification which is made to obtain $\mathcal{A}(H)$ will also occur in the construction of $\mathcal{A}(K)$. Hence there is a morphism $\mathcal{A}(H) \to \mathcal{A}(K)$.

Suppose next that there is an injective morphism $\mathcal{A}(H) \to \mathcal{A}(K)$. Choose for $\mathcal{A}(H)$ a generating tree. Its image in $\mathcal{A}(K)$ is still a tree and so it can be expanded to a generating tree of $\mathcal{A}(K)$. Hence there is a free generating set for $K$ which contains a free generating set for $H$ and this is equivalent to $H$ being a free factor of $K$. □

Let $\mathcal{A}$ be an inverse automaton. A congruence on $\mathcal{A}$ is an equivalence relation $\sim$ on the state set of $\mathcal{A}$ which is compatible with the action of the input alphabet $A$:

- if $q_1, q_2$ are states, $a \in A \cup A^{-1}$, $q_1 a, q_2 a$ are both defined, and $q_1 \sim q_2$, then $q_1 a \sim q_2 a$.

We may then consider the quotient automaton $\mathcal{A}/\sim$, whose states are the $\sim$-classes of states of $\mathcal{A}$ and such that the action of $A$ is given by $(q/\sim)a = (qa)/\sim$. Note that $\mathcal{A}/\sim$ is an inverse automaton.

## Lemma 13.3

*Let $H$ and $K$ be finitely generated subgroups of the free group on a finite set $A$ and suppose that $H \subseteq K$. For each state $p$, choose a reduced word $u_p$ which labels a path in $\mathcal{A}(H)$ from the initial state to $p$. Then the congruence $\sim_{H,K}$ on $\mathcal{A}(H)$ determined by the kernel of the unique morphism $\varphi : \mathcal{A}(H) \to \mathcal{A}(K)$ satisfies the following condition:*

$$\text{for all states } p, q,\ p \sim_{H,K} q \text{ if and only if } u_p u_q^{-1} \in K. \qquad (2)$$

*Moreover, if $L$ is the fundamental group of the quotient automaton $\mathcal{A}(H)/\sim_{H,K}$, then $H \subseteq L$ and $L$ is a free factor of $K$.*

## Proof.

If $u_p u_q^{-1} \in K$, then $u_p$ and $u_q^{-1}$ label paths in $\mathcal{A}(K)$ from the initial-final state to the states $\varphi(p)$ and $\varphi(q)$. Since $\mathcal{A}(K)$ is an inverse automaton which recognizes $K$, it follows that $\varphi(p) = \varphi(q)$, that is $p \sim_{H,K} q$. Conversely, if $p \sim_{H,K} q$, then $\varphi(p) = \varphi(q)$ and so the reduced form of $u_p u_q^{-1}$ labels a loop at the initial-final state in $\mathcal{A}(K)$, that is $u_p u_q^{-1} \in K$. This proves condition (2). The last part of the statement of the lemma follows from Proposition 13.2. □

## Proposition 13.4

*Let $H$ be a finitely generated subgroup of the finitely generated free group $G$ on a finite set $A$, which is endowed with the pro-$\mathbf{V}$ topology. Then the following hold:*

1. *if $H$ is a clopen normal subgroup then $\mathcal{A}(H)$ is a permutation automaton whose transition monoid is isomorphic to $G/H$ and belongs to $\mathbf{V}$;*
2. *$H$ is clopen if and only if $\mathcal{A}(H)$ is a permutation automaton whose transition monoid belongs to $\mathbf{V}$.*

## Proof.

By Lemma 12.3, if $H$ is a clopen normal subgroup then $G/H \in \mathbf{V}$. The Cayley graph of the finite group $G/H$ with respect to $A$ can be viewed as a reduced inverse automaton which recognizes $H$ as the set of reduced group words which label loops at the vertex 1. Hence it is isomorphic to $\mathcal{A}(H)$ and $\mathcal{A}(H)$ is a (complete) permutation automaton. The states in the Cayley graph are precisely the cosets of $H$, on which the input alphabet acts by right translation. Hence the transition monoid is isomorphic to $G/H$ and it belongs to $\mathbf{V}$.

Next we assume only that $H$ is clopen. By Lemma 12.3, $H_G$ is a clopen normal subgroup. The quotient automaton $\mathcal{A}(H_G)/{\sim_{H_G,H}}$ embeds in $\mathcal{A}(H)$. Since $\mathcal{A}(H_G)$ is a complete automaton by (1), so is its quotient $\mathcal{A}(H_G)/{\sim_{H_G,H}}$. Since $\mathcal{A}(H)$ is a reduced inverse automaton, it follows that $\mathcal{A}(H)$ is also a permutation automaton as there is no room in $\mathcal{A}(H_G)/{\sim_{H_G,H}}$ to add vertices or edges. The transition monoid of $\mathcal{A}(H)$ is therefore a quotient of that of $\mathcal{A}(H_G)$, which is isomorphic to $G/H_G$ by (1), and therefore it belongs to $\mathbf{V}$.

(. . . )

Conversely, suppose that $\mathcal{A}(H)$ is a permutation automaton whose transition monoid $M$ belongs to $\mathbf{V}$ and consider the natural homomorphism $\varphi : G \to M$ and $K = \varphi^{-1}(1)$. Then $K$ consists of all reduced words which map every state of $\mathcal{A}(H)$ to itself while $H$ consists of all reduced words which map the state 1 to itself. Hence $K \subseteq H$ and $H$ is clopen since $K$ is clopen by Lemma 12.3. □

A simple application of Proposition 13.4 is the following theorem due to M. Hall [Hal50] in a paper which first introduced profinite topologies on free groups.

### Theorem 13.5

*Every finitely generated subgroup of a free group $G$ on a finite set $A$ is closed in the profinite metric of $G$.*

## Proof.

Let $H$ be a finitely generated subgroup of $G$. If $H = G$, then of course $H$ is closed. Otherwise, it suffices to show that, for every reduced word $g \in G \setminus H$, there is a clopen subgroup which contains $H$ but not $g$. Consider the automaton $\mathcal{A}(H)$ and add to it, starting from the initial-final state, a linear automaton which reads $g$. By applying the folding procedure, we end up with an inverse automaton, which may not be reduced, in which the end state of the added linear automaton is not identified to the initial-final state. Each generator $a \in A$ determines in this automaton a partial permutation of the state set. Now, every partial permutation of a finite set may be completed to a full permutation and we choose such a completion for each generator $a \in A$. This leads to a permutation automaton $\mathcal{B}$ in which $\mathcal{A}(H)$ embeds. By Proposition 13.4, the fundamental group $K$ of $\mathcal{B}$ is a clopen subgroup of $G$. By Proposition 13.2, $K$ contains $H$. On the other hand, $g \notin K$ since in $\mathcal{B}$ the reduced word $g$ does not label a loop at the initial-final state. □

## Note 13.6

An alternative proof of Theorem 13.5 is obtained as follows. Complete the automaton $\mathcal{A}(H)$ of the given finitely generated subgroup of $G$ to a permutation automaton $\mathcal{B}$, with the same initial-final state. By Proposition 13.4, the fundamental group $K$ of $\mathcal{B}$ is a clopen subgroup. By Proposition 13.2, $H$ is contained in $K$. By Corollary 12.11, since **G** is extension closed, $H$ is closed.

# Example 3

In Example 1 we obtained the first inverse automaton in Figure 2

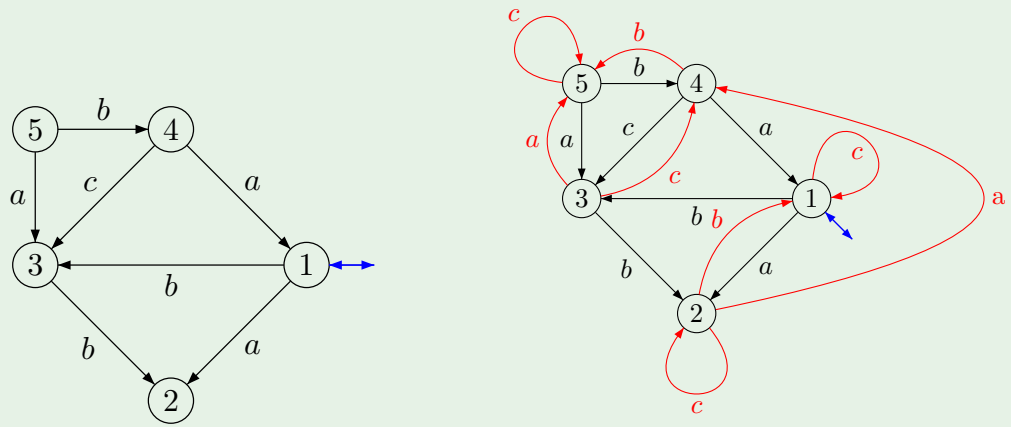



Figure: An inverse automaton and one of its completions

which gives the partial permutations defined in the table on the left and one of their possible completions to permutations in the table on the right

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $a$ | 2 | – | – | 1 | 3 |
| $b$ | 3 | – | 2 | – | 4 |
| $c$ | – | – | – | 3 | – |

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $a$ | 2 | 4 | 5 | 1 | 3 |
| $b$ | 3 | 1 | 2 | 5 | 4 |
| $c$ | 1 | 2 | 4 | 3 | 5 |

and the corresponding permutation automaton in Figure 2. This permutation automaton determines a clopen subgroup $K$, in the profinite metric of the free group, of which the original subgroup is a free factor.

More generally, we say that a finitely generated subgroup $H$ of the free group $G$ on the finite set $A$ is **V**-extendible if $\mathcal{A}(H)$ can be extended to a permutation automaton whose transition monoid belongs to **V**. In such an extension, both states and transitions may be added.

## Lemma 13.7

*The finitely generated subgroup $H$ of the free group $G$ on a finite set $A$ is **V**-extendible if and only if there is a clopen subgroup $K$ of $G$, in the pro-**V** metric of $G$, such that the congruence $\sim_{H,K}$ on $\mathcal{A}(H)$ is the equality.*

## Proof.

If $H$ is **V**-extendible, then there is a permutation automaton $\mathcal{B}$ containing $\mathcal{A}(H)$, with the same initial-final state, whose transition monoid belongs to **V**. By Proposition 13.4, the fundamental group $K$ of $\mathcal{B}$ is clopen in the pro-**V** metric of $G$. Then $\mathcal{A}(H)$ embeds in $\mathcal{A}(K)$ and so, by definition of the congruence $\sim_{H,K}$ (cf. Lemma 13.3), this congruence is the equality relation on the state set of $\mathcal{A}(H)$. The converse is proved similarly. □

By definition of pro-**V** metric, the closure of a subgroup of a group $G$ is the intersection of the clopen subgroups that contain it. In the case of finitely generated subgroups of a finitely generated free group, we can use the previous results to obtain a more precise statement.

### Proposition 13.8

*Let $H$ be a finitely generated subgroup of the free group $G$ on a finite set $A$, which is endowed with the pro-**V** metric, and let $\overline{H}$ be the closure of $H$ in $G$. Then the following hold:*

1. *there is a clopen subgroup $K$ of $G$ such that $\sim_{H,\overline{H}}$ coincides with $\sim_{H,K}$;*
2. *there is a smallest **V**-extendible subgroup containing $H$, namely the subgroup $\tilde{H}$ such that $\mathcal{A}(\tilde{H})$ is the image of $\mathcal{A}(H)$ in $\mathcal{A}(\overline{H})$;*
3. *$H \subseteq \tilde{H} \subseteq \overline{H}$ and $\tilde{H}$ is a free factor of $\overline{H}$.*

## Proof.

By Proposition 13.2, for each clopen subgroup $K$ containing $H$, there is a morphism $\mathcal{A}(H) \to \mathcal{A}(K)$, which determines a congruence on $\mathcal{A}(H)$. The intersection $\sim$ of all such congruences is still a congruence on $\mathcal{A}(H)$. Since the automaton $\mathcal{A}(H)$ is finite, the intersection $\sim$ involves only finitely many congruences and so $\mathcal{A}(H)/\sim$ is the largest quotient of $\mathcal{A}(H)$ which embeds in a permutation automaton of a clopen subgroup. The fundamental group of $\mathcal{A}(H)/\sim$ is therefore a finitely generated subgroup $L$ containing $H$ which is a free factor of the clopen subgroup $K$, whose automaton $\mathcal{A}(K)$ is the smallest permutation automaton in which $\mathcal{A}(L)$ embeds and which has a transition monoid in $\mathbf{V}$. This proves the proposition. □

The following result reduces the computation of $\tilde{H}$ (and therefore also the question as to whether $H$ is $\mathbf{V}$-extendible) to the membership problem of the pro-$\mathbf{V}$ closure $\overline{H}$.

## Proposition 13.9

*Let $G$ be a finitely generated free group, endowed with the pro-$\mathbf{V}$ metric, and let $H$ be a given finitely generated subgroup of $G$. If the membership problem for $\overline{H}$ is decidable then one can effectively compute the smallest $\mathbf{V}$-extendible subgroup $\tilde{H}$ of $G$ containing $H$.*

## Proof.

By Proposition 13.8, it suffices to compute the congruence $\sim_{H,\overline{H}}$ on the automaton $\mathcal{A}(H)$. By condition (2) of Lemma 13.3, this congruence can be computed by the choice of a label $u_q$ for a path from the initial-final state to each state $q$ by using the solution of the membership problem for $\overline{H}$. □

Thus, one may concentrate on the membership problem for the closure subgroup $\overline{H}$.

Proposition 13.8 is insufficient to guarantee the existence of an algorithm to compute the closure $\overline{H}$ of a given finitely generated subgroup $H$. In case $\mathbf{V}$ is an extension-closed pseudovariety, we obtain some more precise results.

## Theorem 13.10

*Let $H$ be a finitely generated subgroup of a finitely generated free group, which is endowed with the pro-$\mathbf{V}$ metric for an extension-closed pseudovariety $\mathbf{V}$. The following conditions are equivalent:*

1. *$H$ is closed;*
2. *$H$ is $\mathbf{V}$-extendible;*
3. *$H$ is a free factor of a clopen subgroup.*

## Proof.

By Proposition 13.8, (1) implies $H = \tilde{H} = \overline{H}$ which yields (2) since $\tilde{H}$ is $\mathbf{V}$-extendible. Condition (2) implies (3) by Proposition 13.2. Finally, (3) implies (1) by Corollary 12.11. □

## Corollary 13.11

*Under the hypotheses of Theorem 13.10, $\tilde{H} = \overline{H}$.* □

## Exercise 13.12

Let $G$ be a finitely generated free group and endow it with the pro-**V** metric. Let $H$ be a finitely generated subgroup of $G$. Prove the following:

1. for every $g \in G$, the automaton $\mathcal{A}(g^{-1}Hg)$ is obtained by modifying $\mathcal{A}(H)$ as follows: if the initial-final state of $\mathcal{A}(H)$ is $q_0$ then set that of $\mathcal{A}(g^{-1}Hg)$ to be the state $q_0 g$;
2. $H$ is **V**-extendible if and only if all its conjugates are **V**-extendible;
3. $H$ is closed (respectively open) if and only if all its conjugates have the same property.

# Outline

# Relative invertibility of endomorphisms

- Given a continuous endomorphism $\varphi$ of $\overline{\Omega}_n\mathbf{M}$, we denote by $M(\varphi)$ the $n \times n$-matrix over the profinite ring $\hat{\mathbb{Z}}$ whose $(i,j)$-coordinate is the image of $\varphi(x_i)$ of the $i$-th generator of $\overline{\Omega}_n\mathbf{M}$ under the unique continuous homomorphism $\overline{\Omega}_n\mathbf{M} \to \hat{\mathbb{Z}}$ which maps $x_j$ to 1 and all other generators to 0.
- The determinant and trace of the matrix $M(\varphi)$ are also called, respectively, the determinant and trace of $\varphi$ and are denoted $\det\varphi$ and $\operatorname{tr}\varphi$.

## Exercise 14.1

Let $M$ be a profinite monoid. Show that $m \in M$ is invertible if and only if $m$ is right invertible, if and only if $m$ is left invertible, if and only if $m^\omega = 1$.

- For a metric semigroup $S$, denote by $\operatorname{End} S$ the monoid of continuous endomorphisms of $S$.
- For a pseudovariety $\mathbf{V}$ of monoids and $w \in \overline{\Omega}_n\mathbf{M}$, denote by $w_{\mathbf{V}}$ the restriction of the implicit operation $w$ to $\mathbf{V}$.
- For $\varphi \in \operatorname{End} \overline{\Omega}_n\mathbf{M}$, denote by $\varphi_{\mathbf{V}}$ the continuous endomorphism of $\overline{\Omega}_n\mathbf{V}$ induced by $\varphi$, which maps the generator $x_i$ to $(\varphi(x_i))_{\mathbf{V}}$.
- Say that $\varphi$ is $\mathbf{V}$-invertible if $\varphi_{\mathbf{V}}$ is invertible in $\operatorname{End} \overline{\Omega}_n\mathbf{V}$.

## Proposition 14.2

*A continuous endomorphism $\varphi$ of $\overline{\Omega}_n\mathbf{M}$ is $\mathbf{V}$-invertible if and only if $\overline{\Omega}_n\mathbf{V}$ is generated by the set $\{\varphi_{\mathbf{V}}(x_i) : i = 1, \ldots, n\}$.*

## Proof.

Let $M$ be the (closed) submonoid of $\overline{\Omega}_n\mathbf{V}$ generated by $\{\varphi_{\mathbf{V}}(x_i) : i = 1, \ldots, n\}$.
Suppose first that $\varphi$ is $\mathbf{V}$-invertible. Then $(\varphi^\omega)_{\mathbf{V}} = (\varphi_{\mathbf{V}})^\omega$ is the identity mapping on $\overline{\Omega}_n\mathbf{V}$. Given $u \in \overline{\Omega}_n\mathbf{V}$, letting $w = \varphi_{\mathbf{V}}^{\omega-1}(u)$, we conclude that

$$u = \varphi_{\mathbf{V}}(w) = \varphi_{\mathbf{V}}\big(w_{\overline{\Omega}_A\mathbf{V}}(x_1, \ldots, x_n)\big) = w_{\overline{\Omega}_A\mathbf{V}}\big(\varphi_{\mathbf{V}}(x_1), \ldots, \varphi_{\mathbf{V}}(x_n)\big),$$

where the last equality is justified since implicit operations on $\mathbf{V}$ commute with continuous homomorphisms between pro-$\mathbf{V}$ semigroups. Since $w$ is the limit of a sequence of words, it follows that $u \in M$, which shows that $M = \overline{\Omega}_n\mathbf{V}$.

## $(\dots)$

Conversely, suppose that $M = \overline{\Omega}_n\mathbf{V}$. Given $u \in \overline{\Omega}_n\mathbf{V}$, there exists a sequence of words $(w_n)_n$ such that

$$u = \lim_{n\to\infty} (w_n)_{\overline{\Omega}_n\mathbf{V}}\big(\varphi_\mathbf{V}(x_1), \dots, \varphi_\mathbf{V}(x_n)\big) = \lim_{n\to\infty} \varphi_\mathbf{V}(w_n).$$

Since $\overline{\Omega}_n\mathbf{M}$ is a compact metric space, we may assume that the sequence $(w_n)_n$ converges to some $w \in \overline{\Omega}_n\mathbf{M}$. For such an implicit operation $w$, we have $\varphi_\mathbf{V}(w) = u$. In particular, for each generator $x_i$ there exists $v_i \in \overline{\Omega}_n\mathbf{M}$ such that $x_i = \varphi_\mathbf{V}(v_i)$. Let $\psi$ be the continuous endomorphism of $\overline{\Omega}_n\mathbf{M}$ which maps $x_i$ to $v_i$. Then the composite continuous endomorphism $\varphi_\mathbf{V} \circ \psi_\mathbf{V}$ fixes the generators $x_i$ and, therefore it is the identity mapping of $\overline{\Omega}_n\mathbf{V}$. Hence $\varphi_\mathbf{V}$ is invertible. □

- Let **Ab** denote the pseudovariety of all finite Abelian groups.
- Let $\mathfrak{A}_m$ denote the pseudovariety of all finite Abelian groups of exponent $m$.

## Proposition 14.3

*The following conditions are equivalent for a continuous endomorphism $\varphi$ of $\overline{\Omega}_n\mathbf{M}$ and a prime integer $p$:*

1. *$\varphi$ is $\mathbf{G}_p$-invertible;*
2. *$\varphi$ is $\mathfrak{A}_p$-invertible;*
3. *$\det\varphi$ is not divisible by $p$.*

## Proof.

Since $\mathfrak{A}_p \subseteq \mathbf{G}_p$, clearly (1)⇒(2). On the other hand, (2)⇔(3) follows from elementary Linear Algebra since $\overline{\Omega}_n\mathfrak{A}_p$ is the additive reduct of the $n$-dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$. We prove (2)⇒(1) by contraposition and so we assume that $\varphi$ is not $\mathbf{G}_p$-invertible. Then, by Proposition 14.2, the set $\{\varphi_{\mathbf{G}_p}(x_i) : i = 1, \ldots, n\}$ generates a proper closed subgroup $H$ of $\overline{\Omega}_n\mathbf{G}_p$. Since $\overline{\Omega}_n\mathbf{G}_p$ is a profinite group, it follows that $H$ is contained in some proper clopen subgroup $K$ of $\overline{\Omega}_n\mathbf{G}_p$. Hence there is a continuous homomorphism $\psi : \overline{\Omega}_n\mathbf{G}_p \to F$ onto a finite $p$-group $F$ such that $\psi(H)$ is the trivial subgroup. We may assume that $\psi$ is the restriction mapping $\overline{\Omega}_n\mathbf{G}_p \to \overline{\Omega}_n\mathfrak{A}_p$, from which we deduce that $\varphi_{\mathfrak{A}_p}$ is the trivial endomorphism of $\overline{\Omega}_n\mathfrak{A}_p$ and, therefore, it is not $\mathfrak{A}_p$-invertible. □

## Exercise 14.4

Show that the following conditions are equivalent for an element $u$ of the ring $\hat{\mathbb{Z}}$:

1. $u$ is multiplicatively invertible (or a unit);
2. no prime integer divides $u$;
3. $u$ is invertible in each $p$-adic completion $\mathbb{Z}_p$.

Hence, if $u \in \mathbb{Z}$, then $u$ is invertible in $\hat{\mathbb{Z}}$ if and only if $u = \pm 1$.

# Outline

Here is a first result with an algorithmic flavour towards the computation of the closure of a finitely generated subgroup of the free group.

### Proposition 15.1

*Let* $\mathbf{V}$ *be a non-trivial extension-closed pseudovariety of groups and let* $G$ *be a finitely generated free group which is endowed with the pro-*$\mathbf{V}$ *metric. Suppose that a finitely generated subgroup* $H$ *of* $G$ *is not dense in* $G$ *and let* $\varphi : G \to F$ *be a homomorphism onto* $F \in \mathbf{V}$ *such that* $\varphi(H) \subsetneq F$*. Then one can compute from* $\varphi$ *a closed finitely generated free factor* $L$ *of some clopen subgroup* $K$ *of* $G$ *such that* $\mathcal{A}(L)$ *is a quotient of the automaton* $\mathcal{A}(H)$*.*

## Proof.

Put $K = \varphi^{-1}\big(\varphi(H)\big)$. Then $K$ is a clopen subgroup of finite index in $G$. Consider the congruence $\sim_{H,K}$ on the inverse automaton $\mathcal{A}(H)$ and let $L$ be the finitely generated subgroup of $G$ such that $\mathcal{A}(L) \simeq \mathcal{A}(H)/\sim_{H,K}$. By Lemma 13.3, $L$ is a free factor of $K$. By Corollary 12.11, $L$ is a closed subgroup of $G$.

It remains to argue that all constructions are effective. Given the finite group $F$ and the onto homomorphism $\varphi$, and the free generating set $A$ of $G$, consider the right action of $A$ on the set $F/\varphi(H)$ of all right cosets of $\varphi(H)$. This defines a permutation automaton which is precisely the automaton $\mathcal{A}(K)$. Given $H$ by means of a finite set of generators, one may also construct its automaton $\mathcal{A}(H)$. The construction of the quotient automaton $\mathcal{A}(H)/\sim_{H,K}$ then can be made from the knowledge of both automata $\mathcal{A}(H)$ and $\mathcal{A}(K)$. The quotient automaton in turn determines the closed subgroup $L$, for which we may exhibit a finite set of generators. □

## Definition 15.2

We say that a pseudovariety $\mathbf{V}$ of groups has decidable denseness if, given a finite set $A$ and a finite subset $B$ of the free group $G$ on $A$, it is decidable whether $B$ generates a dense subgroup in the pro-$\mathbf{V}$ metric of $G$.

The following theorem summarizes and completes some of the above results.

## Theorem 15.3

*Let $\mathbf{V}$ be an extension-closed pseudovariety of groups. Let $H$ be a finitely generated subgroup of the finitely generated free group $G$ and let $\overline{H}$ be the closure of $H$ in the pro-$\mathbf{V}$ metric of $G$.*

1. *The group $\overline{H}$ is finitely generated and a free factor of a clopen subgroup of $G$.*
2. *The automaton $\mathcal{A}(\overline{H})$ is a quotient of $\mathcal{A}(H)$.*
3. *If $\mathbf{V}$ is recursively enumerable and has decidable denseness then there is an algorithm to construct a finite set of generators of $\overline{H}$.*

## Proof.

By Corollary 13.11, the subgroup $\overline{H}$ coincides with $\tilde{H}$, which in turn is finitely generated by Proposition 13.8. The remainder of the statement of (1) is a direct consequence of Theorem 13.10 while (2) now also follows from Proposition 13.8.

It remains to prove (3). Let $A$ be a set of free generators for $G$. Here is how the algorithm proceeds. Since $\mathbf{V}$ has decidable denseness, we first check whether $H$ is dense in $G$. In the affirmative case, we have found $\overline{H}$ to be $G$. In the negative case, we know that there is some homomorphism $\varphi : G \to F$ onto some group $F$ in $\mathbf{V}$ such that $\varphi(H) \subsetneqq G$. Since $\mathbf{V}$ is recursively enumerable and $G$ is finitely generated, we may successively enumerate candidates to such homomorphisms until we find one with this property.
Once such a homomorphism is found, by Proposition 15.1 one can compute from $\varphi$ a finite set $A' = \{v_1, \ldots, v_r\}$ of free generators for a closed free factor $L$ of some clopen subgroup $K$ of $G$ such that $\mathcal{A}(L)$ is a quotient $\mathcal{A}(H)/\sim_1$ of $\mathcal{A}(H)$.

(. . . )

If $\{w_1, \ldots, w_m\}$ is a set of generators for $H$, then we may express each $w_i$ as a group word $w_i'(v_1, \ldots, v_r)$ on the groups words $v_j$. Consider the subgroup $H'$ of the free group $G'$ on the set $A'$ generated by $\{w_1', \ldots, w_m'\}$. The mapping which sends each free generator $v_j$ to itself, viewed as a group word in the given free generators of $G$, extends uniquely to a continuous homomorphism $\psi : G' \to G$ which is an isomorphism with $L$. Since the induced metric on $L$ is the pro-**V** metric of $L$ by Theorem 12.10, $\psi : G' \to L$ is a continuous isomorphism with respect to the corresponding pro-**V** topologies. Since $\psi$ preserves the index of subgroups, as well as quotients for normal subgroups, $\psi$ is an isomorphism of topological groups. Since $L$ is closed in $G$ by Corollary 12.11, the problem of computing the closure of $H$ in $G$ is thus reduced to the computation of the closure of $H'$ in $G'$.

## $(\ldots)$

Now, if we apply the above procedure to $H'$ as a subgroup of $G'$, either $H'$ is dense in $G'$, in which case we conclude that $\overline{H} = L$, or we obtain a free factor $L'$ of a clopen subgroup $K'$ of $G'$ such that $H' \subseteq L' \subseteq K' \subsetneqq G'$ and $\mathcal{A}_{A'}(L')$ is a quotient of $\mathcal{A}_{A'}(H')$. It follows that $H \subseteq \psi(L') \subseteq \psi(K') \subsetneqq L$, $\psi(L')$ is a free factor of the clopen subgroup $\psi(K')$ (of $G$). Moreover, it is easy to see that $\mathcal{A}\big(\psi(L')\big)$ is the quotient of $\mathcal{A}(H)$ by a congruence $\sim_2$. Since $H \subseteq \psi(L') \subsetneqq L$, the congruence $\sim_2$ is properly contained in $\sim_1$.

Thus, applying the above procedure recursively, in a finite number of steps we must obtain an affirmative answer to the question as to whether the current subgroup is a free factor of the current free group. At that stage, the closure will be computed and then it is a matter of substituting back the free generators to their expressions in the original alphabet $A$ to obtain $\overline{H}$. □

## Corollary 15.4

*Let* $\mathbf{V}$ *be an extension-closed pseudovariety of groups with decidable denseness. Then it is decidable whether a given finitely generated subgroup of a finitely generated free group is* $\mathbf{V}$*-extendible.* □

- Since the closure of a finitely generated subgroup is computed by successively taking closed factors of clopen subgroups, combining with Theorem 12.10, we also obtain the following result.

## Corollary 15.5

*Let* $H$ *be a finitely generated subgroup of a finitely generated free group* $G$ *and suppose that* $H$ *is closed with respect to the pro-*$\mathbf{V}$ *metric of* $G$*, where* $\mathbf{V}$ *is an extension-closed pseudovariety of groups. Then the completion of* $H$ *with respect to the restriction to* $H$ *of the pro-*$\mathbf{V}$ *metric of* $G$ *is a free pro-*$\mathbf{V}$ *group.* □

- We consider the special case of the extension-closed pseudovariety $\mathbf{G}_p$ for a prime integer $p$, for which the denseness test can be done efficiently.
- The next result may now be deduced from Proposition 14.2 and Proposition 14.3.
- For group words $w_1, \ldots, w_m$ on $n$ letters $x_1, \ldots, x_n$, let $M(w_1, \ldots, w_m)$ be the (integer) matrix whose $(i, j)$-entry is the exponent of the reduced word in $x_j$ which is obtained from $w_i$ by replacing by 1 all $x_k$ with $k \neq j$.
- In particular, when $m = n$, $M(w_1, \ldots, w_n)$ is the matrix of the continuous endomorphism of $\overline{\Omega}_n\mathbf{M}$ which is determined by the implicit operator defined by the group terms $w_1, \ldots, w_n$.

## Proposition 15.6

*Let $G$ be a free group on $n$ free generators and let $H = \langle w_1, \ldots, w_n \rangle$ be an $n$-generated subgroup of $G$. Then $H$ is dense in $G$ if and only if $M(w_1, \ldots, w_n)$ is invertible mod $p$.*

## Proof.

By Baumslag's Theorem asserting that the free group is residually in $\mathbf{G}_p$, we may regard $G$ as the subgroup of $\overline{\Omega}_n\mathbf{G}_p$ generated by $\{x_1, \ldots, x_n\}$. Since the pro-$\mathbf{G}_p$ metric of $G$ is the induced metric from the metric of $\overline{\Omega}_n\mathbf{G}_p$ by Proposition 12.1, $H$ is dense in $G$ if and only if it is dense in $\overline{\Omega}_n\mathbf{G}_p$.

On the other hand, by Proposition 14.2, if $H = \langle w_1, \ldots, w_n \rangle$, then $H$ is dense in $\overline{\Omega}_n\mathbf{G}_p$ if and only if the associated implicit operator $(w_1, \ldots, w_n)$ is $\mathbf{G}_p$-invertible. By Proposition 14.3, the latter condition is equivalent to the integer matrix $M(w_1, \ldots, w_n)$ being invertible mod $p$. □

- Finally, the next result improves the general-purpose algorithm in the proof of Theorem 15.3 by providing the means to compute efficiently a proper clopen subgroup containing a given non-dense finitely generated subgroup.

## Proposition 15.7

*Let $H$ be a finitely generated subgroup of the free group $G$ on $n$ free generators $x_1, \ldots, x_n$ and let $\{w_1, \ldots, w_m\}$ be generating subset of $H$. Let $A = (\mathbb{Z}/p\mathbb{Z})^n$ and consider the homomorphism $\varphi : G \to A$ which sends $x_i$ to $(0, \ldots, 0, 1, 0, \ldots, 0)$, where $1$ is in the $i$th position.*

1. *The subgroup $H$ is dense in the pro-$\mathbf{G}_p$ metric of $G$ if and only if, mod $p$, the matrix $M(w_1, \ldots, w_m)$ has rank $n$.*
2. *If, mod $p$, the submatrix $M(w_{r_1}, \ldots, w_{r_n})$ has rank $n$, then the subgroup $\langle w_{r_1}, \ldots, w_{r_n} \rangle$ is dense.*
3. *If, mod $p$, the matrix $M(w_1, \ldots, w_m)$ has rank less than $n$, then $\varphi^{-1}\varphi(H)$ is a proper clopen subgroup of $G$ containing $H$.*

## Proof.

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, a square matrix with entries in it is invertible if and only if the matrix has rank $n$. Moreover, an $m \times n$ matrix has rank $n$ if and only if it contains $n$ rows whose corresponding submatrix has rank $n$. On the other hand, since $\varphi(H)$ is generated by the rows of the matrix $M(w_1, \ldots, w_m)$, with the entries viewed in $\mathbb{Z}/p\mathbb{Z}$, if, mod $p$, this matrix has rank less than $n$, then $\varphi(H)$ is a proper subgroup of the group $A \in \mathbf{G}_p$. This proves (3) and shows that $H$ is not dense in $G$. The statements (1) and (2) now follow using Proposition 15.6. □

- Thus, for the pro-$\mathbf{G}_p$ metric of a finitely generated free group $G$, combining part (3) of Proposition 15.7 and Proposition 15.1, one may compute a proper clopen subgroup containing a given finitely generated subgroup $H$ which is not dense in $G$.

To illustrate the above algorithms, we present an example in detail. For this purpose, we consider again the subgroup $H$ of the free group $G$ on the free generators $a, b, c$ of Example 1: $H$ is generated by the group words $ab^{-1}c^{-1}a, a^{-1}b^{-1}ac^{-1}a, bc^{-1}a$. The corresponding integer matrix is

$$M_0 = \begin{pmatrix} 2 & -1 & -1 \\ 1 & -1 & -1 \\ 1 & 1 & -1 \end{pmatrix}$$

and has determinant 2. Hence $H$ is dense in $G$ with respect to the pro-$\mathbf{G}_p$ metric for every odd prime $p$. For the pro-$\mathbf{G}_2$ metric of $G$, the rank of the matrix $M_0$ mod 2 is 2. More precisely, if $\varphi_0 : G \to (\mathbb{Z}/2\mathbb{Z})^3$ is the appropriate mapping given by Proposition 15.7, then $H \subseteq \varphi_0^{-1}\varphi_0(H) \subsetneqq G$. The clopen subgroup $\varphi_0^{-1}\varphi_0(H)$ may be computed as the fundamental group of the automaton which represents the action of $a, b, c$ on the right of the right cosets of $\varphi_0(H)$, which is represented in Figure 3.

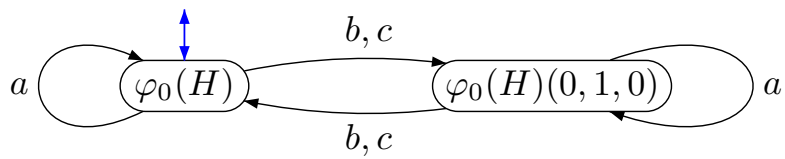



FIGURE: The automaton of $K_1$

The clopen subgroup $K_1$ in question is therefore freely generated by $\{a, bab^{-1}, b^2, bc, cb^{-1}\}$. The free factor $L_1$ is obtained by taking the fundamental group of the image of $\mathcal{A}(H)$ in $\mathcal{A}(K_1)$. Recall the automaton $\mathcal{A}(H)$ as given in Figure 177.

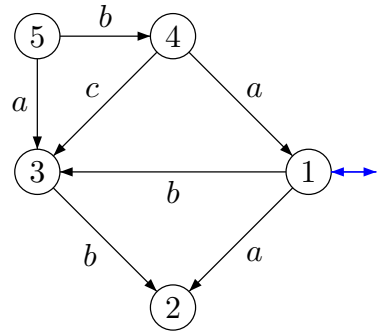



FIGURE: The automaton $\mathcal{A}(H)$

The states $1, 2, 4$ are mapped to $\varphi(H)$ while $3, 5$ are mapped to $\varphi(H)(0, 1, 0)$ and the only missing edge from the automaton of $\mathcal{A}(K_1)$ is the edge $c$ from the state $\varphi(H)(0, 1, 0)$ to $\varphi(H)$, which corresponds to the generator $bc$ of $K_1$. Hence $L_1$ is the subgroup generated by $\{a, bab^{-1}, b^2, cb^{-1}\}$. Let $b_1 = bab^{-1}$, $b_2 = b^2$ and $c_1 = cb^{-1}$. Then the elements of $H$ may be expressed as follows:

$$ab^{-1}c^{-1}a = ab_2^{-1}c_1^{-1}a$$
$$a^{-1}b^{-1}ac^{-1}a = a^{-1}b_2^{-1}b_1$$
$$bc^{-1}a = c_1^{-1}a$$

which are now viewed as generating a subgroup $H_1$ of the free group $G_1$ on the set $a, b_1, b_2, c_1$. The matrix corresponding to the generators of $H_1$ is

$$M_1 = \begin{pmatrix} 2 & 0 & -1 & -1 \\ -1 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \end{pmatrix}$$

which, mod 2, has rank 3. Hence $H$ is not dense in $L_1$ and we need to compute a clopen subgroup $K_2$ of $L_1$ and a free factor $L_2$ of $K_2$ containing $H$.

Since the rank of $M_1$ mod 2 is 3, the image of $H_1$ under the homomorphism $\varphi_1 : G_1 \to (\mathbb{Z}/2\mathbb{Z})^4$ has index 2 and again we obtain a 2-state permutation automaton for $K_2$, which is represented in Figure 5.

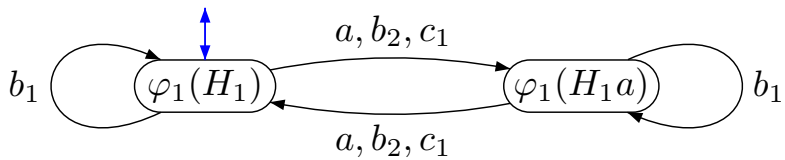



FIGURE: The automaton of $K_2$

To obtain the image of $\mathcal{A}(H_1)$ in this automaton, it suffices to read through each of the generators of $H_1$, starting from the initial state, and keeping only the states and edges which are used. Figure 6 represents the subautomaton which is thus obtained, whose fundamental group is the required free factor $L_2$ of $K_2$.

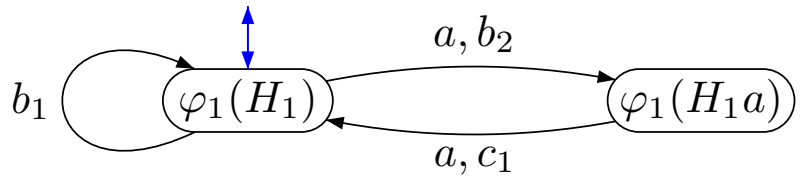



FIGURE: The automaton of $L_2$

Choosing the edge labeled $b_2$ for the generating tree, we obtain the following free generators for $L_2$:

$$b_1,\ a_1 = ab_2^{-1},\ a_2 = b_2 a,\ c_2 = b_2 c_1. \tag{3}$$

In terms of these generators, the expressions for the generators of $H_1$ are the following:

$$\begin{aligned} ab_2^{-1}c_1^{-1}a &= a_1 c_2^{-1} a_2 \\ a^{-1}b_2^{-1}b_1 &= a_2^{-1} b_1 \\ c_1^{-1}a &= c_2^{-1} a_2 \end{aligned}$$

The matrix of these generators with respect to the generators of $L_2$ in the order given by (3) is

$$M_2 = \begin{pmatrix} 0 & 1 & 1 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

which again has rank 3.

Proceeding as above, we get a canonical homomorphism $\varphi_2 : G_2 \to (\mathbb{Z}/2\mathbb{Z})^4$, where $G_2$ is the free group on the generators $b_1, a_1, a_2, c_2$. Let $H_2$ be the subgroup of $G_2$ generated by $a_1 c_2^{-1} a_2, a_2^{-1} b_1, c_2^{-1} a_2$. The new clopen subgroup $K_3$ is the fundamental group of the automaton in Figure 7.

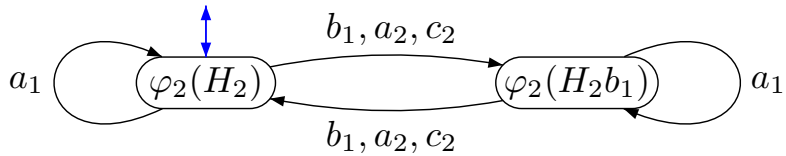



FIGURE: The automaton of $K_3$

Figure 8 gives the subautomaton which is obtained by reading through the preceding automaton the generators of $H_2$.

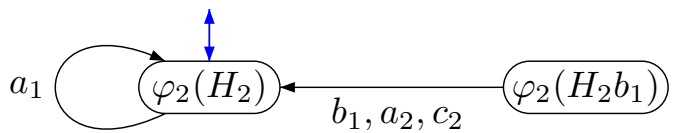
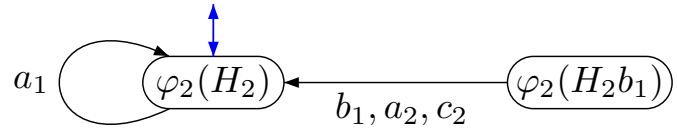



FIGURE: The automaton of $L_3$

Choosing the edge labeled $c_2$ for the generating tree, we obtain the following free generators for $L_3$:

$$a_1, \ a_3 = c_2^{-1} a_2, \ b_3 = c_2^{-1} b_1. \tag{4}$$




$$a_1,\ a_3 = c_2^{-1}a_2,\ b_3 = c_2^{-1}b_1.$$

The corresponding expressions for the generators of $H_2$ are:

$$\begin{aligned} a_1c_2^{-1}a_2 &= a_1a_3 \\ a_2^{-1}b_1 &= a_3^{-1}b_3 \\ c_2^{-1}a_2 &= a_3 \end{aligned}$$

whose matrix has rank 3 mod 2, 3 being also the rank of $L_3$. Hence $H_2$ is dense in $L_3$ and the closure of $H = \langle ab^{-1}c^{-1}a, a^{-1}b^{-1}ac^{-1}a, bc^{-1}a\rangle$ in $G$ is obtained by substituting back in terms of $a, b, c$ the expressions for the generators of $L_3$ given in (4):

$$\begin{aligned} a_1 &= a_1 = ab_2^{-1} = ab^{-2} \\ a_3 &= c_2^{-1}a_2 = c_1^{-1}b_2^{-1}b_2a = bc^{-1}a \\ b_3 &= c_2^{-1}b_1 = c_1^{-1}b_2^{-1}b_1 = bc^{-1}b^{-2}bab^{-1} = bc^{-1}b^{-1}ab^{-1} \end{aligned}$$

Since the generators of $L_3$ are all recognized by $\mathcal{A}(H)$, we conclude that $H$ is closed in the pro-$\mathbf{G}_2$ metric of $G$.

In terms of generators, we obtained the following chain of subgroups approximating the closure of $H$, where we also indicate on the right the corresponding congruences on $\mathcal{A}(H)$ as given by the partitions of the state set:

$$
\begin{aligned}
G &= \langle a, b, c\rangle \\
&\ \ \cup \\
K_1 &= \langle a, bab^{-1}, b^2, bc, cb^{-1}\rangle \\
&\ \ \cup \\
L_1 &= \langle a, bab^{-1}, b^2, cb^{-1}\rangle && \{1,2,4|3,5\} \\
&\ \ \cup \\
K_2 &\simeq \langle bab^{-1}, ab^{-2}, b^2a, b^2cb^{-1}, cb^{-3}, b^3ab^{-3}, b^4\rangle \\
&\ \ \cup \\
L_2 &\simeq \langle bab^{-1}, ab^{-2}, b^2a, b^2cb^{-1}\rangle && \{1|2,4|3,5\} \\
&\ \ \cup \\
K_3 &\simeq \langle ab^{-2}, bc^{-1}a, bc^{-1}b^{-1}ab^{-1}, b^2ab^2cb^{-1}, babcb^{-1}, b^2cbcb^{-1}, bc^{-1}b^{-2}acb^{-1}\rangle \\
&\ \ \cup \\
L_3 &\simeq \langle ab^{-2}, bc^{-1}a, bc^{-1}b^{-1}ab^{-1}\rangle && \{1|2|3|4|5\} \\
&\ \ = \\
H &= \langle ab^{-1}c^{-1}a, a^{-1}b^{-1}ac^{-1}a, bc^{-1}a\rangle
\end{aligned}
$$

## Exercise 15.8

Verify that the above calculations are correct.

The above calculations also show that $H$ is not $\mathbf{G}_p$-extendible for every odd prime $p$ while it is $\mathbf{G}_2$-extendible. An $\mathbf{G}_2$-extension of the automaton $\mathcal{A}(H)$ may be recovered from our calculations. It is the permutation automaton associated with the following clopen subgroup:

$$\begin{aligned} K = \langle & ab^{-2}, bc^{-1}a, bc^{-1}b^{-1}ab^{-1}, \\ & b^2ab^2cb^{-1}, babcb^{-1}, b^2cbcb^{-1}, bc^{-1}b^{-2}acb^{-1}, \\ & cb^{-3}, b^3ab^{-3}, b^4, \\ & b^2a \cdot cb^{-3} \cdot (b^2a)^{-1}, b^2a \cdot b^3ab^{-3} \cdot (b^2a)^{-1}, b^2a \cdot b^4 \cdot (b^2a)^{-1}, \\ & bc, a \cdot bc \cdot a^{-1}, \\ & b^2a \cdot bc \cdot (b^2a)^{-1}, b^2a \cdot abca^{-1} \cdot (b^2a)^{-1} \rangle. \end{aligned}$$

## Exercise 15.9

Explain in general how to compute a $\mathbf{V}$-extension of a $\mathbf{V}$-extendible finite inverse reduced automaton, assuming the appropriate hypotheses on the extension-closed pseudovariety of groups $\mathbf{V}$.

One may calculate the following picture for $\mathcal{A}(K)$ and that the transition monoid of this automaton is a group of order 128. Since it would be too tedious to do it by hand, this calculation was carried out using some adequate *Mathematica* routines for the symbolic computations and the package *graphviz* for the drawing itself, which was then converted by hand to *GasTeX* for readability. The numbering of states was chosen to facilitate the identification of the subautomaton $\mathcal{A}(H)$. New edges and states are in red.

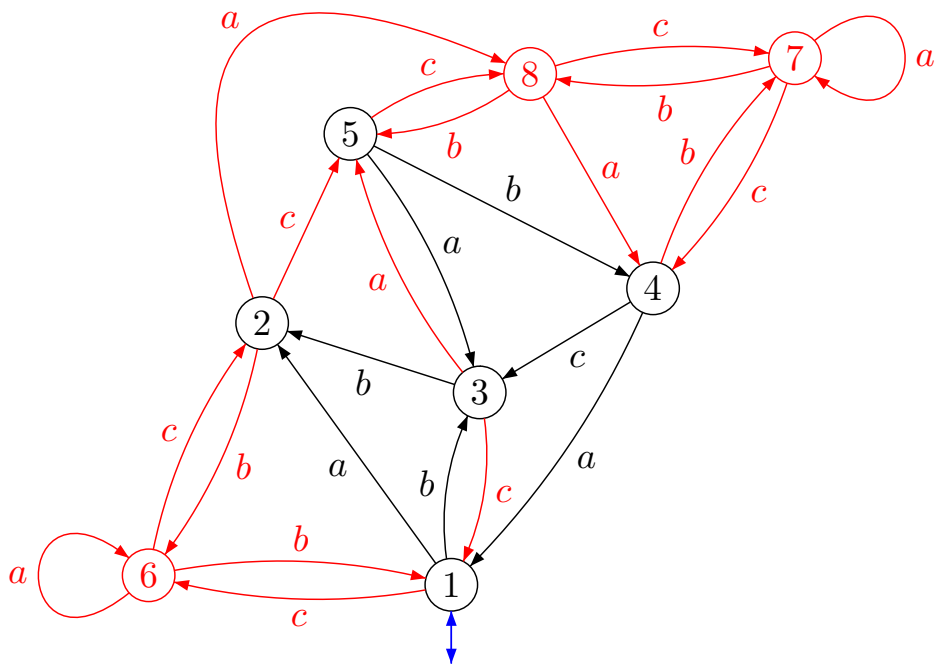



FIGURE: A $\mathbf{G}_2$-extension of $\mathcal{A}(H)$

## Exercise 15.10

Show that the above algorithms for the pseudovariety $\mathbf{G}_p$ (to test denseness, to compute the closure, to exhibit a $\mathbf{G}_p$-extension, if one exists) require only polynomial time in the input, which may be either a finite list of group words over a finite alphabet $A$, or the reduced inverse automaton of the subgroup of the free group on $A$ that they generate. More precisely, estimate the time complexity of the algorithms.

# Outline

# The Pin-Reutenauer procedure

- Let us consider again the problem studied by Pin and Reutenauer [PR91]: given a regular language $L \subseteq A^+$ and a word $w \in A^+$, decide whether $w$ can be separated from $L$ by a **G**-recognizable language.
- Since **G** is $\kappa$-reducible for the separation problem, the problem is equivalent to deciding whether $w \in \mathrm{cl}_{\kappa,\mathbf{G}}(L)$.
- So, the idea is to compute the subset $\mathrm{cl}_{\kappa,\mathbf{G}}(L)$ of the free group $\Omega_A^\kappa \mathbf{G}$.
- Since $L$ is regular, we may assume that it is given by some regular expression.
- As every finite subset of $\Omega_A^\kappa \mathbf{G}$ fullfullis closed and closure behaves well with respect to union, the key question is how the closure operator $\mathrm{cl}_{\kappa,\mathbf{G}}(\_)$ behaves well with respect to the multiplication of subsets and the Kleene star operation.

- In general, for an arbitrary pseudovariety $\mathbf{V}$ and implicit signature $\sigma$, we have the inclusion

$$\mathrm{cl}_{\sigma,\mathbf{V}}(K\,L) \supseteq \mathrm{cl}_{\sigma,\mathbf{V}}(K)\,\mathrm{cl}_{\sigma,\mathbf{V}}(L), \tag{5}$$

  simply because the multiplication in $\Omega_A^\kappa \mathbf{V}$ is continuous.
  - Note: in a compact semigroup, the equality $\overline{K\,L} = \overline{K}\,\overline{L}$ holds.
- For a subset $X$ of a $\sigma$-algebra $S$, denote by $\langle S\rangle_\sigma$ the $\sigma$-subalgebra generated by $X$.
- The analogue of (5) for Kleene star is the inclusion

$$\mathrm{cl}_{\sigma,\mathbf{V}}(L^+) \supseteq \langle \mathrm{cl}_{\sigma,\mathbf{V}}(L)\rangle_\sigma \tag{6}$$

  The proof of (6) is a bit more delicate and depends on the following lemma.

## Lemma 16.1

*Let* $\mathbf{V}$ *be a pseudovariety of semigroups and let* $S$ *be a pro-*$\mathbf{V}$ *semigroup. Then the following evaluation mapping is continuous for every positive integer* $n$*:*

$$\overline{\Omega}_n\mathbf{V} \times S^n \to S$$
$$(w, s_1, \ldots, s_n) \mapsto w_S(s_1, \ldots, s_n).$$

## Proof.

Since $\mathbf{V}$-implicit operations commute with continuous homomorphisms between pro-$\mathbf{V}$ semigroups, in view of Proposition 5.1 it suffices to consider the case where $S \in \mathbf{V}$.

Note that $\overline{\Omega}_n\mathbf{V}(S)$ is finite, say again by Proposition 5.1. Moreover, when $\overline{\Omega}_n\mathbf{V}$ and $S$ are both finite, the continuity of the evaluation mapping is trivial.

Since, in terms of implicit operations, the natural projection $\overline{\Omega}_n\mathbf{V} \to \overline{\Omega}_n\mathbf{V}(S)$ is given by restriction, we deduce the general case. □

- The inclusion $\langle \mathrm{cl}_{\sigma,\mathbf{V}}(L)\rangle_\sigma \subseteq \mathrm{cl}_{\sigma,\mathbf{V}}(L^+)$ follows from the next proposition.

## Proposition 16.2

*Let $\mathbf{V}$ be a pseudovariety, $\sigma$ and implicit signature, and $L$ a subset of $\Omega_A^\sigma\mathbf{V}$. Then $\mathrm{cl}_{\sigma,\mathbf{V}}(L^+)$ is a $\sigma$-subalgebra of $\Omega_A^\sigma\mathbf{V}$.*

## Proof.

Let $u \in \overline{\Omega}_m\mathbf{S}$ be an implicit operation from $\sigma$, and let $v_1, \ldots, v_m$ be elements of $\mathrm{cl}_{\sigma,\mathbf{V}}(L^+)$. There are sequences with the following properties:

- a sequence $(u_n)_n$, of words from $\{x_1, \ldots, x_m\}^+$, converging to $u$;
- for each $i \in \{1, \ldots, m\}$, a sequence $(v_{i,n})_n$, of elements of $L^+$, converging to $v_i$.

For each $n$, the element $(u_n)_{\overline{\Omega}_A\mathbf{V}}(v_{1,n}, \ldots, v_{m,n})$ is a product of elements from $L^+$ and, therefore, also belongs to $L^+$. By Lemma 16.1, we have

$$\lim (u_n)_{\overline{\Omega}_A\mathbf{V}}(v_{1,n}, \ldots, v_{m,n}) = u_{\overline{\Omega}_A\mathbf{V}}(v_1, \ldots, v_m).$$

Hence $u_{\overline{\Omega}_A\mathbf{V}}(v_1, \ldots, v_m)$ belongs to $\mathrm{cl}_{\sigma,\mathbf{V}}(L^+)$. □

## Theorem 16.3 (Pin and Reutenauer [PR91])

*For the pseudovariety* $\mathbf{V} = \mathbf{G}$*, the signature* $\sigma = \kappa$*, and a regular language* $L \subseteq A^+$*, equality holds in both formulas* (5) *and* (6)*.*

Some comments on the proof:

- The proof establishes a stronger result than (6), namely that

$$\mathrm{cl}_{\kappa,\mathbf{G}}(L^+) = \langle L \rangle_\kappa.$$

  The main reason for not needing to use $\mathrm{cl}_{\kappa,\mathbf{G}}(L)$ instead of $L$ on the right hand side is M. Hall's Theorem 13.5.

- The proof depends on several ingredients from language theory, such as a theorem of Anissimov and Seifert, stating that the rational[7] subgroups of $\Omega_A^\kappa \mathbf{G}$ are the finitely generated subgroups, and a theorem of Fliess, stating that the rational subsets of $\Omega_A^\kappa \mathbf{G}$ form a Boolean algebra. (See [Ber79, Section III.2] — http://www-igm.univ-mlv.fr/∼berstel/LivreTransductions/LivreTransductions.html.)

[7] A subset of a monoid $M$ is said to be rational if it can be obtained from the empty set and the singleton subsets of $M$ by using the operations of subset multiplication and taking the submonoid $X^*$ generated by a subset $X$.

- The theorem was initially deduced from a conjectured property of free groups: that the product of finitely many finitely generated subgroups of $\Omega_A^\kappa \mathbf{G}$ is closed in the pro-$\mathbf{G}$ metric.
- This property follows from Ash's Theorem on inevitable graphs [Ash91] and was proved independently by Ribes and Zalesskiĭ [RZ93], using profinite group theory.
- The theorem was found as an approach to a conjecture of J. Rhodes (known as the Rhodes Type II Conjecture), which it implies. Ash's Theorem on inevitable graphs was also proved to establish Rhodes' conjecture. (See [HMPR91] for the original statement and the history of this conjecture.)
- The Rhodes Type II Conjecture, now theorem, may be stated as follows [AS00a].

## Theorem 16.4 (Rhodes Type II)

*Let $S$ be a finite semigroup and let $A$ be a generating subset. Consider the $\kappa$-subsemigroup $T$ of $S \times \Omega_A^\kappa \mathbf{G}$ generated by the pairs $(a, a)$ $(a \in A)$. Then, for an element $s \in S$, $(s, 1) \in T$ if and only if, for every finite group $G$, and every subsemigroup $U$ of $S \times G$, which projects onto the first component, $(s, 1) \in U$.*

# Other pseudovarieties for which the Pin-Reutenauer procedure holds

- We say that the Pin-Reutenauer procedure holds for a pseudovariety $\mathbf{V}$ and an implicit signature $\sigma$ if the following equalities hold for all subsets $L$ of $\Omega_A^\sigma \mathbf{V}$:

$$\mathrm{cl}_{\sigma,\mathbf{V}}(K\,L) = \mathrm{cl}_{\sigma,\mathbf{V}}(K)\,\mathrm{cl}_{\sigma,\mathbf{V}}(L) \tag{7}$$

$$\mathrm{cl}_{\sigma,\mathbf{V}}(L^+) = \langle \mathrm{cl}_{\sigma,\mathbf{V}}(L) \rangle_\sigma. \tag{8}$$

- Note that if the pseudovariety $\mathbf{V}$ contains $\mathbf{N}$, then there is always an implicit signature for which the Pin-Reutenauer procedure holds (cf. Proposition 7.3), for example the trivial signature $\{\_ \cdot \_\}$. But, this in general too small for the pseudovariety to be full with respect to it.

- In a sense at the other extreme, if we take $\sigma$ to consist of all (finitary) implicit operations, then $\Omega_A^\sigma \mathbf{V} = \overline{\Omega}_A \mathbf{V}$ and $\mathrm{cl}_{\sigma,\mathbf{V}}(L) = \overline{L}$ is the closure of $L$ in $\overline{\Omega}_A \mathbf{V}$. So, the equality (7) certainly holds in this case, by compactness of $\overline{\Omega}_A \mathbf{V}$. On the other hand, $\mathrm{cl}_{\sigma,\mathbf{V}}(L^+)$ is the closure of a subsemigroup, whence a closed subsemigroup of $\overline{\Omega}_A \mathbf{V}$, namely the closed subsemigroup generated by $L$, which is therefore contained in $\langle \mathrm{cl}_{\sigma,\mathbf{V}}(L) \rangle_\sigma$. The reverse inclusion is given by Proposition 16.2.
- Hence, for every pseudovariety $\mathbf{V}$, there is some implicit signature for which the Pin-Reutenauer procedure holds and $\mathbf{V}$ is $\sigma$-full. The question is whether it holds for small such signatures, such as $\kappa$.
- The other key question is under what conditions one can turn the Pin-Reutenauer procedure into an algorithm to test membership of a given word $w \in L$ in the closure $\mathrm{cl}_{\sigma,\mathbf{V}}(L)$ of a given regular language $L \subseteq A^+$.

- Here are some recent results.

### Theorem 16.5 (JA-JCCosta-MZeitoun)

*Suppose that* $\mathbf{V}$ *and* $\mathbf{W}$ *are* $\sigma$*-full pseudovarieties of semigroups such that* $\mathbf{V} \subseteq \mathbf{W}$*. If the Pin-Reutenauer procedure holds for* $\mathbf{W}$ *then it also holds for* $\mathbf{V}$*.*

### Theorem 16.6 (JA-JCCosta-MZeitoun)

*The Pin-Reutenauer procedure holds for* $\mathbf{A}$ *in the signature* $\kappa$*.*

- As was already mentioned, the same authors proved that $\mathbf{A}$ and $\mathbf{R}$ are $\kappa$-full. Hence the preceding two theorems yield the following result.

### Corollary 16.7

*The Pin-Reutenauer procedure holds for* $\mathbf{R}$ *in the signature* $\kappa$*.*

# Part III

*Relatively free profinite semigroups and Symbolic Dynamics*

# Outline

# Semigroups of implicit operators

- Let $w_i \in \overline{\Omega}_n \mathbf{S}$ be an $n$-ary implicit operation for each $i \in \{1, \ldots, n\}$.
- Given a profinite semigroup $S$, the $n$-tuple induces a continuous mapping

$$[w_1, \ldots, w_n]_S : S^n \to S^n$$
$$(s_1, \ldots, s_n) \mapsto \big((w_1)_S(s_1, \ldots, s_n), \ldots, (w_n)_S(s_1, \ldots, s_n)\big).$$

- The composition of two such transformations of $S^n$ is again a transformation of the same form, and thus they constitute a semigroup, which we call the semigroup of $n$-ary implicit operators of $S$ and denote $\mathcal{O}_n(S)$.
- In particular, we may iterate an implicit operator $f = [w_1, \ldots, w_n]_S$ by considering its successive powers $f, f^2, f^3, \ldots$.

- The following result is immediate from the commutation of implicit operations with comtinuous homomorphisms between profinite semigroups.

## Lemma 17.1

*Let $w_1, \ldots, w_n \in \overline{\Omega}_n\mathbf{S}$ be n-ary implicit operations and let $\varphi : S \to T$ be a continuous homomorphism between profinite semigroups. Then the following diagram commutes:*

$$\begin{array}{ccc} S^n & \xrightarrow{[w_1,\ldots,w_n]_S} & S^n \\ \downarrow{\scriptstyle \varphi^n} & & \downarrow{\scriptstyle \varphi^n} \\ T^n & \xrightarrow{[w_1,\ldots,w_n]_T} & T^n. \end{array}$$

## Lemma 17.2

*Let $S$ be a profinite semigroup and let $f \in \mathcal{O}_n(S)$ be an $n$-ary implicit operator on $S$. Then, for every $(s_1, \ldots, s_n) \in S^n$, the sequence $\left(f^{k!}(s_1, \ldots, s_n)\right)_k$ of elements of $S^n$ converges. In other words, the sequence $(f^{k!})_k$ of transformations of $S^n$ converges pointwise. Moreover, the limit is an idempotent transformation of $S^n$.*

## Proof.

By definition of profinite semigroup, $S$ admits a complete metric $d$. We may endow the product space $S^n$ with various metrics, among which the maximum metric $d'$ defined by

$$d'\big((s_1,\ldots,s_n),(t_1,\ldots,t_n)\big) = \max\{d(s_i,t_i) : i = 1,\ldots,n\}.$$

This defines a complete metric structure on $S^n$. Thus, to prove that the sequence $\left(f^{k!}(s_1,\ldots,s_n)\right)_k$ converges, it suffices to show that it is a Cauchy sequence.
By Proposition 5.1 and Lemma 17.1, it suffices to consider the case where $S$ is a finite semigroup, in which case the result amounts to the convergence of the corresponding sequence $f^{k!}$ in the finite monoid of transformations of $S^n$, where indeed we have observed that it converges to an idempotent. □

- We denote the limit $\lim[w_1, \ldots, w_n]_S^{k!}$ by $[w_1, \ldots, w_n]_S^{\omega}$.
- In particular, given $w_1, \ldots, w_n \in \overline{\Omega}_n \mathbf{S}$, we may consider the following $n$-tuple of $n$-ary implicit operations:

$$(v_1, \ldots, v_n) = [w_1, \ldots, w_n]^{\omega}_{\overline{\Omega}_n \mathbf{S}}(x_1, \ldots, x_n).$$

## Lemma 17.3

*With the above notation, if $S$ is a profinite semigroup, then*

$$[v_1, \ldots, v_n]_S = [w_1, \ldots, w_n]_S^{\omega}.$$

*Thus, the transformation $[w_1, \ldots, w_n]_S^{\omega}$ is again an implicit operator and the semigroup $\mathcal{O}_n(S)$ is closed under taking $\omega$-powers.*

## Proof.

Let $(s_1, \dots, s_n)$ be an $n$-tuple of elements of $S$. Then there is a unique continuous homomorphism $\varphi : \overline{\Omega}_n\mathbf{S} \to S$ such that $\varphi(x_i) = s_i$ $(i = 1, \dots, n)$.
In view of Lemma 17.1 and taking into account that $\varphi^n$ is continuous, we obtain

$$\begin{aligned}
&[v_1, \dots, v_n]_S(s_1, \dots, s_n) \\
&\qquad = \varphi^n\big([v_1, \dots, v_n]_{\overline{\Omega}_n\mathbf{S}}(x_1, \dots, x_n)\big) \\
&\qquad = \varphi^n\big(\lim[w_1, \dots, w_n]^{k!}_{\overline{\Omega}_n\mathbf{S}}(x_1, \dots, x_n)\big) \\
&\qquad = \lim \varphi^n\big([w_1, \dots, w_n]^{k!}_{\overline{\Omega}_n\mathbf{S}}(x_1, \dots, x_n)\big) \\
&\qquad = \lim[w_1, \dots, w_n]^{k!}_S(s_1, \dots, s_n) \\
&\qquad = [w_1, \dots, w_n]^{\omega}_S(s_1, \dots, s_n),
\end{aligned}$$

which establishes the desired equality. □

- Since $\overline{\Omega}_n\mathbf{S}$ is a profinite semigroup freely generated by the set $\{x_1, \ldots, x_n\}$, the $n$-tuples of $n$-ary implicit operations $(w_1, \ldots, w_n)$ are in bijection with the continuous endomorphisms $\varphi_{(w_1,\ldots,w_n)}$ of $\overline{\Omega}_n\mathbf{S}$, where $\varphi_{(w_1,\ldots,w_n)}(x_i) = w_i$ $(i = 1, \ldots, n)$.
- On the other hand, they are also in bijection with $n$-ary implicit operators on $\overline{\Omega}_n\mathbf{S}$, namely through the formula

$$(w_1, \ldots, w_n) = [w_1, \ldots, w_n]_{\overline{\Omega}_A\mathbf{S}}(x_1, \ldots, x_n).$$

- For a profinite semigroup $S$, denote by $\operatorname{End} S$ the monoid of continuous endomorphisms of $S$, acting on the left.

## Proposition 17.4

*The following mapping is an anti-isomorphism of semigroups:*

$$\begin{aligned}\Theta : \operatorname{End} \overline{\Omega}_n \mathbf{S} &\to \mathcal{O}_n(\overline{\Omega}_n \mathbf{S}) \\ \varphi &\mapsto [\varphi(x_1), \dots, \varphi(x_n)]_{\overline{\Omega}_n \mathbf{S}}.\end{aligned}$$

## Proof.

We have already observed that the above mapping is a bijection, and described its inverse. So, it remains to verify that it is an anti-homomorphism of semigroups.

Let $\varphi, \psi \in \operatorname{End} \overline{\Omega}_n \mathbf{S}$ and let $w_i = \psi(x_i)$ $(i = 1, \dots, n)$. Taking into account Lemma 17.1, we obtain

$$\begin{aligned}\Theta(\varphi \circ \psi) &= [\varphi(\psi(x_1)), \dots, \varphi(\psi(x_n))]_{\overline{\Omega}_n \mathbf{S}} \\ &= [\varphi(w_1), \dots, \varphi(w_n))]_{\overline{\Omega}_n \mathbf{S}} \\ &= [w_1(\varphi(x_1), \dots \varphi(x_n)), \dots, w_n(\varphi(x_1), \dots \varphi(x_n))]_{\overline{\Omega}_n \mathbf{S}} \\ &= [w_1, \dots, w_n]_{\overline{\Omega}_n \mathbf{S}} \circ [\varphi(x_1), \dots \varphi(x_n)]_{\overline{\Omega}_n \mathbf{S}} \\ &= \Theta(\psi) \circ \Theta(\varphi).\end{aligned}$$

## Lemma 17.5

*Let $\varphi_k, \varphi \in \operatorname{End} \overline{\Omega}_n\mathbf{S}$ $(k \geq 0)$. Then $(\varphi_k)_k$ convergences pointwise to $\varphi$ if and only if $(\Theta(\varphi_k))_k$ converges pointwise to $\Theta(\varphi)$.*

## Proof.

Let $v_{k,i} = \varphi_k(x_i)$ and $v_i = \varphi(x_i)$ $(i = 1, \ldots, n;\ k \geq 0)$.

$(\Rightarrow)$ For $w_1, \ldots, w_n \in \overline{\Omega}_n\mathbf{S}$, we have

$$
\begin{aligned}
&\Theta(\varphi_k)(w_1, \ldots, w_n) \\
&\qquad = [v_{k,1}, \ldots, v_{k,n}]_{\overline{\Omega}_n\mathbf{S}}(w_1, \ldots, w_n) \\
&\qquad = \big((v_{k,1})_{\overline{\Omega}_n\mathbf{S}}(w_1, \ldots, w_n), \ldots, (v_{k,n})_{\overline{\Omega}_n\mathbf{S}}(w_1, \ldots, w_n)\big) \\
&\qquad \to \big((v_1)_{\overline{\Omega}_n\mathbf{S}}(w_1, \ldots, w_n), \ldots, (v_n)_{\overline{\Omega}_n\mathbf{S}}(w_1, \ldots, w_n)\big) \\
&\qquad\qquad = [v_1, \ldots, v_n]_{\overline{\Omega}_n\mathbf{S}}(w_1, \ldots, w_n) \\
&\qquad\qquad = \Theta(\varphi)(w_1, \ldots, w_n),
\end{aligned}
$$

where the convergence step follows from Lemma 16.1.

(...)

($\Leftarrow$) Let $w \in \overline{\Omega}_n\mathbf{S}$. Then we have

$$\begin{aligned}
\varphi_k(w) &= \varphi_k\big(w_{\overline{\Omega}_n\mathbf{S}}(x_1,\ldots,x_n)\big)\\
&= w_{\overline{\Omega}_n\mathbf{S}}\big(v_{k,1},\ldots,v_{k,n}\big)\\
&= w_{\overline{\Omega}_n\mathbf{S}}\big([v_{k,1},\ldots,v_{k,n}]_{\overline{\Omega}_n\mathbf{S}}(x_1,\ldots,x_n)\big)\\
&\to w_{\overline{\Omega}_n\mathbf{S}}\big([v_1,\ldots,v_n]_{\overline{\Omega}_n\mathbf{S}}(x_1,\ldots,x_n)\big)\\
&= \varphi\big(w_{\overline{\Omega}_n\mathbf{S}}(x_1,\ldots,x_n)\big)\\
&= \varphi(w),
\end{aligned}$$

where we use again Lemma 16.1 for the convergence step. □

## Corollary 17.6

*For a continuous endomorphism $\varphi$ of $\overline{\Omega}_n\mathbf{S}$, the sequence $(\varphi^{k!})$ converges pointwise to an idempotent continuous endomorphism of $\overline{\Omega}_n\mathbf{S}$.* □

- The idempotent in question is denoted $\varphi^\omega$ and is called the $\omega$-power or $\omega$-iterate of $\varphi$.
- More generally, Hunter [Hun83] has shown that the monoid $\operatorname{End} S$ of continuous endomorphisms of a finitely generated profinite semigroup $S$ is profinite. Since it is usually not finitely generated, this result does not fit in the realm of our metric approach to profinite semigroups. For those that know about topology of function spaces, the topology used in $\operatorname{End} S$ is the topology of pointwise convergence (i.e., as a subspace of the product space $S^S$), and turns out to coincinde with the compact-open topology (i.e., the topology of uniform convergence). See also [Alm02, AV06a, Alm05, Ste11].

# Examples

- The $\omega$-iteration of continuous endomorphisms of $\overline{\Omega}_n\mathbf{S}$, or of implicit operators on $\overline{\Omega}_n\mathbf{S}$ can be used to construct useful implicit operations.
- Let $\varphi \in \operatorname{End} \overline{\Omega}_1\mathbf{S}$ be defined by $\varphi(x_1) = x_1^p$. Then $\varphi^k(x_1) = x_1^{p^k}$ and $\varphi^\omega(x_1) = x_1^{p^\omega}$. Recall that we used the implicit operation $x_1^{p^\omega}$ previously to define the pseudovariety $\mathbf{G}_p$ in terms of pseudoidentities: $\mathbf{G}_p = [\![x_1^{p^\omega} = 1]\!]$.

- Given elements $u$ and $v$ of a profinite semigroup $S$, let

$$[u, v] = u^{\omega-1} v^{\omega-1} uv,$$

  an extension of the group commutator. Note, however, that, if $S$ is not a group, $[u, v]$ idempotent may not be equivalent to $uv = vu$.
- Let $\varphi \in \operatorname{End} \overline{\Omega}_2\mathbf{S}$ be defined by $\varphi(x_1) = [x_1, x_2]$ and $\varphi(x_2) = x_2$. Note that $\varphi^k(x_1)$ is the iterated commutator defined recursively by $[x_1,_1 x_2] = [x_1, x_2]$ together with

$$[x_1,_{k+1} x_2] = [[x_1,_k x_2], x_2].$$

- We let $[x_1,_\omega x_2] = \varphi^\omega(x_1)$, which is an implicit operation in $\overline{\Omega}_2\mathbf{S}$.
- Using a theorem of Zorn [Zor36], that states that a finite group is nilpotent (i.e., a direct product of groups of prime power order) if and only if it satisfies some identity of the form $[x,_n y] = 1$, it is now easy to solve Exercise 6.5(2):

$$\mathbf{G}_{\text{nil}} = [\![[x,_\omega y] = 1]\!].$$

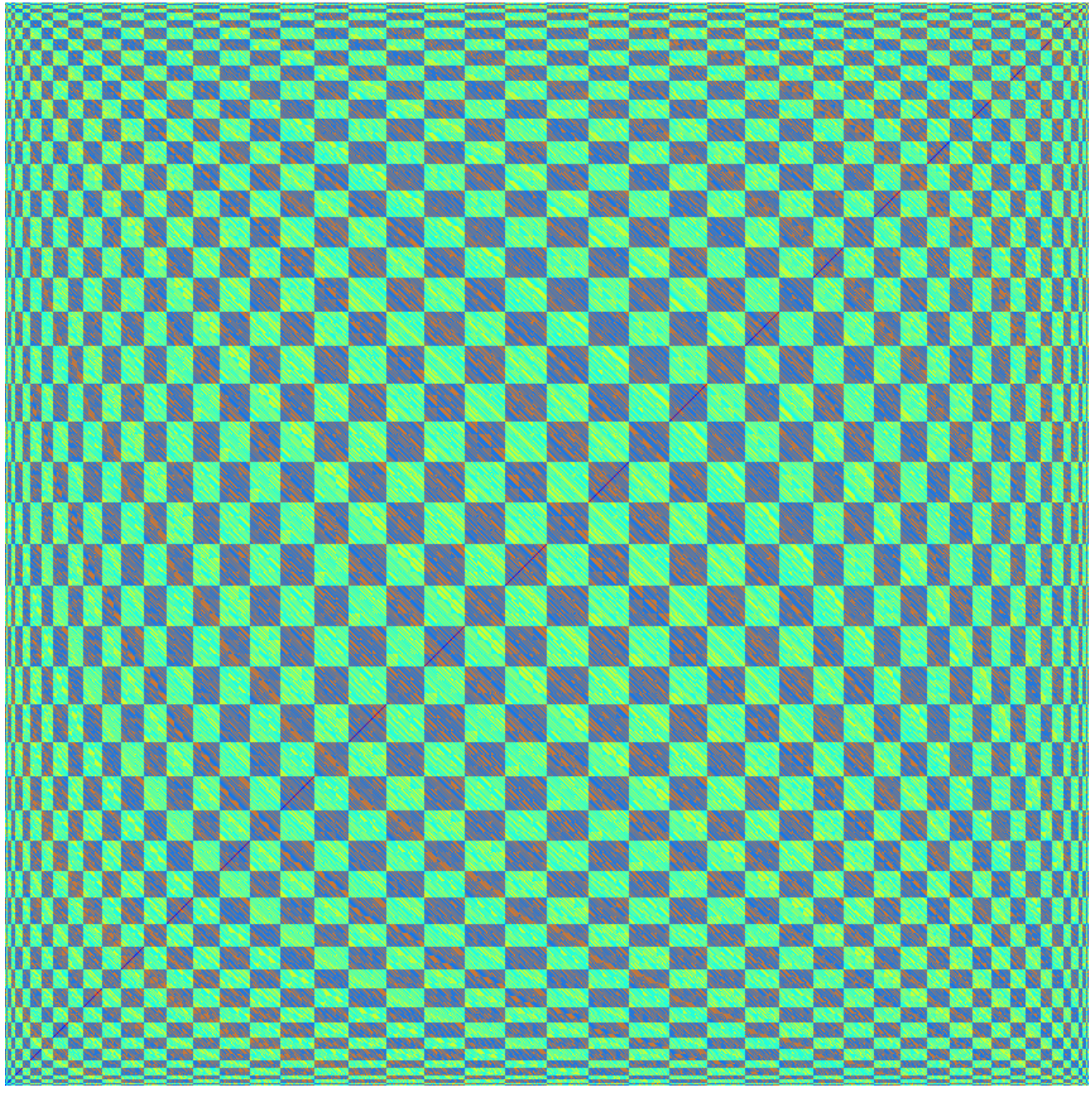
# The Prouhet-Thue-Morse substitution

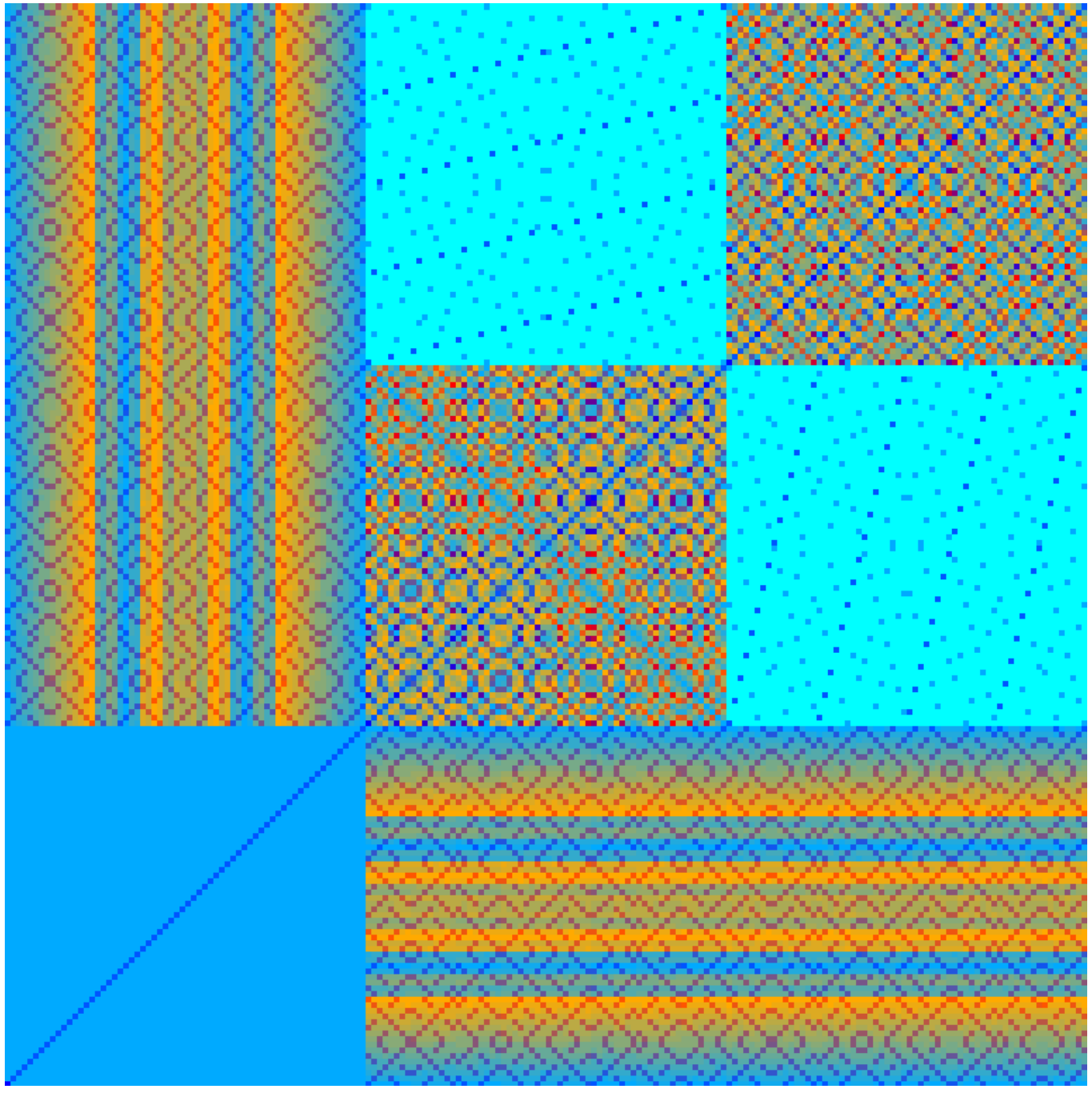
- When $\varphi \in \overline{\Omega}_A\mathbf{S}$ extends an endomorphism of $A^+$ it is also called a (finite) substitution since applying $\varphi$ to a word corresponds to substituting each letter $a \in A$ by the word $\varphi(a)$.
- The substitution over the alphabet $\{a, b\}$ defined by $\tau(a) = ab$ and $\tau(b) = ba$ was first considered by Prouhet [Pro51], and rediscovered by Thue [Thu06, Thu12] and Hedlund and Morse [HM38].
- Here is an example of a result involving it:

**Theorem 17.7 (Širšov [Š63])**

*The pseudovariety* $[\![\tau^\omega(a) = \tau^\omega(b), x^\omega = 1]\!]$ *consists of all finite groups admitting a normal nilpotent subgroup whose corresponding factor group is a 2-group.*

- The substitution $\tau$ determines a binary implicit operator $[ab, ba]_S$ on every profinite semigroup $S$. How does it behave on a finite group?
- When iterating a transformation on a finite set, in a finite number steps one must enter into a periodic orbit.
- One possible way to visualize the action of our Prouhet-Thue-Morse implicit operator on a finite group $G$ is to draw a square in which the sides stand for $G$, and a pixel, an elementary square, for an element of $G \times G$. One may color each pixel so as to encode for instance how many applications of the operator it takes to reach a periodic orbit, and to distinguish between the different periodic orbits.
- It is somewhat striking that one obtains pictures like those in the following two pages. The ordering of the elements in the groups is that given by GAP [GAP06], a computer algebra system that was used to carry out the calculations. The groups are $\mathbb{Z}/858\mathbb{Z}$ and $V_4 \wr A_3$.





# Outline

- Given $w \in \overline{\Omega}_A\mathbf{S}$, denote by $F(w)$ the set of words $u \in A^+$ which are factors of $w$, and let $F_n(w) = F(w) \cap A^n$.
- The complexity sequence $q_w(n)$ is defined by letting $q_w(n) = |F_n(w)|$, where $n$ is a positive integer.

**LEMMA 18.1**

*Let $w \in \overline{\Omega}_A\mathbf{S} \setminus A^+$ and let $u \in F(w)$. If there is no $a \in A$ such that $ua \in F(w)$, then there is factorization of the form $w = vu$.*

## Proof.

Let $(w_n)_n$ be a sequence of finite words converging to $w$. For each $z \in A^+$, the set $C_z = (\overline{\Omega}_A \mathbf{S})^1 z (\overline{\Omega}_A \mathbf{S})^1 = \overline{A^* z A^*}$ is a clopen set such that $C_z \cap A^+ = A^* z A^*$. By hypothesis, $w$ belongs to $C_u$ and so we may assume that so do all $w_n$, since $C_u$ is open. On the other hand, since $C_{ua}$ is closed, we may assume that no $w_n \in C_{ua}$, for any $a \in A$. This leaves only one place for $u$ to be a factor of each $w_n$, namely as a suffix: $w_n = v_n u$ for some $v_n \in A^*$. Since $\overline{\Omega}_A \mathbf{S}$ is compact, some subsequence of $(v_n)_n$ converges to some $v \in \overline{\Omega}_A \mathbf{S}$. By continuity of multiplication, it follows that $w = vu$. □

## Lemma 18.2

*Let $w \in \overline{\Omega}_A \mathbf{S}$. Then the following formula holds for every positive integer $n$:*

$$q_w(n+1) - q_w(n) = \sum_{u \in F_n(w)} (|\{a \in A : \ ua \in F_{n+1}(w)\}| - 1). \quad (9)$$

## Proof.

Each factor of $w$ of length $n+1$ is of the form $ua$, for some $a \in A$, which yields the following formula:

$$q_w(n+1) = \sum_{u \in F_n(w)} |\{a \in A : \ ua \in F_{n+1}(w)\}|.$$

Subtracting $q_w(n) = \sum_{u \in F_n(w)} 1$, we obtain formula (9). □

- Because of the suffix of length $n$ appearing nowhere else in $w$ (cf. Lemma 18.1), there may be one negative term in the sum (9). However, the sum is always nonnegative for $w \in \overline{\Omega}_A\mathbf{S} \setminus A^+$.

**Lemma 18.3**

*Let $w \in \overline{\Omega}_A\mathbf{S} \setminus A^+$. Then the sequence $q_w(n)$ is increasing.*

## Proof.

Suppose that $q_w(n+1) < q_w(n)$. Then, as argued above, the suffix $u$ of length $n$ of $w$ must not appear elsewhere in $w$ as a factor, and all other terms in the sum must be zero: for every $v \in F_n(w) \setminus \{u\}$, there is exactly one letter $a_v \in A$ such that $va_v \in F_{n+1}(w)$.

Now, suppose that $tz$ is a finite suffix of $w$, with $|t| = n$. Then there is no word $z'$ with $|z'| > |z|$ such that $tz'$ is a suffix of $w$. For, otherwise, we may take a counterexample $(t, z)$ with $|z|$ minimum. Then $z \neq 1$ for, else, we must have $t = u$ and we know that $u$ does not appear elsewhere in $w$. Hence, $z = a_t z_1$ and, if we write $t = bt_1$, with $b \in A$, then $(t_1, z_1)$ is still a counterexample and $|z_1| < |z|$, which contradicts our choice of counterexample.

Hence every factor of length $n$ of $w$ which appears as part of a finite suffix, can be found as such in only one position. Since $F_n(w) \subseteq A^n$ is finite, we conclude that $w$ cannot have arbitrarily long finite suffixes, whence $w \in A^+$, contrary to the hypothesis. □

- We say that a finite word $u$ is primitive if it is not of the form $v^n$ for some integer $n > 1$.

## Theorem 18.4 ([AV06a])

*Suppose that $w \in \overline{\Omega}_A \mathbf{S} \setminus A^+$ is such that $q_w(n) \leq n$ for some $n$. Then there exist finite words $x$, $y$, and $z$ and an infinite $\nu \in \hat{\mathbb{Z}}_+$ such that $w = xy^\nu z$, $|xy| \leq n$, and $|yz| \leq n$.*

## Corollary 18.5 ([AV06a])

*Let $w$ be any pseudoword which is not of the form $xy^\nu z$ for some finite words $x, y, z$ and some $\nu \in \hat{\mathbb{Z}}_+$. Then $q_w(n) \geq n + 1$ for every $n$.* □

- The next result identifies maximal subgroups of $\overline{\Omega}_A\mathbf{S}$ of small complexity.

## Theorem 18.6 ([AV06a])

*Suppose that $w$ lies in a subgroup of $\overline{\Omega}_A\mathbf{S}$ and $q_w(n) \leq n$ for some $n$. Then the $\mathcal{H}$-class of $w$ is a free procyclic group with generator of the form $y^{\omega+1}$ for some word $y$ of length at most $n$. In particular, for each positive $n$, there are only finitely many $\mathcal{H}$-classes of such pseudowords $w$.*

- Note that $\mathcal{J}$-equivalent elements of $\overline{\Omega}_A\mathbf{S}$ have the same complexity.

## Corollary 18.7

*The complexity of any non-procyclic subgroup of $\overline{\Omega}_A\mathbf{S}$ is at least $q(n) \geq n+1$.* □

# Sturmian pseudowords

- Thus, the minimum possible complexity for a non-procyclic subgroup of $\overline{\Omega}_A\mathbf{S}$ is $q(n) = n + 1$.
- Then $q(1) = 2$, which means that there are exactly two letters involved in the subgroup in question.
- We say that $w \in \overline{\Omega}_A\mathbf{S}$ is Sturmian if $q_w(n) = n + 1$ for every $n \geq 1$.

# Outline

# Primitive substitutions

- Since substitutions over a one-letter alphabet are not very interesting, we assume from hereon that $|A| \geq 2$.
- A finite substitution $\varphi \in \operatorname{End} \overline{\Omega}_A \mathbf{S}$ is said to be primitive if there is some positive integer $N$ such that, for every two letters $a, b \in A$, $a$ appears in the word $\varphi^N(b)$.

## Proposition 19.1

*Let $\varphi \in \operatorname{End} \overline{\Omega}_A \mathbf{S}$ be a primitive finite substitution. Then all pseudowords of the form $\varphi^\omega(a)$, with $a \in A$, lie in the same $\mathcal{J}$-class.*

## Proof.

Let $N$ be as above and let $a, b \in A$. Then $a$ is a factor of $\varphi^{kN}(b)$ for every $k$. By compactness, it follows that $a$ is also a factor of $\varphi^\omega(b) = (\varphi^N)^\omega(b)$, say $\varphi^\omega(b) = uav$. Since $\varphi^\omega$ is idempotent, we deduce that $\varphi^\omega(b) = \varphi^\omega(u) \cdot \varphi^\omega(a) \cdot \varphi^\omega(v)$, which shows that $\varphi^\omega(a)$ is a factor of $\varphi^\omega(b)$. □

- We have already seen one classical example of primitive finite substitution, namely the Prouhet-Thue-Morse substitution $a \mapsto ab$, $b \mapsto ba$.
- Another classical example is that of the so-called Fibonacci substitution $\varphi(a) = ab$, $\varphi(b) = a$. Note that the $f_n = |\varphi^n(b)|$ satisfies the recurrence relation $f_{n+2} = f_{n+1} + f_n$, with $f_1 = f_2 = 1$.
- $\varphi^\omega(b)$ is an example of Sturmian pseudoword.
- More generally, the following is a consequence of a theorem of Mignosi and Séébold [MS93] on infinite words.

**Theorem 19.2**

*Let $\varphi \in \operatorname{End} \overline{\Omega}_2\mathbf{S}$ be a primitive substitution. Then $\varphi^\omega(x_1)$ is Sturmian if and only if $\varphi$ induces an automorphism of the free group $\Omega_2^\kappa\mathbf{G}$.*

- By Proposition 19.1, one may consider the complexity of a primitive finite substitution $\varphi \in \operatorname{End} \overline{\Omega}_A \mathbf{S}$.

**Theorem 19.3 ([ELR75, Pan84])**

*The complexity of a primitive finite substitution is at most linear.*

## Proof.

Let $\varphi \in \operatorname{End} \overline{\Omega}_A \mathbf{S}$ be a primitive finite substitution, let $q$ be its complexity, and let $n$ be a positive integer. There is some $p$ such that

$$\min_{a \in A} |\varphi^{p-1}(a)| \leq n \leq \min_{a \in A} |\varphi^p(a)|. \tag{10}$$

Then, every word in $F_n(\varphi^\omega(a))$ must be a factor of some $\varphi^p(a)$ or of some $\varphi^p(ab)$, with $ab$ a factor of $\varphi^\omega(ab)$. For each such two-letter word $ab$, there are at most $|\varphi^p(ab)|$ factors of length $n$. Hence, if we let $r = |A|^2$, then we have

$$q(n) \leq 2r \max_{a \in A} |\varphi^p(a)|. \tag{11}$$

By the Perron-Frobenius Theorem (19.4), there are constants $\alpha, c, d > 0$ such that

$$c\alpha^p \leq \min_{a \in A} |\varphi^p(a)| \leq \max_{a \in A} |\varphi^p(a)| \leq d\alpha^p. \tag{12}$$

Combining the inequalities (11) and (12) and taking also into account (10), we obtain

$$q(n) \leq 2r\, d\alpha^p \leq 2r \frac{d}{c} \alpha\, n.$$

□

# The Perron-Frobenius Theorem

- Let $\varphi \in \operatorname{End} \overline{\Omega}_A\mathbf{S}$ be a finite substitution. For each $a, b \in A$, one may consider the number $|\varphi(a)|_b$ of occurrences of the letter $b$ in the word $\varphi(a)$. This defines a matrix $M(\varphi)$ with nonnegative integer entries.
- Note that:
  - the sum of the entries in the row corresponding to $a \in A$ is $|\varphi(a)|$;
  - for another finite substitution $\psi \in \operatorname{End} \overline{\Omega}_A\mathbf{S}$, $M(\varphi \circ \psi) = M(\varphi)M(\psi)$;
  - thus $M(\varphi^k) = (M(\varphi))^k$ for every $k \geq 1$;
  - hence $\varphi$ is primitive if and only if tere exists $k \geq 1$ such that $(M(\varphi))^k$ has all entries positive; a matrix with nonnegative real entries satisfying this property is said to be primitive;
- An $n \times n$ real matrix $M$ is said to be irreducible if, for every pair of indices $i, j$, there is a power $M^k$ whose $i, j$-entry is nonzero.

## Theorem 19.4 (Perron-Frobenius)

*Let $M$ be a nonnegative irreducible matrix. Then there is a positive simple eigenvalue $\alpha$ such that*

- *$\alpha \geq |\lambda|$ for every other eigenvalue $\lambda$ and*
- *$\alpha$ admits an eigenvector whose coordinates are all positive.*

*In case $M$ is primitive, $\alpha > |\lambda|$ for every other eigenvalue $\lambda$.*

- The special, dominant eigenvalue $\alpha$, is called the Perron-Frobenius eigenvalue of the matrix $M$.
- See http://en.wikipedia.org/wiki/Perron-Frobenius_theorem for the significance of the theorem and several proofs.

- For the proof of the existence of constants $c, d$ such that the inequalities (12) hold, let $M$ be a $r \times r$ nonnegative primitive matrix and let $\alpha$ be its Perron-Frobenius eigenvalue. Let $v = (v_1, \ldots, v_r)$ be a corresponding positive eigenvector: $Mv = \alpha v$, whence $M^p v = \alpha^p v$ for all $p \geq 1$.
- Let $(M^p)_{i,j}$ denote the $i, j$ entry of the matrix $M^p$.
- For $i = 1, \ldots, r$, we have

$$\sum_{j=1}^{r} (M^p)_{i,j} v_j = \alpha^p v_i.$$

- Hence, if $c_0 = \min_i v_i$ and $d_0 = \max_i v_i$, then we get $c_0 \sum_{j=1}^{r} (M^p)_{i,j} \leq d_0 \alpha^p$ for every $i$, whence

$$\max_i \sum_{j=1}^{r} (M^p)_{i,j} \leq \frac{d_0}{c_0} \alpha^p.$$

- On the other hand, we have $c_0 \alpha^p \leq d_0 \sum_{j=1}^{r} (M^p)_{i,j}$ for every $i$, which gives

$$\frac{c_0}{d_0} \alpha^p \leq \min_i \sum_{j=1}^{r} (M^p)_{i,j}.$$

# Examples

- Consider the Prouhet-Thue-Morse substitution $\tau(a) = ab$, $\tau(b) = ba$.
- Then $M(\tau) = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ has characteristic polynomial $(1-x)^2 - 1 = x(x-2)$ and eigenvalues $0 < 2$.
- So, 2 is the Perron-Frobenius eigenvalue. The corresponding eigenspace is generated by $(1, 1)$.
- For $w = \tau^\omega(a)$, the proof of Theorem 19.3 gives

$$q_w(n) \leq 2 \times 2^2 \times \frac{1}{1} \times 2n = 16n.$$

- It turns out that this is about double the exact value, which has been computed (see [Fog02, Proposition 5.1.9]).

- Let $\varphi$ be the Fibonacci substitution: $\varphi(a) = ab$, $\varphi(b) = a$.
- Then $M(\varphi) = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ has characteristic polynomial $(1-x)(-x) - 1 = x^2 - x - 1$ and eigenvalues $\frac{1-\sqrt{5}}{2} < \frac{1+\sqrt{5}}{2}$.
- The Perron-Frobenius eigenvalue, $\frac{1+\sqrt{5}}{2}$, has eigenspace generated by the vector $(\frac{1+\sqrt{5}}{2}, 1)$.
- For $w = \varphi^\omega(a)$, the proof of Theorem 19.3 gives

$$q_w(n) \leq 2 \times 2^2 \times \left(\frac{1+\sqrt{5}}{2}\right)^2 \times \frac{1+\sqrt{5}}{2} n = 2(1+\sqrt{5})^3 n \simeq 68n,$$

while we know that $q_w(n) = n + 1$.

# Outline

- The complexity (function) of a pseudoword has the following log-subadditive property:

**Lemma 20.1**

*Let $w \in \overline{\Omega}_A\mathbf{S}$. Then the inequality $q_w(r+s) \leq q_w(r)\, q_w(s)$ holds for all positive integers $r$ and $s$.*

**Proof.**

A factor of $w$ of length $r+s$ is of the form $uv$, where $u \in F_r(w)$ and $v \in F_s(w)$. □

**Lemma 20.2 (Fekete's Lemma)**

*Let $(t_n)_n$ be a sequence of real numbers such that $t_{r+s} \leq t_r + t_s$ for all $r, s \geq 1$. Then we have $\lim \frac{t_n}{n} = \inf \frac{t_n}{n}$.*

## Proof.

Let $\ell = \inf \frac{t_n}{n}$ and let $\epsilon$ be a positive real number. Let $K$ be an index such that $\frac{t_K}{K} < \ell + \frac{\epsilon}{2}$. There is also a positive integer $M$ such that $\frac{t_r}{KM} < \frac{\epsilon}{2}$ for $r < K$.

Let $n \geq KM$ and write $n = qK + r$ with $r < K$. Then

$$\ell \leq \frac{t_n}{n} \leq \frac{qt_K}{qK + r} + \frac{t_r}{n} \leq \frac{qt_K}{qK} + \frac{t_r}{KM} \leq \frac{t_K}{K} + \frac{t_r}{KM} \leq \ell + \frac{\epsilon}{2} + \frac{\epsilon}{2}$$

which establishes the lemma. □

- Let $A$ be a finite alphabet and $m = |A|$.
- For a pseudoword $w \in \overline{\Omega}_A\mathbf{S} \setminus A^+$, by Lemmas 20.1 and 20.2, the following limit exists:

$$h(w) = \lim_{n\to\infty} \frac{1}{n} \log_m q_w(n).$$

  It is called the entropy of $w$.
- Since $1 \leq q_w(n) \leq m^n$, the entropy $h(w)$ is a real number in the interval $[0, 1]$.
- If $u, v \in \overline{\Omega}_A\mathbf{S} \setminus A^+$ are such that $u$ is a factor of $v$, then $h(u) \leq h(v)$.

- Iteration of primitive finite substitutions leads to minimum entropy:

**Theorem 20.3**

*Let $\varphi \in \operatorname{End} \overline{\Omega}_A \mathbf{S}$ be a primitive finite substitution. Then we have $h(\varphi^\omega(a)) = 0$.*

**Proof.**

Let $w = \varphi^\omega(a)$. By Theorem 19.3, there is some constant $C$ such that $q_w(n) \leq Cn$, for every $n \geq 1$. Hence $h(w) = 0$. □

- A much more general result is uncovered below in Theorem 20.8.

## Proposition 20.4

*Let $w \in \overline{\Omega}_A\mathbf{S} \setminus A^+$. Then $h(w) = 1$ if and only if every $u \in \overline{\Omega}_A\mathbf{S}$ is a factor if $w$.*

## Proof.

Since $h(w) = \inf \frac{1}{n} \log_m q_w(n)$, we have $h(w) = 1$ if and only if $q_w(n) = m^n$ for every $n$, that is if and only if every finite word is a factor of $w$. But every element of $\overline{\Omega}_A\mathbf{S}$ is the limit of a sequence of finite words. Hence every finite word is a factor of $w$ if and only if every pseudoword is a factor of $w$. □

- An ideal in a semigroup $S$ is a nonempty subset $I$ such that $SI \cup IS \subseteq I$.
- A minimal ideal is an ideal which is not properly contained in any other ideal.
- Some semigroups, such as $A^+$, have no minimal ideals.
- Note that a semigroup cannot have more than one minimal ideal: given two ideals $I$ and $J$, $IJ$ is an ideal contained in both of them.
- When there is one minimal ideal, we call it the minimum ideal, since it is indeed contained in every ideal. The minimum ideal of a semigroup is often also called its kernel and denoted $K(S)$.
- For a semigroup $S$, the elements of the minimum ideal, if it exists, are precisely those elements of $S$ which admit every element of $S$ as a factor.

## Proposition 20.5

*Every compact metric semigroup has a minimum ideal.*

## Proof.

Let $S$ be a compact metric semigroup. For each $n$, by compactness $S$ is covered by a finite number of open balls of radius $\frac{1}{n}$. If we choose such balls and collect their centers for varying $n$ in a set, we obtain a countable dense subset $X$.

Let $X = \{x_1, x_2, \ldots, x_n, \ldots\}$ be an enumeration of the elements of $X$. Let $s$ be any limit of a subsequence of the sequence $(x_1 \cdots x_n)_n$. Then $s$ admits every element of $X$ as a factor and, since $X$ is dense in $S$, every element of $S$ must be a factor of $S$. Hence $s \in K(S)$. □

- In particular, every finite and every profinite semigroup has a minimum ideal.
- Proposition 20.4 means that $w \in \overline{\Omega}_A \mathbf{S}$ has maximum entropy (one) if and only if $w \in K(\overline{\Omega}_A \mathbf{S})$.

### Theorem 20.6 ([AV06b])

*Let $w' = w(v_1, \ldots, v_r)$ where the $v_i \in \overline{\Omega}_A \mathbf{S}$ $(i = 1, \ldots, r)$ and $w \in \overline{\Omega}_r \mathbf{S}$. The entropy operator satisfies the following inequality:*

$$h(w') \leq \max\{h(w) \log_m r, h(v_1), \ldots, h(v_r)\}. \tag{13}$$

- An ideal $I$ of a semigroup $S$ is said to be prime if $st \in I$ implies $s \in I$ or $t \in I$.

### Corollary 20.7

*The minimum ideal of $\overline{\Omega}_A \mathbf{S}$ is prime.*

## Theorem 20.8 ([AV06b])

*Let* $u_1, \ldots, u_n \in \overline{\Omega}_n\mathbf{S}$ *and let*

$$(v_1, \ldots, v_n) = [u_1, \ldots, u_n]^{\omega}_{\overline{\Omega}_A\mathbf{S}}(x_1, \ldots, x_n).$$

*Then the entropy operator satisfies the following inequality:*

$$\max_{1 \leq i \leq m} h(v_i) \leq \max_{1 \leq i \leq m} h(u_i).$$

- The following result is a considerable strengthening of Corollary 20.9.

## Corollary 20.9

*For* $m > 1$, *the set* $\overline{\Omega}_m\mathbf{S} \setminus K(\overline{\Omega}_m\mathbf{S})$ *is a subsemigroup of* $\overline{\Omega}_m\mathbf{S}$ *which is closed under composition and iteration.*

- All the results we have presented involving complexity and entropy apply to $\overline{\Omega}_A\mathbf{V}$ with $\mathbf{V}$ a pseudovariety containing **LSI**:
  - all we require is to be able to test finite factors, that is sets of the form $(\overline{\Omega}_A\mathbf{V})^1 w (\overline{\Omega}_A\mathbf{V})^1 = \overline{A^* w A^*}$, with $w \in A^+$, which we need to be clopen;
  - since $A^* w A^*$ is **LSI**-recognizable, such sets are indeed clopen by Theorem 5.9.

Section 21

# *References*

[ABR92] D. Albert, R. Baldinger, and J. Rhodes, The identity problem for finite semigroups (the undecidability of), J. Symbolic Logic **57** (1992), 179–192.

[AE03] J. Almeida and A. Escada, Semidirect products with the pseudovariety of all finite groups, Proceedings of the International Conference Words, Languages and Combinatorics (Kyoto, March, 2000) (Singapore) (M. Ito and T. Imaoka, eds.), World Scientific, 2003, pp. 1–21.

[Alm95] J. Almeida, Finite semigroups and universal algebra, World Scientific, Singapore, 1995, English translation.

[Alm02] _____, Dynamics of implicit operations and tameness of pseudovarieties of groups, Trans. Amer. Math. Soc. **354** (2002), 387–411.

[Alm05] _____, Profinite semigroups and applications, Structural Theory of Automata, Semigroups, and Universal Algebra (New York) (Valery B. Kudryavtsev and Ivo G. Rosenberg, eds.), NATO Science Series II: Mathematics, Physics and Chemistry, vol. 207, Springer, 2005, Proceedings of the NATO Advanced Study Institute on Structural Theory of Automata, Semigroups and Universal Algebra, Montréal, Québec, Canada, 7-18 July 2003, pp. 1–45.

[AS00a] J. Almeida and B. Steinberg, On the decidability of iterated semidirect products and applications to complexity, Proc. London Math. Soc. **80** (2000), 50–74.

[AS00b] _____, Syntactic and global semigroup theory, a synthesis approach, Algorithmic Problems in Groups and Semigroups (J. C. Birget, S. W. Margolis, J. Meakin, and M. V. Sapir, eds.), Birkhäuser, 2000, pp. 1–23.

[AS01] J. Almeida and P. V. Silva, SC-hyperdecidability of **R**, Theor. Comp. Sci. **255** (2001), 569–591.

[AS03] K. Auinger and B. Steinberg, On the extension problem for partial permutations, Proc. Amer. Math. Soc. **131** (2003), 2693–2703.

[Ash87] C. J. Ash, Finite semigroups with commuting idempotents, J. Austral. Math. Soc., Ser. A **43** (1987), 81–90.

[Ash91] _____, Inevitable graphs: a proof of the type II conjecture and some related decision procedures, Int. J. Algebra Comput. **1** (1991), 127–146.

[AT01] J. Almeida and P. G. Trotter, The pseudoidentity problem and reducibility for completely regular semigroups, Bull. Austral. Math. Soc. **63** (2001), 407–433.

[AV06a] J. Almeida and M. V. Volkov, Subword complexity of profinite words and subgroups of free profinite semigroups, Int. J. Algebra Comput. **16** (2006), 221–258.

[AV06b] _____, Subword complexity of profinite words and subgroups of free profinite semigroups, Int. J. Algebra Comput. **16** (2006), 221–258.

[AZ07] J. Almeida and M. Zeitoun, An automata-theoretic approach of the word problem for $\omega$-terms over R, Theor. Comp. Sci. **370** (2007), 131–169.

[Bau65] G. Baumslag, Residual nilpotence and relations in free groups, J. Algebra **2** (1965), 271–282.

[Ber79] J. Berstel, Transductions and context-free languages, B. G. Teubner, Stuttgart, 1979.

[BS73] J. A. Brzozowski and I. Simon, Characterizations of locally testable events, Discrete Math. **4** (1973), 243–271.

[CT04] J. C. Costa and M. L. Teixeira, Tameness of the pseudovariety LSI, Int. J. Algebra Comput. **14** (2004), 627–654.

[Del01] M. Delgado, On the hyperdecidability of pseudovarieties of groups, Int. J. Algebra Comput. **11** (2001), 753–771.

[Eil76] S. Eilenberg, Automata, languages and machines, vol. B, Academic Press, New York, 1976.

[ELR75] A. Ehrenfeucht, K. P. Lee, and G. Rozenberg, Subword complexities of various classes of deterministic developmental languages without interaction, Theor. Comp. Sci. **1** (1975), 59–75.

[Fog02] N. Pytheas Fogg, Substitutions in dynamics, arithmetics and combinatorics, Lecture Notes in Mathematics, vol. 1794, Springer-Verlag, Berlin, 2002.

[GAP06] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4, 2006, (`http://www.gap-system.org`).

[Hal50] M. Hall, A topology for free groups and related groups, Ann. Math. **52** (1950), 127–139.

[Hen88] Karsten Henckell, Pointlike sets: the finest aperiodic cover of a finite semigroup, J. Pure Appl. Algebra **55** (1988), 85–126.

[HM38] G. A. Hedlund and M. Morse, Symbolic dynamics, Amer. J. Math. **60** (1938), 815–866.

[HMPR91] K. Henckell, S. Margolis, J.-E. Pin, and J. Rhodes, Ash's type II theorem, profinite topology and Malcev products. Part I, Int. J. Algebra Comput. **1** (1991), 411–436.

[HR91] K. Henckell and J. Rhodes, The theorem of Knast, the PG=BG and Type II Conjectures, Monoids and Semigroups with Applications (Singapore) (J. Rhodes, ed.), World Scientific, 1991, pp. 453–463.

[Hun83] R. P. Hunter, Some remarks on subgroups defined by the Bohr compactification, Semigroup Forum **26** (1983), 125–137.

[Hun88] _____, Certain finitely generated compact zero-dimensional semigroups, J. Austral. Math. Soc., Ser. A **44** (1988), 265–270.

[KM02] I. Kapovich and A. Myasnikov, Stallings foldings and subgroups of free groups, J. Algebra **248** (2002), 608–668.

[KP86] Jiři Kad'ourek and Libor Polák, On the word problem for free completely regular semigroups, Semigroup Forum **34** (1986), 127–138.

[KR65] K. Krohn and J. Rhodes, Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines, Trans. Amer. Math. Soc. **116** (1965), 450–464.

[McC01] J. McCammond, Normal forms for free aperiodic semigroups, Int. J. Algebra Comput. **11** (2001), 581–625.

[MP71] R. McNaughton and S. Papert, Counter-free automata, MIT Press, Cambridge, MA, 1971.

[MP84] S. W. Margolis and J.-E. Pin, Varieties of finite monoids and topology for the free monoid, Proc. 1984 Marquette Semigroup Conference (Milwaukee), Marquette University, 1984, pp. 113–129.

[MP87] _____, Inverse semigroups and varieties of finite semigroups, J. Algebra **110** (1987), 306–323.

[MS93] F. Mignosi and P. Séébold, Morphismes sturmiens et règles de rauzy, J. Théor. Nombres Bordeaux **5** (1993), 221–233.

[MSW01] S. Margolis, M. Sapir, and P. Weil, Closed subgroups in pro-V topologies and the extension problem for inverse automata, Int. J. Algebra Comput. **11** (2001), 405–445.

[Num57] K. Numakura, Theorems on compact totally disconnetced semigroups and lattices, Proc. Amer. Math. Soc. **8** (1957), 623–626.

[Pan84] J.-J. Pansiot, Complexité des facteurs des mots infinis engendrés par morphismes itérés, Automata, Languages and Programming (Antwerp, 1984) (Berlin), Lect. Notes Comput. Sci., no. 172, Springer, 1984, pp. 380–389.

[Pin95] J.-E. Pin, BG=PG: A success story, Semigroups, Formal Languages and Groups (Dordrecht) (J. Fountain, ed.), vol. 466, Kluwer, 1995, pp. 33–47.

[PR91] J.-E. Pin and C. Reutenauer, A conjecture on the Hall topology for the free group, Bull. London Math. Soc. **23** (1991), 356–362.

[Pro51] E. Prouhet, Mémoire sur quelques relations entre les puissances des nombres, C. R. Acad. Sci. Paris **33** (1851), 31.

[PS85] J.-E. Pin and H. Straubing, Monoids of upper triangular matrices, Semigroups: structure and universal algebraic problems (Amsterdam) (G. Pollák, ed.), North-Holland, 1985, pp. 259–272.

[Rei82] J. Reiterman, The Birkhoff theorem for finite algebras, Algebra Universalis **14** (1982), 1–10.

[RZ93] L. Ribes and P. A. Zalesskiĭ, On the profinite topology on a free group, Bull. London Math. Soc. **25** (1993), 37–43.

[Sch65] M. P. Schützenberger, On finite monoids having only trivial subgroups, Inform. and Control **8** (1965), 190–194.

[Sim75] I. Simon, Piecewise testable events, Proc. 2nd GI Conf. (Berlin), Lect. Notes in Comput. Sci., vol. 33, Springer, 1975, pp. 214–222.

[Sta83] J. R. Stallings, Topology of finite graphs, Inventiones Mathematicae **71** (1983), 551–565.

[Ste01] B. Steinberg, Inevitable graphs and profinite topologies: some solutions to algorithmic problems in monoid and automata theory, stemming from group theory, Int. J. Algebra Comput. **11** (2001), 25–71.

[Ste11] _____, On the endomorphism monoid of a profinite semigroup, Portugal. Math. **68** (2011), 177–183.

[Sti73] P. Stiffler, Extension of the fundamental theorem of finite semigroups, Advances in Math. **11** (1973), 159–209.

[Thu06] A. Thue, Über unendlichen zeichenreihen, Kra. Vidensk. Selsk. Skrifter, I. Mat. Nat. Kl. (1906), no. 7, 1–22.

[Thu12] A. Thuë, Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen, Norske Vid. Selsk. Skr. I. Mat.-nat. Kl., Christiana **1** (1912), 1–67.

[Š63] A. I. Širšov, On certain near-engel groups, Algebra i Logika **2** (1963), no. 5, 5–18.

[Zor36] M. Zorn, Nilpotency of finite groups (abstract), Bull. Amer. Math. Soc. **42** (1936), 485–486.