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:

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.
2. 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.
3. Relatifely 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 σ_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^*/σ_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^*/σ_L on A^* is finite;*

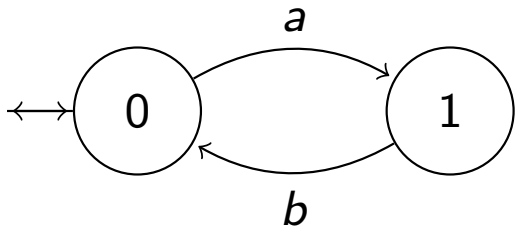
(5) *L is recognized by some homomorphism $\varphi : A^* \to M$ into a finite monoid, in the sense that $L = \varphi^{-1}\varphi L$.*

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 ($M(L_1)$):

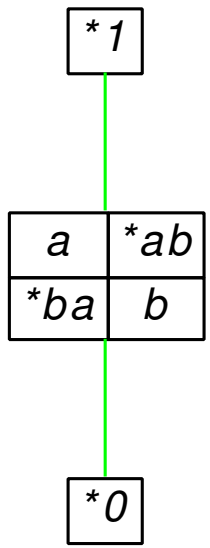
	0	1
a	1	-
b	-	0
ab	0	-
ba	-	1
0	-	-

	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

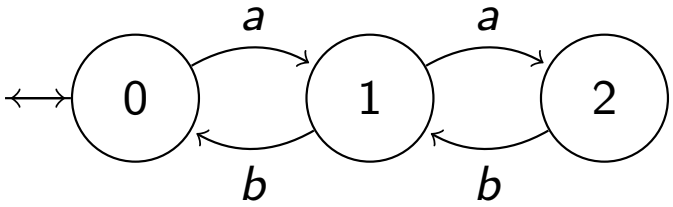
- Presentation: $\langle a, b;\ aba = a,\ bab = b,\ a^2 = b^2 = 0 \rangle$.

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, $\mathcal{D} = \mathcal{J}$



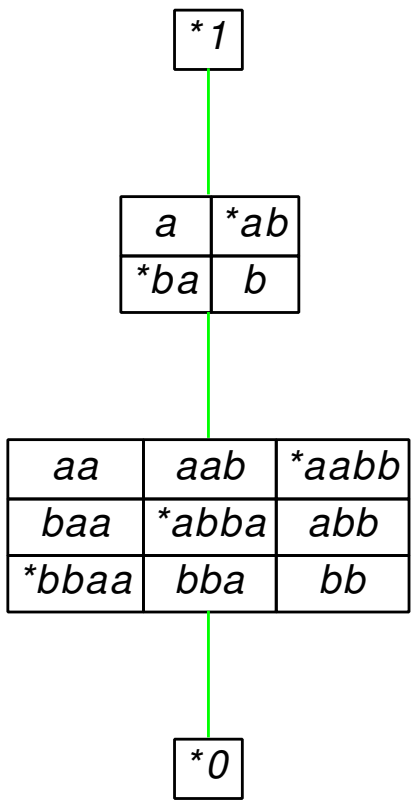
- Regular expression: $L_2 = (a(ab)^*b)^*$
- Minimal (incomplete) automaton:



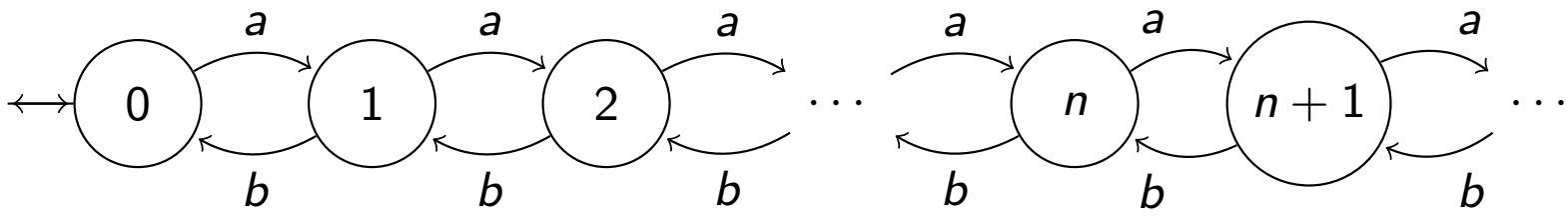
- Presentation of syntactic monoid $M(L_2)$:

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

- 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:

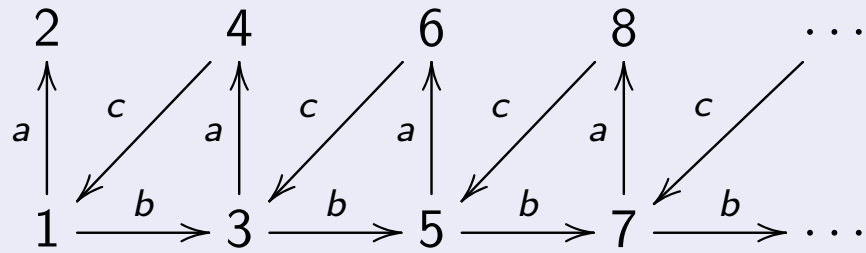


- Syntactic monoid: $M(L_\infty) = \langle a, b; ab = 1\rangle$.
- Eggbox picture:

^{*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 σ_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^+/σ_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, δ, 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?

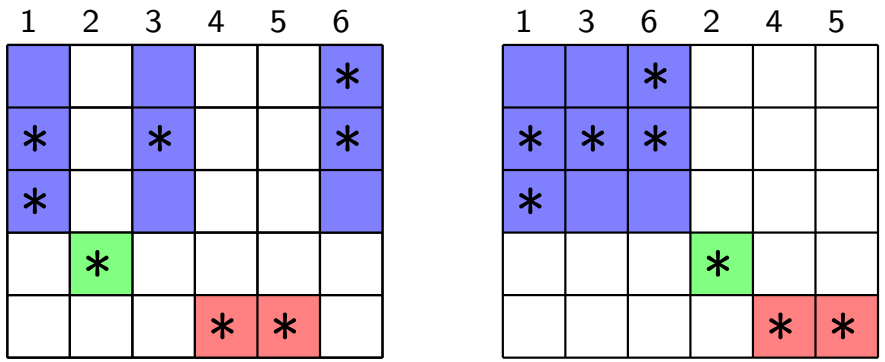
There are many ways to construct new pseudovarieties from known ones, that is by applying operators to pseudovarieties.
We proceed to introduce some natural operators.

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 μ 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 Σ 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 ϵ, consider the open ball

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

The point u is the center and ϵ 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 $A^+ = \bigcup_{s \in S} B_\epsilon(u_s)$. □

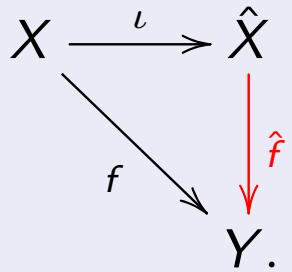
- A sequence $(u_n)_n$ in a (pseudo-ultra)metric space X is said to be a Cauchy sequence if

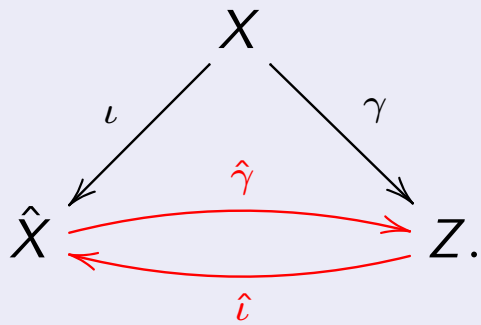
$$\forall\, \epsilon > 0\ \exists\, N\ \big(m, n \geq N \Rightarrow d(u_m, u_n) < \epsilon\big).$$

- 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:

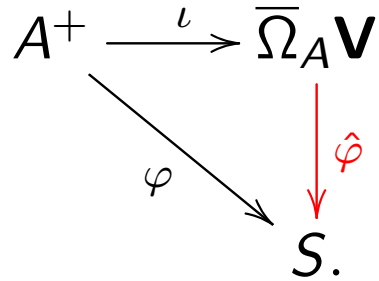
$$d(s,t) = \begin{cases} 0 & \text{if } s = t \\ 1 & \text{otherwise} \end{cases}$$

- 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, φ 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

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

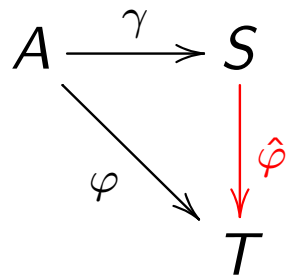
where d_n is the discrete metric on S_n. Then φ is uniformly continuous. In particular, the image T of φ is closed in $\prod_{n\in\mathbb{N}} S_n$, being a compact subset.

- 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 aribtrary mapping into a pro-$\mathbf{V}$ semigroup T, and $\hat{\varphi}$ is a unique continuous homomorphism:

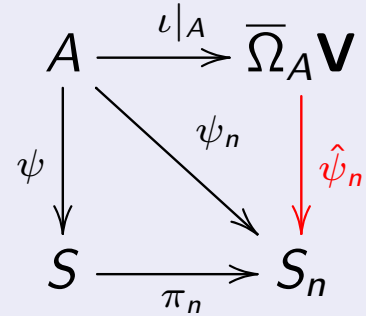


Theorem 5.3

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 φ.

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 φ is continuous and $\overline{\Omega}_A\mathbf{V}$ is compact, φ 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 ρ 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, φ 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/σ_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 σ_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 ι 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 $\overline{\Omega}_A\mathbf{V}$.

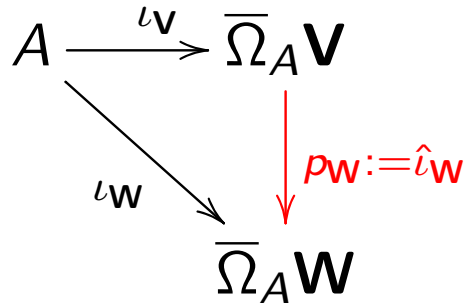
Proof.

($\Rightarrow$) 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 Σ 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 Σ.
- 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 Σ of $\mathbf{V}$-pseudoidentities.

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

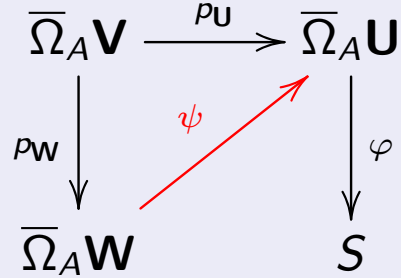
Proof of Theorem 6.2.

($\Leftarrow$) 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 Σ 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 Σ, 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^{ω}.

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 ι 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 ot $\overline{\Omega}_A\mathbf{N}$, 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.

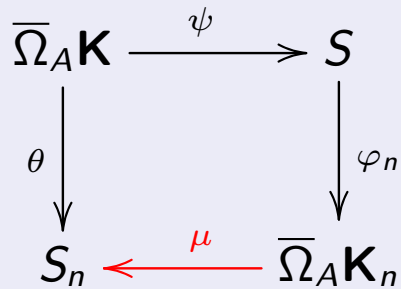
It is easy to check that the multiplication defined on S is associative and that d is an totally bounded complete ultrametric.
Consider the set S_n consisting of all words of A^+ of length at most n, endowed with the operation

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

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 φ_n is a continuous homomorphism into a semigroup from $\mathbf{K}$ which distinguishes u from v. Thus, S is a pro-$\mathbf{K}$ semigroup.

(. . .)

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 μ shows that $\psi(u) \neq \psi(v)$. Hence ψ is injective. □

Outline

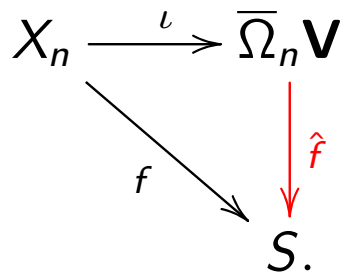
Implicit operations

- Let n be a positive integer.
- An *n*-ary implicit operation on pro-**V** semigroups is a correspondence π associating to each pro-**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-**V** semigroups, the following diagam 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 $s_1, \ldots, s_2 \in S$.
- 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 π_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 $\hat{f}$ completes the following diagram:

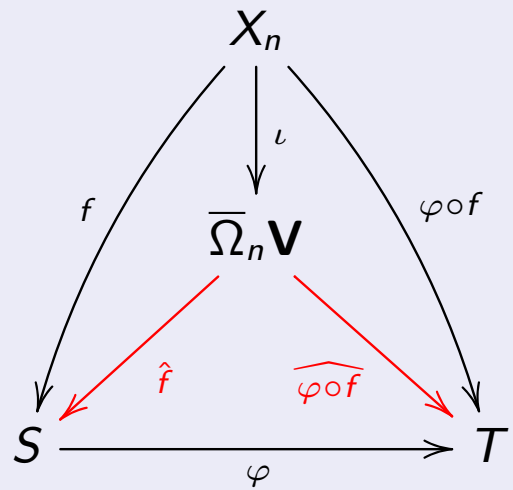


Proposition 8.1

1. *For each $w \in \overline{\Omega}_n \mathbf{V}$, π_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 π_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 π_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 π_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

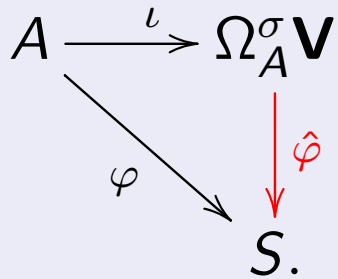
- By an implicit signature we mean a set σ of implicit operations (on $\mathbf{S}$) which includes the binary operation of multiplication.
- Example: $\kappa = \{\_ \cdot \_,\ \_^{\omega-1}\}$.
- Given an implicit signature σ, each profinite semigroup S becomes a natural σ-algebra in which each operation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

[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 σ-algebra $\Omega_A^\sigma \mathbf{V}$ is a $\mathbf{V}$-free σ-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 σ-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 σ;
- $\Omega_A^\kappa \mathbf{J} = \overline{\Omega}_A \mathbf{J}$ [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 σ-algebra $\Omega_A^\sigma \mathbf{V}$: to find an algorithm, if one exists, that given two σ-terms over A, determines whether $u_{\mathbf{V}} = v_{\mathbf{V}}$.
  If such 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 κ-terms coincide in $\Omega_A^\sigma \mathbf{N}$ 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 κ-terms can be effectively reduced (over $\mathbf{G}$) to κ-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 κ-terms over $\mathbf{G}$; two κ-terms are equal over $\mathbf{G}$ if and only if they have the same canonical form.
- Word problem for $\overline{\Omega}_A \mathbf{K}$: 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 $L \subseteq \iota_{\mathbf{V}}^{-1}(\iota_{\mathbf{V}}(L))$. □

- Note that, while $\overline{\Omega}_A\mathbf{V}$ is in general uncountable, by Theorem 5.9 it has only countably many clopen subsets, since there are only that many $\mathbf{V}$-recognizable subsets of A^+ (for instance since they are all recognized by finite automata).
- An idea due to Pin and Reutenauer [PR91] in the case of the pseudovariety $\mathbf{G}$ 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 $\mathbf{G}$, they produced an algorithm for computing the required closure, which solves our problem for $\mathbf{G}$.
- 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 $\mathrm{cl}_{\sigma,\mathbf{V}}(L) = \mathrm{cl}_{\mathbf{V}}(L) \cap \Omega_A^\sigma\mathbf{V}$.
- 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 a 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 σ-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 $p_{\mathbf{V}}(w') = w$.

Examples:

- The pseudovariety **N** is κ-full: for a regular language $L \subseteq A^+$ and a κ-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 κ-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 κ-full follows from the structure theorem for $\overline{\Omega}_A\mathbf{J}$.
- The pseudovariety **G** is κ-full: the essential ingredient is a seminal theorem of Ash [Ash91]; the details follow from [AS00] and [Del01].
- The pseudovariety **Ab** is κ-full [Del01].

- The pseudovariety $\mathbf{G}_p$ is not κ-full: this follows from a weak version of Ash's theorem proved by Steinberg [Ste01] for $\mathbf{G}_p$ together with fact that the conjunction of this weaker property with κ-fullness implies that the pseudovariety is defined by pseudoidentities in which both sides are given by κ-terms [AS00]; 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 κ-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

- 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.

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 11.1

*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 11.2

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 11.1, 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 11.3

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 11.4

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 11.2, 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 11.5

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 11.1, 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 11.4, 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 11.2. Since L is a union of cosets of U, L is also open in the pro-$\mathbf{H}$ metric of G. □

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

Proposition 11.6

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 11.4, 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).

. . .

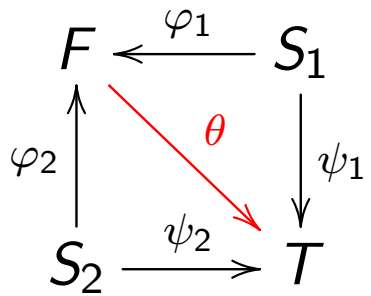
From the first inequality in (1) we deduce that every Cauchy sequence with respect to d' is also a Cauchy sequence with respect to d. For the converse, let $f(n) = \big((G : H) \cdot n\big)!$. Then f is an increasing sequence and a simple calculation shows that, for every $\varepsilon > 0$,

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

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 11.7

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 11.8

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.

Section 12

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.

[AS00] J. Almeida and B. Steinberg, On the decidability of iterated semidirect products and applications to complexity, Proc. London Math. Soc. **80** (2000), 50–74.

[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.

[AZ07] J. Almeida and M. Zeitoun, An automata-theoretic approach of the word problem for ω-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.

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

[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.

[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.

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

[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.

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

[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.

[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.

[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.

[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.

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