THE MYSTERIES OF FREE PROFINITE SEMIGROUPS
A SNEAK PREVIEW

Jorge Almeida

Centro de Matemática
Departamento de Matemática Pura
Faculdade de Ciências
Universidade do Porto

http://www.fc.up.pt/cmup/jalmeida

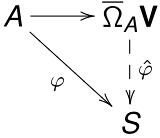
North British Semigroups and Applications Network Meeting

in memory of W. D. Munn

University of York
28 January, 2009

- Let $\mathbf{V}$ be a *pseudovariety* of semigroups (class of finite semigroups closed under taking homomorphic images, subsemigroups, and finite direct products).
- Finite semigroups are viewed as topological semigroups under the discrete topology.
- *Pro-$\mathbf{V}$ semigroup*: compact semigroup that is *residually* $\mathbf{V}$ as a topological semigroup.
- *Profinite semigroup*: compact semigroup that is residually finite as a topological semigroup.
  Equivalently: compact zero-dimensional (or totally disconnected) semigroup.

- $\overline{\Omega}_A\mathbf{V}$: pro-$\mathbf{V}$ semigroup freely generated by the totally disconnected space A. In general, we assume that $|A| \geq 2$.
- It is characterized by the following *universal property*:



where $\varphi : A \to S$ denotes an arbitrary continuous mapping into a pro-$\mathbf{V}$ semigroup.
- It may be constructed as the *projective limit* of all *A-generated* members of $\mathbf{V}$.
- Elements of $\overline{\Omega}_A\mathbf{V}$ will be called *pseudowords (over* $\mathbf{V}$*)*.
- For A finite, they may be viewed as *(implicit) operations* on pro-$\mathbf{V}$ semigroups: for $w \in \overline{\Omega}_A\mathbf{V}$ and S pro-$\mathbf{V}$,

$$\begin{aligned} w_S : S^A &\longrightarrow S \\ \varphi &\longmapsto \hat{\varphi}(w) \end{aligned}$$

- Denote by $\iota_{\mathbf{V}}$ the natural homomorphism $A^+ \to \overline{\Omega}_A\mathbf{V}$.

THEOREM (JA'1989)

A language $L \subseteq A^+$ is $\mathbf{V}$-recognizable if and only if the following conditions hold:

1. *the closure $\overline{\iota_{\mathbf{V}}(L)}$ of $\iota_{\mathbf{V}}(L)$ in $\overline{\Omega}_A\mathbf{V}$ is open;*
2. $L = \iota_{\mathbf{V}}^{-1}\left(\overline{\iota_{\mathbf{V}}(L)}\right)$.

- Note: the second condition is superfluous if $\iota_{\mathbf{V}}$ is injective and the induced topology in A^+ (i.e., the *pro-$\mathbf{V}$ topology*) is discrete.
- This is the case for instance for any pseudovariety containing all finite nilpotent semigroups.

- In other words: the topological space $\overline{\Omega}_A\mathbf{V}$ is the *Stone dual* of the Boolean algebra of $\mathbf{V}$-recognizable subsets of A^+.
- Gehrke-Grigorieff-Pin'2008: the multiplication operation on $\overline{\Omega}_A\mathbf{V}$ is the dual of the residuation operations.
- Thus, to understand the algebraic/topological structure of $\overline{\Omega}_A\mathbf{V}$ is equivalent to understanding the algebra/combinatorics of $\mathbf{V}$-recognizable languages over the alphabet A.

- From hereon, we assume that A is a finite set with $|A| \geq 2$.

THEOREM (BINZ-NEUKIRCH-WENZEL'1971)

Every open subgroup of a free profinite group is also a free profinite group.

THEOREM (RIBES'1970)

A profinite group is projective if and only if it is isomorphic to a closed subgroup of a free profinite group.

THEOREM (NOVIKOV-SEGAL'2003,2007)

Every subgroup of finite index of a finitely generated profinite group is open.

- In other words, every homomorphism from a finitely generated profinite group into a finite group is continuous.
  - It follows that every homomorphism from a finitely generated profinite semigroup into a finite group is continuous.
  - This is not the case for all finite semigroups: for instance, $\chi_{A^+} : \overline{\Omega}_A\mathbf{S} \to \{0, 1\}$ is a discontinuous homomorphism into the two-element semilattice.
  - Problem. *For which finite semigroups is it true that every homomorphism from a finitely generated profinite semigroup into it is continuous?*
- In particular, the topology of a finitely generated profinite group is completely determined by its algebraic structure.

THEOREM (RHODES-STEINBERG'2008)

The closed subgroups of $\overline{\Omega}_A\mathbf{S}$ are precisely the projective profinite groups. In particular, every subgroup of $\overline{\Omega}_A\mathbf{S}$ is torsion-free.

- Combining with Ribes' Theorem, we deduce that $\overline{\Omega}_A\mathbf{S}$ has the same closed subgroups as $\overline{\Omega}_A\mathbf{G}$.
- Zalesskiĭ asked which profinite groups may appear as *maximal subgroups* of $\overline{\Omega}_A\mathbf{S}$.
- In particular, can a free pro-p group appear as a maximal subgroup of $\overline{\Omega}_A\mathbf{S}$?
- More generally, the theorem holds for every pseudovariety $\mathbf{V}$ such that $(\mathbf{V} \cap \mathbf{Ab}) * \mathbf{V} = \mathbf{V}$.

Theorem (Rhodes-Steinberg'2008)

Every finite subsemigroup of $\overline{\Omega}_A\mathbf{S}$ is a band.

- More generally, this holds for every pseudovariety **V** such that $\mathbf{A} ⓜ \mathbf{V} = \mathbf{V}$ (that is for which the corresponding variety of languages is closed under concatenation) provided we replace "*a band*" by "*completely regular*".

THEOREM (JA-STEINBERG'2008)

A clopen subsemigroup of $\overline{\Omega}_A\mathbf{S}$ is a free profinite semigroup if and only if it is the closure of a rational free subsemigroup of A^+.

- Margolis-Sapir-Weil'1998: reverse direction for a finitely generated free subsemigroup of A^+.
- Holds more generally for pseudovarieties of the form $\overline{\mathbf{H}}$ (all finite semigroups whose subgroups lie in **H**) for an arbitrary pseudovariety **H** of groups which is *extension-closed*.

THEOREM (STEINBERG'2008)

The maximal subgroups of the minimum ideal of $\overline{\Omega}_A\mathbf{S}$ are free profinite groups of countable rank.

- This holds more generally for pseudovarieties of the form $\overline{\mathbf{H}}$ for a pseudovariety $\mathbf{H}$ of groups which is extension-closed and *contains cyclic groups of infinitely many prime orders*.
- Steinberg asked whether the latter hypothesis may be dropped.

Theorem (Steinberg'2008)

Let G be a maximal subgroup of the minimum ideal of $\overline{\Omega}_A\mathbf{S}$ and let $\varphi : G \to \overline{\Omega}_A\mathbf{G}$ be the restriction to G of the natural continuous homomorphism $\overline{\Omega}_A\mathbf{S} \to \overline{\Omega}_A\mathbf{G}$. Then $\ker\varphi$ is a free profinite group of countable rank.

- This holds more generally under the same more general hypotheses as in the preceding theorem if we replace the pair of pseudovarieties $(\mathbf{S}, \mathbf{G})$ by $(\overline{\mathbf{H}}, \mathbf{H})$.
- Steinberg also conjectured that the maximal subgroup of the subsemigroup of $\overline{\Omega}_A\mathbf{S}$ generated by the idempotents in the minimum ideal is free profinite.

index

- For a topological semigroup S, denote by $End(S)$ its endomorphism monoid.

THEOREM (JA'2003)

Let S be a finitely generated profinite semigroup. Then $End(S)$ is a profinite semigroup under the pointwise convergence topology (i.e., with the subspace topology induced from the direct power S^S). Moreover, this topology coincides with the compact-open topology, which entails the continuity of the evaluation mapping

$$\begin{aligned} End(S) \times S &\longrightarrow S \\ (\varphi, s) &\longmapsto \varphi(s). \end{aligned}$$

- In a compact semigroup S, given $s \in S$, the minimum ideal of $\overline{\langle s\rangle}$ is a group, and therefore has a unique idempotent, denoted s^ω. The inverse of $s^{\omega+1} = ss^\omega$ is denoted $s^{\omega-1}$.
- In case S is profinite, $s^{\omega(-1)} = \lim_{n\to\infty} s^{n!(-1)}$.

- Call the elements of $\mathrm{End}(\overline{\Omega}_A\mathbf{S})$ *substitutions*.
- Given a substitution φ, we may therefore consider its "infinite iterate" φ^ω, which is an idempotent substitution.
- Examples for $A = \{a, b\}$:
  - *Fibonacci substitution*: $\varphi(a) = ab$, $\varphi(b) = a$;

    $$\varphi^7(a) = abaababaabaababaababaabaababaabaab$$

  - *Prouhet-Thue-Morse substitution*: $\tau(a) = ab$, $\tau(b) = ba$;

    $$\tau^5(a) = abbabaabbaababbabaababbaabbabaab.$$

- From hereon, we let $\mathbf{V}$ be a pseudovariety containing $\mathbf{LSI}$, so that, in particular, $\iota_{\mathbf{V}} : A^+ \to \overline{\Omega}_A\mathbf{V}$ is injective.
- We identify each $u \in A^+$ with its image under $\iota_{\mathbf{V}}$ and call the elements of A^+ the *finite elements* of $\overline{\Omega}_A\mathbf{V}$, while the remaining elements are said to be *infinite*.
- We say that $w \in \overline{\Omega}_A\mathbf{V}$ is *uniformly recurrent* if, for every finite factor u of w, there is some positive integer N such that every finite factor v of w of length at least N admits u as a factor.

THEOREM (JA'2005)

An element of $\overline{\Omega}_A\mathbf{V}$ is uniformly recurrent if and only if it is $\mathcal{J}$-maximal.

- Note: since every infinite pseudoword has some idempotent factor, $\mathcal{J}$-maximal infinite pseudowords are regular.

- A substitution $\varphi \in \mathrm{End}(\overline{\Omega}_A \mathbf{V})$ is said to be *primitive* if there exists a positive integer n such that, for every $a, b \in A$, a is a factor of $\varphi^n(b)$.
- It is said to be *group-invertible* if it induces an automorphism of $\overline{\Omega}_A(\mathbf{V} \cap \mathbf{G})$.

THEOREM (JA'2005)

Let $\varphi \in \mathrm{End}(\overline{\Omega}_A \mathbf{V})$ be a primitive substitution. Then all $\varphi^\omega(a)$ ($a \in A$) all lie in the same $\mathcal{J}$-maximal regular $\mathcal{J}$-class J_φ.

- For a primitive substitution, denote by G_φ any of the maximal subgroups of J_φ.

THEOREM (JA'2005)

Let $\varphi \in \mathrm{End}(\overline{\Omega}_A \mathbf{S})$ be a primitive, group invertible substitution. Then G_φ is a finitely generated free profinite group.

- The second theorem applies to the Fibonacci substitution, $\varphi(a) = ab$, $\varphi(b) = a$.
- For a generalization, given $w \in \overline{\Omega}_A\mathbf{S}$, let $q_w(n)$ be the number of finite factors of w of length n.
- Say that $w \in \overline{\Omega}_{\{a,b\}}\mathbf{S}$ is *Sturmian* if $q_w(n) = n + 1$ for all $n \geq 1$.
- For the Fibonacci substitution φ, J_φ consists of Sturmian pseudowords.

THEOREM (JA'2004)

If $w \in \overline{\Omega}_A\mathbf{S}$ is Sturmian then w is uniformly recurrent and the maximal subgroups of its $\mathcal{J}$-class are free profinite groups freely generated by two pseudowords.

- For the Prouhet-Thue-Morse substitution, $\tau(a) = ab$, $\tau(b) = ba$,

THEOREM (JA-A. COSTA'2008+)

The minimum number of generators of the group G_τ is 3 and the group is not free profinite.

- An easier example of non-free profinite (uniformly recurrent) maximal subgroup of $\overline{\Omega}_A\mathbf{S}$ is given by G_φ where $\varphi(a) = ab$, $\varphi(b) = a^3b$ (JA'2005); it is a 2-generated non-pro-cyclic group.
- Problem. *Find profinite presentations for the above groups G_τ and G_φ.*

- Let $w \in \overline{\Omega}_A \mathbf{V}$.
- Note that $q_w(n)$ is defined by counting certain finite factors of w, which do not depend on $\mathbf{V}$ (for $\mathbf{V} \supseteq \mathbf{LSI}$).
- It is easy to see that the *complexity sequence* $q_w(n)$ satisfies the subadditive inequality

$$q_w(r+s) \leq q_w(r) + q_w(s)$$

- It follows that the following limit exists

$$h(w) = \lim_{n \to \infty} \frac{1}{n} \log_{|A|} q_w(n)$$

- It is called the *entropy* of w.

PROPOSITION

The minimum ideal of $\overline{\Omega}_A\mathbf{V}$ *consists of the pseudowords of entropy 1.*

THEOREM

Let $w \in \overline{\Omega}_A\mathbf{V}$, $v_1, \ldots, v_r \in \overline{\Omega}_B\mathbf{S}$, *where* $r = |A|$, *and let* $u = w_{\overline{\Omega}_B\mathbf{V}}(v_1, \ldots, v_r)$ *and* $m = |B|$. *Then*

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

THEOREM

Let $\varphi \in End(\overline{\Omega}_A\mathbf{V})$ *be a substitution. Then,*

$$\max_{a \in A} h\big(\varphi^\omega(a)\big) \leq \max_{a \in A} h\big(\varphi(a)\big).$$

Corollary

The complement of the minimum ideal of $\overline{\Omega}_A\mathbf{V}$ is a subsemigroup that is closed under composition and iteration.

- A weaker form of this result was previously obtained by the same authors in 2003 by a completely different approach:

Theorem

Let $\mathbf{H}$ be a pseudovariety of finite groups such that $\mathbf{H} \supseteq \mathbf{Ab}$. The smallest subset of $\overline{\Omega}_A\overline{\mathbf{H}}$ which contains A and is closed under multiplication, composition of operations and arbitrary powers has empty intersection with the minimum ideal.

- This was then obtained as a corollary of the following result, whose proof in turn depends on the theory of Burnside semigroups as developed by McCammond'1991, de Luca and Varricchio'1992, Guba'1993, and do Lago'1996:

THEOREM

Let $\mathbf{H}$ *be a pseudovariety of finite groups. Then the pseudovariety* $\overline{\mathbf{H}}$ *can be defined by a system of pseudoidentities using only multiplication and arbitrary powers if and only if membership of a finite group in* $\mathbf{H}$ *depends only on its cyclic subgroups.*

- This also implies the following ($100) conjecture of Rhodes'1986, which he had previously proved for $n \geq 665$, based on Adian's solution of the Burnside problem for groups:

COROLLARY

For all $n \geq 3$*, the pseudovariety* $\overline{\mathbf{Ab}} \cap [\![x^{2n} = x^n]\!]$ *is not equational.*

- View elements of $A^{\mathbb{Z}}$ as biinfinite words in the alphabet A, with a marked origin.
- The *shift mapping* shifts the origin but otherwise retains the the biinfinite word.
- By a *subshift* we mean a nonempty subset $\mathcal{X} \subseteq A^{\mathbb{Z}}$ that is stable under the shift (in either direction) and is closed for the product topology.
- It is well known that such sets $\mathcal{X}$ are completely characterized by their languages $L(\mathcal{X})$ of finite blocks, which are precisely the languages that are both factorial and prolongable.
- Since, for any language $L \subseteq A^+$, its closure $\overline{L} \subseteq \overline{\Omega}_A \mathbf{S}$ satisfies $\overline{L} \cap A^+ = L$, it follows that a subshift $\mathcal{X} \subseteq A^{\mathbb{Z}}$ is also completely determined by the set $\overline{L(\mathcal{X})}$.

- Subshifts are viewed as topological dynamical systems, consisting of a compact space and a continuous transformation of this space.
- As such, they are essentially unary topological algebras, which immediately gives a natural notion of isomorphism of subshifts, which is known as *conjugacy*.
- The fundamental problem in the area consists in classifying subshifts up to conjugacy.
- The problem has an algorithmic nature if the subshifts can be described by a finite amount of data.
- This is the case, for instance, for the classes of subshifts of finite type and, more generally, sofic subshifts.
- The decidability of conjugacy for subshifts in such classes remains an open problem.
- Hence the interest in looking for invariants for subshifts.

- Let $\mathcal{X} \subseteq A^{\mathbb{Z}}$ be an *irreducible* subshift, i.e.,

$$\forall u, w \in L(\mathcal{X})\ \exists v : \ uvw \in L(\mathcal{X}).$$

THEOREM

There is a unique minimal $\mathcal{J}$-class J of $\overline{\Omega}_A \mathbf{S}$ among those that contain elements of $\overline{L(\mathcal{X})}$.
The maximal subgroups of J are conjugation invariants $G(\mathcal{X})$ of $\mathcal{X}$.

- Associate with $\mathcal{X}$ a profinite graph $\Sigma(\mathcal{X})$ as follows:
  - the vertices are the elements of $\mathcal{X}$;
  - edges:

$$\cdots a_{-2}a_{-1} \cdot a_0 a_1 a_2 \cdots \longrightarrow \cdots a_{-2}a_{-1}a_0 \cdot a_1 a_2 \cdots$$

  - tolopogy: induced from $A^{\mathbb{Z}} \uplus A^{\mathbb{Z}} \times A^{\mathbb{Z}}$.
- Let $\hat{\Sigma}(\mathcal{X})$ denote the profinite semigroupoid freely generated by the profinite graph $\Sigma(\mathcal{X})$.

THEOREM

The semigroupoid $\hat{\Sigma}(\mathcal{X})$ is strongly connected if and only if $\mathcal{X}$ is irreducible,
in which case the maximal subgroups of the minimal ideals of the local subsemigroups are all isomorphic.
These groups are also isomorphic to $G(\mathcal{X})$.

- We know that the finite words are at the *top* of $\overline{\Omega}_A\mathbf{S}$ in the sense that the complement is an ideal.
- We have also seen that we cannot go very deep in $\overline{\Omega}_A\mathbf{S}$ by adding the ability to take arbitrary powers.

PROBLEM

Does the subalgebra of $\overline{\Omega}_A\mathbf{S}$ with respect to the signature consisting of multiplication and arbitrary powers generated by A also lie at the top?

- This problem becomes much more tractable if we reduce significantly the range of powers to be considered by identifying all infinite powers, that is in the *aperiodic* case.

- In the aperiodic case, we can take advantage of McCammond's normal form for the elements in our subalgebra of $\overline{\Omega}_A\mathbf{A}$, denoted $\Omega_A^\omega\mathbf{A}$.
- McCammond'2001 proved that it solves the word problem for $\Omega_A^\omega\mathbf{A}$ by applying his earlier solution of the word problem for free aperiodic Burnside semigroups.
- We have obtained a direct proof which also leads to new applications, among which the following

THEOREM

$\Omega_A^\omega\mathbf{A}$ sits at the top of $\overline{\Omega}_A\mathbf{A}$.

Theorem

An element w of $\overline{\Omega}_A\mathbf{A}$ belongs to $\Omega_A^\omega\mathbf{A}$ if and only if it satisfies the following two finiteness conditions:

1. *there are no infinite anti-chains of factors of w;*
2. *the language of McCammond normal forms of elements of $\Omega_A^\omega\mathbf{A}$ that are factors of w is rational.*

- We do not know whether the first condition is superfluous, that is whether it follows from the second one.

index