A GUIDE TO RECENT PROGRESS IN THE PROFINITE FRONT





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





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

ABCD Worshop on Equational Theory of Regular Languages

> Masaryk University Brno, 5 March, 2009

PRELIMINARIES

- Profinite semigroups
- V-recognizable languages
- Implicit operations
- The monoid of continuous endomorphisms

2 TAMENESS

- Implicit signatures
- Tameness
- Computing closures and fullness
- **3** Some case studies
 - Groups
 - p-groups
 - J-trivial
 - R-trivial
 - Aperiodic

4 STRUCTURE

- Equidivisibility
- Pseudovarieties closed under concatenation
- Connection with symbolic dynamics
- Subgroups and free submonoids

 Pseudovariety: class of finite semigroups (or of finite monoids) closed under taking homomorphic images, subsemigroups (resp. submonoids) and finite direct products.

$$S = \{all finite semigroups\}$$

$$\mathbf{G} = \{\text{groups}\}$$

$$\mathbf{G}_{p} = \{p\text{-groups}\}$$

$$\mathbf{G}_{sol} = \{ solvable groups \}$$

$$CR = \{unions of groups\}$$

- $N = {nilpotent semigroups}$
- $D = \{idempotents are right zeros\}$
- $\mathbf{K} = \{ \text{idempotents are left zeros} \}$
- **SI** = {semilattices}

$$\mathbf{J} = \{\mathcal{J}\text{-trivial}\}$$

$$\mathbf{R} = \{\mathcal{R}\text{-trivial}\}$$

$$L = \{\mathcal{L}\text{-trivial}\}$$

 $A = \{aperiodic semigroups\}$

$$\begin{aligned} \mathsf{D}\mathsf{V} &= \{ \text{regular } \mathcal{J}\text{-classes form subsemigroups in } \mathsf{V} \} \\ \mathsf{E}\mathsf{V} &= \{ S \in \mathsf{S} : \langle E(S) \rangle \in \mathsf{V} \} \\ \mathsf{L}\mathsf{V} &= \{ S \in \mathsf{S} : \forall e \in E(S), \ eSe \in \mathsf{V} \} \\ \mathsf{B}\mathsf{V} &= \{ S \in \mathsf{S} : every \ block \ of \ S \ belongs \ to \ \mathsf{V} \} \\ \bar{\mathsf{H}} &= \{ S \in \mathsf{S} : \forall H \in \mathsf{G} \ (H \leq S \implies H \in \mathsf{V}) \} \quad (\mathsf{H} \subseteq \mathsf{G}) \\ \mathcal{I} * \mathsf{W} &= \langle V * W : V \in \mathsf{V}, \ W \in \mathsf{W} \rangle \\ \hline \widehat{\mathcal{D}} \; \mathsf{W} &= \langle S \in \mathsf{S} : \exists T \in \mathsf{W} \ \exists \ homo. \ h : S \to T \ \forall e \in E(T), \ h^{-1}(t) \end{cases} \end{aligned}$$

- A topological semigroup is a semigroup S endowed with a topology such that the multiplication S × S → S is continuous.
- If X is a topological space, then a continuous mapping

 $\varphi: X \to S$ is said to generate S if $S = \overline{\langle \varphi(X) \rangle}$.

- We then also say that *S* is *X*-generated (via φ).
- A *compact semigroup* is a topological semigroup whose topology is compact (and Hausdorff).
- Finite semigroups are viewed as topological semigroups under the discrete topology.
- A *residually* V semigroup is a topological semigroup S such that

 $\forall s_1, s_2 \in S \left(s_1 \neq s_2 \implies \exists T \in \mathbf{V} \exists \text{ cont. homo. } h : S \rightarrow T : h(s_1) \neq h(s_2) \right)$

- A *pro-V semigroup* is a compact semigroup that is residually V.
- A *profinite semigroup* is a pro-**S** semigroup.
 - Equivalently, it is a compact totally disconnected semigroup.

• The free pro-V semigroup on a topological space X is defined by the following universal property: it is given by a continuous mapping $\iota : X \to \overline{\Omega}_X V$ into a pro-V semigroup such that, for every continuous mapping $\varphi : X \to S$ into a pro-V semigroup there is a unique continuous homomorphism $\hat{\varphi}$ such that the following diagram commutes



- The obvious way to *construct* Ω_XV is to take the direct product of all X-generated pro-V semigroups S_i, via φ_i (i ∈ I), in the category of all X-generated topological semigroups, that is the closure of the subsemigroup generated by {(φ_i(x))_{i∈I} : x ∈ X}.
 - In fact, it suffices to take X-generated semigroups from V.
 - This is usually viewed as the projective limit of all *X*-generated semigroups from **V**.

 Another convenient way to *construct* Ω_XV is to consider the following pseudo-metric on the free semigroup X⁺:

 $d(u,v)=2^{-r(u,v)}$

 $r(u, v) = \min\{|S| : S \in V, \exists \text{ cont. mapping } h : X \to S; S \not\models u = v[h]\}$

and to take the completion $\widehat{X^+}$, which is a metric space.

- The multiplication in X^+ is uniformly continuous with respect the pseudo-metric *d* and, therefore, it extends to a continuous multiplication on $\widehat{X^+}$.
- This only works well in case X is finite since otherwise Ω_XV is in general not metrizable.
- The problem lies in that, for X infinite, X^+ is in general not covered by finitely many balls of radius 2^{-n} (for instance if V is nontrivial and X is totally disconnected), which entails that the completion $\widehat{X^+}$ is not compact, and therefore not a pro-V semigroup.
- From hereon, unless something is explicitly stated to the contrary, *X* is taken to be a finite (discrete) set.

• A language $L \subseteq X^+$ is said to be V-recognizable if

$$\exists S \in \mathbf{V} \exists$$
 homo. $\varphi : X^+ \to S : L = \varphi^{-1} \varphi(L)$

- It is simple to show that L ⊆ X⁺ is V-recognizable if and only if, denoting *ī* : X⁺ → Ω_XV the natural homomorphism, *ī*(*L*) ⊆ Ω_XV is an open set
 L = *ī*⁻¹(*ī*(*L*)).
- The second condition is superfluous if *ī* is injective and the induced topology on X⁺ (the pro-V topology) is discrete.
- This is the case whenever $V \supseteq N$. In fact

PROPOSITION (JA-JCCOSTA-ZEITOUN)

 $\mathbf{V} \supseteq \mathbf{N}$ if and only if for every finite alphabet *X*, the natural mapping $X^+ \to \overline{\Omega}_X \mathbf{V}$ is injective and its image is an open discrete subset of $\overline{\Omega}_X \mathbf{V}$.

IMPLICIT OPERATIONS AND PSEUDOIDENTITIES

• The diagram describing the universal property of $X \to \overline{\Omega}_X \mathbf{V}$ suggests a natural way to interpret each $w \in \overline{\Omega}_X \mathbf{V}$ as an operation $w_S : S^X \to S$ on each pro-**V** semigroup *S*:



$$\mathbf{W}_{\mathcal{S}}(\varphi) = \hat{\varphi}(\mathbf{W})$$

- This interpretation commutes with all continuous homomorphisms between pro-V semigroups.
- Operations with this property with respect to a certain class of topological semigroups are called (|X|-ary) implicit operations on the class.
- In particular, the homomorphisms between the members of V respect the enriched algebraic structure, obtained by adding all such operations.
- It is well-known that the correspondence w → (w_S)_{S∈V} is a bijection from Ω_XV to the set of all |X|-ary implicit operations on V.

Descriptive power of $\overline{\Omega}_X \mathbf{V}$

- Given $u, v \in \overline{\Omega}_X V$ and a pro-V semigroup *S*, we write $S \models u = v$ if $u_S = v_S$.
- Such a formal equality u = v is known as a (V-)pseudoidentity.
- Given a set Σ of pseudoidentities, the class

$$\llbracket \Sigma \rrbracket_{\mathbf{V}} = \{ \boldsymbol{S} \in \mathbf{V} : \forall \sigma \in \Sigma, \ \boldsymbol{S} \models \sigma \}$$

THEOREM (**REITERMAN**)

Every subpseudovariety of V is of this form.

• In case V = S, we drop the index V.

EXAMPLES

- Note that, every profinite semigroup S, given s ∈ S, the sequence (s^{n!-1})_n converges to some element, denoted s^{ω-1}.
- In fact, s^{ω-1} is the inverse of *es* in the group minimum ideal of ⟨s⟩, with idempotent *e* = s^{ω-1}s.
- We naturally also write s^{ω} for $ss^{\omega-1}$ and $s^{\omega+1}$ for ss^{ω} .

- Let *S* be a compact semigroup. Then the continuous endomorphisms of *S* constitute a monoid *End*(*S*) under composition.
- As a function space, there are two classical candidates for topologies on End(*S*), namely:
 - the pointwise convergence topology, i.e., as a subspace of the product space S^S or in which a sequence converges if and only if it converges pointwise;
 - the *compact open topology*, which in our context can be described by stating that a sequence converges if and only if it converges it converges uniformly.
- The former topology is in a sense very familiar while the latter has the advantage that the *evaluation mapping*

$$\mathsf{End}(\mathcal{S}) imes \mathcal{S} \longrightarrow \mathcal{S} \ (arphi, oldsymbol{s}) \longmapsto arphi(oldsymbol{s})$$

is continuous.

THEOREM (JA (2003))

If S is a finitely generated profinite semigroup, then the two topologies coincide on End(S) and End(S) is a profinite semigroup with respect to them.

- In particular, if *X* is a finite set and **V** is any pseudovariety of semigroups, given $\varphi \in \text{End}(\overline{\Omega}_X \mathbf{V})$, there is an idempotent $\varphi^{\omega} = \lim_{n \to \infty} \varphi^{n!}$, which we view as a canonical infinite iteration of the *substitution* φ .
- For example, the substitution φ(x) = x^ρ, where x is a variable, induces the idempotent φ^ω ∈ End(Ω
 [x]S), which satisfies

$$\varphi^{\omega}(x) = \lim_{n \to \infty} \varphi^{n!}(x) = \lim_{n \to \infty} x^{p^{n!}}.$$

We define $x^{p^{\omega}}$ to be $\varphi^{\omega}(x)$. It is easy to show that

$$\mathbf{G}_{\boldsymbol{\rho}} = \llbracket \boldsymbol{x}^{\boldsymbol{\rho}^{\omega}} = \mathbf{1} \rrbracket.$$

 Let σ be a set of implicit operations (on S), containing the binary multiplication. We call σ an *implicit signature*.

• *Canonical* example: $\kappa = \{_\cdot_, _^{\omega-1}\}.$

- Recall that every profinite semigroup has a natural structure as a σ -algebra.
- Given a pseudovariety V and a finite set X, let ι : X → Ω_XV be the natural mapping.
- Denote by $\Omega_X^{\sigma} \mathbf{V}$ the σ -subalgebra generated by $\iota(X)$. The mapping $X \to \Omega_X^{\sigma} \mathbf{V}$ determined by ι has the suitable universal property of the *free* σ -algebra on X in the Birkhoff variety generated by \mathbf{V} :



where now *S* is any member of the variety and $\hat{\varphi}$ is a homomorphism of σ -algebras.

We say that a system of equations (u_i = v_i)_{i∈l} over an alphabet X, with a set of clopen constraints K_x ⊆ Ω_AS has a solution γ modulo V if γ : Ω_XS → Ω_AS is a continuous homomorphism such that the following two conditions hold:

$$\forall x \in X, \ \gamma(x) \in K_x; \\ \forall i \in I, \ \mathbf{V} \models \gamma(u_i) = \gamma(v_i).$$

We say that V is *σ*-reducible with respect to a class C of constrained systems of equations if every constrained system in the class that has a solution *γ* : Ω_XS → Ω_AS modulo V admits such a solution satisfying *γ*(X) ⊆ Ω^σ_AS.

TAMENESS

- Finally, we say that V is σ-tame with respect to a class C of constrained systems of equations if σ is an implicit signature such that:
 - **1** σ is recursively enumerable;
 - 2) the operations in σ are computable;
 - **(3)** the word problem for $\Omega_X^{\sigma} \mathbf{V}$ is decidable for every finite set X;
 - **V** is σ -reducible with respect to C.
- If this property holds, then
 - in case C consists of all constrained systems of equations associated with finite digraphs

$$x \xrightarrow{y} z \longmapsto xy = z$$

we simply say that **V** is σ -tame;

 in case C consists of all constrained systems of equations of the form u = v with u, v ∈ Ω^σ_XS, we say that V is completely σ-tame.

- Given a subset L ⊆ S of a topological semigroup, let cl_S(L) denote its closure.
 - In the special case $S = \overline{\Omega}_X \mathbf{S}$, we let $cl(L) = cl_{\overline{\Omega}_X \mathbf{S}}(L)$.
 - If $S = \overline{\Omega}_X V$, we let $cl_{\sigma,V}(L) = cl_{\Omega_X^{\sigma}V}(L)$.
- We say that the pseudovariety V is *σ*-full if it satisfies the following condition for every rational language L ⊆ X⁺:

 $\operatorname{cl}_{\sigma,\mathbf{V}}(L) = p_{\mathbf{V}}(\operatorname{cl}(L) \cap \Omega_X^{\sigma} \mathbf{S})$

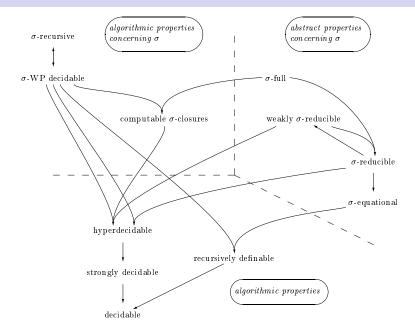
THEOREM (JA-STEINBERG (2000))

If **V** is a recursively enumerable pseudovariety of semigroups and σ is a recursively enumerable implicit signature consisting of computable operations such that the word problem for Ω_X^{σ} **V** is decidable and **V** is σ -full, then there is an algorithm to compute the closure $cl_{\sigma,\mathbf{V}}(L) \subseteq \Omega_X^{\sigma}$ **V** for every rational language $L \subseteq X^+$.

- The proof of the preceding theorem is obtained by exhibiting two semi-algorithms, one for enumerating the elements in the closure, the other for its complement.
- Given a rational expression for the language, can one do better?
- For a subset *L* of a *σ*-algebra *S*, denote by (*L*)_σ the *σ*-subalgebra generated by *L*.
- We say that the *Pin-Reutenauer procedure holds for a* pseudovariety V in the implicit signature σ if, for all rational languages K, L ⊆ X⁺, the following equations hold:

$$\begin{aligned} \mathrm{cl}_{\sigma,\mathbf{V}}(\mathsf{KL}) &= \mathrm{cl}_{\sigma,\mathbf{V}}(\mathsf{K}) \cdot \mathrm{cl}_{\sigma,\mathbf{V}}(\mathsf{L}), \\ \mathrm{cl}_{\sigma,\mathbf{V}}(\mathsf{L}^+) &= \langle \mathrm{cl}_{\sigma,\mathbf{V}}(\mathsf{L}) \rangle_{\sigma}. \end{aligned}$$

A DIAGRAM BORROWED FROM JA-STEINBERG (2000)



G (GROUPS)

 Ω^κ_XG is the free group on X and so the solution of the word problem for Ω^κ_XG is simple and well known.

THEOREM (ASH (1991) + JA-STEINBERG (2000))

G is κ -tame.

THEOREM (PIN-REUTENAUER (1991) + RIBES-ZALESSKIĬ (1993) OR ASH (1991))

The Pin-Reutenauer procedure holds for G.

THEOREM (DELGADO (2001))

G is κ -full.

THEOREM (COULBOIS-KHÉLIF (1999))

G is not completely κ -tame.

\mathbf{G}_{p} (*p*-GROUPS)

- Since the free group is residually G_p [Baumslag (1965)],
 G_p cannot be κ-tame.
- G_ρ is not κ-full either [Steinberg (2001)].

Theorem (JA (2002), building on results of Ribes-Zalesskiı (1994), Margolis-Sapir-Weil (2001), Steinberg (2001))

Let **H** be an extension-closed pseudovariety of finite groups. If there is an algorithm to decide whether a finite subset of the free group Ω_X^{κ} **G** generates a dense subgroup in the pro-**H** topology (i.e., in the subspace topology Ω_X^{κ} **G** = Ω_X^{κ} **H** $\subseteq \overline{\Omega}_X$ **H**), then **H** is σ -tame, for a certain infinite implicit signature constructed by the infinite iteration of appropriate substitutions.

• From the proof of this result, it follows that **H** is σ -full.

Ribes-Zalesskiĭ (1994): an algorithm to compute the closure cl_{κ,G_ρ}(L) ⊆ Ω^κ_XG_ρ for a rational language L ⊆ X⁺.

COROLLARY

 \mathbf{G}_{p} is tame.

- Can one decide denseness of finitely generated subgroups of the free group for the pro-**G**_{sol} topology?
- Likewise for the pro-G_{odd} topology?

THEOREM

- The variety of κ-algebras generated by J is defined by the identities

$$x^{\omega-1}x = xx^{\omega-1} = x^{\omega-1}, \ (x^{\omega})^{\omega} = x^{\omega} (xy)z = x(yz), \ (xy)^{\omega} = (yx)^{\omega} = (x^{\omega}y^{\omega})^{\omega}$$

- Solution of the word problem for $\Omega_X^{\kappa} \mathbf{J}$.
- **3** J is completely κ -tame.
- J is κ-full.
- The Pin-Reutenauer procedure holds for J. (Follows from the results presented by M. Zeitoun.)

- JA-Weil (1997), JA-Zeitoun (2007): structural descriptions of Ω_A**R**.
- JA-Zeitoun (2007): efficient solution of the word problem for Ω^κ_X**R**.
- JA-JCCosta-Zeitoun (2007): **R** is completely *κ*-tame
- JA-JCCosta-Zeitoun: R is κ-full and the Pin-Reutenauer procedure holds for R. (See M. Zeitoun's talk.)
- Partial extension:
 - Moura: structural description of Ω_XDA and solution of the word problem for Ω^κ_XDA.

- McCammond (2001): an algorithm to decide the word problem for Ω^κ_XA.
- The algorithm consists in the rewriting of any given description of an element of Ω^κ_XA, as a κ-term, in a certain normalized form.
- The hard part of the proof of correctness of the algorithm consists in showing that distinct κ-terms in normal form represent distinct elements of Ω^κ_XA.
- McCammond's proof uses his own solution (1991) of the word problem for free Burnside semigroups

$$\langle X: \forall t, t^{n+1} = t^n \rangle$$

for sufficiently large *n* (which he had achieved for $n \ge 6$).

A NEW PROOF

- JA-JCCosta-Zeitoun: a new proof of correctness of McCammond's algorithm is obtained as follows:
 - to each κ-term w, a descending sequence L_n(w) of rational languages is associated;
 - L_n(w) is shown to be star-free (i.e., A-recognizabe [Schützenberger (1965)]) provided w is in normal form and n is sufficiently large;
 - for distinct κ -terms in normal form v and w, it is shown that $L_n(v) \cap L_n(w) = \emptyset$ for sufficiently large n.

See J. C. Costa's talk for details.

- So far, complete structural results for relatively free profinite semigroups Ω_XV concern relatively small pseudovarieties, like J, R, DA, CR [JA-Trotter (2001)] and some related pseudovarieties.
- These are all subpseudovarieties of **DS**, a pseudovariety for which there are plenty of idempotents: it is precisely characterized by the property that every regular *H*-class contains an idempotent.
- Outside **DA**, there are not many cases for which the structure has been identified.
- Examples are the pseudovarieties LSI = SI * D and ESI = SI * G, usually taking advantage of such decompositions to obtain the desired structural results.
 - JCCosta-Nogueira: LSI is completely κ -tame.

- For *large* pseudovarieties, say containing **A**, there are so far no such structural results but only partial information.
- There is nevertheless a free semigroup-like property that many large pseudovarieties share that may lead to complete structural results: *equidivisibility*.
- A *refinement* of a factorization $s_1 \cdots s_n$ in a semigroup is obtained by further factorizing some (possibly none) of the factors.
- A semigroup *S* is said to be *equidivisible* [McKnight-Storey (1969)] if any two factorizations of the same element admit a common refinement.

PROPOSITION (JA-ACOSTA (2009))

If **V** is a pseudovariety closed under concatenation, then $\overline{\Omega}_X \mathbf{V}$ is equidivisible.

THEOREM (STRAUBING (1979))

A pseudovariety V is closed under concatenation if and only if it satisfies the equation $V = A \bigoplus V$.

- It is easy to deduce that every pseudovariety of the form H
 , where H is a pseudovariety of groups, is closed under concatenation.
- In particular, $\overline{\Omega}_X \mathbf{S}$ and $\overline{\Omega}_X \mathbf{A}$ are equidivisible.

THEOREM (JA-ACOSTA-JCCOSTA-ZEITOUN)

The following are equivalent for $V \supseteq N \cap Com$:

• V is closed under concatenation;

2 $A \odot V = V;$

- the multiplication $\overline{\Omega}_X \mathbf{V} \times \overline{\Omega}_X \mathbf{V} \to \overline{\Omega}_X \mathbf{V}$ is an open mapping for every finite set *X*;
- (lifting factorizations) for every finite set X, if $u, v, w \in \overline{\Omega}_X S$ are such that $\mathbf{V} \models uv = w$ then there is a factorization w = u'v' in $\overline{\Omega}_X S$ such that $\mathbf{V} \models u = u', v = v'$.

COROLLARY

If **V** is closed under concatenation and the products $u_1 \cdots u_m$ and $v_1 \cdots v_n$ of elements of $\overline{\Omega}_X \mathbf{S}$ coincide in **V**, then they admit refinements whose factors in corresponding positions are equal over **V**.

- By a subshift over a finite alphabet X we mean a closed subset of X^ℤ that is stable under arbitrary shifts of the origin (in the elements of X^ℤ, which are viewed as bi-infinite words in the letters of X).
- It is well known that a subshift X is characterized by its language of finite blocks (or finite factors) L(X), which is an arbitrary factorial extendable language.

THEOREM (JA (2005,2007))

For every $V \supseteq LSI$, the correspondence

$$\mathcal{S}\longmapsto \mathcal{J}(\mathcal{X})=\overline{\mathcal{L}(\mathcal{X})}\setminus \mathcal{X}^+\subseteq\overline{\Omega}_{\mathcal{X}}\mathbf{V}$$

defines a bijection between minimal subshifts and the \mathcal{J} -maximal regular \mathcal{J} -classes of $\overline{\Omega}_X \mathbf{V}$.

• We say that an endomorphism φ of X^+ is *primitive* if

 $\exists n \ \forall x, y \in X, x \text{ apears in } \varphi(y).$

- The continuous extension φ̂ to Ω_XS of an endomorphism φ of X⁺ is also called a *finite substitution (of X)*.
- A finite substitution φ (of X) defines a subshift X_φ whose finite factors are the factors of some φⁿ(x) for arbitrarily large n.
- It is well known that, if φ is primitive, then X_φ is a minimal subshift.

Theorem (JA (2005,2007))

Let $\varphi \in End(\overline{\Omega}_X S)$ be a finite primitive substitution. If φ induces an automorphism of the free group $\Omega_X^{\kappa} G$, then the maximal subgroups of $J(\mathcal{X}_{\varphi})$ are finitely generated free profinite groups.

• For further recent developments, se A. Costa's talk.

 So, just which profinite groups may appear as closed subgroups of free profinite semigroups?

THEOREM (RHODES-STEINBERG (2008))

Precisely the same that appear as closed subgroups of free profinite groups, namely the projective profinite groups.

• What about clopen subsemigroups?

THEOREM (JA-STEINBERG (2009))

Let **H** be an extension-closed pseudovariety of groups and X a finite set. Then the free clopen subsemigroups of $\overline{\Omega}_X \overline{\mathbf{H}}$ are the closures of $\overline{\mathbf{H}}$ -recognizable free subsemigroups of X⁺.

• See B. Steinberg's talk for more details and results on the minimum ideal.