Rational Codes
and
Free Clopen Submonoids of Free Profinite Monoids

Benjamin Steinberg
(Carleton University)

joint work with

Jorge Almeida (University of Porto)

E-mail:

`bsteinbg@math.carleton.ca`

Webpage:

`http://www.mathstat.carleton.ca/~bsteinbg`

Profinite spaces

- A profinite space is a compact totally disconnected space.
- M. Stone in the 30s defined a duality between Boolean algebras and profinite spaces associating to each profinite space its Boolean algebra of clopen subsets.
- E.g. A^ω is the Stone dual of the Boolean algebra of finitely generated right ideals of A^*.
- Almeida observed the Stone dual of $\mathrm{Rat}(A^*)$ is the free profinite monoid $\widehat{A^*}$.
- The isomorphism corresponds $L \in \mathrm{Rat}(A^*)$ with $\overline{L} \subseteq \widehat{A^*}$ and a clopen subset K of $\widehat{A^*}$ with $K \cap A^*$.
- If M is any monoid, then its profinite completion $\widehat{M}$ is the Stone dual of $\mathrm{Rec}(M)$.

Construction of the Free Profinite Monoid

- Let A be a finite alphabet.
- Define the *complexity* of a rational language to be the size of its syntactic monoid.
- For words $u, v \in A^*$, define their *separation number* $\mathrm{sep}(u, v)$ to be the minimal complexity of a rational language containing u, but not v.
- Define the profinite metric on A^* by

$$d(u, v) = 2^{-\mathrm{sep}(u,v)}$$

- It is an ultrametric:

$$d(u, v) \leq \max\{d(u, w), d(w, v)\}.$$

- The completion $\widehat{A^*}$ is the free profinite monoid on A.
- Any map from A to a profinite monoid extends continuously to $\widehat{A^*}$.

History

- (1982) Reiterman proves a Birkhoff theorem for finite algebras using profinite algebras.
- (Late 80s) Almeida pushes profinite methods in finite semigroup theory.
- (Early 90s) Almeida's book appears. Almeida asks: does a free profinite semigroup on n generators embed as a closed submonoid of a free profinite monoid on 2 generators?
- (1995) Koryakov shows the prefix code $C_n = \{y, xy, \ldots, x^{n-1}y\}$ freely generates a free clopen submonoid of $\widehat{\{x, y\}^*}$.
- (1998) Margolis, Sapir and Weil prove any finite code $C \subseteq A^*$ freely generates a free clopen profinite submonoid of $\widehat{A^*}$.
- As an application they prove the variety of all rational subsets is join irreducible in the lattice of varieties of formal languages.

History II

- (1999) Almeida and Volkov give examples of maximal subgroups of free profinite monoids that are free profinite groups. Question arises are maximal subgroups free or at least projective profinite groups?
- (2005) Almeida gives a bijection between minimal symbolic dynamical systems in A^ω and maximal principal ideals of $\widehat{A^*} \setminus A^*$.
- He associates in this way a maximal subgroup to each such dynamical system and shows certain systems give free profinite groups.
- He finds the first non-free maximal subgroup, but it is projective.
- (2005) Almeida presents these results at Fields Institute Workshop on Profinite Groups at Carleton. Lubotzky asks whether maximal subgroups must be projective.

History III

- (August 2005) Motivated by this question, Almeida and I classify all free clopen submonoids of $\widehat{A^*}$ (today's talk).
- (November 2006) Rhodes and I answer Lubotzky's question in the affirmative: Closed subgroups of free profinite monoids are precisely the projective profinite groups.
- As an application we prove free profinite monoids are torsion-free.
- Projective profinite groups are precisely Galois groups of pseudo-algebraically closed fields.
- Almeida's profinite group associated to a minimal dynamical system should link symbolic dynamics with field theory.

A Topological Obstruction

- One would guess that free clopen submonoids correspond bijectively to rational codes.
- An obstruction: If X is an infinite discrete set, then $\overline{X} \subseteq \widehat{X^*}$ must be the Stone-Czech compactification βX by abstract nonsense.
- βX is highly non-metrizable.
- $\widehat{A^*}$ is metrizable when A is finite.
- Conclusion: if C is an infinite code, then $\overline{C^*} \subseteq \widehat{A^*}$ cannot be freely generated by C.
- But $\overline{C}$ is a clopen subspace of $\widehat{A^*}$ and there is an obvious (and useful) notion of a free profinite monoid on a profinite space. So perhaps $\overline{C^*}$ is free on $\overline{C}$?

More Problems

- It is true that every clopen subgroup of a free profinite group is again a free profinite group.
- If $U \subseteq \widehat{FG(A)}$ is clopen, $U \cap FG(A)$ is a finite index subgroup, necessarily free by Nielsen-Schreier.
- If K is a free clopen submonoid of $\widehat{A^*}$, there is no reason *a priori* $K \cap A^*$ is a free submonoid (perhaps the basis of K is some strange closed subset which is not clopen).

The Main Result

Theorem 1 (Almeida, BS). *The clopen free profinite submonoids of* $\widehat{A^*}$ *are precisely the closures of rational free submonoids of* A^**. Moreover, if* C *is a rational code, then* $\overline{C}$ *is the unique closed basis for* $\overline{C^*}$*.*

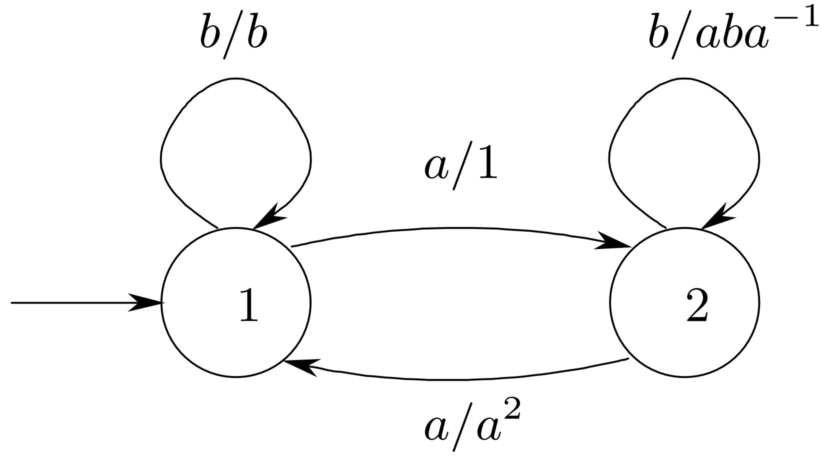
- If K is a clopen submonoid, a topological argument lets us deduce $K \cap A^*$ is free. The key point is that A^* is discrete in $\widehat{A^*}$ so we may deduce the basis for K is clopen.
- The difficult direction uses the theory of unambiguous automata and unambiguous wreath products.
- The idea follows that of Margolis, Sapir and Weil, but there is a difficulty arising from lack of a "canonical" unambiguous finite automaton for an infinite rational code.

The Case of Groups

- Usual proof uses cosets; this proof is mine.
- Let $U \leq \widehat{FG(A)}$ be clopen, so U has finite index and $H := U \cap FG(A)$ is finite index.
- Let $\varphi : H \to G$ be a homomorphism with G a finite group. We must show φ extends continuously to U.
- Consider the representation τ of $FG(A)$ by permutation matrices associated to the action on $FG(A)/H$.
- Essential idea: Reidemeister-Schreier rewriting is a rational transduction from $FG(A)$ to H (extending the identity map on H) and so yields a wreath product embedding.

The Case of Groups II

- For example, take $H = \langle b, aba^{-1}, a^2 \rangle$.



- $a \longmapsto \begin{pmatrix} 0 & 1 \\ a^2 & 0 \end{pmatrix}$, $b \longmapsto \begin{pmatrix} \boxed{b} & 0 \\ 0 & aba^{-1} \end{pmatrix}$

- $a^2 \longmapsto \begin{pmatrix} \boxed{a^2} & 0 \\ 0 & a^2 \end{pmatrix}$

- $aba^{-1} \longmapsto \begin{pmatrix} \boxed{aba^{-1}} & 0 \\ 0 & a^2ba^{-2} \end{pmatrix}$

The Case of Groups III

- $FG(A)$ embeds in the wreath product of $H \wr \tau$. This wreath product consists of all matrices obtained by replacing 1s in the permutation matrices of τ by elements of H.
- Embedding takes elements $h \in H$ to a block form $\begin{pmatrix} \boxed{h} & 0 \\ 0 & * \end{pmatrix}$.
- Apply $\varphi : H \to G$ entrywise to get a map $FG(A)$ to $G \wr \tau$, a finite group, and extend to $\widehat{FG(A)}$.
- Restricting to the upper left entry gives our extension of φ to U.

The Case of Finite Codes

- Let $C \subseteq A^*$ be a finite code. The Sagittal automaton $\mathrm{Sag}(C)$ is:
  - States: proper prefixes of C
  - Initial/terminal state: 1
  - Transitions: $p \xrightarrow{a/1} q$ if $pa = q$ and q is a proper prefix; $p \xrightarrow{a/pa} 1$ if $pa \in C$
- $\mathrm{Sag}(C)$ is unambiguous and recognizes C^*.
- Let τ be the associated unambiguous matrix representation of A^*.
- Then A^* embeds in the unambiguous wreath product $C^* \wr \tau$ and $u \in C^*$ maps to a matrix with itself in the upper left entry.
- Same proof as group case works.

The Case of Rational Codes

- Let $C \subseteq A^*$ be a rational code.
- In this setting there is no canonical wreath product embedding of A^* into $C^* \wr \tau$.
- Suppose $\varphi : C \to M$ is a map with M a finite monoid, which extends continuously to $\overline{C}$. We need to extend it to $\overline{C^*}$.
- Definition of the topology yields a homomorphism $\gamma : A^* \to N$ with N a finite monoid so that $\ker \gamma|_C$ refines $\ker \varphi$.
- Recognize C by the automaton $\mathscr{A}$ obtained from the direct product of its minimal automaton with the Cayley graph of N.

The Case of Rational Codes II

- One can construct an unambiguous automaton $\mathscr{A}^*$ from $\mathscr{A}$ accepting C^* by a standard method:
  - Add a new state that is both initial and terminal, which simulates the original initial state and all terminal states.
- Let τ be the associated unambiguous matrix representation of A^*.
- We have no natural map of A^* into the wreath product $C^* \wr \tau$.
- But we can go directly via φ to the wreath product $M \wr \tau$ instead! (recall $\varphi : C \to M$ was our original map to extend)
- Getting the map well defined relies on the map $\gamma : A^* \to N$ with $\gamma|_C$ refining φ and that $\mathscr{A}$ contains the Cayley graph of N as a factor.
- C'est Tout!