On the presentation of (semi)groups defined by Mealy machines

Emanuele Rodaro

Department of Mathematics
Politecnico di Milano

05/05/2021

Describe a semigroup

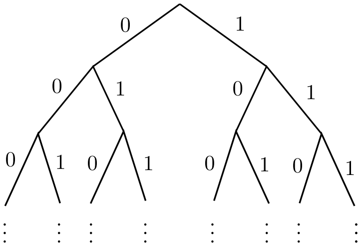
- Traditional presentation of a semigroup S: $\langle Q \mid R \rangle$, where Q set of generators, and relations $R \subseteq Q^+ \times Q^+$. For instance:

$$\langle a, b, c \mid ab = ba, bc = cb \rangle$$

  $S \simeq Q^+/\rho$, ρ the smallest congruence containing the relations R.
- Alternative: describing the action of that semigroup on some geometric object.

Action on a rooted tree

- Regular rooted tree on a finite alphabet Σ, i.e., Σ^*



- Semigroup $S \hookrightarrow End(\Sigma^*)$ acting faithfully on Σ^*, action: $\forall g \in S, w \in \Sigma^*$ $g \circ w$, and length preserving: $|g \circ w| = |w|$.
- The action is self-similar if:

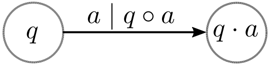
$$g \circ (aw) = (g \circ a)(g' \circ w) \quad \forall w \in \Sigma^*, a \in \Sigma$$

for some $g' \in S$.

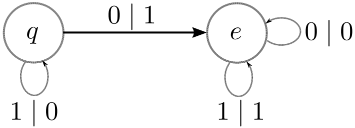
- $g' \in S$ is called the restriction of g by a, denoted $g \cdot a$.

Self-similar semigroups via transducers/automata

- Suppose that S is generated by a (finite) set Q.
  If $q \cdot a \in Q$ *for all* $a \in \Sigma$, we may associate a finite automaton (Mealy automaton) with set of states Q on the alphabet Σ and transitions:



- The adding machine: $Q = \{q, e\}$, $\Sigma = \{0, 1\}$



$$q \circ (1101) = (q \circ 1)\,(q \cdot 1) \circ (101)$$

$$q \circ (1110) = 0\,q \circ 101$$

$$q \circ (1101) = 0\,q \circ 101 = 0\,(q \circ 1)\,(q \cdot 1) \circ (01)$$

Automata semigroups

- Mealy automaton (simply an automaton), is an alphabetical transducer: $\mathscr{A} = \langle Q, \Sigma, \delta, \lambda \rangle$, with two (in general partial) functions:
  - $\lambda : Q \times \Sigma \to \Sigma$ is the output (partial) function;
  - $\delta : Q \times \Sigma \to Q$ is the restriction (partial) function;

  Transition can be depicted: $q \xrightarrow{a|b} p$, whenever $\lambda(q, a) = b$ and $\delta(q, a) = p$.
  The automaton is deterministic: $\forall a \in \Sigma, q \in Q$ there is at most one transition $q \xrightarrow{a|b} p$.
- Q acts (partially) on Σ on the left: $\lambda(q, a) = b \Rightarrow q \circ a = b$, Σ acts (partially) on Q on the right: $\delta(q, a) = p \Rightarrow q \cdot a = p$.
- Each state q of $\mathscr{A}$ acts (partially) on the free monoid Σ^*:

$$q \circ (a_1 a_2 a_3 \dots a_k) = (q \circ a_1)[q \cdot a_1] \circ (a_2 a_3 \dots a_k)$$

- This action on the rooted tree Σ^* may be extended to Q^* giving rise to a semigroup $\mathcal{S}(\mathscr{A})$, called an automaton semigroup.

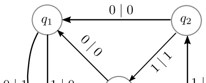
Completeness and invertibility

- The action is full = completeness of the automaton $\forall a \in \Sigma, q \in Q$ there is a transition $q \xrightarrow{a|b} p$
- If the automaton is inverse deterministic: swap input with output, we obtain an automaton $\mathscr{A}^{-1}$ that is still deterministic.
- In this case we may also consider the action of the states Q^{-1} on Σ^*, giving rise to partial one-to-one action. In this case $\mathcal{S}(\mathscr{A} \cup \mathscr{A}^{-1})$ is an *inverse semigroup*.

Theorem (D'Angeli, R., Wächter, Semigr. Forum)

An automaton semigroup that is an inverse semigroup is also defined by an automaton that is inverse deterministic.

- In case $\mathscr{A}$ is inverse deterministic and complete $\mathcal{S}(\mathscr{A} \cup \mathscr{A}^{-1})$ is a group (denoted by $\mathcal{G}(\mathscr{A})$).
- Automata groups: a source of important examples, like the Grigorchuk group (intermediate growth (Milnor problem), Burnside problem).



Structure of an automaton (semi)group: open problems

- Very few is known: residually finite, word problem is decidable, conjugacy problem undecidable (automata groups), order problem undecidable (automata groups)...
- Checking whether an automaton semigroup is finite is undecidable, for automata groups is still open.
- Understanding the kind of (semi)group defined by an automaton is very difficult.
- There are not tools to disprove if a semigroup is NOT an automaton semigroup (a kind of "pumping lemma").

The standard presentation and the freeness problem

Checking whether an automaton group is free is very difficult, and there are few examples of automata groups defining a free group.

The Freeness problem (Grigorchuk, Nekrashevych and Sushchansky)

Given an automaton group (complete, inverse deterministic automaton) $\mathscr{A}$, is it decidable to check whether $\mathcal{G}(\mathscr{A})$ is free? What about $\mathcal{S}(\mathscr{A})$?

The standard presentation and the freeness problem

- Given an automaton $\mathscr{A} = \langle Q, \Sigma, \delta, \lambda \rangle$, the (standard) presentation of the semigroup $\mathcal{S}(\mathscr{A})$ is $\langle Q \mid R \rangle$ where $R \subseteq Q^* \times Q^*$;
- we have a non-trivial relation $(u, v) \in R$ (written also as $u = v$) if and only if

$$u \circ w = v \circ w \text{ for all } w \in \Sigma^* \quad u \neq v$$

- Finding/describing a defining relation is also quite difficult

Emptiness of the defining relations for the standard presentation

- input: An automaton (semi)group $\mathscr{A} = \langle Q, \Sigma, \delta, \lambda \rangle$;
- output: Is the set $R \neq \emptyset$?

An intermediate step: positive relations

Theorem (D'Angeli, R., Wächter, Isr. J. Math.)

The following algorithmic problem:

- *Input: An automaton group* $\mathscr{A}$ *(complete inverse-deterministic);*
- *Output:* $\mathcal{P}(\mathcal{T}) = \{u \in Q^* : u = 1 \text{ in } \mathcal{G}(\mathscr{A})\} \neq \emptyset$*?*

is undecidable.

- Some connection with the dynamics in the boundary: the emptiness of $\mathcal{P}(\mathcal{T})$ implies that almost all orbital graphs in the boundary of the tree Σ^* are either finite or acyclic.

Idea of the proof

Idea of the proof:

- Modifying a construction of Brunner and Sidki (rediscovered by Sunic and Ventura): given a set of $d \times d$ matrices $\mathcal{M}$ over $\mathbb{Z}$ and a finite set of d-vectors V over $\mathbb{Z}$ it is possibile to construct an automaton $\mathscr{M}$ s.t. $\mathcal{S}(\mathscr{M})$ is isomorphic to the semigroup generated by the affine transformations $u \mapsto v + Mu$, $M \in \mathcal{M}, v \in V$;
- By taking the matrices invertible, $\mathscr{M}$ becomes an automaton group;
- The identity correspondence problem is undecidable (Bell and Potapov): $\{(u_1, v_1), \ldots, (u_n, v_n)\}$ with $u_i, v_i \in FG(A)$, is there a sequence $i_1, \ldots, i_k \in [1, n]$ such that $u_{i_1} \ldots u_{i_k} = v_{i_1} \ldots v_{i_k} = 1$ in $FG(A)$;
- Reduce the previous problem to the non-emptiness of $\mathcal{P}(\mathscr{M})$ via the usual embedding of $FG(a, b)$ into $SL_2(\mathbb{Z})$:

$$\rho : a \mapsto \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \rho : b \mapsto \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Idea of the proof

- For each (u_i, v_i) consider the 4×4 matrix

$$M_i = \begin{pmatrix} \rho(u_i) & O_2 \\ O_2 & \rho(v_i) \end{pmatrix}$$

- Then it is possibile to prove that $\mathcal{P}(\mathscr{M}) \neq \emptyset$ iff and only if there is a sequence of integers $i_1, \ldots, i_k \in [1, n]$ such that

$$M_{i_1} \ldots M_{i_k} = I$$

  if and only if $u_{i_1} \ldots u_{i_k} = v_{i_1} \ldots v_{i_k} = 1$ in $FG(A)$.

Freeness for automata monoids

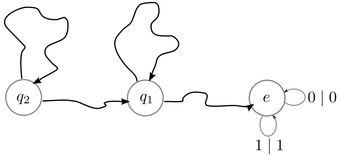
Theorem (D'Angeli, R., Wächter)

The following algorithmic problem:

- *Input: An automaton monoid $\mathscr{B}$ (complete deterministic);*
- *Output: Is $\mathcal{S}(\mathscr{B})$ free?*

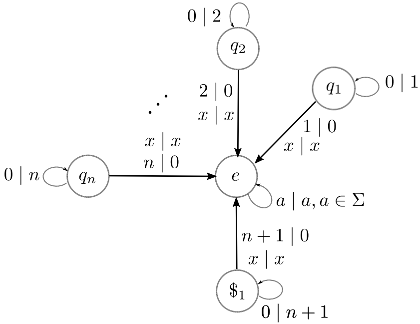
is undecidable.

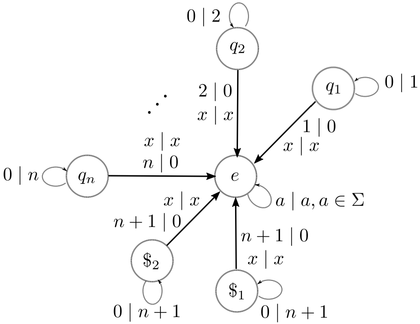
- It is possibile to show that the activity of $\mathscr{B}$ is cubic;
- Activity (notion introduced by S.Sidki): roughly speaking there is a state e acting like the identity, and the activity is a measure of the growth of the number of paths not ending in the state e;
- Here each state $q \neq e$ has a unique cycle, cycles do not intersect: in this case the activity is linear;



Sketch of the proof: existence of free monoid of any rank

- The proof heavily relies on the existence of a bounded activity automaton group whose semigroup is a free monoid of rank sufficiently large;
- In our case: automaton group $\mathcal{F}'$ on $Q' = \{e, q_1 \dots, q_n, \$_1\}$, $\Sigma' = \{0, 1, \dots, n+1\}$ with $\mathcal{S}(\mathcal{F}')$ free monoid of rank $n+1$;
- We duplicate the dollar state obtaining a new automaton $\mathcal{F}$ on $Q = \{e, q_1 \dots, q_n, \$_1, \$_2\}$





Sketch of the proof: reduction to PCP

- In this way the defining relations of $\mathcal{S}(\mathcal{F})$ are the form:

$$w_1\$_{i_1}w_2\$_{i_2}\dots w_\ell\$_{i_\ell}w_{\ell+1} = w_1\$_{j_1}w_2\$_{j_2}\dots w_\ell\$_{j_\ell}w_{\ell+1}$$

  $w_i \in \{e, q_1, \dots, q_n\}^*$

- By increasing the alphabet $\Sigma' = \{0, \dots, n+1\}$ and complicating the action, we restrict the kind of relations such that either we do not have relations or if there exist, there is one of the form:

$$\$_1 q_{i_1}\dots q_{i_k}\$_1 = \$_2 q_{i_1}\dots q_{i_k}\$_2$$

  where $i_1, \dots, i_k$ is a solution to the PCP:

Theorem (E.Post)

The Post correspondence problem:

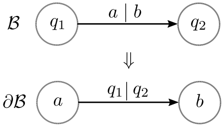
- *Input: a finite family of pairs of words $(u_1, v_1), \dots, (u_m, v_m)$ on some alphabet Γ;*
- *Output: is there a set of indexes $i_1, \dots, i_k$ such that $u_{i_1}\dots u_{i_k} = v_{i_1}\dots v_{i_k}$?*

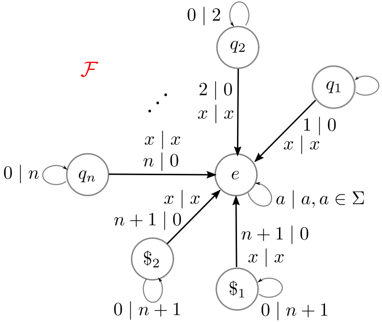
is undecidable.

- So there is a defining relation iff there is a relation $\$_1 q_{i_1}\dots q_{i_k}\$_1 = \$_2 q_{i_1}\dots q_{i_k}\$_2$ iff there

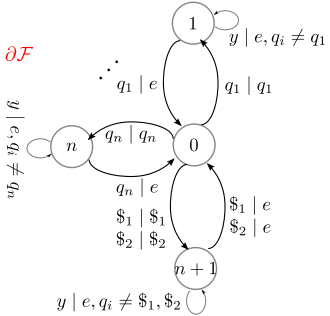
Sketch of the proof: complicating the action via the dual

- Increasing the alphabet Σ' to complicate the action of the automaton.
- Working with dual of an automaton helps to control the kind of defining relations:
- Thus by adding to the previous automaton $\partial\mathcal{F}$ another automaton $\partial\mathcal{H}$ we are able to restrict the kind of relations

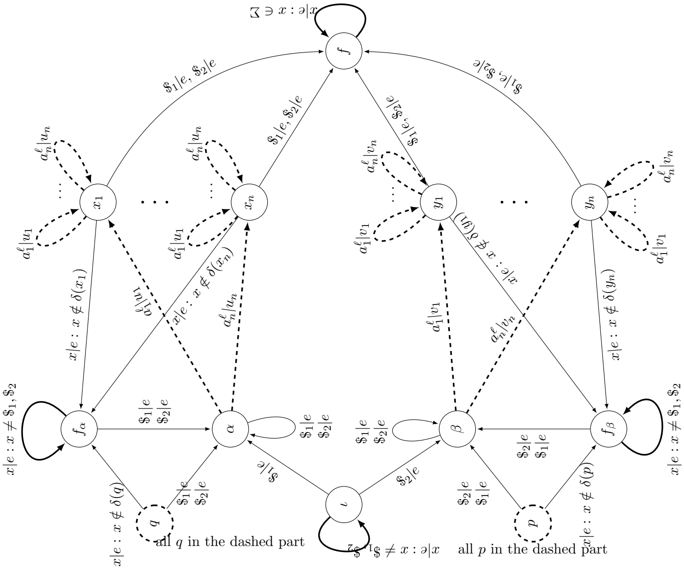




$\Rightarrow$



The automaton $\partial\mathcal{H}$:



Freeness for automata semigroups

The previous result heavily uses the existence of a state e acting like the identity, but it is possibile to modify it to get

Theorem (D'Angeli, R., Wächter)

The following algorithmic problem:

- *Input: An automaton semigroup* $\mathscr{B}$ *(complete deterministic);*
- *Output: Is* $\mathcal{S}(\mathscr{B})$ *free?*

is undecidable.

The case of an automaton group

Trying to "embed" a Turing machine into an automaton that is complete and inverse-deterministic (automaton group) is quite a challenge...

Open problem

Given an automaton group (complete, inverse deterministic automaton) $\mathscr{A}$, are these two problems undecidable:

- the semigroup $\mathcal{S}(\mathscr{A})$ generated by the "positive" states Q is free?
- is the group $\mathcal{G}(\mathscr{A})$ free?

Thank you!