# Decision Problems for Automaton Semigroups and Groups

Jan Philipp **Wächter**

Universität des Saarlandes

21 June 2024

# Presentations

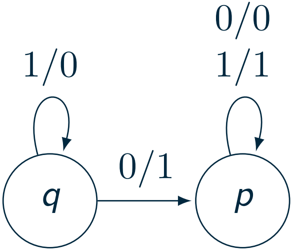
In this talk: semigroups, monoids or groups

- traditional presentation of algebraic structures:
$$\langle q_1, \ldots, q_n \mid \ell_1 = r_1, \ldots, \ell_m = r_m \rangle$$
$Q = \{q_1, \ldots, q_n\}$: generators,
$(\ell_1, r_1), \ldots (\ell_m, r_m) \in Q^+ \times Q^+$: relations
- possible input to algorithms if both sets are finite
- alternative: use automata $\rightsquigarrow$ automaton structures
- Why? Many examples of groups with interesting properties arise in this way (intermediate growth, Burnside problem, …) and it
allows for a finite description of possibly non-finitely presented (semi)groups (Lamplighter group, Grigorchuk's group, …).
- How? $\rightsquigarrow$ short recap

# Automata

In this setting, an automaton $\mathcal{T} = (Q, \Sigma, \delta)$ is a

- finite, directed graph whose
- nodes from $Q$ are called states and
- edges given by $\delta \subseteq Q \times \Sigma \times \Sigma \times Q$ are called transitions and
- are labeled by pairs $a/b$ of letters from the alphabet $\Sigma$.
- A transition $p \xrightarrow{a/b} q$
  - starts in $p$ and
  - ends in $q$. Its
  - input is $a$ and its
  - output is $b$.




⇝ It's a $\mathscr{G}$-automaton!

An automaton is

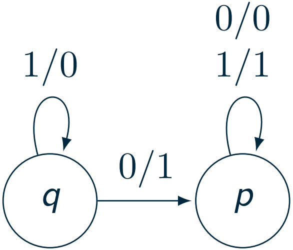
- deterministic if $\forall a \in \Sigma \, \forall q \in Q$ : $q$ has at most one outgoing transition with input $a$.
- complete if $\forall a \in \Sigma \, \forall q \in Q$ : $q$ has at least one outgoing transition with input $a$.
- invertible if $\forall b \in \Sigma \, \forall q \in Q$ : $q$ has at most one outgoing transition with output $b$.

Today we mostly consider complete automata!

# Automata

In this setting, an automaton $\mathcal{T} = (Q, \Sigma, \delta)$ is a

- finite, directed graph whose
- nodes from $Q$ are called states and
- edges given by $\delta \subseteq Q \times \Sigma \times \Sigma \times Q$ are called transitions and
- are labeled by pairs $a/b$ of letters from the alphabet $\Sigma$.
- A transition $p \xrightarrow{a/b} q$
  - starts in $p$ and
  - ends in $q$. Its
  - input is $a$ and its
  - output is $b$.




⇝ It's a $\mathscr{G}$-automaton!

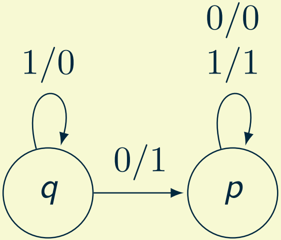
| An automaton is | $\mathscr{S}$-automaton | complete $\mathscr{S}$-automaton | $\mathscr{G}$-automaton | $\overline{\mathscr{S}}$-automaton |
|---|---|---|---|---|
| • deterministic | ✓ | ✓ | ✓ | ✓ |
| • complete | – | ✓ | ✓ | – |
| • invertible | – | – | ✓ | ✓ |

Today we mostly consider complete automata!

# State Actions of $\mathscr{S}$-automata

- Idea: every state $q$ induces a partial action $\Sigma^* \to_p \Sigma^*, u \mapsto q \circ u$

## Example




"Adding Machine"

- The action of $p$ is the identity.
- $$q \circ 000 = 100$$ $$qq \circ 000 = q \circ 100 = 010$$ $$qqq \circ 000 = \cdots = 110$$

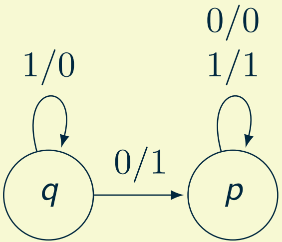
$\rightsquigarrow$ the action of $q$ increments (reverse) binary representation (least significant bit first)

- All state actions are total if the automaton is complete.
- All state actions are injective if the automaton is invertible. $\rightsquigarrow$ $\mathscr{G}$-automata induce bijections.

# Automaton Semigroups, Monoids and Groups

- semigroup $\mathscr{S}(\mathcal{T})$ generated by $\mathcal{T}$: closure under composition of the functions induced by the states "automaton semigroup"
- monoid $\mathscr{M}(\mathcal{T})$ generated by $\mathcal{T}$: $\mathscr{M}(\mathcal{T}) = \mathscr{S}(\mathcal{T}) \cup \{\mathrm{id}\}$ "automaton monoid"
- group $\mathscr{G}(\mathcal{T})$ generated by $\mathcal{T}$: include inverse functions "automaton group"

## Example




- $p$: identity
- $q$: increment
- $qp = pq = q$ in $\mathscr{S}(\mathcal{T})$
- $q^i \neq q^j$ in $\mathscr{S}(\mathcal{T})$ for $i \neq j$

$$\mathscr{S}(\mathcal{T}) \simeq q^* \simeq \mathscr{M}(\mathcal{T})$$

$$\mathscr{G}(\mathcal{T}) \simeq F(q)$$

# Summary

Other people usually simply use "automaton semigroup" for this!

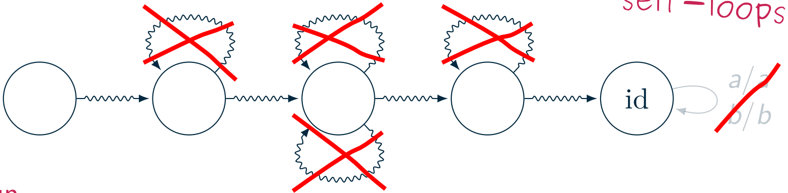
| automaton | properties | structure |
|---|---|---|
| $\mathscr{S}$-automaton | deterministic | (partial) automaton semigroup<br>(partial) automaton monoid |
| complete $\mathscr{S}$-automaton | deterministic, complete | complete automaton semigroup<br>complete automaton monoid |
| $\overline{\mathscr{S}}$-automaton | deterministic, invertible | automaton-inverse semigroup<br>automaton-inverse monoid |
| $\mathscr{G}$-automaton | deterministic, complete, invertible | automaton group |

This is the same as "inverse automaton semigroup" / "inverse automaton monoid" (D'Angeli, Rodaro, W.; 2020)

# Sidki's Activity for Automata

Consider a subautomaton/run ending in an identity state:

We ignore the self-loops at id




If every such run...

- has no cycles, the automaton is finitary. ⇝ finitary automaton group ≡ finite group
- has at most one cycle, the automaton has bounded activity. ⇝ bounded automaton group
- has no "entangled" cycles, the automaton has polynomial activity.

Grigorchuk's group

There is a generalization to monoids (Bartholdi, Godin, Klimann, Picantin; 2018)

but without the above geometric characterization!

# Lines of Research

1. Research on individual automaton semigroups
   for example: Grigorchuk's group
2. Research on the structure theory
   structure of the automaton vs. algebraic properties
   for example: classification results (e. g. activity hierarchy), non-automaton (semi)groups, closure properties, automaton constructions
3. Research on decision problems over automaton structures
   for example: word problem, finiteness problem, freeness problem

We will mostly discuss line 3!

# Important Complexity Classes

| Class of problems | solvable in … | | by … Turing machines |
|---|---|---|---|
| LogSpace | logarithmic | space | deterministic |
| NL | logarithmic | space | non-deterministic |
| P | polynomial | time | deterministic |
| NP | polynomial | time | non-deterministic |
| PSpace | polynomial | space | deterministic or non-deterministic |

$$\mathrm{NC}^1 \subseteq \textsc{LogSpace} \subseteq \mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \textsc{PSpace}$$

Most inclusions are suspected to be strict but we only know $\mathrm{NL} \subsetneq \textsc{PSpace}$.

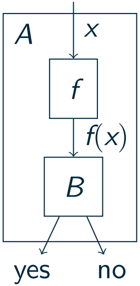
We will also encounter the circuit complexity class $\mathrm{NC}^1$ (which is a bit different to the others).

# Reductions

## Definition (many-one LogSpace-reducible)

$A \leq_{\log} B \iff$ there is a LogSpace-computable total function $f$ mapping instances of $A$ to instances of $B$ such that

$$A \ni x \iff f(x) \in B.$$




**Idea:** An algorithm for $B$ also yields one for $A$.

## Definition

$B$ is $\mathcal{C}$-hard (for a complexity class $\mathcal{C}$) if $\forall A \in \mathcal{C} : A \leq_{\log} B$.
$B$ is $\mathcal{C}$-complete if $B \in \mathcal{C}$ and $B$ is $\mathcal{C}$-hard.

Typically:
$\forall A \in \mathcal{C} : A \leq_{\log} B' \leq_{\log} B$

"An algorithm for B solves any problem in C."

# Word Problem

## Definition (Uniform Word Problem)

The word problem of an automaton groups is the problem

**Constant:** a $\mathscr{G}$-automaton $\mathcal{T} = (Q, \Sigma, \delta)$ and
**Input:** $\boldsymbol{p} \in Q^{\pm *}$
**Question:** is $\boldsymbol{p} = \mathbb{1}$ in $\mathscr{G}(\mathcal{T})$?

For monoids:
**Input:** $\mathscr{S}$-automaton $\mathcal{T} = (Q, \Sigma, \delta)$
$\boldsymbol{p}, \boldsymbol{q} \in Q^*$
**Question:** $\boldsymbol{p} = \boldsymbol{q}$ in $\mathscr{M}(\mathcal{T})$?

| | general automaton groups | bounded automaton groups | finitary automaton groups | general complete automaton monoids | bounded automaton monoids |
|---|---|---|---|---|---|
| word problem | PSpace-complete<br>W., Weiß; 2020 | ∈ LogSpace<br>Bond., Nek.; 2003<br>$\mathrm{NC}^1$-hard<br>by finitary case | regular<br>$\mathrm{NC}^1$-complete<br>Barrington; 1989 | PSpace-complete<br>D'A RW 2017<br>by group case | *open*<br>∈ PSpace<br>$\mathrm{NC}^1$-hard |
| uniform word problem | PSpace-complete<br>by non-unif. case | *open*<br>∈ PSpace<br>coNP-hard | coNP-complete<br>Kotowsky, W.; 2023 | PSpace-complete<br>by non-unif. case | *open*<br>∈ PSpace<br>coNP-hard |

Recall: $\mathrm{NC}^1 \subseteq \mathrm{LogSpace} \subseteq \mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSpace}$

# Finiteness Problem

## Definition (Finiteness Problem) monoids

The finiteness problem for automaton ~~groups~~ is the problem

**Input:** a ~~$\mathscr{G}$-automaton~~ $\mathcal{T}$ $\mathscr{S}$-automaton

**Question:** is $\mathscr{G}(\mathcal{T})$ finite? $\iff$ $\mathscr{M}(\mathcal{T})$ is finite

| | general automaton groups | bounded automaton groups | finitary automaton groups | general complete automaton monoids | bounded automaton monoids |
|---|---|---|---|---|---|
| finiteness problem | *open* | decidable<br>Bondarenko, W.; 2021 | *trivial*<br>all finite | undecidable<br>Gillibert 2014 | decidable<br>D'A RW WIP |

## Theorem (D'Angeli, Francoeur, Rodaro, W.; 2020)

*An automaton semigroup is infinite if and only if it admits an infinite word with infinite orbit.*

## Theorem (Bondarenko, W.; 2021)

*For bounded automaton groups, the language of words with infinite orbit is $\omega$-regular.*

# Freeness Problem

## Definition (Freeness Problem) monoids

The freeness problem for automaton ~~groups~~ is the problem

**Input:** a ~~$\mathscr{G}$-automaton~~ $\mathcal{T}$ $\mathscr{S}$-automaton

**Question:** is $\mathscr{G}(\mathcal{T})$ a free group? $\not\Leftrightarrow$ $\mathscr{M}(\mathcal{T})$ is a free monoid

| | general automaton groups | bounded automaton groups | finitary automaton groups | general complete automaton monoids | bounded automaton monoids |
|---|---|---|---|---|---|
| freeness problem | *open* | decidable<br>by order/finiteness prob. | *trivial*<br>all finite | undecidable<br>D'A RW; 2024 | *open* |

## Theorem (Sidki; 2004)

*An automaton group of polynomial activity cannot contain a free subgroup of rank $2$.*

# More Details

## Theorem (D'Angeli, Rodaro, W.; arXiv/2024)

*The following problem is undecidable for given automaton semigroups and monoids:*

**Input:** an $\mathscr{S}$-automaton $\mathcal{T} = (Q, \Sigma, \delta)$

**Question:** is $\mathscr{S}(\mathcal{T}) / \mathscr{M}(\mathcal{T})$ ~~free~~?

$\mathscr{M}(\mathcal{T}) \simeq (Q \setminus \{\mathrm{id}\})^*$?

$st = st' \implies t = t'$

~~(left) cancellative~~ equidivisible

- This is based on a general reduction from Post's Correspondence Problem and
- yields further results.

## Lemma (Levi's Lemma)

*A semigroup (monoid) if free if and only if*

1. *it has a (proper) length function and*
2. *is equidivisible.*

What about this part? ⇝ WIP

# Future Work and Open Problems

- What about the free presentation problem for semigroups?
- At what activity level becomes the problem undecidable?
  Decidable for bounded activity monoids?

$\mathrm{NC}^1 \subseteq \textsc{LogSpace} \subseteq \mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \textsc{PSpace}$

Thank you!

| | general automaton groups | bounded automaton groups | finitary automaton groups | general complete automaton monoids | bounded automaton monoids |
|---|---|---|---|---|---|
| word problem | PSPACE-complete<br>W., Weiß; 2020 | $\in$ LOGSPACE<br>Bond., Nek.; 2003<br>$\mathrm{NC}^1$-hard<br>by finitary case | regular<br>$\mathrm{NC}^1$-complete<br>Barrington; 1989 | PSPACE-complete<br>D'A RW 2017<br>by group case | *open*<br>$\in$ PSPACE<br>$\mathrm{NC}^1$-hard |
| uniform word problem | PSPACE-complete<br>by non-unif. case | *open*<br>$\in$ PSPACE<br>coNP-hard | coNP-complete<br>Kotowsky, W.; 2023 | PSPACE-complete<br>by non-unif. case | *open*<br>$\in$ PSPACE<br>coNP-hard |
| finiteness problem | *open* | decidable<br>Bondarenko, W.; 2021 | *trivial*<br>all finite | undecidable<br>Gillibert 2014 | decidable<br>D'A RW WIP |
| freeness problem | *open* | decidable<br>by order/finiteness prob. | *trivial*<br>all finite | undecidable<br>D'A RW; 2024 | *open* |