

Decidability and Complexity in Automatic Monoids

Markus Lohrey

University of Stuttgart, Germany

Developments in Language Theory 2004

Idea: Multiplication with generators can be defined by automata.

Let $\mathcal{M} = (M, \circ)$ be a finitely generated monoid.

Then, \mathcal{M} is **automatic**, if there exists a finite generating set Γ for \mathcal{M} with:

- There exists a regular language $L \subseteq \Gamma^*$ such that
- the canonical morphism $\Gamma^* \rightarrow \mathcal{M}$ restricted to L is a bijection and
- for every generator $a \in \Gamma$, the relation $\{(u, v) \in L \times L \mid h(u) \circ a = h(v)\}$ is **synchronized rational**.

Idea: Multiplication with generators can be defined by automata.

Let $\mathcal{M} = (M, \circ)$ be a finitely generated monoid.

Then, \mathcal{M} is **automatic**, if there exists a finite generating set Γ for \mathcal{M} with:

- There exists a regular language $L \subseteq \Gamma^*$ such that
- the canonical morphism $\Gamma^* \rightarrow \mathcal{M}$ restricted to L is a bijection and
- for every generator $a \in \Gamma$, the relation $\{(u, v) \in L \times L \mid h(u) \circ a = h(v)\}$ is **synchronized rational**.

Synchronized Rational Relations

A binary synchronized rational relation: In order to accept a pair $(u, v) \in \Sigma^* \times \Sigma^*$ a two-tape automaton operates as follows:

v	b_0	b_1	b_2	\dots	b_{m-1}	b_m	$\#$	\dots	$\#$
u	a_0	a_1	a_2	\dots	a_{m-1}	a_m	a_{m+1}	\dots	a_n

Synchronized Rational Relations

A binary synchronized rational relation: In order to accept a pair $(u, v) \in \Sigma^* \times \Sigma^*$ a two-tape automaton operates as follows:

	q_0								
v	b_0	b_1	b_2	\dots	b_{m-1}	b_m	$\#$	\dots	$\#$
u	a_0	a_1	a_2	\dots	a_{m-1}	a_m	a_{m+1}	\dots	a_n

Synchronized Rational Relations

A binary synchronized rational relation: In order to accept a pair $(u, v) \in \Sigma^* \times \Sigma^*$ a two-tape automaton operates as follows:

		q_1							
v	b_0	b_1	b_2	\dots	b_{m-1}	b_m	$\#$	\dots	$\#$
u	a_0	a_1	a_2	\dots	a_{m-1}	a_m	a_{m+1}	\dots	a_n

Synchronized Rational Relations

A binary synchronized rational relation: In order to accept a pair $(u, v) \in \Sigma^* \times \Sigma^*$ a two-tape automaton operates as follows:

		q_2							
v	b_0	b_1	b_2	\dots	b_{m-1}	b_m	$\#$	\dots	$\#$
u	a_0	a_1	a_2	\dots	a_{m-1}	a_m	a_{m+1}	\dots	a_n

Synchronized Rational Relations

A binary synchronized rational relation: In order to accept a pair $(u, v) \in \Sigma^* \times \Sigma^*$ a two-tape automaton operates as follows:

						q_m			
v	b_0	b_1	b_2	\dots	b_{m-1}	b_m	$\#$	\dots	$\#$
u	a_0	a_1	a_2	\dots	a_{m-1}	a_m	a_{m+1}	\dots	a_n

Synchronized Rational Relations

A binary synchronized rational relation: In order to accept a pair $(u, v) \in \Sigma^* \times \Sigma^*$ a two-tape automaton operates as follows:

						q_{m+1}			
v	b_0	b_1	b_2	\dots	b_{m-1}	b_m	#	\dots	#
u	a_0	a_1	a_2	\dots	a_{m-1}	a_m	a_{m+1}	\dots	a_n

Synchronized Rational Relations

A binary synchronized rational relation: In order to accept a pair $(u, v) \in \Sigma^* \times \Sigma^*$ a two-tape automaton operates as follows:

									q_n
v	b_0	b_1	b_2	\dots	b_{m-1}	b_m	$\#$	\dots	$\#$
u	a_0	a_1	a_2	\dots	a_{m-1}	a_m	a_{m+1}	\dots	a_n

Word problems

Let \mathcal{M} be a monoid, finitely generated by the set Γ .

The **word problem** for \mathcal{M} is the following computational problem:

INPUT: Two words $u, v \in \Gamma^*$

QUESTION: Do u and v represent the same monoid element of the monoid \mathcal{M} ?

Well-known: For every automatic monoid, the word problem can be solved in quadratic time.

Word problems

Let \mathcal{M} be a monoid, finitely generated by the set Γ .

The **word problem** for \mathcal{M} is the following computational problem:

INPUT: Two words $u, v \in \Gamma^*$

QUESTION: Do u and v represent the same monoid element of the monoid \mathcal{M} ?

Well-known: For every automatic monoid, the word problem can be solved in quadratic time.

Complexity of the word problem

Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:

Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:

Complexity of the word problem

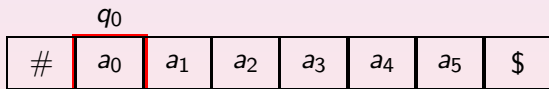
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

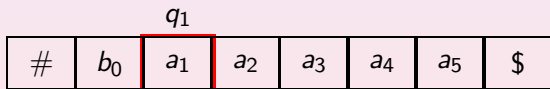
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

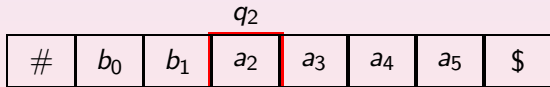
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

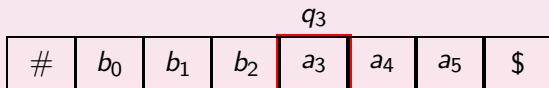
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

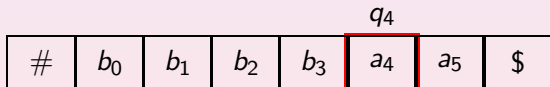
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

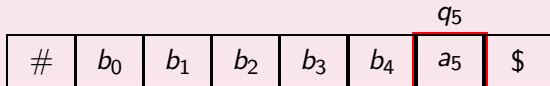
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

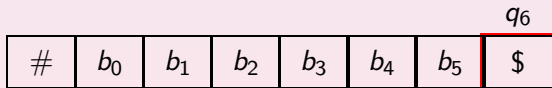
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

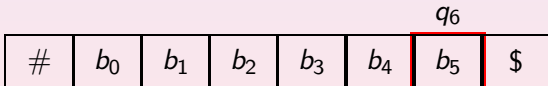
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

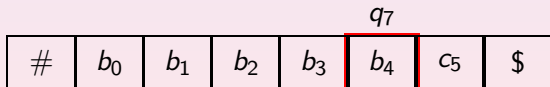
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

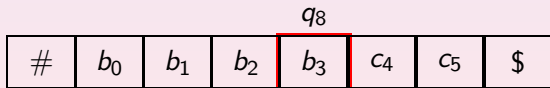
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

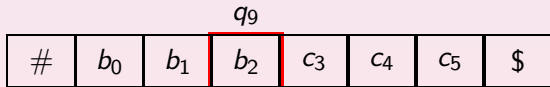
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

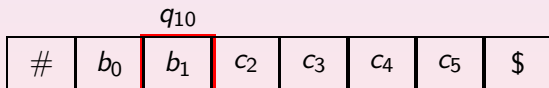
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

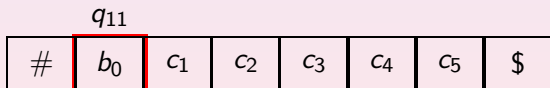
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

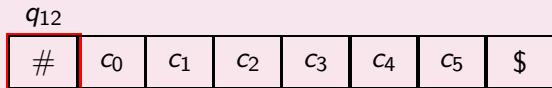
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

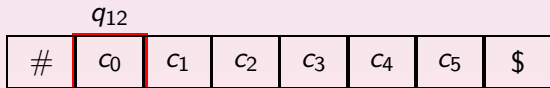
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



Complexity of the word problem

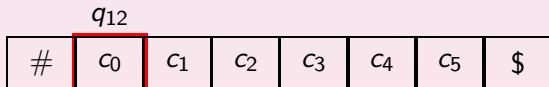
Theorem

There exists a fixed automatic monoid with a P-complete word problem.

Proof: Let M be a Turing-machine with a P-complete acceptance problem.

W.l.o.g. assume that:

- The tape is $\# \square \square \dots \square \$$ when M terminates.
- M operates in a zick-zack way:



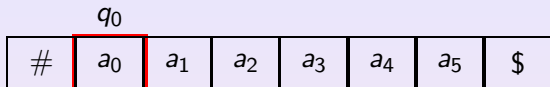
- M makes precisely $p(n)$ complete left-right-transversals for an input of size n .

Complexity of the word problem

We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

Complexity of the word problem

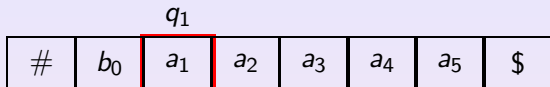


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

q_0 a_0 a_1 a_2 a_3 a_4 a_5 \$ \$ \$...

Complexity of the word problem

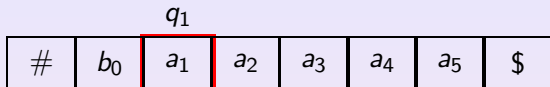


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 q_1 a_1 a_2 a_3 a_4 a_5 \$ \$ \$ \dots

Complexity of the word problem

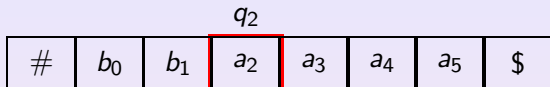


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 q_1 a_1 a_2 a_3 a_4 a_5 \$ \$ \$ \dots

Complexity of the word problem

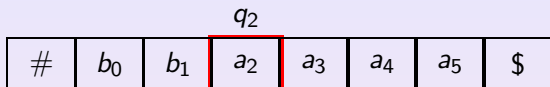


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 \bar{b}_1 q_2 a_2 a_3 a_4 a_5 \$ \$ \$ \dots

Complexity of the word problem

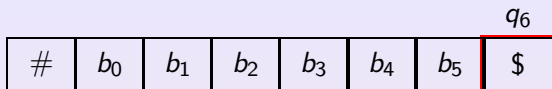


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

#	\bar{b}_0	\bar{b}_1	q_2	a_2	a_3	a_4	a_5	\$	\$	\$...
---	-------------	-------------	-------	-------	-------	-------	-------	----	----	----	-----

Complexity of the word problem

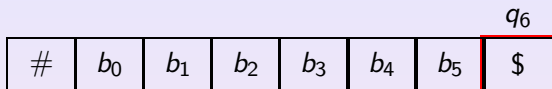


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 \bar{b}_1 \bar{b}_2 \bar{b}_3 \bar{b}_4 \bar{b}_5 q_6 \$ \$ \$ \dots

Complexity of the word problem

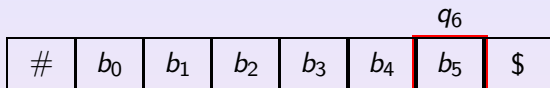


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 \bar{b}_1 \bar{b}_2 \bar{b}_3 \bar{b}_4 \bar{b}_5 \bar{q}_6 \$ \$ \dots

Complexity of the word problem

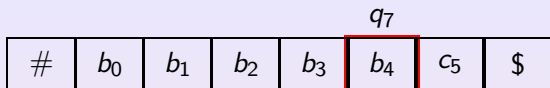


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 \bar{b}_1 \bar{b}_2 \bar{b}_3 \bar{b}_4 \bar{b}_5 \bar{q}_6 \$ \$ \dots

Complexity of the word problem

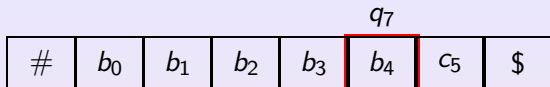


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

#	\bar{b}_0	\bar{b}_1	\bar{b}_2	\bar{b}_3	\bar{b}_4	\bar{q}_7	c_5	\$	\$...
---	-------------	-------------	-------------	-------------	-------------	-------------	-------	----	----	-----

Complexity of the word problem

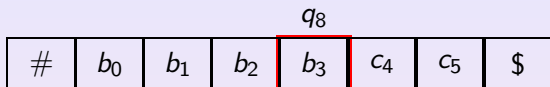


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 \bar{b}_1 \bar{b}_2 \bar{b}_3 \bar{b}_4 \bar{q}_7 c_5 \$ \$ \dots

Complexity of the word problem

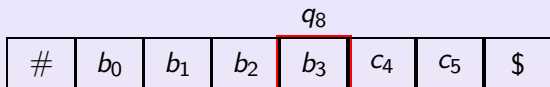


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

\bar{b}_0 \bar{b}_1 \bar{b}_2 \bar{b}_3 \bar{q}_8 c_4 c_5 \$ \$ \dots

Complexity of the word problem

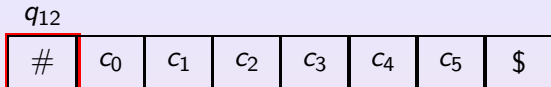


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

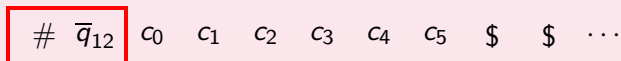
#	\bar{b}_0	\bar{b}_1	\bar{b}_2	\bar{b}_3	\bar{q}_8	c_4	c_5	\$	\$	\dots
---	-------------	-------------	-------------	-------------	-------------	-------	-------	----	----	---------

Complexity of the word problem

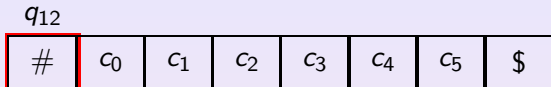


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

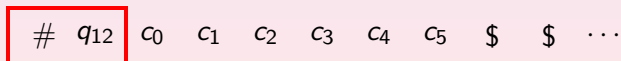


Complexity of the word problem

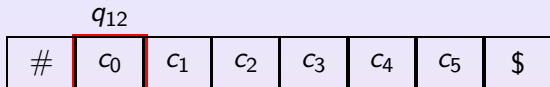


We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.



Complexity of the word problem



We simulate M with a semi-Thue system (string rewriting system) R over an alphabet Γ such that:

- R is terminating and confluent. $\Rightarrow \text{IRR}(R) \cong \Gamma^*/R$ bijectively
- For every $a \in \Gamma$, the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

$q_{12} c_0$ c_1 c_2 c_3 c_4 c_5 \$ \$ \dots

Complexity of the word problem

The semi-Thue system R :

$$\begin{array}{ll} qa \rightarrow \bar{b}p & \text{if } \boxed{q \begin{array}{l} a \\ a * \end{array} \Rightarrow_M \begin{array}{l} p \\ b * \end{array}} \\ \bar{a}\bar{q} \rightarrow \bar{p}b & \text{if } \boxed{* \begin{array}{l} q \\ a \end{array} \Rightarrow_M \begin{array}{l} p \\ * b \end{array}} \\ q\$ \rightarrow \bar{q} & \text{for all states } q \\ \#\bar{q} \rightarrow \#q & \text{for all states } q \end{array}$$

Then we have:

- An input w of length n is accepted by the machine M if and only if

$$\#q_0 w \square^{n-p(n)} \$^{p(n)} \stackrel{*}{\leftrightarrow}_R \#q_f \square^{p(n)}$$

Thus the word problem for Γ^*/R is P-complete.

- For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \stackrel{*}{\rightarrow}_R v\}$ is synchronized rational.

Complexity of the word problem

The semi-Thue system R :

$$qa \rightarrow \bar{b}p \quad \text{if} \quad \boxed{q \begin{matrix} a \\ a_* \end{matrix} \Rightarrow_M \begin{matrix} p \\ b_* \end{matrix}} \quad \bar{a}\bar{q} \rightarrow \bar{p}b \quad \text{if} \quad \boxed{*_a \begin{matrix} q \\ a \end{matrix} \Rightarrow_M \begin{matrix} p \\ b \end{matrix} *_q}$$
$$q\$ \rightarrow \bar{q} \quad \text{for all states } q \quad \# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

Then we have:

- An input w of length n is accepted by the machine M if and only if

$$\#q_0 w \square^{n-p(n)} \$^{p(n)} \stackrel{*}{\leftrightarrow}_R \#q_f \square^{p(n)}$$

Thus the word problem for Γ^*/R is P-complete.

- For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \stackrel{*}{\rightarrow}_R v\}$ is synchronized rational.

Complexity of the word problem

The semi-Thue system R :

$$qa \rightarrow \bar{b}p \quad \text{if} \quad \boxed{q \begin{matrix} a \\ a * \end{matrix} \Rightarrow_M \begin{matrix} p \\ b * \end{matrix}} \quad \bar{a}\bar{q} \rightarrow \bar{p}b \quad \text{if} \quad \boxed{* \begin{matrix} q \\ a \end{matrix} \Rightarrow_M \begin{matrix} p \\ * b \end{matrix}}$$
$$q\$ \rightarrow \bar{q} \quad \text{for all states } q \quad \# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

Then we have:

- An input w of length n is accepted by the machine M if and only if

$$\#q_0 w \square^{n-\rho(n)} \$^{\rho(n)} \stackrel{*}{\leftrightarrow}_R \#q_f \square^{\rho(n)}$$

Thus the word problem for Γ^*/R is P-complete.

- For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \stackrel{*}{\rightarrow}_R v\}$ is synchronized rational.

Complexity of the word problem

The semi-Thue system R :

$$qa \rightarrow \bar{b}p \quad \text{if} \quad \boxed{q \begin{matrix} a \\ a * \end{matrix} \Rightarrow_M \begin{matrix} p \\ b * \end{matrix}} \quad \bar{a}\bar{q} \rightarrow \bar{p}b \quad \text{if} \quad \boxed{* \begin{matrix} q \\ a \end{matrix} \Rightarrow_M \begin{matrix} p \\ * b \end{matrix}}$$
$$q\$ \rightarrow \bar{q} \quad \text{for all states } q \quad \# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

Then we have:

- An input w of length n is accepted by the machine M if and only if

$$\#q_0 w \square^{n-\rho(n)} \$^{\rho(n)} \stackrel{*}{\leftrightarrow}_R \#q_f \square^{\rho(n)}$$

Thus the word problem for Γ^*/R is P-complete.

- For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \stackrel{*}{\rightarrow}_R v\}$ is synchronized rational.

Complexity of the word problem

The semi-Thue system R :

$$qa \rightarrow \bar{b}p \quad \text{if} \quad \boxed{q \begin{matrix} a \\ a * \end{matrix} \Rightarrow_M \begin{matrix} p \\ b * \end{matrix}} \quad \bar{a}\bar{q} \rightarrow \bar{p}b \quad \text{if} \quad \boxed{* \begin{matrix} q \\ a \end{matrix} \Rightarrow_M \begin{matrix} p \\ * b \end{matrix}}$$
$$q\$ \rightarrow \bar{q} \quad \text{for all states } q \quad \# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

Then we have:

- An input w of length n is accepted by the machine M if and only if

$$\#q_0 w \square^{n-\rho(n)} \$^{\rho(n)} \stackrel{*}{\leftrightarrow}_R \#q_f \square^{\rho(n)}$$

Thus the word problem for Γ^*/R is P-complete.

- For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \stackrel{*}{\rightarrow}_R v\}$ is synchronized rational.

Complexity of the word problem

$$q a \rightarrow \bar{b} p \quad \text{if} \quad \boxed{q \begin{smallmatrix} a \\ * \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ b \\ * \end{smallmatrix}}$$

$$\bar{a} \bar{q} \rightarrow \bar{p} b \quad \text{if} \quad \boxed{* \begin{smallmatrix} q \\ a \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ * \\ b \end{smallmatrix}}$$

$$q \$ \rightarrow \bar{q} \quad \text{for all states } q$$

$$\# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

Let e.g. $a = \bar{q}$ for a state q , and $u = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n$ with n maximal.

- 1 u' does not end with $\#$: Then

$$u \bar{q} = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u' \bar{p} b_1 b_2 \cdots b_n \in \text{IRR}(R)$$

- 2 $u' = u'' \#$: Then

$$u \bar{q} = u'' \# \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u'' \# \bar{p} b_1 b_2 \cdots b_n$$

$$\rightarrow_R u'' \# p b_1 b_2 \cdots b_n$$

$$\xrightarrow{*}_R u'' \# \bar{c}_1 \bar{c}_2 \cdots \bar{c}_n r \in \text{IRR}(R)$$

Complexity of the word problem

$$q a \rightarrow \bar{b} p \quad \text{if} \quad \boxed{q \begin{smallmatrix} a \\ * \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ b \\ * \end{smallmatrix}}$$

$$\bar{a} \bar{q} \rightarrow \bar{p} b \quad \text{if} \quad \boxed{* \begin{smallmatrix} q \\ a \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ * \\ b \end{smallmatrix}}$$

$$q \$ \rightarrow \bar{q} \quad \text{for all states } q$$

$$\# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

Let e.g. $a = \bar{q}$ for a state q , and $u = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n$ with n maximal.

- ① u' does not end with $\#$: Then

$$u \bar{q} = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u' \bar{p} b_1 b_2 \cdots b_n \in \text{IRR}(R)$$

- ② $u' = u'' \#$: Then

$$u \bar{q} = u'' \# \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u'' \# \bar{p} b_1 b_2 \cdots b_n$$

$$\rightarrow_R u'' \# p b_1 b_2 \cdots b_n$$

$$\xrightarrow{\Delta}_R u'' \# \bar{c}_1 \bar{c}_2 \cdots \bar{c}_n r \in \text{IRR}(R)$$

Complexity of the word problem

$$q a \rightarrow \bar{b} p \quad \text{if} \quad \boxed{q \begin{smallmatrix} a \\ * \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ b \\ * \end{smallmatrix}}$$

$$\bar{a} \bar{q} \rightarrow \bar{p} b \quad \text{if} \quad \boxed{* \begin{smallmatrix} q \\ a \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ * \\ b \end{smallmatrix}}$$

$$q \$ \rightarrow \bar{q} \quad \text{for all states } q$$

$$\# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

Let e.g. $a = \bar{q}$ for a state q , and $u = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n$ with n maximal.

- ① u' does not end with $\#$: Then

$$u \bar{q} = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u' \bar{p} b_1 b_2 \cdots b_n \in \text{IRR}(R)$$

- ② $u' = u'' \#$: Then

$$u \bar{q} = u'' \# \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u'' \# \bar{p} b_1 b_2 \cdots b_n$$

$$\rightarrow_R u'' \# p b_1 b_2 \cdots b_n$$

$$\xrightarrow{*}_R u'' \# \bar{c}_1 \bar{c}_2 \cdots \bar{c}_n r \in \text{IRR}(R)$$

Complexity of the word problem

$$q a \rightarrow \bar{b} p \quad \text{if} \quad \boxed{q \begin{matrix} a \\ * \end{matrix} \Rightarrow_M \begin{matrix} p \\ b \\ * \end{matrix}}$$

$$\bar{a} \bar{q} \rightarrow \bar{p} b \quad \text{if} \quad \boxed{* \begin{matrix} q \\ a \end{matrix} \Rightarrow_M \begin{matrix} p \\ * \\ b \end{matrix}}$$

$$q \$ \rightarrow \bar{q} \quad \text{for all states } q$$

$$\# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

Let e.g. $a = \bar{q}$ for a state q , and $u = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n$ with n maximal.

- ① u' does not end with $\#$: Then

$$u \bar{q} = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u' \bar{p} b_1 b_2 \cdots b_n \in \text{IRR}(R)$$

- ② $u' = u'' \#$: Then

$$\begin{aligned} u \bar{q} &= u'' \# \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u'' \# \bar{p} b_1 b_2 \cdots b_n \\ &\rightarrow_R u'' \# p b_1 b_2 \cdots b_n \\ &\xrightarrow{*}_R u'' \# \bar{c}_1 \bar{c}_2 \cdots \bar{c}_n r \in \text{IRR}(R) \end{aligned}$$

Complexity of the word problem

$$q a \rightarrow \bar{b} p \quad \text{if} \quad \boxed{q \begin{smallmatrix} a \\ * \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ b \\ * \end{smallmatrix}}$$

$$\bar{a} \bar{q} \rightarrow \bar{p} b \quad \text{if} \quad \boxed{* \begin{smallmatrix} q \\ a \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ * \\ b \end{smallmatrix}}$$

$$q \$ \rightarrow \bar{q} \quad \text{for all states } q$$

$$\# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

Let e.g. $a = \bar{q}$ for a state q , and $u = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n$ with n maximal.

- ① u' does not end with $\#$: Then

$$u \bar{q} = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u' \bar{p} b_1 b_2 \cdots b_n \in \text{IRR}(R)$$

- ② $u' = u'' \#$: Then

$$\begin{aligned} u \bar{q} &= u'' \# \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u'' \# \bar{p} b_1 b_2 \cdots b_n \\ &\rightarrow_R u'' \# p b_1 b_2 \cdots b_n \\ &\xrightarrow{*}_R u'' \# \bar{c}_1 \bar{c}_2 \cdots \bar{c}_n r \in \text{IRR}(R) \end{aligned}$$

Complexity of the word problem

$$q a \rightarrow \bar{b} p \quad \text{if} \quad \boxed{q \begin{smallmatrix} a \\ * \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ b \\ * \end{smallmatrix}}$$

$$\bar{a} \bar{q} \rightarrow \bar{p} b \quad \text{if} \quad \boxed{\begin{smallmatrix} q \\ * \end{smallmatrix} \Rightarrow_M \begin{smallmatrix} p \\ * \\ b \end{smallmatrix}}$$

$$q \$ \rightarrow \bar{q} \quad \text{for all states } q$$

$$\# \bar{q} \rightarrow \# q \quad \text{for all states } q$$

For every symbol a , the relation $\{(u, v) \mid u, v \in \text{IRR}(R), ua \xrightarrow{*}_R v\}$ is synchronized rational.

Let e.g. $a = \bar{q}$ for a state q , and $u = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n$ with n maximal.

- ① u' does not end with $\#$: Then

$$u \bar{q} = u' \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u' \bar{p} b_1 b_2 \cdots b_n \in \text{IRR}(R)$$

- ② $u' = u'' \#$: Then

$$\begin{aligned} u \bar{q} &= u'' \# \bar{a}_1 \bar{a}_2 \cdots \bar{a}_n \bar{q} \xrightarrow{*}_R u'' \# \bar{p} b_1 b_2 \cdots b_n \\ &\rightarrow_R u'' \# p b_1 b_2 \cdots b_n \\ &\xrightarrow{*}_R u'' \# \bar{c}_1 \bar{c}_2 \cdots \bar{c}_n r \in \text{IRR}(R) \end{aligned}$$

Complexity of the word problem

Open problem: Is there an **automatic group** with a P-complete word problem.

Important subclass of automatic groups: **hyperbolic groups**.

Cai, 1982: For every hyperbolic group, the word problem belongs to NC^2 .

Theorem

For every hyperbolic group, the word problem belongs to $LOGCFL \subseteq NC^2$.

Proof: Every hyperbolic group can be presented as Γ^*/R for a semi-Thue system R that is length-reducing and confluent on ε :

$$U \xrightarrow{*} R \varepsilon \Leftrightarrow U \xrightarrow{*} R \varepsilon.$$

The language $\{u \in \Gamma^* \mid u \xrightarrow{*} R \varepsilon\}$ is growing context-sensitive and hence belongs to $LOGCFL$ (Dahlhaus, Warmuth).

Complexity of the word problem

Open problem: Is there an **automatic group** with a P-complete word problem.

Important subclass of automatic groups: **hyperbolic groups**.

Cai, 1982: For every hyperbolic group, the word problem belongs to NC^2 .

Theorem

For every hyperbolic group, the word problem belongs to $LOGCFL \subseteq NC^2$.

Proof: Every hyperbolic group can be presented as Γ^*/R for a semi-Thue system R that is length-reducing and confluent on ε :

$$U \overset{*}{\leftrightarrow}_R \varepsilon \Leftrightarrow U \overset{*}{\rightarrow}_R \varepsilon.$$

The language $\{U \in \Gamma^* \mid U \overset{*}{\rightarrow}_R \varepsilon\}$ is growing context-sensitive and hence belongs to LOGCFL (Dahlhaus, Warmuth).

Complexity of the word problem

Open problem: Is there an **automatic group** with a P-complete word problem.

Important subclass of automatic groups: **hyperbolic groups**.

Cai, 1982: For every hyperbolic group, the word problem belongs to NC^2 .

Theorem

For every hyperbolic group, the word problem belongs to $LOGCFL \subseteq NC^2$.

Proof: Every hyperbolic group can be presented as Γ^*/R for a semi-Thue system R that is length-reducing and confluent on ε :

$$U \stackrel{*}{\leftrightarrow}_R \varepsilon \Leftrightarrow U \stackrel{*}{\rightarrow}_R \varepsilon.$$

The language $\{U \in \Gamma^* \mid U \stackrel{*}{\rightarrow}_R \varepsilon\}$ is growing context-sensitive and hence belongs to LOGCFL (Dahlhaus, Warmuth).

Complexity of the word problem

Open problem: Is there an **automatic group** with a P-complete word problem.

Important subclass of automatic groups: **hyperbolic groups**.

Cai, 1982: For every hyperbolic group, the word problem belongs to NC^2 .

Theorem

For every hyperbolic group, the word problem belongs to $LOGCFL \subseteq NC^2$.

Proof: Every hyperbolic group can be presented as Γ^*/R for a semi-Thue system R that is length-reducing and confluent on ε :

$$u \stackrel{*}{\leftrightarrow}_R \varepsilon \Leftrightarrow u \stackrel{*}{\rightarrow}_R \varepsilon.$$

The language $\{u \in \Gamma^* \mid u \stackrel{*}{\rightarrow}_R \varepsilon\}$ is growing context-sensitive and hence belongs to $LOGCFL$ (Dahlhaus, Warmuth).

Complexity of the word problem

Open problem: Is there an **automatic group** with a P-complete word problem.

Important subclass of automatic groups: **hyperbolic groups**.

Cai, 1982: For every hyperbolic group, the word problem belongs to NC^2 .

Theorem

For every hyperbolic group, the word problem belongs to $LOGCFL \subseteq NC^2$.

Proof: Every hyperbolic group can be presented as Γ^*/R for a semi-Thue system R that is length-reducing and confluent on ε :

$$u \overset{*}{\leftrightarrow}_R \varepsilon \Leftrightarrow u \overset{*}{\rightarrow}_R \varepsilon.$$

The language $\{u \in \Gamma^* \mid u \overset{*}{\rightarrow}_R \varepsilon\}$ is growing context-sensitive and hence belongs to LOGCFL (Dahlhaus, Warmuth)

Let \mathcal{M} be a finitely generated monoid.

Let Γ be a finite generating set of \mathcal{M} .

Then, the **Cayley-graph** of \mathcal{M} w.r.t. is the following edge-labeled graph:

$$\mathcal{C}(\mathcal{M}, \Gamma) = (\mathcal{M}, (\{(u, ua) \mid u \in \mathcal{M}\})_{a \in \Gamma})$$

The Cayley-graph of an automatic monoid is an **automatic graph** (in the sense of Khoussainov, Nerode).

Consequence: The first-order theory of the Cayley-graph of an automatic monoid is decidable.

Let \mathcal{M} be a finitely generated monoid.

Let Γ be a finite generating set of \mathcal{M} .

Then, the **Cayley-graph** of \mathcal{M} w.r.t. is the following edge-labeled graph:

$$\mathcal{C}(\mathcal{M}, \Gamma) = (\mathcal{M}, (\{(u, ua) \mid u \in \mathcal{M}\})_{a \in \Gamma})$$

The Cayley-graph of an automatic monoid is an **automatic graph** (in the sense of Khoussainov, Nerode).

Consequence: The first-order theory of the Cayley-graph of an automatic monoid is decidable.

Let \mathcal{M} be a finitely generated monoid.

Let Γ be a finite generating set of \mathcal{M} .

Then, the **Cayley-graph** of \mathcal{M} w.r.t. is the following edge-labeled graph:

$$\mathcal{C}(\mathcal{M}, \Gamma) = (\mathcal{M}, (\{(u, ua) \mid u \in \mathcal{M}\})_{a \in \Gamma})$$

The Cayley-graph of an automatic monoid is an **automatic graph** (in the sense of Khoussainov, Nerode).

Consequence: The first-order theory of the Cayley-graph of an automatic monoid is decidable.

First-order logic

Let $G = (V, (E_a)_{a \in \Gamma})$ be an edge-labeled graph.

Let Ω be an infinite set of variables ranging over V .

The set of all **first-order formulas** over G is defined as follows:

- $x = y$ and $E_a(x, y)$ are FO-formulas, where $x, y \in \Omega$ and $a \in \Gamma$
- If ϕ and ψ are FO-formulas then also

$$\neg\phi, \quad \phi \wedge \psi, \quad \phi \vee \psi, \quad \exists x : \phi, \quad \forall x : \phi$$

are FO-formulas.

A **first-order sentence** is a first-order formula without free variables.

The **first-order theory** of G is the set of all first-order sentences that are true in G .

First-order theory of the Cayley-graph

Recall: The first-order theory of the Cayley-graph of an automatic monoid is decidable.

A problem is **elementary decidable** if it can be solved in time $\mathcal{O}(2^{\dots^{2^n}})$, where the height of this tower of exponents is constant.

Theorem

There exists a fixed automatic monoid \mathcal{M} such that the first-order theory of the Cayley-graph of \mathcal{M} is not elementary decidable.

Proof: Construct a fixed automatic monoid \mathcal{M} such that the theory of all finite words can be reduced to the first-order theory of \mathcal{M} .

First-order theory of the Cayley-graph

Recall: The first-order theory of the Cayley-graph of an automatic monoid is decidable.

A problem is **elementary decidable** if it can be solved in time $\mathcal{O}(2^{\dots^{2^n}})$, where the height of this tower of exponents is constant.

Theorem

There exists a fixed automatic monoid \mathcal{M} such that the first-order theory of the Cayley-graph of \mathcal{M} is not elementary decidable.

Proof: Construct a fixed automatic monoid \mathcal{M} such that the theory of all finite words can be reduced to the first-order theory of \mathcal{M} .

First-order theory of the Cayley-graph

Recall: The first-order theory of the Cayley-graph of an automatic monoid is decidable.

A problem is **elementary decidable** if it can be solved in time $\mathcal{O}(2^{\dots^{2^n}})$, where the height of this tower of exponents is constant.

Theorem

There exists a fixed automatic monoid \mathcal{M} such that the first-order theory of the Cayley-graph of \mathcal{M} is not elementary decidable.

Proof: Construct a fixed automatic monoid \mathcal{M} such that the **theory of all finite words** can be reduced to the first-order theory of \mathcal{M} .

First-order theory of the Cayley-graph

Recall: The first-order theory of the Cayley-graph of an automatic monoid is decidable.

A problem is **elementary decidable** if it can be solved in time $\mathcal{O}(2^{\dots^{2^n}})$, where the height of this tower of exponents is constant.

Theorem

There exists a fixed automatic monoid \mathcal{M} such that the first-order theory of the Cayley-graph of \mathcal{M} is not elementary decidable.

Proof: Construct a fixed automatic monoid \mathcal{M} such that the **theory of all finite words** can be reduced to the first-order theory of \mathcal{M} .

First-order theory of the Cayley-graph

A finitely generated monoid \mathcal{M} has **finite geometric type** if for some constant c , every $x \in \mathcal{M}$ has degree at most c in the Cayley-graph of \mathcal{M} .

Example: **Cancellative monoids** are of finite geometric type.

Theorem

Let \mathcal{M} be an automatic of finite geometric type. Then the first-order theory of the Cayley-graph of \mathcal{M} is in $\text{DSPACE}(2^{2^{2^{O(n)}}})$.

Proof: The Cayley-graph of an automatic of finite geometric type is an automatic graph of bounded degree.

For every automatic graph of bounded degree the first-order theory belongs to $\text{DSPACE}(2^{2^{2^{O(n)}}})$.

First-order theory of the Cayley-graph

A finitely generated monoid \mathcal{M} has **finite geometric type** if for some constant c , every $x \in \mathcal{M}$ has degree at most c in the Cayley-graph of \mathcal{M} .

Example: **Cancellative monoids** are of finite geometric type.

Theorem

Let \mathcal{M} be an automatic of finite geometric type. Then the first-order theory of the Cayley-graph of \mathcal{M} is in $\text{DSPACE}(2^{2^{2^{\mathcal{O}(n)}}})$.

Proof: The Cayley-graph of an automatic of finite geometric type is an automatic graph of bounded degree.

For every automatic graph of bounded degree the first-order theory belongs to $\text{DSPACE}(2^{2^{2^{\mathcal{O}(n)}}})$.

First-order theory of the Cayley-graph

A finitely generated monoid \mathcal{M} has **finite geometric type** if for some constant c , every $x \in \mathcal{M}$ has degree at most c in the Cayley-graph of \mathcal{M} .

Example: **Cancellative monoids** are of finite geometric type.

Theorem

Let \mathcal{M} be an automatic of finite geometric type. Then the first-order theory of the Cayley-graph of \mathcal{M} is in $\text{DSPACE}(2^{2^{2^{\mathcal{O}(n)}}})$.

Proof: The Cayley-graph of an automatic of finite geometric type is an automatic graph of bounded degree.

For every automatic graph of bounded degree the first-order theory belongs to $\text{DSPACE}(2^{2^{2^{\mathcal{O}(n)}}})$.

First-order theory of the Cayley-graph

A finitely generated monoid \mathcal{M} has **finite geometric type** if for some constant c , every $x \in \mathcal{M}$ has degree at most c in the Cayley-graph of \mathcal{M} .

Example: **Cancellative monoids** are of finite geometric type.

Theorem

Let \mathcal{M} be an automatic of finite geometric type. Then the first-order theory of the Cayley-graph of \mathcal{M} is in $\text{DSpace}(2^{2^{O(n)}})$.

Proof: The Cayley-graph of an automatic of finite geometric type is an automatic graph of bounded degree.

For every automatic graph of bounded degree the first-order theory belongs to $\text{DSpace}(2^{2^{O(n)}})$.

Theorem

There exists a fixed automatic monoid \mathcal{M} such that for given $u, v \in \mathcal{M}$ it is undecidable whether $\exists x \in \mathcal{M} : ux = v$ in \mathcal{M} .

Reformulation: There exists a fixed automatic monoid \mathcal{M} such that **reachability** in the Cayley-graph of \mathcal{M} is undecidable.

Proof: Similarly to the P-hardness proof for the word problem.

Theorem

There exists a fixed automatic monoid \mathcal{M} such that for given $u, v \in \mathcal{M}$ it is undecidable whether $\exists x \in \mathcal{M} : ux = v$ in \mathcal{M} .

Reformulation: There exists a fixed automatic monoid \mathcal{M} such that **reachability** in the Cayley-graph of \mathcal{M} is undecidable.

Proof: Similarly to the P-hardness proof for the word problem.

Theorem

There exists a fixed automatic monoid \mathcal{M} such that for given $u, v \in \mathcal{M}$ it is undecidable whether $\exists x \in \mathcal{M} : ux = v$ in \mathcal{M} .

Reformulation: There exists a fixed automatic monoid \mathcal{M} such that **reachability** in the Cayley-graph of \mathcal{M} is undecidable.

Proof: Similarly to the P-hardness proof for the word problem.

- Is there an automatic group with a P-complete word problem?
- Is there a hyperbolic group with a LOGCFL-complete word problem?

- Is there an automatic group with a P-complete word problem?
- Is there a hyperbolic group with a LOGCFL-complete word problem?