Extended finite automata and decision problems for matrix semigroups

Özlem Salehi, Ahmet Celal Cem Say

Department of Computer Engineering, Boğaziçi University
İstanbul, Turkey

NCMA'18

Introduction

Aim: Make a connection between extended finite automata over matrix semigroups and decision problems for matrix semigroups

Let G be a group. *Extended finite automaton over* G, (G-automaton, group automaton) is defined as

Let G be a group. *Extended finite automaton over* G, (G-automaton, group automaton) is defined as

- *One-way finite state automaton equipped with a register*

Let G be a group. *Extended finite automaton over G*, (G-automaton, group automaton) is defined as

- *One-way finite state automaton equipped with a register*
- *Register is initialized with the identity element of G*

Let G be a group. *Extended finite automaton over G*, (G-automaton, group automaton) is defined as

- *One-way finite state automaton equipped with a register*
- *Register is initialized with the identity element of G*
- *Register is multiplied with an element of G at each step*

Let G be a group. *Extended finite automaton over G*, (G-automaton, group automaton) is defined as

- *One-way finite state automaton equipped with a register*
- *Register is initialized with the identity element of G*
- *Register is multiplied with an element of G at each step*
- *An input string is accepted if the register is equal to the identity at the end of the computation*

Let G be a group. *Extended finite automaton over* G, (G-automaton, group automaton) is defined as

- *One-way finite state automaton equipped with a register*
- *Register is initialized with the identity element of* G
- *Register is multiplied with an element of* G *at each step*
- *An input string is accepted if the register is equal to the identity at the end of the computation*

Let M be a monoid. M-automaton is defined analogously.

- Let S be a semigroup. We want to allow the register to be multiplied elements from S.

- Let S be a semigroup. We want to allow the register to be multiplied elements from S.
- We define S-automaton by letting 1 to be the identity element.

- Let S be a semigroup. We want to allow the register to be multiplied elements from S.
- We define S-automaton by letting 1 to be the identity element.
- If S is not a monoid nor a group, then only the empty string can be accepted.

Let S be a matrix semigroup finitely generated by a generating set of square matrices F. The **membership problem** *is to decide whether or not a given matrix Y belongs to the matrix semigroup S.*

Background
Membership problem for matrix semigroups

Let S be a matrix semigroup finitely generated by a generating set of square matrices F. The **membership problem** *is to decide whether or not a given matrix Y belongs to the matrix semigroup S.*

Given: $F = \{Y_1, Y_2, \ldots, Y_n\}$ *and a matrix* Y
Problem: *Determine if there exist an integer* $k \geq 1$ *and* $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$ *such that* $Y_{i_1} Y_{i_2} \cdots Y_{i_k} = Y$.

When Y is restricted to be the identity matrix, the problem is called the **identity problem**.

When Y is restricted to be the identity matrix, the problem is called the **identity problem**.

Given: $F = \{Y_1, Y_2, \ldots, Y_n\}$
Problem: *Determine if there exist an integer $k \geq 1$ and $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$ such that $Y_{i_1} Y_{i_2} \cdots Y_{i_k} = I$.*

Let G be a finitely generated group and let H be a subgroup of G. **Subgroup membership problem** *or* **generalized word problem** *for H in G is to decide whether or not a given element $g \in G$ belongs to the subgroup H.*

Let G be a finitely generated group and let H be a subgroup of G. **Subgroup membership problem** *or* **generalized word problem** *for H in G is to decide whether or not a given element $g \in G$ belongs to the subgroup H.*

Word problem *for G is the membership problem for the trivial group generated by 1.*

Let G be a finitely generated group and let H be a subgroup of G. **Subgroup membership problem** *or* **generalized word problem** *for H in G is to decide whether or not a given element $g \in G$ belongs to the subgroup H.*

Word problem *for G is the membership problem for the trivial group generated by 1.*

The subgroup membership problem can be seen as a special case of the (semigroup) membership problem.

Previous work

	Identity problem	**Membership problem**
$\mathbb{Z}^{2\times 2}$	decidable	decidable
H	decidable	?
$SL(3,\mathbb{Z})$	?	?
$\mathbb{Z}^{3\times 3}$	?	undecidable
$SL(4,\mathbb{Z})$	undecidable	undecidable

The emptiness problem and subgroup membership problem

Theorem

Let H be a finitely generated subgroup of G. If the emptiness problem for G-automata is decidable, then the subgroup membership problem for H in G is decidable.

The emptiness problem and subgroup membership problem

Theorem

Let H be a finitely generated subgroup of G. If the emptiness problem for G-automata is decidable, then the subgroup membership problem for H in G is decidable.

Proof.

- Let g be an element from G. We should decide whether $g \in H$.

The emptiness problem and subgroup membership problem

Theorem

Let H be a finitely generated subgroup of G. If the emptiness problem for G-automata is decidable, then the subgroup membership problem for H in G is decidable.

Proof.

- Let g be an element from G. We should decide whether $g \in H$.
- Construct G-automaton V.

The emptiness problem and subgroup membership problem

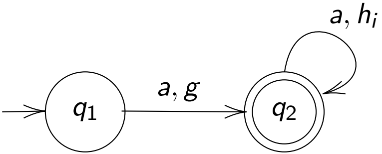
Theorem

Let H be a finitely generated subgroup of G. If the emptiness problem for G-automata is decidable, then the subgroup membership problem for H in G is decidable.

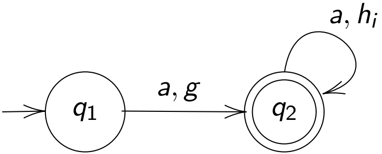
Proof.

- Let g be an element from G. We should decide whether $g \in H$.
- Construct G-automaton V.
- We are going to show that $g \in H$ iff $L(V)$ is nonempty.

The emptiness problem and subgroup membership problem



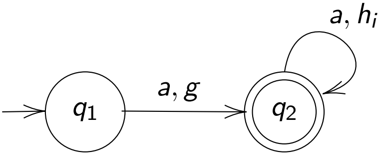
The emptiness problem and subgroup membership problem



Proof.

- $\{h_1, \ldots, h_n\}$ generates H

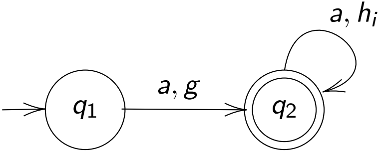
The emptiness problem and subgroup membership problem



Proof.

- $\{h_1, \ldots, h_n\}$ generates H
- Claim: $g \in H$ iff $L(V)$ is nonempty.

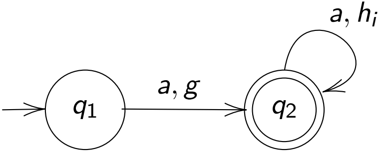
The emptiness problem and subgroup membership problem



Proof.

- $g \in H \implies g^{-1} \in H$

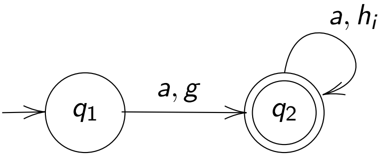
The emptiness problem and subgroup membership problem



Proof.

- $g \in H \implies g^{-1} \in H$
- $h_{i_1} h_{i_2} \cdots h_{i_k} = g^{-1}$ for some $k \geq 1$ and $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$

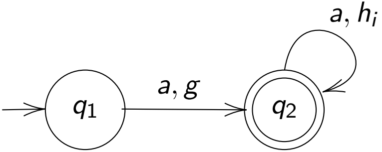
The emptiness problem and subgroup membership problem



Proof.

- $g \in H \implies g^{-1} \in H$
- $h_{i_1} h_{i_2} \cdots h_{i_k} = g^{-1}$ for some $k \geq 1$ and $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$
- $gg^{-1} = 1 \implies a^{k+1} \in L(V)$

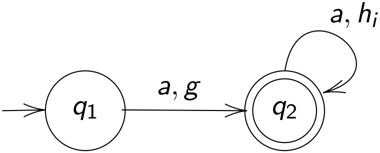
The emptiness problem and subgroup membership problem



Proof.

- $g \in H \implies g^{-1} \in H$
- $h_{i_1} h_{i_2} \cdots h_{i_k} = g^{-1}$ for some $k \geq 1$ and $i_1, i_2, \ldots, i_k \in \{1, \ldots, n\}$
- $gg^{-1} = 1 \implies a^{k+1} \in L(V)$
- $L(V)$ is nonempty

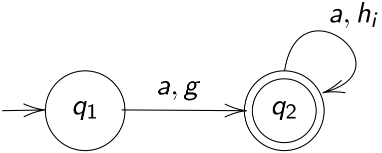
The emptiness problem and subgroup membership problem



Proof.

- Suppose $L(V)$ is nonempty

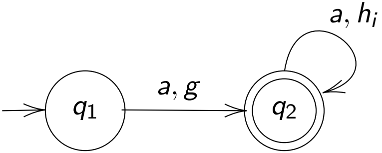
The emptiness problem and subgroup membership problem



Proof.

- Suppose $L(V)$ is nonempty
- Acceptance condition: register is equal to identity

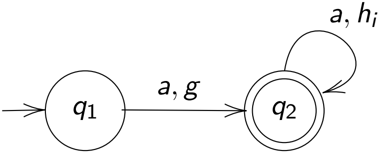
The emptiness problem and subgroup membership problem



Proof.

- Suppose $L(V)$ is nonempty
- Acceptance condition: register is equal to identity
- Register is initially multiplied by $g \implies H$ contains g^{-1}.

The emptiness problem and subgroup membership problem



Proof.

- Suppose $L(V)$ is nonempty
- Acceptance condition: register is equal to identity
- Register is initially multiplied by $g \implies H$ contains g^{-1}.
- $g^{-1} \in H \implies g \in H$

The emptiness problem and subgroup membership problem

Proof.

- Suppose that the emptiness problem for G-automaton is decidable.

Proof.

- Suppose that the emptiness problem for G-automaton is decidable.
- To check if $g \in H$,

The emptiness problem and subgroup membership problem

Proof.

- Suppose that the emptiness problem for G-automaton is decidable.
- To check if $g \in H$,
  - Construct V

The emptiness problem and subgroup membership problem

Proof.

- Suppose that the emptiness problem for G-automaton is decidable.
- To check if $g \in H$,
  - Construct V
  - Check if $L(V)$ is nonempty

The emptiness problem and subgroup membership problem

Proof.

- Suppose that the emptiness problem for G-automaton is decidable.
- To check if $g \in H$,
  - Construct V
  - Check if $L(V)$ is nonempty

$\implies$ subgroup membership problem for H is decidable .

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Theorem

Given a matrix Y *from* $\mathbb{Z}^{2\times 2}$ *and a subgroup* H *of* $\mathbb{Z}^{2\times 2}$*, it is decidable whether* Y *belongs to* H.

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Theorem

Given a matrix Y from $\mathbb{Z}^{2\times 2}$ and a subgroup H of $\mathbb{Z}^{2\times 2}$, it is decidable whether Y belongs to H.

Proof.

- We will prove that the emptiness problem for $\mathbb{Z}^{2\times 2}$-automata is decidable

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Theorem

Given a matrix Y from $\mathbb{Z}^{2\times 2}$ and a subgroup H of $\mathbb{Z}^{2\times 2}$, it is decidable whether Y belongs to H.

Proof.

- We will prove that the emptiness problem for $\mathbb{Z}^{2\times 2}$-automata is decidable
- Suppose that a $\mathbb{Z}^{2\times 2}$-automaton V is given.

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Theorem

Given a matrix Y from $\mathbb{Z}^{2\times 2}$ and a subgroup H of $\mathbb{Z}^{2\times 2}$, it is decidable whether Y belongs to H.

Proof.

- We will prove that the emptiness problem for $\mathbb{Z}^{2\times 2}$-automata is decidable
- Suppose that a $\mathbb{Z}^{2\times 2}$-automaton V is given.
  - Remove edges labeled by a non-invertible matrix from V

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Theorem

Given a matrix Y from $\mathbb{Z}^{2\times 2}$ and a subgroup H of $\mathbb{Z}^{2\times 2}$, it is decidable whether Y belongs to H.

Proof.

- We will prove that the emptiness problem for $\mathbb{Z}^{2\times 2}$-automata is decidable
- Suppose that a $\mathbb{Z}^{2\times 2}$-automaton V is given.
  - Remove edges labeled by a non-invertible matrix from V
  - Matrices multiplied by the register are invertible and belong to $GL(2, \mathbb{Z})$

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Theorem

Given a matrix Y from $\mathbb{Z}^{2\times 2}$ and a subgroup H of $\mathbb{Z}^{2\times 2}$, it is decidable whether Y belongs to H.

Proof.

- We will prove that the emptiness problem for $\mathbb{Z}^{2\times 2}$-automata is decidable
- Suppose that a $\mathbb{Z}^{2\times 2}$-automaton V is given.
  - Remove edges labeled by a non-invertible matrix from V
  - Matrices multiplied by the register are invertible and belong to $GL(2,\mathbb{Z})$
- V is a $GL(2,\mathbb{Z})$-automaton

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Lemma

Let G be a finitely generated group and let H be a subgroup of finite index. Any G-automaton can be converted into an H-automaton recognizing the same language.

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Lemma

Let G be a finitely generated group and let H be a subgroup of finite index. Any G-automaton can be converted into an H-automaton recognizing the same language.

Lemma

Any $\mathbf{F}_2$-automaton can be converted into a pushdown automaton recognizing the same language.

Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$

Theorem

Given a matrix Y from $\mathbb{Z}^{2\times 2}$ and a subgroup H of $\mathbb{Z}^{2\times 2}$, it is decidable whether Y belongs to H.

Proof.

- A pushdown automaton recognizing $L(V)$ can be constructed
  - $\mathbf{F}_2$ has finite index in $GL(2, \mathbb{Z})$
  - $\mathbf{F}_2$-automaton recognizing $L(V)$ can be constructed
  - $\mathbf{F}_2$-automaton can be converted to a pushdown automaton
- Emptiness problem for pda is decidable $\implies$ Emptiness problem for $\mathbb{Z}^{2\times 2}$-automata is decidable

The emptiness problem and identity problem

Theorem

Let S be a semigroup. The identity problem for S is decidable if the emptiness problem for S-automaton is decidable.

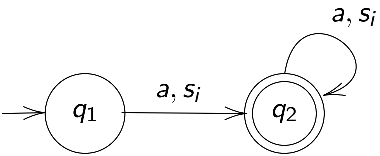
The emptiness problem and identity problem

Theorem

Let S be a semigroup. The identity problem for S is decidable if the emptiness problem for S-automaton is decidable.

Proof.

- Construct an S-automaton V such that $1 \in S$ iff $L(V)$ is nonempty.



Undecidability of the emptiness problem for $\mathbb{Z}^{4\times 4}$-automata

Fact

Given a semigroup S generated by eight 4×4 integer matrices, determining whether the identity matrix belongs to S is undecidable. [KNP17]

Undecidability of the emptiness problem for $\mathbb{Z}^{4\times 4}$-automata

Fact

Given a semigroup S generated by eight 4×4 integer matrices, determining whether the identity matrix belongs to S is undecidable. [KNP17]

Corollary

Let S be a subsemigroup of $\mathbb{Z}^{4\times 4}$ generated by eight matrices. The emptiness problem for S-automaton is undecidable.

Undecidability of the emptiness problem for $\mathbb{Z}^{4\times 4}$-automata

Fact

Given a semigroup S generated by eight 4×4 integer matrices, determining whether the identity matrix belongs to S is undecidable. [KNP17]

Corollary

Let S be a subsemigroup of $\mathbb{Z}^{4\times 4}$ generated by eight matrices. The emptiness problem for S-automaton is undecidable.

Proof.

We know that the identity problem for S is undecidable. By the above theorem the result follows.

The universe problem and subgroup membership problem

Theorem

Let H be a finitely generated subgroup of G. If the universe problem for G-automata is decidable, then the subgroup membership problem for H in G is decidable.

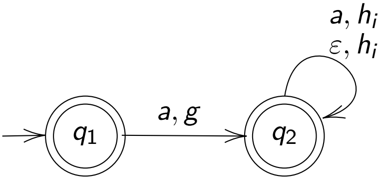
The universe problem and subgroup membership problem

Theorem

Let H be a finitely generated subgroup of G. If the universe problem for G-automata is decidable, then the subgroup membership problem for H in G is decidable.

Proof.

- Construct G-automaton V such that $g \in H$ iff $L(V) = \Sigma^*$.



The universe problem and identity problem

Theorem

Let S be a finitely generated semigroup. If the universe problem for S-automata is decidable, then the identity problem for S is decidable.

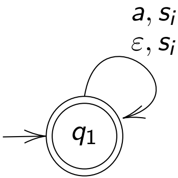
The universe problem and identity problem

Theorem

Let S be a finitely generated semigroup. If the universe problem for S-automata is decidable, then the identity problem for S is decidable.

Proof.

- Construct an S-automaton V such that $1 \in S$ iff $L(V) = \Sigma^*$



Remark

Converses are not true:

Remark

Converses are not true:

- Universe problem for $\mathbf{F}_2$-automaton is undecidable

Remark

Converses are not true:

- Universe problem for $\mathbf{F}_2$-automaton is undecidable
  - For a given pushdown automaton, an $\mathbf{F}_2$-automaton recognizing the same language can be constructed

Remark

Converses are not true:

- Universe problem for $\mathbf{F}_2$-automaton is undecidable
  - For a given pushdown automaton, an $\mathbf{F}_2$-automaton recognizing the same language can be constructed
  - Universe problem for pushdown automata is undecidable

Remark

Converses are not true:

- Universe problem for $\mathbf{F}_2$-automaton is undecidable
  - For a given pushdown automaton, an $\mathbf{F}_2$-automaton recognizing the same language can be constructed
  - Universe problem for pushdown automata is undecidable
- $\mathbf{F}_2$ is a subgroup of $SL(2, \mathbb{Z})$ and the membership and identity problems for $SL(2, \mathbb{Z})$ are decidable

Conclusion

We make a connection between the decidability of the subgroup membership and identity problems and the universe and emptiness problems for extended finite automata

Conclusion

We make a connection between the decidability of the subgroup membership and identity problems and the universe and emptiness problems for extended finite automata

- Emptiness problem for S-automata
  - Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$
  - Undecidability of the emptiness problem for $\mathbb{Z}^{4\times 4}$-automata
- Universe problem for S-automata

Conclusion

We make a connection between the decidability of the subgroup membership and identity problems and the universe and emptiness problems for extended finite automata

- Emptiness problem for S-automata
  - Decidability of the subgroup membership problem for $\mathbb{Z}^{2\times 2}$
  - Undecidability of the emptiness problem for $\mathbb{Z}^{4\times 4}$-automata
- Universe problem for S-automata

Identity and membership problems for 3×3 integer matrix groups are open.

Thank You!