Rational subsets and submonoids of wreath products

Markus Lohrey¹ Benjamin Steinberg² Georg Zetzsche³

¹Universität Leipzig ²City College of New York ³Technische Universität Kaiserslautern

ICALP 2013

Rational sets in arbitrary monoids: Definition 1

Let M be a monoid.

For $L \subseteq M$ let L^* denote the submonoid of M generated by L.

Let M be a monoid.

For $L \subseteq M$ let L^* denote the submonoid of M generated by L.

The set $Rat(M) \subseteq 2^M$ of all rational subsets of M is the smallest set such that:

- Every finite subset of M belongs to Rat(M).
- If $L_1, L_2 \in \operatorname{Rat}(M)$, then also $L_1 \cup L_2, L_1L_2 \in \operatorname{Rat}(M)$.
- If $L \in \operatorname{Rat}(M)$, then also $L^* \in \operatorname{Rat}(M)$.

A finite automaton over M is a tuple $A = (Q, \Delta, q_0, F)$ where

- Q is a finite set of states,
- $q_0 \in Q$, $F \subseteq Q$, and
- $\Delta \subseteq Q \times M \times Q$ is finite.

The subset $L(A) \subseteq M$ is the set of all products $m_1m_2\cdots m_k$ such that there exist $q_1, \ldots, q_k \in Q$ with

$$(q_{i-1}, m_i, q_i) \in \Delta$$
 for $1 \leq i \leq k$ and $q_k \in F$.

Then:

$$L \in \operatorname{Rat}(M) \iff \exists$$
 finite automaton A over $M : L(A) = L$

Let Σ be a finite (group) generating set for G.

Let Σ be a finite (group) generating set for G.

Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

Let Σ be a finite (group) generating set for G.

Elements of G can be represented by finite words over $\Sigma \cup \Sigma^{-1}$.

The rational subset membership problem for G (RatMP(G)) is the following computational problem:

INPUT: A finite automaton A over G and $g \in G$ QUESTION: $g \in L(A)$? The submonoid membership problem for G is the following computational problem:

```
INPUT: A finite subset A \subseteq G and g \in G
QUESTION: g \in A^*?
```

The subgroup membership problem for G (or generalized word problem for G) is the following computational problem: INPUT: A finite subset $A \subseteq G$ and $g \in G$ QUESTION: $g \in \langle A \rangle$ (= $(A \cup A^{-1})^*$)?

The generalized word problem is a widely studied problem in combinatorial group theory.

Wreath products

Let A and B be groups and let

$$K = \bigoplus_{b \in B} A$$

be the direct sum of copies of A.

Let A and B be groups and let

$$K = \bigoplus_{b \in B} A$$

be the direct sum of copies of A.

Elements of K: mappings $k : B \to A$ with finite support (i.e., $k^{-1}(A \setminus 1)$ is finite).

Let A and B be groups and let

$$K = \bigoplus_{b \in B} A$$

be the direct sum of copies of A.

Elements of K: mappings $k : B \to A$ with finite support (i.e., $k^{-1}(A \setminus 1)$ is finite).

The wreath product $A \wr B$ is the set of all pairs $K \times B$ with the following multiplication, where $(k_1, b_1), (k_2, b_2) \in K \times B$:

$$(k_1, b_1)(k_2, b_2) = (k, b_1b_2)$$
 with $\forall b \in B : k(b) = k_1(b)k_2(b_1^{-1}b)$.



cbcb⁻¹*cabcb*⁻¹*ca*:























For every nontrivial group H, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

For every nontrivial group *H*, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

Proof idea: The grid-like structure of the Cayley graph of $\mathbb{Z}\times\mathbb{Z}$ allows to encode a tiling problem.

For every nontrivial group *H*, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

Proof idea: The grid-like structure of the Cayley graph of $\mathbb{Z}\times\mathbb{Z}$ allows to encode a tiling problem.

Theorem

The submonoid membership problem for the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

For every nontrivial group *H*, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

Proof idea: The grid-like structure of the Cayley graph of $\mathbb{Z}\times\mathbb{Z}$ allows to encode a tiling problem.

Theorem

The submonoid membership problem for the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.

For every nontrivial group *H*, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

Proof idea: The grid-like structure of the Cayley graph of $\mathbb{Z}\times\mathbb{Z}$ allows to encode a tiling problem.

Theorem

The submonoid membership problem for the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.



For every nontrivial group *H*, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

Proof idea: The grid-like structure of the Cayley graph of $\mathbb{Z}\times\mathbb{Z}$ allows to encode a tiling problem.

Theorem

The submonoid membership problem for the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.



For every nontrivial group *H*, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

Proof idea: The grid-like structure of the Cayley graph of $\mathbb{Z}\times\mathbb{Z}$ allows to encode a tiling problem.

Theorem

The submonoid membership problem for the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.



For every nontrivial group H, RatMP($H \wr (\mathbb{Z} \times \mathbb{Z})$) is undecidable.

Proof idea: The grid-like structure of the Cayley graph of $\mathbb{Z}\times\mathbb{Z}$ allows to encode a tiling problem.

Theorem

The submonoid membership problem for the wreath product $\mathbb{Z} \wr \mathbb{Z}$ is undecidable.



Rational subsets in wreath products: Decidability

Theorem

 $RatMP(H \wr V)$ is decidable for every finite group H and virtually free group V.

 $RatMP(H \wr V)$ is decidable for every finite group H and virtually free group V.

We only consider a wreath product

$$G = H \wr F(a, b)$$

with H finite and F(a, b) the free group generated by a and b.

RatMP($H \wr V$) is decidable for every finite group H and virtually free group V.

We only consider a wreath product

$$G = H \wr F(a, b)$$

with H finite and F(a, b) the free group generated by a and b.

G is generated as a monoid by $H \cup \{a, b, a^{-1}, b^{-1}\}$.

 $RatMP(H \wr V)$ is decidable for every finite group H and virtually free group V.

We only consider a wreath product

$$G = H \wr F(a, b)$$

with H finite and F(a, b) the free group generated by a and b.

G is generated as a monoid by $H \cup \{a, b, a^{-1}, b^{-1}\}$.

Fix an automaton $A = (Q, \Delta, q_0, F)$ over the finite alphabet $H \cup \{a, b, a^{-1}, b^{-1}\}.$

 $RatMP(H \wr V)$ is decidable for every finite group H and virtually free group V.

We only consider a wreath product

$$G = H \wr F(a, b)$$

with H finite and F(a, b) the free group generated by a and b.

G is generated as a monoid by $H \cup \{a, b, a^{-1}, b^{-1}\}$.

Fix an automaton $A = (Q, \Delta, q_0, F)$ over the finite alphabet $H \cup \{a, b, a^{-1}, b^{-1}\}$.

We want to check whether there is a $w \in L(A)$ with w = 1 in G.

Let $p, q \in Q$, $d \in \{a, b, a^{-1}, b^{-1}\}$. A (p, d, q)-loop is an A-path

$$\pi = (p = p_0 \xrightarrow{d} p_1 \xrightarrow{\alpha_1} p_2 \xrightarrow{\alpha_2} p_3 \cdots \xrightarrow{\alpha_{n-1}} p_n \xrightarrow{d^{-1}} p_{n+1} = q)$$

with the following properties, where $\alpha_1 \cdots \alpha_i = (k_i, u_i) \in H \wr F_2$ for $1 \le i \le n-1$:

3

Let $p, q \in Q$, $d \in \{a, b, a^{-1}, b^{-1}\}$. A (p, d, q)-loop is an A-path

$$\pi = (p = p_0 \xrightarrow{d} p_1 \xrightarrow{\alpha_1} p_2 \xrightarrow{\alpha_2} p_3 \cdots \xrightarrow{\alpha_{n-1}} p_n \xrightarrow{d^{-1}} p_{n+1} = q)$$

with the following properties, where $\alpha_1 \cdots \alpha_i = (k_i, u_i) \in H \wr F_2$ for $1 \le i \le n-1$:

 For all 1 ≤ i ≤ n − 1, the unique reduced word for u_i does not start with d⁻¹.

Let $p, q \in Q$, $d \in \{a, b, a^{-1}, b^{-1}\}$. A (p, d, q)-loop is an A-path

$$\pi = (p = p_0 \xrightarrow{d} p_1 \xrightarrow{\alpha_1} p_2 \xrightarrow{\alpha_2} p_3 \cdots \xrightarrow{\alpha_{n-1}} p_n \xrightarrow{d^{-1}} p_{n+1} = q)$$

with the following properties, where $\alpha_1 \cdots \alpha_i = (k_i, u_i) \in H \wr F_2$ for $1 \le i \le n-1$:

 For all 1 ≤ i ≤ n − 1, the unique reduced word for u_i does not start with d⁻¹.

•
$$u_{n-1} = 1$$
 in F_2

3

Let $p, q \in Q$, $d \in \{a, b, a^{-1}, b^{-1}\}$. A (p, d, q)-loop is an A-path

$$\pi = (p = p_0 \xrightarrow{d} p_1 \xrightarrow{\alpha_1} p_2 \xrightarrow{\alpha_2} p_3 \cdots \xrightarrow{\alpha_{n-1}} p_n \xrightarrow{d^{-1}} p_{n+1} = q)$$

with the following properties, where $\alpha_1 \cdots \alpha_i = (k_i, u_i) \in H \wr F_2$ for $1 \le i \le n-1$:

 For all 1 ≤ i ≤ n − 1, the unique reduced word for u_i does not start with d⁻¹.

•
$$u_{n-1} = 1$$
 in F_2

We define

• depth(π) = max{ $|u_i| + 1 | 1 \le i \le n - 1$ }

Let $p, q \in Q$, $d \in \{a, b, a^{-1}, b^{-1}\}$. A (p, d, q)-loop is an A-path

$$\pi = (p = p_0 \xrightarrow{d} p_1 \xrightarrow{\alpha_1} p_2 \xrightarrow{\alpha_2} p_3 \cdots \xrightarrow{\alpha_{n-1}} p_n \xrightarrow{d^{-1}} p_{n+1} = q)$$

with the following properties, where $\alpha_1 \cdots \alpha_i = (k_i, u_i) \in H \wr F_2$ for $1 \le i \le n-1$:

 For all 1 ≤ i ≤ n − 1, the unique reduced word for u_i does not start with d⁻¹.

•
$$u_{n-1} = 1$$
 in F_2

We define

- depth(π) = max{ $|u_i| + 1 | 1 \le i \le n 1$ }
- effect $(\pi) = d\alpha_1 \cdots \alpha_{n-1} d^{-1} \in K$.

For all types $t \in \{1, a, a^{-1}, b, b^{-1}\}$ define

$$C_t = \{a, a^{-1}, b, b^{-1}\} \setminus \{t^{-1}\}$$



э

For all types $t \in \{1, a, a^{-1}, b, b^{-1}\}$ define

$$C_t = \{a, a^{-1}, b, b^{-1}\} \setminus \{t^{-1}\}$$

$$X_t = \{(p, d, q) \mid d \in C_t, \exists (p, d, q)\text{-loop}\}$$



э

For all types $t \in \{1, a, a^{-1}, b, b^{-1}\}$ define

$$C_t = \{a, a^{-1}, b, b^{-1}\} \setminus \{t^{-1}\}$$

$$X_t = \{(p, d, q) \mid d \in C_t, \exists (p, d, q)\text{-loop}\}$$





Loop patterns

Let $t \in \{1, a, a^{-1}, b, b^{-1}\}$ be a type.

Lohrey, Steinberg, Zetzsche Wreath Products

< D > < B > < E</p>

ъ

æ

Let
$$t \in \{1, a, a^{-1}, b, b^{-1}\}$$
 be a type.

$$w = (p_1, d_1, q_1)(p_2, d_2, q_2) \cdots (p_n, d_n, q_n) \in X_t^*.$$

such that for every $1 \le i \le n$ there exists a (p_i, d_i, q_i) -loop π_i with

 $\operatorname{effect}(\pi_1)\operatorname{effect}(\pi_2)\cdots\operatorname{effect}(\pi_n)=1$ in K.

Let
$$t \in \{1, a, a^{-1}, b, b^{-1}\}$$
 be a type.

$$w = (p_1, d_1, q_1)(p_2, d_2, q_2) \cdots (p_n, d_n, q_n) \in X_t^*.$$

such that for every $1 \le i \le n$ there exists a (p_i, d_i, q_i) -loop π_i with

$$effect(\pi_1)effect(\pi_2)\cdots effect(\pi_n) = 1$$
 in K.

The depth of this loop pattern is min $(\max_{1 \le i \le n} \text{depth}(\pi_i))$, where the min is taken over all π_1, \ldots, π_n as above.

Let
$$t \in \{1, a, a^{-1}, b, b^{-1}\}$$
 be a type.

$$w = (p_1, d_1, q_1)(p_2, d_2, q_2) \cdots (p_n, d_n, q_n) \in X_t^*.$$

such that for every $1 \le i \le n$ there exists a (p_i, d_i, q_i) -loop π_i with

$$effect(\pi_1)effect(\pi_2)\cdots effect(\pi_n) = 1$$
 in K.

The depth of this loop pattern is $\min(\max_{1 \le i \le n} \operatorname{depth}(\pi_i))$, where the min is taken over all π_1, \ldots, π_n as above.

Let P_t be the set of all loop patterns at t.

Let
$$t \in \{1, a, a^{-1}, b, b^{-1}\}$$
 be a type.

$$w = (p_1, d_1, q_1)(p_2, d_2, q_2) \cdots (p_n, d_n, q_n) \in X_t^*.$$

such that for every $1 \le i \le n$ there exists a (p_i, d_i, q_i) -loop π_i with

$$effect(\pi_1)effect(\pi_2)\cdots effect(\pi_n) = 1$$
 in K.

The depth of this loop pattern is $\min(\max_{1 \le i \le n} \operatorname{depth}(\pi_i))$, where the min is taken over all π_1, \ldots, π_n as above.

Let P_t be the set of all loop patterns at t.

We will show:

• P_t is regular and

Let
$$t \in \{1, a, a^{-1}, b, b^{-1}\}$$
 be a type.

$$w = (p_1, d_1, q_1)(p_2, d_2, q_2) \cdots (p_n, d_n, q_n) \in X_t^*.$$

such that for every $1 \le i \le n$ there exists a (p_i, d_i, q_i) -loop π_i with

$$effect(\pi_1)effect(\pi_2)\cdots effect(\pi_n) = 1$$
 in K.

The depth of this loop pattern is min $(\max_{1 \le i \le n} \text{depth}(\pi_i))$, where the min is taken over all π_1, \ldots, π_n as above.

Let P_t be the set of all loop patterns at t.

We will show:

- P_t is regular and
- an automaton for P_t can be computed.

A WQO (well quasi order) is a reflexive and transitive relation \leq (on a set *A*) such that for every infinite sequence a_1, a_2, a_3, \ldots there exist i < j with $a_i \leq a_j$.

A WQO (well quasi order) is a reflexive and transitive relation \leq (on a set A) such that for every infinite sequence a_1, a_2, a_3, \ldots there exist i < j with $a_i \leq a_j$.

For a group H, we define a partial order \leq_H on X^* (X any finite alphabet) as follows: $u \leq_H v$ iff there exist factorizations

$$u = x_1 x_2 \cdots x_n \quad (x_i \in X)$$

$$v = v_0 x_1 v_1 x_2 \cdots v_{n-1} x_n v_n$$

such that for every homomorphism $\varphi : X^* \to H$ we have $\varphi(v_0) = \varphi(v_1) = \cdots \varphi(v_n) = 1.$

A WQO (well quasi order) is a reflexive and transitive relation \leq (on a set A) such that for every infinite sequence a_1, a_2, a_3, \ldots there exist i < j with $a_i \leq a_j$.

For a group H, we define a partial order \leq_H on X^* (X any finite alphabet) as follows: $u \leq_H v$ iff there exist factorizations

$$u = x_1 x_2 \cdots x_n \quad (x_i \in X)$$

$$v = v_0 x_1 v_1 x_2 \cdots v_{n-1} x_n v_n$$

such that for every homomorphism $\varphi : X^* \to H$ we have $\varphi(v_0) = \varphi(v_1) = \cdots \varphi(v_n) = 1.$

Lemma

For every finite group H, \leq_H is a WQO.

Lemma

For every $t \in \{1, a, a^{-1}, b, b^{-1}\}$, the set of loop patterns P_t is upward closed w.r.t. \leq_H .

Lemma

For every $t \in \{1, a, a^{-1}, b, b^{-1}\}$, the set of loop patterns P_t is upward closed w.r.t. \leq_H .

This implies that P_t is regular, but can we compute an NFA for P_t ?

For $i \in \mathbb{N}$, let $P_t^{(i)} \subseteq X_t^*$ be the set of loop patterns of depth $\leq i$.

Observation

There is an operator Φ with

$$\Phi\left[(P_t^{(i)})_{t\in\mathcal{T}}\right] = (P_t^{(i+1)})_{t\in\mathcal{T}}$$

such that Φ is effectively regularity perserving: For regular sets R_t , the languages in the tuple $\Phi[(R_t)_{t \in T}]$ are effectively regular.

For $i \in \mathbb{N}$, let $P_t^{(i)} \subseteq X_t^*$ be the set of loop patterns of depth $\leq i$.

Observation

There is an operator Φ with

$$\Phi\left[(P_t^{(i)})_{t\in\mathcal{T}}\right] = (P_t^{(i+1)})_{t\in\mathcal{T}}$$

such that Φ is effectively regularity perserving: For regular sets R_t , the languages in the tuple $\Phi[(R_t)_{t \in T}]$ are effectively regular.

Lemma

 $(P_t)_{t \in T}$ is the smallest fixpoint of Φ containing $(\{\lambda\})_{t \in T}$.

1:
$$U_t^{(0)} := \{\lambda\} \uparrow_H$$
 for each $t \in T$.
2: while $\exists w \in \Phi\left[(U_t^{(i)})_{t \in T} \right]_t \setminus U_t^{(i)}$ for some $t \in T$ do
3: $U_t^{(i+1)} := U_t^{(i)} \cup \{w\} \uparrow_H$
4: $i := i + 1$
5: end while

• The sets $U_t^{(i)}$ are upward closed w.r.t. \leq_H .

æ

1:
$$U_t^{(0)} := \{\lambda\} \uparrow_H$$
 for each $t \in T$.
2: while $\exists w \in \Phi\left[(U_t^{(i)})_{t \in T} \right]_t \setminus U_t^{(i)}$ for some $t \in T$ do
3: $U_t^{(i+1)} := U_t^{(i)} \cup \{w\} \uparrow_H$
4: $i := i + 1$
5: end while

◆□ > ◆□ > ◆臣 > ◆臣 > ─臣 ─のへで

1:
$$U_t^{(0)} := \{\lambda\} \uparrow_H$$
 for each $t \in T$.
2: while $\exists w \in \Phi\left[(U_t^{(i)})_{t \in T} \right]_t \setminus U_t^{(i)}$ for some $t \in T$ do
3: $U_t^{(i+1)} := U_t^{(i)} \cup \{w\} \uparrow_H$
4: $i := i + 1$
5: end while

Ξ.

イロト イヨト イヨト イヨト

1:
$$U_t^{(0)} := \{\lambda\} \uparrow_H$$
 for each $t \in T$.
2: while $\exists w \in \Phi\left[(U_t^{(i)})_{t \in T} \right]_t \setminus U_t^{(i)}$ for some $t \in T$ do
3: $U_t^{(i+1)} := U_t^{(i)} \cup \{w\} \uparrow_H$
4: $i := i + 1$
5: end while

Ξ.

イロト イヨト イヨト イヨト

 Complexity of RatMP(H ≥ V) for H finite and V virtually-free. Is RatMP(Z₂ ≥ Z) primitive recursive?

Open problems

- Complexity of RatMP(H ≥ V) for H finite and V virtually-free. Is RatMP(Z₂ ≥ Z) primitive recursive?
- Rational subset membership problem for wreath products
 H ≥ *V* with *V* virtually free and *H* a f.g. infinite torsion group.

- Complexity of RatMP(H ≥ V) for H finite and V virtually-free. Is RatMP(Z₂ ≥ Z) primitive recursive?
- Rational subset membership problem for wreath products
 H ≥ *V* with *V* virtually free and *H* a f.g. infinite torsion group.
- Rational subset membership problem for wreath products *H* ≥ *G* with *H* ≠ 1 and *G* not virtually-free.

- Complexity of RatMP(H ≥ V) for H finite and V virtually-free. Is RatMP(Z₂ ≥ Z) primitive recursive?
- Rational subset membership problem for wreath products
 H ≥ *V* with *V* virtually free and *H* a f.g. infinite torsion group.
- Rational subset membership problem for wreath products *H* ≥ *G* with *H* ≠ 1 and *G* not virtually-free.
- Conjecture: Whenever H is non-trivial and G is not virtually-free, then RatMP(H ≥ G) is undecidable.

- Complexity of RatMP(H ≥ V) for H finite and V virtually-free. Is RatMP(Z₂ ≥ Z) primitive recursive?
- Rational subset membership problem for wreath products
 H ≥ *V* with *V* virtually free and *H* a f.g. infinite torsion group.
- Rational subset membership problem for wreath products *H* ≥ *G* with *H* ≠ 1 and *G* not virtually-free.
- Conjecture: Whenever H is non-trivial and G is not virtually-free, then RatMP(H ≥ G) is undecidable.
- Is there a (necessarily one-ended) group G, for which the submonoid membership problem is decidable but RatMP(G) is undecidable?