Membership Problems in Nilpotent Groups

Corentin Bodart

Université de Genève

February 6th, 2024

Two algorithmic problems

Fix a group G and a finite generating set S.

Definition (Submonoid Membership)

Input: Elements g and $g_1, g_2, \ldots, g_k \in G$ (given as words over S).

Output: Decide whether $g \in \{g_1, g_2, \ldots, g_k\}^*$.

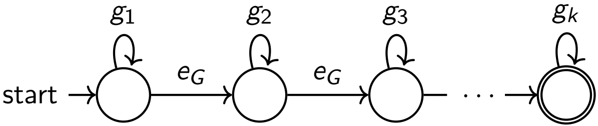
Definition (Rational Subset Membership)

Input: An element $g \in G$ (given as a word over S) and a rational subset $R \subseteq G$ (defined by a FSA, labeled by words over S).

Output: Decide whether $g \in R$.

Two (or three) algorithmic problems

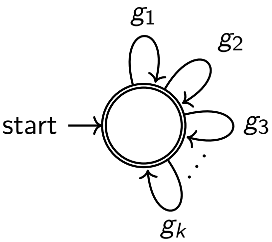
Example: Consider the automaton



We need to decide if $g \overset{?}{\in} R = \left\{ g_1^{n_1} g_2^{n_2} \cdots g_k^{n_k} \;\middle|\; n_1, n_2, \ldots, n_k \in \mathbb{Z}_{\geq 0} \right\}$.
This case of the Rational Subset Membership problem (for varying k) is the **Knapsack problem**.

Two algorithmic problems

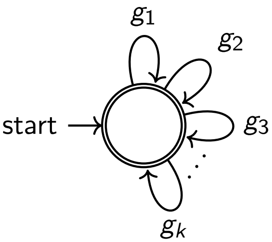
Example:



This case of the Rational Subset Membership problem is the ...

Two algorithmic problems

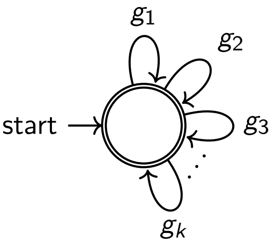
Example:



This case of the Rational Subset Membership problem is the ...
Submonoid Membership problem.

Two algorithmic problems

Example:



This case of the Rational Subset Membership problem is the ...
Submonoid Membership problem.

Question (Lohrey-Steinberg 2008)

Does there exist a group with decidable Submonoid Membership, and undecidable Rational Subset Membership?

(No among right-angled Artin groups and infinitely-ended groups.)

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G,G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0			
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1			
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$			

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G,G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0	✓	✓	✓[1]
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1			
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$			

[1] Grunschlag 1999, uses integer linear programming

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G,G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0	✓	✓	✓
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1			
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$			✗[2]

[2] Roman'kov 1999 (unpublished)

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G,G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0	✓	✓	✓
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1			
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$		✗[3]	✗

[3] König-Lohrey-Zetzsche 2016, Mishchenko-Treier 2017, uses the negative solution to Hilbert 10th problem: no algorithm can decide if a system of Diophantine equations admits a solution

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G, G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0	✓	✓	✓
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1			
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$	✗[4]	✗	✗

[4] Roman'kov 2022, negative solution to Hilbert 10th problem

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G,G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0	✓	✓	✓
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1		✓[5]	
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$	✗	✗	✗

[5] König-Lohrey-Zetzsche 2016, uses the existence of an algorithm deciding if a quadratic Diophantine equation (in multiple variables) admits a solution

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G, G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0	✓	✓	✓
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1	✓[6]	✓	
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$	✗	✗	✗

[6] Colcombet-Ouaknine-Semukhin-Worrell 2019, elementary! (Just some linear programming.)

State of the arts in nilpotent groups

- Subgroup Membership is decidable in nilpotent groups (Mal'cev 1958)
- For other Membership problems, the list goes as follows

Decidable?	$h([G, G])$	Semigroup	Knapsack	Rational Subset
Virtually abelian	0	✓	✓	✓
$H_{2m+1}(\mathbb{Z}) \times \mathbb{Z}^n$	1	✓[6]	✓	??
$N_{2,m}$ with $m \gg 1$	$\binom{m}{2}$	✗	✗	✗

[6] Colcombet-Ouaknine-Semukhin-Worrell 2019, elementary! (Just some linear programming.)

A Reduction Theorem

Theorem

There exists an algorithm with specifications

Input: *A f.p. nilpotent group G, a finite set $S \subset G$, and $g \in G$.*

Output: *Finitely many instances $h_i \overset{?}{\in} R_i$ of Rational Subset Membership in a subgroup $H \leq G$ such that $g \in S^*$ iff $h_i \in R_i$ for some i.*

Moreover, the algorithm solves these instances if $h([H, H]) = h([G, G])$.

Proof of the Theorem

We may assume $e_G \in S$.

(1) Compute the "torsionfree-abelian-isation"

$$\pi\colon G \twoheadrightarrow G/[G,G] \xrightarrow{\sim} \mathbb{Z}^r \times T \twoheadrightarrow \mathbb{Z}^r$$

(2) Compute $P = \mathrm{ConvHull}(\pi(S))$ and F the minimal face supporting $\mathbf{0}$.

Let $H = \pi^{-1}(\mathrm{Vect}(F))$. We denote $S_0 = S \cap H$ and $S_+ = S \setminus H$.

⚠ If $\mathbf{0}$ lie in the interior of P, then $F = P$ and $H = G$.

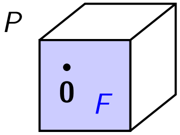
Proof of the Theorem

We may assume $e_G \in S$.

(1) Compute the "torsionfree-abelian-isation"

$$\pi\colon G \twoheadrightarrow G/[G,G] \xrightarrow{\sim} \mathbb{Z}^r \times T \twoheadrightarrow \mathbb{Z}^r$$

(2) Compute $P = \mathrm{ConvHull}(\pi(S))$ and F the minimal face supporting $\mathbf{0}$.



Let $H = \pi^{-1}(\mathrm{Vect}(F))$. We denote $S_0 = S \cap H$ and $S_+ = S \setminus H$.

⚠ If $\mathbf{0}$ lie in the interior of P, then $F = P$ and $H = G$.

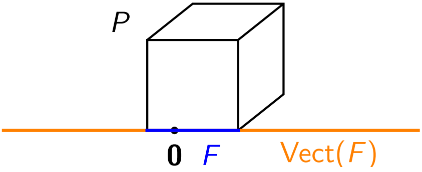
Proof of the Theorem

We may assume $e_G \in S$.

(1) Compute the "torsionfree-abelian-isation"

$$\pi\colon G \twoheadrightarrow G/[G,G] \xrightarrow{\sim} \mathbb{Z}^r \times T \twoheadrightarrow \mathbb{Z}^r$$

(2) Compute $P = \mathrm{ConvHull}(\pi(S))$ and F the minimal face supporting $\mathbf{0}$.



Let $H = \pi^{-1}(\mathrm{Vect}(F))$. We denote $S_0 = S \cap H$ and $S_+ = S \setminus H$.

⚠ If $\mathbf{0}$ lie in the interior of P, then $F = P$ and $H = G$.

Proof of the Theorem

(3) For any $g \in G$, there exists finitely many words $u_1 \dots u_k \in (S_+)^*$ s.t.

$$\pi(u_1 u_2 \dots u_k) - \pi(g) \in \mathrm{Vect}(F).$$

(4) For each of those word $u_1 u_2 \dots u_k$, we have to decide if

$$g \overset{?}{\in} S_0^* u_1 S_0^* u_2 S_0^* \dots S_0^* u_k S_0^*$$

$$\iff g(u_1 \dots u_k)^{-1} \overset{?}{\in} S_0^* \cdot (u_1 S_0 u_1^{-1})^* \dots ((u_1 \dots u_k) S_0 (u_1 \dots u_k)^{-1})^*$$

This is an instance of the Rational Subset Membership in H!

- If $h([H,H]) < h([G,G])$, then ☺.

Proof of the Theorem

(3) For any $g \in G$, there exists finitely many words $u_1 \dots u_k \in (S_+)^*$ s.t.

$$\pi(u_1 u_2 \dots u_k) - \pi(g) \in \mathrm{Vect}(F).$$

(4) For each of those word $u_1 u_2 \dots u_k$, we have to decide if

$$g \overset{?}{\in} S_0^* u_1 S_0^* u_2 S_0^* \dots S_0^* u_k S_0^*$$

$$\iff g(u_1 \dots u_k)^{-1} \overset{?}{\in} S_0^* \cdot \left(u_1 S_0 u_1^{-1}\right)^* \dots \left((u_1 \dots u_k) S_0 (u_1 \dots u_k)^{-1}\right)^*$$

This is an instance of the Rational Subset Membership in H!

- If $h([H, H]) < h([G, G])$, then ☺.

Proof of the Theorem

- Suppose $h([H,H]) = h([G,G])$ (eg. if $H = G$),

Lemma (B.-Ciobanu-Metcalfe)

Let H be a finitely generated nilpotent group and $S_0 \subset H$. TFAE

(a) $\mathbf{0}$ *lies in the interior of* $\mathrm{ConvHull}(\tau(S_0))$ *where*

$$\tau\colon H \twoheadrightarrow H/[H,H] \xrightarrow{\sim} \mathbb{Z}^s \times T \twoheadrightarrow \mathbb{Z}^s$$

(b) *The submonoid S_0^* is a finite-index subgroup in H.*

$h([H,H]) = h([G,G])$ implies $\tau = \pi|_H$ hence $\mathrm{ConvHull}(\tau(S_0)) = F$. We conclude that S_0^* is a finite-index subgroup in H, hence

$$g(u_1 \ldots u_k)^{-1} \overset{?}{\in} S_0^* \cdot \left(u_1 S_0 u_1^{-1}\right)^* \ldots \left((u_1 \ldots u_k) S_0 (u_1 \ldots u_k)^{-1}\right)^*$$

is easily decidable. □

Proof of the Theorem

- Suppose $h([H,H]) = h([G,G])$ (eg. if $H = G$),

Lemma (B.-Ciobanu-Metcalfe)

Let H be a finitely generated nilpotent group and $S_0 \subset H$. TFAE

(a) $\mathbf{0}$ *lies in the interior of* $\mathrm{ConvHull}(\tau(S_0))$ *where*

$$\tau \colon H \twoheadrightarrow H/[H,H] \xrightarrow{\sim} \mathbb{Z}^s \times T \twoheadrightarrow \mathbb{Z}^s$$

(b) *The submonoid S_0^* is a finite-index subgroup in H.*

$h([H,H]) = h([G,G])$ implies $\tau = \pi|_H$ hence $\mathrm{ConvHull}(\tau(S_0)) = F$. We conclude that S_0^* is a finite-index subgroup in H, hence

$$g(u_1 \ldots u_k)^{-1} \overset{?}{\in} S_0^* \cdot \left(u_1 S_0 u_1^{-1}\right)^* \ldots \left((u_1 \ldots u_k) S_0 (u_1 \ldots u_k)^{-1}\right)^*$$

is easily decidable. □

Submonoid Membership $\not\Rightarrow$ Rational Subset Membership

Corollary

There exist a group with decidable Submonoid Membership problem and undecidable Rational Subset Membership.

Proof.

Consider $G = N_{2,m} \times \mathbb{Z}^n$ with undecidable Rational Subset Membership and m minimum. We prove G has decidable Submonoid Membership.

Fact. All subgroups $H \leq G$ are virtually isomorphic to

$$N_{2,k} \times \mathbb{Z}^\ell \quad \text{with } k \leq m \text{ and } \ell \leq \binom{m}{2} - \binom{k}{2} + n.$$

By minimality of m, there exist a uniform(!) algorithm solving the Rational Subset Membership in all subgroups H with $h([H, H]) < h([G, G])$. □

Submonoid Membership $\not\Rightarrow$ Rational Subset Membership

Corollary

There exist a group with decidable Submonoid Membership problem and undecidable Rational Subset Membership.

Proof.

Consider $G = N_{2,m} \times \mathbb{Z}^n$ with undecidable Rational Subset Membership and m minimum. We prove G has decidable Submonoid Membership.

Fact. All subgroups $H \leq G$ are virtually isomorphic to

$$N_{2,k} \times \mathbb{Z}^\ell \quad \text{with } k \leq m \text{ and } \ell \leq \binom{m}{2} - \binom{k}{2} + n.$$

By minimality of m, there exist a uniform(!) algorithm solving the Rational Subset Membership in all subgroups H with $h([H, H]) < h([G, G])$. □

Other results

Theorem

Rational Subset Membership is decidable in $H_3(\mathbb{Z})$.

Idea: Reduction to the Knapsack problem in $H_3(\mathbb{Z})$, which is solvable.

Corollary

Submonoid Membership is decidable in the filiform 3-step nilpotent group

$$E = \left\langle x, y_1, y_2, y_3 \;\middle|\; [x, y_1] = y_2,\ [x, y_2] = y_3,\ [x, y_3] = [y_i, y_j] = 1 \right\rangle .$$

Conjecture

Rational Subset Membership is decidable in $H_{2m+1}(\mathbb{Z})$.

Other results

Theorem

Rational Subset Membership is decidable in $H_3(\mathbb{Z})$.

Idea: Reduction to the Knapsack problem in $H_3(\mathbb{Z})$, which is solvable.

Corollary

Submonoid Membership is decidable in the filiform 3-step nilpotent group

$$E = \left\langle x, y_1, y_2, y_3 \;\middle|\; [x, y_1] = y_2,\ [x, y_2] = y_3,\ [x, y_3] = [y_i, y_j] = 1 \right\rangle .$$

Conjecture

Rational Subset Membership is decidable in $H_{2m+1}(\mathbb{Z})$.

Other results

Theorem

Rational Subset Membership is decidable in $H_3(\mathbb{Z})$.

Idea: Reduction to the Knapsack problem in $H_3(\mathbb{Z})$, which is solvable.

Corollary

Submonoid Membership is decidable in the filiform 3-step nilpotent group

$$E = \left\langle x, y_1, y_2, y_3 \;\middle|\; [x, y_1] = y_2,\ [x, y_2] = y_3,\ [x, y_3] = [y_i, y_j] = 1 \right\rangle.$$

Conjecture

Rational Subset Membership is decidable in $H_{2m+1}(\mathbb{Z})$.

Thank you !