Decision problems for one-relator monoids and groups

Islam Foniqi
joint work with R. D. GRAY & C.-F. NYBERG-BRODDA

School of Mathematics

University of East Anglia

North British Semigroups and Applications Network
April 14th, 2023
Manchester

Decision problems

Decision problem $=$ question with YES/NO answer,
on a countable set of inputs.

Example

(i) Is $n \in \mathbb{N}$ a prime number?

Trial division.

(ii) Are $m, n \in \mathbb{N}$ relatively prime?

Euclid's algorithm.

(iii) Are two finite simplicial complexes homeomorphic?

Undecidable (passes through the isomorphism problem in groups)

Decision problems

A set $S \subseteq \mathbb{N}$ is called decidable if there is an algorithm:

- which takes $n \in \mathbb{N}$ as input,
- terminates after a finite amount of time, and
- correctly decides whether n belongs to S or not.

There are undecidable sets $S \subset \mathbb{N}$.

A decision problem is called decidable $\iff$ there is an algorithm:

- taking as input each instance of the problem,
- terminates in finitely many steps, and
- correctly decides an answer YES/NO for each instance.

Key points of algorithms

- Finite nature; no infinite length.
- “Infinite loops” are not allowed.
- No infinitely many distinct algorithms, one for each instance.

Some early results on undecidability

- (Logic, 1930s, Church and Turing) There is no method (algorithm) for deciding which formulas of first-order logic are valid.

- (1950s) Undecidable decision problems appeared outside the area of Logic (e.g. in monoid/group theory).

Some algebraic structures

This talk consists of decision problems in three algebraic structures:

(i) Monoids, (ii) Inverse monoids, (iii) Groups.

Definition

Let $(S, \cdot)$ be a set together with a operation $\cdot \colon S \times S \to S$. Then:

$$\left.\begin{array}{l}\left.\begin{array}{rl}\left.\begin{array}{rl}(as) & a \cdot (b \cdot c) = (a \cdot b) \cdot c\end{array}\right\}\text{semigroup} \\ (id) & (\exists\, 1 \in S)\,(\forall a \in S) : 1 \cdot a = a \cdot 1 = a\end{array}\right\}\text{monoid} \\ (inv) \quad (\forall a \in S)\,(\exists a' \in S) : a \cdot a' = a' \cdot a = 1\end{array}\right\}\text{group}$$

Example

(1) $(\mathbb{N}, +)$ is a semigroup.

(2) $(\mathbb{N}_0, +)$ is a monoid.

(3) $(\mathbb{Z}, +)$ is a group.

Some algebraic structures

Definition

An inverse monoid is a monoid M such that
$\forall x \in M, \ \exists! x' \in M$ with $xx'x = x$ and $x'xx' = x'$.

- **groups** $\longleftrightarrow$ **symmetries**,
- **monoids** $\longleftrightarrow$ **transformations**,
- **inverse monoids** $\longleftrightarrow$ **partial symmetries**.

Example

Let S be a given set. Then

- Permutations $f : S \hookrightarrow\!\!\!\!\rightarrow S$ form a group.
- Functions $f : S \to S$ form a monoid.
- $\mathcal{I}_S = \{$bijections $f : A \hookrightarrow\!\!\!\!\rightarrow B \mid A, B \subset S\}$ forms an inverse monoid, operation = "compose wherever possible".

Presentations by generators and relators

$A =$ finite set. Denote by A^* the free monoid over A, i.e.

$$A^* = \{\text{all words with letters in } A\},$$

including the empty word λ. Operation = 'Concatenation of words'.

Example: For $A = \{a, b\}$, we have λ, aba, $baabaaa$ as words in A^*.

Denote by $\mathrm{Gp}\langle A \mid R\rangle$, $\mathrm{Mon}\langle A \mid R\rangle$, $\mathrm{Inv}\langle A \mid R\rangle$
presentations of groups, monoids, and inverse monoids respectively.

Example

- $\mathrm{Gp}\langle a, b \mid ab = ba\rangle \simeq \mathbb{Z}^2$.
- $\mathrm{Mon}\langle a, b \mid ab = ba\rangle \simeq \mathbb{N}_0^2$.

Word problems in monoids

Let $M = \mathrm{Mon}\langle A \mid R \rangle$ be a monoid.

- Word problem for M is decidable if there is an algorithm solving the decision problem:
  Input: $w_1, w_2 \in A^*$.
  Output: YES if $w_1 = w_2$ in M; NO if $w_1 \neq w_2$ in M.

Theorem

The word problem is decidable in free monoids.

Proof.

$A =$ alphabet, $M = A^*$, and $w_1, w_2 \in M$.

$w_1 = w_2$ in $M \iff$ both words look graphically the same.

□

Word problems in monoids

Theorem (Markov, Post (1947))

The word problem for finitely presented monoids is undecidable in general.

Remark. There are known examples of such monoids, with 3 relations.

Remark

The word problem is still open for monoids with 1 (or 2) relations.

Word problems in groups

Word problem for $\mathrm{Gp}\langle A \mid R\rangle$ is decidable if there is an algorithm determining if a word w is the identity.

Theorem

The word problem is decidable in free groups.

Theorem (Novikov (1955), Boone (1958))

There exist finitely presented groups G with undecidable word problem.

Remark. All known examples of such groups have at least 12 relations.

One-relator groups

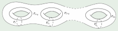
Group presentation with one defining relator:

$$G = \mathrm{Gp}\langle a_1, \ldots, a_n \mid r \rangle$$

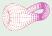
where r is a word in $\{a_1, \ldots, a_n\}^*$.

Example

- $\mathbb{Z}^2 = \mathrm{Gp}\langle a, b \mid ab = ba \rangle = \pi_1$ ()
- Generalizing the first example, we obtain:

$$S_g = \pi_1 \left(\right.$$  $$\left. \right)$$

$$= \mathrm{Gp}\langle a_1, b_1, \ldots, a_g, b_g \mid a_1 b_1 a_1^{-1} b_1^{-1} \cdots a_g b_g a_g^{-1} b_g^{-1} \rangle$$

- $K = \mathrm{Gp}\langle a, b \mid a^2 = b^2 \rangle = \pi_1$ ()
- $K_g = \mathrm{Gp}\langle a_1, \ldots, a_g \mid a_1^2 \cdots a_g^2 \rangle$, non-orientable surfaces.
- $BS(m, n) = \mathrm{Gp}\langle a, b \mid b a^m a^{-1} = a^n \rangle$, Baumslag-Solitar groups.

Classical results on one-relator groups

- Magnus (1932): One-relator groups have solvable word problem.
- Magnus Freiheitssatz: $G = \mathrm{Gp}\langle A \mid r \rangle$, $r =$ cyclically reduced.
  If $B \subsetneq A$, then $\mathrm{Gp}\langle B \rangle$ is free.
  Example: $\mathrm{Gp}\langle a, b \rangle$ is free of rank 2 in $\mathrm{Gp}\langle a, b, c \mid a^2b^2c^2 = 1 \rangle$.
- Newman (1968): If $r = u^k$ with $k > 1$, then G is hyperbolic.
- Howie (1980s): If $r \neq u^k$ for some $k > 1$, the G is locally indicable: i.e. for any fin. gen. $H \leqslant G$, there is a surjective homomorphism
  $$\varphi : H \longrightarrow \mathbb{Z}.$$
- Linton (2023) Coherence: When finitely generated subgroups are finitely presented.
  Louder and Wilton / Wise independently dealt with the torsion case.

Open problems

- Conjugacy problem: Given two elements g_1, g_2 in a group, decide whether $g_1 = hg_2h^{-1}$ for some h.
- The isomorphism problem: Given two one-relator groups G_1, G_2, decide if $G_1 \simeq G_2$.
- Is G hyperbolic if G does not contain Baumslag-Solitar groups?

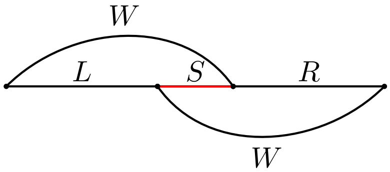
Classical cases of word problem in one-relator monoids

Let $M = \mathrm{Mon}\langle A \mid U = V \rangle$ with $|U| \geq |V|$. M has solvable word problem:

- If $|U| = |V|$,
- If $V = 1$; this case reduces to Magnus' result on 1-relator groups.
- If $|U| > |V|$ and U does not have self-overlaps.

  Moreover, $U \longrightarrow V$ gives a complete rewriting system for M.

A word W has self-overlaps if there is a subword S of W which is both a prefix and a suffix of W, i.e. $W = SR = LS$.



$w = \underline{ab}b\underline{ab}$ has self-overlaps with $S = ab, L = abb, R = bab$

Reductions and remaining cases

Theorem (Adjan, Oganesyan (1987))

WP for 1-relator monoids can be reduced to the case with 2 generators:

$$M = \mathrm{Mon}\langle a, b \mid U = V \rangle.$$

Theorem (Adjan, Oganesyan (1987))

WP for 1-relator monoids can be reduced to the following two cases:

(i) $M = \mathrm{Mon}\langle a, b \mid bQa = aRa \rangle$,

(ii) $M = \mathrm{Mon}\langle a, b \mid bQa = a \rangle$.

A digression to one-relator inverse monoids

Theorem (Ivanov, Margolis, Meakin (2001))

(i) $\mathrm{Mon}\langle a, b \mid bQa = aRa \rangle$ *embeds into* $\mathrm{Inv}\langle a, b \mid a^{-1}R^{-1}a^{-1}bQa \rangle$.

(ii) $\mathrm{Mon}\langle a, b \mid bQa = a \rangle$ *embeds into* $\mathrm{Inv}\langle a, b \mid a^{-1}bQa \rangle$.

One-relator case: Decidable WP for INV $\Longrightarrow$ decidable WP for MON.

Theorem (Gray (2020))

There is a one-relator $\mathrm{Inv}\langle A \mid w = 1 \rangle$ *with undecidable word problem.*

- Gray's example is not of the form $(i), (ii)$ from the IMM theorem.
- One could still investigate the solution of the word problem for one-relator monoids, through their inverse counterpart.

The case $bQa = a$

Theorem (Adjan)

The monoid $M = \mathrm{Mon}\langle a, b \mid bQa = a\rangle$ *is left-cancellative, i.e.*

$$WU = WV \text{ implies } U = V.$$

Given two words, steps to decide if they are equal are given as follows:

$$\begin{aligned}
(i) &\quad (bX, bY) \longrightarrow (X, Y)\\
(ii) &\quad (aX, aY) \longrightarrow (X, Y)\\
(iii) &\quad (bX, aY) \longrightarrow (bX, bQaY) \longrightarrow (X, QaY)
\end{aligned}$$

and we stop if one of the words becomes empty.

Prefix membership problem

The prefix membership problem in $M = \mathrm{Mon}\langle A \mid u = v\rangle$ asks about membership in $P = \mathrm{Mon}\langle$prefixes of the each $u, v\rangle$.

Similarly, one defines the suffix membership problem.

Example

Let $M = \mathrm{Mon}\langle a, b, c \mid ab = aca\rangle$. Then:

$$P = \mathrm{Mon}\langle a, ab, ac\rangle$$
$$S = \mathrm{Mon}\langle b, ab, a, ca\rangle$$

Remark. The prefix/suffix monoid depend on the presentation. Indeed: $G_1 = \mathrm{Gp}\langle a, b \mid aba = 1\rangle$ and $G_2 = \mathrm{Gp}\langle a, b \mid baa = 1\rangle$ are isomorphic to $\mathbb{Z}$.

$$P_1 = \mathrm{Mon}\langle a, ab = a^{-1}\rangle \simeq \mathbb{Z}, \quad P_2 = \mathrm{Mon}\langle b = a^{-2}, ba = a^{-1}\rangle$$
$$= \mathrm{Mon}\langle 1, a^{-1}, a^{-2}, a^{-3}, \ldots\rangle \simeq \mathbb{N}_0.$$

Submonoid (subgroup) membership problem

- **Submonoid membership problem:**
  N - a finitely generated submonoid of $M = \mathrm{Mon}\langle A \mid R \rangle$.
  The submonoid membership problem for N within M is decidable if there is an algorithm solving the decision problem:
  Input: $w \in A^*$.
  Output: YES if $w \in N$; NO if $w \notin N$.

Remark. $M = \mathrm{Mon}\langle A \mid R \rangle$ has decidable submonoid membership problem, if there is a uniform algorithm for submonoid membership within M.

- **Subgroup membership problem:**
  H - a finitely generated submonoid of $G = \mathrm{Gp}\langle A \mid R \rangle$.
  The subgroup membership problem for N within M is decidable if there is an algorithm solving the decision problem:
  Input: $w \in (A \cup A^{-1})^*$.
  Output: YES if $w \in H$; NO if $w \notin H$.

Submonoid membership problem

Theorem (Benois (1969))

The submonoid membership problem is decidable in free groups.

Theorem (Cadilhac et al. (2020))

Baumslag-Solitar groups of the form

$$BS(1,q) = \mathrm{Gp}\langle a, t \mid tat^{-1} = a^q \rangle$$

for $q \in \mathbb{N}$ have decidable submonoid membership problem.

Motivation for the membership problems

Theorem (Guba)

Given $M = \mathrm{Mon}\langle a, b \mid b = bQa \rangle$*, there exists a finite set* C *and a positive word* U *over* $\{a, b\} \cup C$ *such that if* $G = \mathrm{Gp}\langle a, b, C \mid a^{-1}bUa = 1 \rangle$ *has decidable suffix membership problem then* M *has decidable word problem.*

Note. $G = \mathrm{Gp}\langle a, b, C \mid bU = 1 \rangle$, is a positive one-relator group.

Remark

Decidable submonoid membership $\implies$ decidable suffix membership.

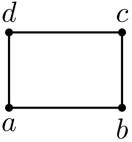
Corollary

$M = \mathrm{Mon}\langle a, b \mid b = bQa \rangle$ would have decidable word problem, if positive one-relator groups had decidable submonoid membership problem.

Motivation: study of submonoid membership problem in positive one-relator groups.

Right-angled Artin groups (RAAGs):

$P_4 =$ 

$C_4 =$ 

Define $A(P_4)$, $A(C_4)$ from the information encoded in P_4, C_4 respectively:

$$A(P_4) \coloneqq \mathrm{Gp}\langle a, b, c, d \mid ab = ba, bc = cb, cd = dc \rangle$$

$$A(C_4) \coloneqq \mathrm{Gp}\langle a, b, c, d \mid ab = ba, bc = cb, cd = dc, da = ad \rangle \simeq F_2 \times F_2$$

Theorem

- *Lohrey and Stainberg (2008) There is a finitely generated submonoid M in $A(P_4)$ with undecidable submonoid membership.*
- *Mihailova (1966) There is a subgroup H in G_2 such that the subgroup membership problem for M within G_2 is undecidable.*

Undecidable submonoid membership problems

Theorem (Gray (2019))

There is a one-relator group, e.g. $G = \mathrm{Gp}\langle a, t \mid a(tat^{-1}) = (tat^{-1})a\rangle$, *with a fixed fin. gen. submonoid* N *where membership is undecidable.*

Question: What about one-relator monoids $\mathrm{Mon}\langle A \mid w = 1\rangle$?

Theorem (Gray, Foniqi, Nyberg-Brodda (2022))

There is a group $G = \mathrm{Gp}\langle a, b \mid w = 1\rangle$ *defined by a positive relation* w, *with undecidable submonoid membership problem.*

E.g. $G = \mathrm{Gp}\langle x, y \mid x^2y^2 = y^2x^{-2}\rangle \cong \mathrm{Mon}\langle a, b \mid ba^2ba^4ba^2b = 1\rangle$; the isomorphism is given by $y = a$ and $x = ba^2$ (Perrin & Schup, (1984).

Corollary

There is a one-relator special monoid $M = \mathrm{Mon}\langle a, b \mid w = 1\rangle$, with undecidable submonoid membership problem.

Rational subset membership problem

Given a monoid M, denote by $RAT(M)$ the smallest subset of $\mathcal{P}(M)$

- containing all finite subsets of M, and
- closed under union, product, and Kleene hull.

Rational subset membership problem:

R - a rational subset of $M = \mathrm{Mon}\langle A \mid R \rangle$.
The rational subset membership problem for R within M is decidable if there is an algorithm solving the decision problem:

Input: $w \in A^*$.
Output: YES if $w \in R$; NO if $w \notin R$.

Rational subset membership problem

Theorem (Kambites, Render (2007))

The bicyclic monoid $B = \mathrm{Mon}\langle a, b \mid ab = 1\rangle$ *has decidable rational subset membership. Moreover, they describe rational subsets of this monoid.*

Theorem (Lohrey, Steinberg (2007))

The rational subset membership problem for RAAGs is decidable if and only if the defining graph does not contain A_4 *and* C_4.

Theorem (Kambites (2009, 2011))

As the length $|u| + |v|$ *increases, the probability that a randomly chosen one-relation monoid* $\mathrm{Mon}\langle A \mid u = v\rangle$ *has a decidable rational subset membership problem tends to* 1.

Rational subset membership problem

Two elements $x, y \in M$ are $\mathcal{L}$-related if $Mx = My$.

Theorem (Gray, Foniqi, Nyberg-Brodda (2023))

Let M be a fin. gen. left-cancellative monoid. If there is $U \subseteq M$ with

- $uv\mathcal{L}v$ *for all* $u, v \in U$,
- $\mathrm{Mon}\langle U \rangle$ *is isomorphic to the trace monoid* $T(P_4)$,

then M contains a rational subset in which membership is undecidable.

Denote $S(P_4) = \mathrm{Sgp}\langle a, b, c, d \mid ab = ba, bc = cb, cd = dc \rangle$.

Corollary

If a left-cancellative monoid embeds $S(P_4)$ in a single $\mathcal{L}$-class, then the monoid contains a rational subset in which membership is undecidable.

Rational subset membership problem

Theorem

For all $m, n \geq 2$, the monoid $\mathcal{M}_{m,n} = \mathrm{Mon}\langle a, b \mid (ba^n)^m (a^n b)^m a = a \rangle$ contains a fixed rational subset in which membership is undecidable.

Note: The monoids above do not contain nontrivial groups.
In particular, $A(P_4)$ does not lie in $\mathcal{M}_{m,n}$.

Corollary

If G is a fin. gen. group which embeds $T(P_4)$ then G contains a fixed rational subset where membership is undecidable.

Prefix membership problem in one-relator structures

Theorem (Gray, Foniqi, Nyberg-Brodda (2023))

G positive one-relator group, Q any finitely generated submonoid of G. There exists a quasi-positive one-relator group G' such that:

decidable prefix membership problem for G'

$$\Downarrow$$

membership problem for Q in G is decidable.

Furthermore, G' can be chosen such that $G' \cong G * \mathbb{Z}$.

Prefix membership problem in one-relator structures

Corollary

There exists a quasi-positive one-relator group

$$G = \mathrm{Gp}\langle a, b, t \mid uv^{-1} \rangle,$$

with undecidable prefix membership problem.

Proof.

(i) $G_1 = \mathrm{Gp}\langle a, b \mid w = 1 \rangle$ positive, with undecidable submonoid membership problem in a fixed $M = \mathrm{Mon}\langle w_1, w_2, \ldots, w_k \rangle$

(ii) encode the w_i into prefixes of the defining relator of a group

$$G_2 = \mathrm{Gp}\langle A \cup \{t\} \mid \beta w \beta^{-1} = 1 \rangle \cong G_1 * \mathbb{Z},$$

technique of Dolinka & Gray

(iii) As β might not be a positive word; use isomorphisms to change to:

$$G_3 = \mathrm{Gp}\langle A \cup \{t\} \mid \alpha w' \alpha^{-1} = 1 \rangle \cong G_2,$$

where α and w' are positive words.

Thank you for your attention!