Some decision problems in finitely presented groups and semigroups

Joint work w. R. D. Gray (East Anglia)

Carl-Fredrik Nyberg-Brodda

Korea Institute for Advanced Study (Seoul, Korea)

($\xrightarrow{\text{1 Feb 2025}}$ June E. Huh Centre for Mathematical Challenges (KIAS))

cfnb@kias.re.kr

The Fourth Korea Logic Day 2025

Changwon, January 13, 2025

1. Undecidable problems

The story begins with early/mid-1900s formalisation of mathematical logic by Church, Gödel, Herbrand, Hilbert, Kleene, Post, Russell, Turing, Whitehead, ...

Theorem (Church[a]/Turing[b], 1936)

[a] Amer. J. Math, **58**:2, 1936
[b] Proc. London Math. Soc. (2), **42**:3, 1936

*The **Entscheidungsproblem** for first-order logic is undecidable in general.*

> *"Imidlertid vil mange kansksje spørre, hvad studied av dette problem [Entscheidungsproblemet] egentlig skal tjene til"*
>
> –Thoralf Skolem, 1937.
> Norsk mat. tids. **19** (1937) 130–133

> *"Hey, Thoralf, I know how to apply this to "real" mathematics."*
>
> –Emil Post, 1947 (paraphrased)

So what problem was this?

E. Post, *Recursive unsolvability of a problem of **Thue***. JSL **12** (1947).

A. Thue (1863–1922) was PhD supervisor of T. Skolem, thesis in 1927 (?!). Now best known for the Thue–Morse–Prouhet sequence and **Thue systems**.

2. Local-to-global combinatorial games

Consider an alphabet A, e.g. $A = \{a, b\}$, subject to some **relations** $R_i = S_i$. We will play the game of deciding if $u = v$ is a consequence of the relations.

Simple example: take the relation $ab = ba$. Then $a^j b^k = b^k a^j$ for all $j, k \in \mathbf{N}$. In fact, we have $u = v$ if and only if $\mathcal{P}(u) = \mathcal{P}(v)$ (Parikh vectors).

Quiz!

Consider words over $\{a, b\}$, with the relation $abab = a$.

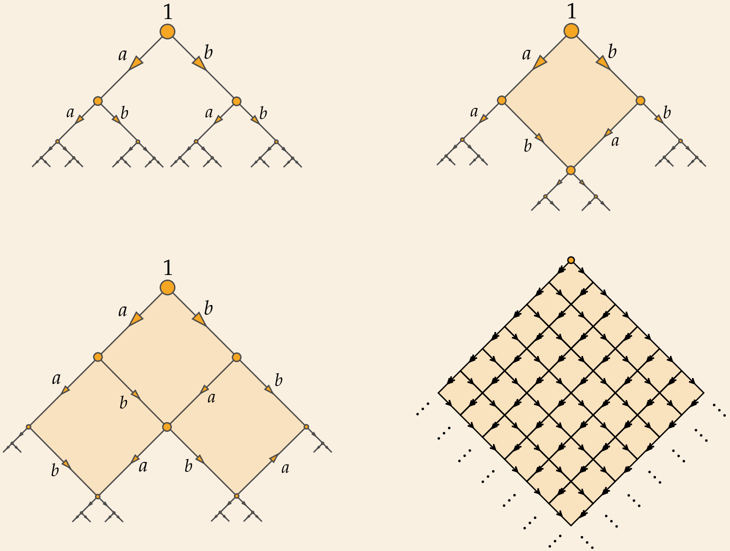
1. Do we have $aabb = a$? **Yes:**

$$aabb = (abab)abb \equiv ab(abab)b = abab = a$$

2. Do we have $bbaa = a$? **No:** any application of the relation cannot change the first letter of the word $bbaa$, so it cannot be equal to a.
3. Do we have $ababab bab = aabbaa$?

We are trying to understand the **word problem** of $\mathrm{Mon}\langle a, b \mid abab = a\rangle$. More generally, we have the word problem in $\mathrm{Mon}\langle A \mid R_1 = S_1,\ R_2 = S_2, \ldots\rangle$.

3. Local to global change; $\mathrm{Mon}\langle a, b \mid ab = ba \rangle$.



НЕВОЗМОЖНОСТЬ НЕКОТОРЫХ АЛГОРИФМОВ В АССОЦИАТИВНЫХ СИСТЕМАХ (ВТОРОЕ СООБЩЕНИЕ)[*]

В ассоциативной системе, определяемой системой соотношений

$$
\begin{aligned}
\alpha\beta &\longleftrightarrow \beta\alpha \qquad (\alpha = a, b, c, d;\ \beta = h, i, j, k, l)\\
ek &\longleftrightarrow ke\\
el &\longleftrightarrow le\\
dh &\longleftrightarrow df\\
hd &\longleftrightarrow gd\\
ea &\longleftrightarrow ie\\
eb &\longleftrightarrow je\\
am &\longleftrightarrow km\\
bm &\longleftrightarrow lm\\
fc &\longleftrightarrow cg\\
fai &\longleftrightarrow af\\
fbj &\longleftrightarrow bf\\
agk &\longleftrightarrow ga\\
bgl &\longleftrightarrow gb
\end{aligned}
$$

в алфавите $\{a, b, c, d, e, f, g, h, i, k, l, m\}$, неразрешима проблема тождества.

4. The first undecidability

Thue (1914): can we **always** solve the word problem in f.p. monoids?

Theorem (Markov[a] / Post[b] 1947)

[a] Dokl. Akad. Nauk, **55**:7, 1947
[b] J. Symb. Logic **12**, 1947

No. There exist finitely presented monoids with undecidable word problem.

Matiyasevich (1967): **three** relations suffice for undecidability.
The word problem for **groups** is old (Dehn, 1912). In Manchester, 1950:

A. M. Turing: *undecidable!* B. H. Neumann: *decidable!*

Both later retract their claims... but Turing was right!

Theorem (Novikov[a]/Boone[b], 1955/1958)

[a] Proc. Steklov Inst. Math. **44**, 1955
[b] Proc. Nat. Acad. Sciences, **44**:10, 1958

*There exist finitely presented **groups** with undecidable word problem.*

Iso. problem undecidable

- Markov (1950)
- Addison Jr/Feeney (1954)
- Adian/Rabin (1958)

Word problem undecidable

- Post (1921/1943): canonical systems
- Markov/Post (1947): semigroups
- Turing (1950): cancellative semigroups
  Adian & Novikov (1965)
- Novikov (1955)/Boone/Britton (1958): groups
- Tseytin (1958): 7-relator semigroup
- Makanin/Matiyasevich (1966): 5-relator semigroup
- Matiyasevich (1967): 3-relator semigroup
- Borisov (1969): 12-relator group

E. Post more famous for Correspondence Problem; **S. I. Adian & P. S. Novikov** more famous for Burnside problem; **A. A. Markov** son of A. A. Markov of the Chains; **J. W. Addison Jr** more famous for Unabomber; **G. S. Makanin** more famous for equations in free (semi)groups; **Yu. V. Matiyasevich** more famous for Hilbert's 10th Problem; **M. O. Rabin** more famous for Tree Theorem; **G. S. Tseytin** more famous for SAT solvers; **A. M. Turing** is more famous.

5. A small universal Turing machine

The following example is due to G. S. Tseytin (1958). Let M be the monoid with five generators $\{a, b, c, d, e\}$ and the following seven defining relations:

$$ac = ca, \quad ad = da,$$
$$bc = cb, \quad bd = db,$$
$$eca = ce,$$
$$edb = de,$$
$$cca = ccae.$$

Then M has **undecidable word problem (!).**
I wrote about this in `arXiv:2401.11757` (to appear in *Festschrift* for Tseytin).

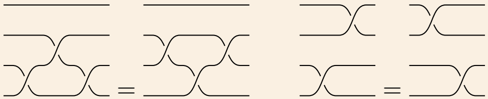
> **Open Problem (since 1914)**: is the word problem decidable in every one-relation monoid $\mathrm{Mon}\langle A \mid u = v\rangle$? What if the relation is $w = a$ for $a \in A$?

Also open for two relations (but undecidable for three relations).

6. Braid groups

The n-**strand braid group** is the mapping class groups of the n-punctured disk.

$$\mathbf{B}_n = \mathsf{Gp}\langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1},\ \ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for } |i-j| \geq 2\rangle$$



$\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$ $\qquad$ $\sigma_1\sigma_3 = \sigma_3\sigma_1$

1. (Artin, 1925) The word problem is decidable in $\mathbf{B}_n$.
   (Artin, 1947) Revisits braids, proves $\mathbf{B}_n \cong \mathbf{B}_m \iff n = m$.
2. (Garside, 1969) The conjugacy problem is decidable in $\mathbf{B}_n$.
3. (Arnol'd, 1969) Determined cohomology of $\mathbf{B}_n$.
4. (Makanin, 1971) Centralizers are finitely generated and computable.
5. (Bigelow/Krammer, 2001) Braid groups are linear.

7. Violent protests

The geometric meaning of the normal form of Theorem 17 and that mentioned after Theorem 18 is now also clear. Every braid is isotopic to another one whose pattern of projection is especially simple and is indicated in Fig. 4 for a special case. This pattern is unique. The braid in Fig. 4 has the expression:

$$A = A_{13}^{2}A_{14}^{-1}A_{12}^{-3}A_{14}A_{15}^{4}\cdot A_{24}^{-1}A_{23}^{2}A_{24}A_{25}^{-2}\cdot A_{34}^{3}A_{35}^{-2}\cdot A_{34}^{-1}\cdot A_{45}^{-4}.$$

Although it has been proved that every braid can be deformed into a similar normal form the writer is convinced that any attempt to carry this out on a living person would only lead to violent protests and discrimination against mathematics. He would therefore discourage such an experiment.

INDIANA UNIVERSITY

From E. Artin, *Theory of braids*, Annals of Mathematics **48**:1 (1947), p. 126.

8. Artin groups

Let Γ be a finite graph, edges labelled by $\mathbf{N}_{\geq 2}$. Then the **Artin group** $A(\Gamma)$ has generators $V(\Gamma)$ and for every edge $a \overset{m}{\text{---}} b$ a relation

$$\underbrace{abab\ldots}_{m \text{ factors}} = \underbrace{baba\ldots}_{m \text{ factors}}$$

Examples:

1. **Right-angled** Artin groups: relations $a_i a_j = a_j a_i$, e.g. $F_n, \mathbf{Z}^n, F_n \times \mathbf{Z}, \ldots$.
2. Braid groups $\mathbf{B}_n$, relations $\sigma_{i+1}\sigma_i\sigma_{i+1} = \sigma_i\sigma_{i+1}\sigma_i$ and $[\sigma_i, \sigma_j] = 1$.
3. **Large**: all $m \geq 3$, **extra large**: all $m \geq 4$. Word and conjugacy problem decidable via $C(4)$ and $T(4)$ small cancellation (Appel & Schupp 1983). Also membership in "Magnus subgroups" decidable and $\langle a_i^2 \mid i \in I \rangle$ is free.

Open Problem!

Is the word problem decidable in every Artin group?

Much more known in right-angled case (conjugacy and word problem, ...).

Theorem (Wise, 2009[a])

[a] Electronic Research Announcements **16** (2009) pp. 44–55

Every one-relator group with torsion virtually embeds in some RAAG.

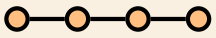
9. Membership problems

Let G be a group. The **submonoid membership problem** asks: given finite set $W, w_1, \ldots, w_n$, does $W \in \langle w_1, \ldots, w_n \rangle_{\mathrm{mon}}$? The **rational subset membership problem** asks: given finite G-automaton $\mathcal{A}$ and W, does $\mathcal{A}$ accept W?

Decidable in:

1. (Nielsen 1921/Benois 1969) Free monoids, free groups
2. (Grunschlag 1994) Abelian groups.
3. (Kambites, Silva & Steinberg 2006) Fundamental groups of graphs of groups where vertex groups have decidability, and edge groups are finite.
4. (Lohrey & Steinberg 2008) $\pi_1(\mathcal{T}_{2,3}) \cong \mathbf{B}_3$ and $\mathrm{BS}(m, m)$.
5. (Cadilhac, Chistikov & Zetsche 2020) Baumslag–Solitar groups $\mathrm{BS}(1, n)$.

Undecidable in:

1. (Mikhailova 1958 / Makanina 1981) $F_2 \times F_2 = A(C_4) \leq \mathbf{B}_5$.
2. (Roman'kov 1999) Free nilpotent groups.
3. (Lohrey & Steinberg 2008) $A(P_4) = A($$)$.
4. (NB, 2023) $\mathrm{Gp}\langle a, b \mid [a^2, b^2] = 1 \rangle$.

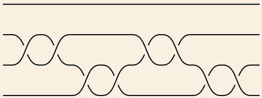
10. Membership in braid groups

Undecidability in $\mathbf{B}_5$, decidability in $\mathbf{B}_3$. Potapov (2013): What about $\mathbf{B}_4$?

Theorem (Gray, NB[a] (2024))

[a] arXiv:2409.11335.

The rational subset/submonoid membership problem is decidable in $\mathbf{B}_n$ if and only if $n \leq 3$. Furthermore, in $\mathbf{B}_4$ there is no algorithm that decides whether $\gamma_0 \in \langle w_1, \dots, w_n \rangle_{\mathrm{mon}}$ for given $w_1, \dots, w_n$, and the subsemigroup intersection problem is undecidable in $\mathbf{B}_4$.



$$\gamma_0 = \sigma_2^2 \sigma_3^2 \sigma_2^{-2} \sigma_3^{-2}$$

Sketch of proof.

We find an embedding of $A(P_4)$ into $\mathbf{B}_4$, which yields undecidable rational subset membership problem. We can then simulate the reading of any automaton H_A by some submonoid H_A of $A(P_4) * \mathbf{Z} \leq \mathbf{B}_4$, with acceptance iff $\gamma_0 \in H_A$. □

11. Membership problems in RAAGs

Theorem (Lohrey & Steinberg, 2005[a])

[a] J. Algebra **320**:2 (2008) pp. 728–755.

The submonoid (rational subset) membership problem is decidable in the right-angled Artin group $A(\Gamma)$ if and only if Γ does not contain P_4 or C_4 as an induced subgraph.

Unknown if subgroup membership problem is decidable in $A(C_n)$ for $n \geq 5$.
Can analogously define *trace monoids* ("right-angled Artin monoids") $T(\Gamma)$.

Theorem (Foniqi, Gray & NB (2024)[a])

[a] Canadian J. of Mathematics, *accepted* (2024).

Let G be a group containing $T(P_4)$. Then G has undecidable rational subset membership problem.

Note that $T(P_4)$ itself has decidable rational subset membership problem!

Proposition (Gray, NB (2024)[a])

[a] arXiv:2409.11335.

Every subgroup separable Artin group has decidable rational subset membership problem.

Proof.

An Artin group is subgroup separable if and only if it lies in $A(\mathcal{S})$, the smallest class of groups containing all Artin groups of rank ≤ 2 and closed under:

1. taking free products, and
2. taking direct products with $\mathbf{Z}$.

The non-cyclic Artin groups of rank ≤ 2 are

$$\mathsf{Gp}\langle a, b \mid (ab)^k a = b(ab)^k \rangle \cong \mathsf{Gp}\langle x, y \mid x^2 = y^{2k+1} \rangle \text{ and}$$
$$\mathsf{Gp}\langle a, b \mid (ab)^k = (ba)^k \rangle \cong \mathsf{Gp}\langle x, y \mid x^k y = y x^k \rangle = \mathrm{BS}(k,k).$$

These groups are all virtually $F_n \times \mathbf{Z}$.

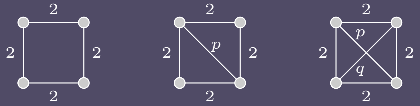
G has decidable RSMP $\iff$ G's word problem is RID $\Longleftarrow$ G is SLI group.
SLI groups are closed under $\times\mathbf{Z}$, free products, and finite extensions.
Hence, all virtually $F_n \times \mathbf{Z}$ groups are SLI, so all rank 2 Artin groups are. □

Theorem (NB & Gray, 2024[a])

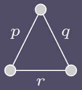
[a] arXiv:2409.11335

Let $A = A(\Gamma)$ be an Artin group. Then the following are equivalent:

- **(i)** *A has decidable submonoid membership problem;*
- **(ii)** *A has decidable rational subset membership problem;*
- **(iii)** *the graph Γ does not contain any induced subgraph isomorphic to:*
  1. *a square, with $p > 2$ and $q > 2$, of one of the following three forms*



  2. *a triangle, with at most one of $\{p, q, r\}$ equal to 2, of the form*



  3. *a path of one of the two forms, with at most one of $\{p, q\}$ equal to 2:*

We thus recover (and generalize) Lohrey & Steinberg's RAAG classification.

Thank you for listening!