Solving equations in one-relator monoids

Robert D. Gray
(joint work with Albert Garreta (Bilbao))[1]

eNBSAN, July 2020

University of East Anglia

[1] This research was initiated during the Heilbronn Focused Research Workshop "Equations in One-Relator Groups and Semigroups", in September 2018, at the ICMS in Edinburgh organised by Laura Ciobanu of Heriot-Watt University.

Equations over free monoids and free groups

- $A = \{a, b, \dots\}$ - alphabet, $\Omega = \{X, Y, \dots\}$ - set of variables,
- Word equation: a pair $(L, R) \in (A \cup \Omega)^* \times (A \cup \Omega)^*$ written $L = R$.
- System of word equations: $\{L_1 = R_1, \dots, L_k = R_k\}$.
- Solution: a homomorphism $\sigma : (A \cup \Omega)^* \to A^*$ leaving A invariant such that $\sigma(L_i) = \sigma(R_i)$ for $1 \leqslant i \leqslant k$.

Example

$A = \{a, b\}, \Omega = \{X, Y, Z, U\}$

$$XaUZaU = YZbXaabY$$

One solution is given by σ defined by

$$X \mapsto abb,\ Y \mapsto ab,\ Z \mapsto ba,\ U \mapsto bab,\ \text{giving}$$

$$(abb)a(bab)(ba)a(bab) = abbababbaabab = (ab)(ba)b(abb)aab(ab).$$

Equations over free groups: Similar but with equations $L = R$ where L and R are words over $A^{\pm 1} \cup \Omega^{\pm 1}$. e.g. $XabX^{-1} = ba$ has solution $X = b$.

Diophantine problem

Diophantine problem - a decision problem

Does there exist an algorithm which for any system of finitely many equations in a given group (or monoid) can determine whether the equation has a solution?

Theorem (Makanin (1977, 1983))

The Diophantine problem is:

- decidable in any free monoid, and
- decidable in any free group.

Equations over finitely presented monoids

$$\langle A \mid R \rangle = \langle \underbrace{a_1, \ \ldots, \ a_n}_{\text{generators}} \quad \mid \quad \underbrace{u_1 = v_1, \ \ldots, \ u_m = v_m}_{\text{defining relations}} \rangle$$

- Defines $M = A^*/\rho$ where ρ is the smallest congruence on A^* containing R.
- Solution to a system of equations $\{L_1 = R_1, \ldots, L_k = R_k\}$: a homomorphism $\sigma : (A \cup \Omega)^* \to A^*$ leaving A invariant such that $\sigma(L_i)/\rho = \sigma(R_i)/\rho$ for $1 \leqslant i \leqslant k$.
- i.e. such that $\sigma(L_i) = \sigma(R_i)$ in the monoid M for $1 \leqslant i \leqslant k$.

Example

$A = \{a, b\}, \;\; \Omega = \{X, Y, Z\}, \;\; \langle A \mid R \rangle = \langle a, b \mid ab = ba \rangle$

$$abbaXbbYabbbb = bYZbbaXbY$$

One solution is

$$X \mapsto a, \; Y \mapsto b, \; Z \mapsto aabbb, \; \text{giving}$$

$$abba(a)bb(b)abbbb = a^4b^9 = b(b)(aabbb)bba(a)b(b).$$

Diophantine problem

Diophantine problem - a decision problem

Does there exist an algorithm which for any system of finitely many equations in a given group (or monoid) can determine whether the equation has a solution?

- There are finitely presented groups and monoids for which the problem is undecidable since e.g.

decidable Diophantine problem $\Rightarrow$ decidable word & conjugacy problem.

- The Diophantine problem is decidable in the following classes
  - hyperbolic groups (Rips & Sela (1995), Dahmani & Guirardel (2016))
  - right-angled Artin groups (Diekert & Muscholl (2006))
    [More generally: free partially commutative monoids (i.e. trace monoids) with involution.]

One-relator monoids and one-relator groups

Groups

Open Problem

Is the Diophantine problem decidable for one-relator groups i.e. groups defined by group presentations of the form $\mathrm{Gp}\langle A \mid w = 1\rangle$?

- If yes, then as a corollay this would resolve positively the open problem of whether the conjugacy problem is decidable for one-relator groups.

Magnus (1932) Proved one-relator groups have decidable word problem.

Monoids

Open Problem

Is the Diophantine problem decidable for one-relator monoids i.e. monoids defined by presentations of the form $\langle A \mid u = v\rangle$?

- If yes, then as a corollay this would resolve positively the open problem of whether the word problem is decidable for one-relator monoids.

One-relator groups

Some known results

Baumslag-Solitar groups

Kharlampovich, López & Miasnikov (2019) proved the Diophantine problem is decidable in all soluble Baumslag-Solitar groups

$$BS(1,k) = \mathrm{Gp}\langle a, b \mid b^{-1}ab = a^k \rangle, \text{where } k \in \mathbb{N}.$$

One-relator groups with torsion

The Diophantine problem is decidable for

- Hyperbolic one-relator groups as a consequence of Rips & Sela (1995), Dahmani & Guirardel (2016), and in particular for
- One-relator groups with torsion

$$\mathrm{Gp}\langle A \mid w^n = 1 \rangle \ (n > 1),$$

since they are hyperbolic by B. B. Newman Spelling Theorem (1968).

One-relator monoids

Open Problem

Is the Diophantine problem decidable for one-relator monoids i.e. monoids defined by presentations of the form $\langle A \mid u = v \rangle$?

- If yes, then as a corollay this would resolve positively the following:

Longstanding open problem

Is the word problem decidable for one-relator monoids $\langle A \mid u = v \rangle$?

While the word problem is open in general, it has been solved in several cases, including

Theorem (Adjan 1966)

The word problem is decidable for the one relator monoids $\langle A \mid w = 1 \rangle$.

- The monoids $\langle A \mid w = 1 \rangle$ are commonly referred to as the special one-relator monoids.

Word problem and divisibility problem in $\langle A \mid w = 1 \rangle$

Word problem

Setting $\Omega = \varnothing$, for $u, v \in A^*$ we are asking whether $u = v$ has a solution.

Theorem (Adjan 1966)

The word problem is decidable for special one relator monoids $\langle A \mid w = 1 \rangle$.

Divisibility problem

For two words $u, v \in A^*$ we say u is left divisible by v if there is a word $z \in A^*$ such that $u = vz$ in the monoid.

Setting $\Omega = \{X\}$ we are asking whether the equation

$$u = vX$$

has a solution.

Theorem (Makanin 1966)

The left divisibility problem is decidable for special one relator monoids $\langle A \mid w = 1 \rangle$.

Conjugacy problems in $\langle A \mid w = 1 \rangle$

Left conjugacy

Set $\Omega = \{X\}$. The words $u, v \in A^*$ are left conjugate if the equation

$$uX = Xv$$

has a solution.

Cyclic conjugacy

Set $\Omega = \{X, Y\}$. The words $u, v \in A^*$ are cyclically conjugate if the system of equations

$$\{u = XY,\ v = YX\}$$

has a solution.

Theorem (Otto 1984 & Zhang 1991)

In $\langle A \mid w = 1 \rangle$ two words are left conjugate if and only if they are cyclically conjugate. These define equivalence relations on the monoid.

The conjugacy problem in $\langle A \mid w = 1 \rangle$

Theorem (Zhang 1989)

Let M be the monoid defined by $\langle A \mid w = 1 \rangle$ and let G be the group of units of M. If G has decidable conjugacy problem then M has decidable (left & cyclic) conjugacy problem.

- Adjan (1966) proved that the group of units of the monoid $\langle A \mid w = 1 \rangle$ is a one-relator group.

Corollary (Zhang 1989)

The one relator monoids $\langle A \mid u^n = 1 \rangle$, with $n > 1$, have decidable (left & cyclic) conjugacy problem.

Proof. Let M the monoid defined by this presentation. By Adjan (1966) G is a one-relator group with torsion. It follows my Newman (1968) that G has decidable conjugacy problem. Then apply the theorem. □

Note: All of these results on the word, divisibility, and conjugacy problems for the monoids $\langle A \mid w = 1 \rangle$ can be proved by a similar "reduction to the group of units" approach.

Equations over one-relator monoids: plan of attack

Conjecture

Let M be the monoid defined by $\langle A \mid w = 1 \rangle$ and let G be the group of units of M. If G has decidable Diophantine problem then M has decidable Diophantine problem.

- Then since hyperbolic groups have decidable Diophantine problem:

Corollary of conjecture

Let M be the monoid defined by $\langle A \mid w = 1 \rangle$ and let G be the group of units of M. If G is hyperbolic then M has decidable Diophantine problem.

- Then since the group of units of $\langle A \mid w^n = 1 \rangle$ $(n > 1)$ is a one-relator group with torsion, which is hyperbolic:

Corollary of corollary of conjecture

The one relator monoids $\langle A \mid w^n = 1 \rangle$, with $n > 1$, have decidable Diophantine problem.

Minimal invertible pieces of the relator

Let $M \cong \langle A \mid w = 1 \rangle$. The word w decomposees uniquely as

$$w \equiv \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k}$$

where each of these factors α_{i_j} is invertible in M and has no proper non-empty prefix which is invertible in M. These are called the minimal invertible pieces of the relator w.

- $\Delta = \{\alpha_i \ (i \in I)\} \subseteq A^+$ be the set of minimal invertible pieces of the relator w.
- $B = \{b_i \mid i \in I\}$ be an alphabet in bijective correspondence with Δ.

Theorem (Adjan 1966)

The group of units G of M is isomorphic to the monoid defined by

$$\langle B \mid b_{i_1} b_{i_2} \ldots b_{i_k} = 1 \rangle .$$

Example

Let $M \cong \langle a, b, c \mid abacab = 1 \rangle$. Then $\Delta = \{ab, ac\}$, $B = \{x, y\}$ and the group of units of M is

$$\langle x, y \mid xyx = 1 \rangle \cong \mathrm{Gp}\langle x, y \mid xyx = 1 \rangle = \mathrm{Gp}\langle x, y \mid y = x^{-2} \rangle \cong \mathrm{Gp}\langle x \mid \rangle .$$

Word equations with length constraints (WELCs)

- $A = \{a, b, \ldots\}$ - alphabet, $\Omega = \{X, Y, \ldots\}$ - set of variables,

A system of word equations with length constraints is a system of word equations Σ together with a finite conjunction $\mathcal{C}$ of formal expressions of the form $\mathsf{L}(w_1, w_2)$, each called a length constraint, where $w_1, w_2 \in (A \cup \Omega)^*$.

A solution is a homomorphism $\sigma : (A \cup \Omega)^* \to A^*$ leaving A invariant such that:

- σ is a solution to the system of word equations Σ, and in addition
- $|\sigma(w_1)| \leqslant |\sigma(w_2)|$ for each length constraint $\mathsf{L}(w_1, w_2)$ appearing in $\mathcal{C}$.

The question of whether solving word equations with length constraints is decidable, is a longstanding open problem in theoretical computer science.

WELCs example

Example

$A = \{a, b\}, \Omega = \{X, Y, Z, U\}$

$$XaUZaU = YZbXaabY,$$
$$\mathsf{L}(YaZ, XU).$$

One solution is given by σ defined by

$$X \mapsto abb,\ Y \mapsto ab,\ Z \mapsto ba,\ U \mapsto bab,$$

since we already saw above that this is a solution to the word equation, and in addition it safisties the length constraint since

$$|\sigma(YaZ)| = |ababa| = 5 \leqslant 6 = |abbbab| = |\sigma(XU)|.$$

Equations over one-relator monoids: plan of attack

Conjecture

Let M be the monoid defined by $\langle A \mid w = 1 \rangle$ and let G be the group of units of M. If G has decidable Diophantine problem then M has decidable Diophantine problem.

- Then since hyperbolic groups have decidable Diophantine problem:

Corollary of conjecture

Let M be the monoid defined by $\langle A \mid w = 1 \rangle$ and let G be the group of units of M. If G is hyperbolic then M has decidable Diophantine problem.

- Then since the group of units of $\langle A \mid w^n = 1 \rangle$ $(n > 1)$ is a one-relator group with torsion, which is hyperbolic:

Corollary of corollary of conjecture

The one relator monoids $\langle A \mid w^n = 1 \rangle$, with $n > 1$, have decidable Diophantine problem.

One-relator monoids with torsion

Theorem (Garreta and RDG (2019))

If the Diophantine problem is decidable for one-relator monoids with torsion $\langle A \mid w^n = 1 \rangle$ ($n > 1$) then the problem of solving systems of word equations with length constraints is decidable.

This is a corollary of the following more general result:

Theorem (Garreta and RDG (2019))

Let $M = \langle A \mid r = 1 \rangle$ and let $\Delta \subseteq A^*$ be the set of minimal invertible pieces of r. Suppose that:

(C1) no word from Δ is a proper subword of any other word from Δ,

(C2) there exist distinct words $\gamma, \delta \in \Delta$ with a common first letter, say a,

(C3) no word in Δ starts with a^2.

Then there exists a free monoid F of finite rank $n \geqslant 2$ such that the problem of solving systems of word equations with length constraints, over F, is reducible to the problem of solving systems of equations in M. Hence, if M has decidable Diophantine problem then the problem of solving systems of word equations with length constraints is decidable.

Many one-relator monoids satisfying these conditions

Some examples of monoids satisfying conditions (C1), (C2) and (C3) are the following (where we indicate the minimal invertible pieces with parentheses):

- $\langle a, b, c \mid (ab)(ac)(ab) = 1 \rangle$
- $\langle a, b, c \mid ((ab)(ac)(ab))^n = 1 \rangle$ for $n \geqslant 1$
- $\langle a, b \mid (ababb)(abaabb)(ababb) = 1 \rangle$
- $\langle a, b \mid ((aba^n b^{n+1})(aba^{n+1} b^{n+1})(aba^n b^{n+1}))^m = 1 \rangle$, for all $n, m \geqslant 1$.

As seen in these examples, the family of one-relator monoids satisfying conditions (C1), (C2), and (C3) includes many one-relator monoids with torsion $\langle A \mid w^n = 1 \rangle$ $(n > 1)$.

Proof ingredients

Let $M = \langle A \mid r = 1 \rangle$ and let $\Delta \subseteq A^*$ be the set of minimal invertible pieces of r. Suppose that:

(C1) no word from Δ is a proper subword of any other word from Δ,

(C2) there exist distinct words $\gamma, \delta \in \Delta$ with a common first letter, say a,

(C3) no word in Δ starts with a^2.

- We prove that there exists a free monoid F of finite rank $n \geqslant 2$ such that the free monoid with length relation $(F, \cdot, 1, =, \mathsf{L})$ is interpretable in M by systems of equations.
- Interpretation of a structure M in another structure N is a technical notion in model theory that approximates the idea of "representing M inside N".

Proof ingredients

Let $M = \langle A \mid r = 1 \rangle$ and let $\Delta \subseteq A^*$ be the set of minimal invertible pieces of r. Suppose that:

(C1) no word from Δ is a proper subword of any other word from Δ,

(C2) there exist distinct words $\gamma, \delta \in \Delta$ with a common first letter, say a,

(C3) no word in Δ starts with a^2.

- a is right invertible in M and the set of right inverses of elements from $\langle a \rangle$ give a submonoid of M which is isomorphic to a free monoid F of rank $\geqslant 2$.
- $\langle a \rangle$ is interpretable in M by the equation $ax = xa$.
- Since $F = \{x \in M \mid a^t x = 1 \text{ for some } t \in \mathbb{N}\}$, it follows that F is interpretable in M by the system of two equations $ay = ya$, $yx = 1$.
- The assumptions imply that $a\gamma = 1$ for every $\gamma \in \mathcal{B}$ where $\mathcal{B} \subseteq F$ is a basis of the free monoid F.
- To compare lengths of elements d_1, d_2 of the free monoid F we have $|d_1| \leqslant |d_2|$ iff there is an element $c \in \langle a \rangle$ such that $cd_2 = 1$ (which ensures $|c| = |d_2|$) and cd_1 belongs to $\langle a \rangle$ (which ensures $|d_1| \leqslant |c|$).

Example

$M \cong \langle a, b, c \mid abacab = 1 \rangle, \quad \gamma \equiv babac, \quad \delta \equiv cabab$

Note: $acab = abac$ and so $bacab = babac$ in M.

- γ and δ are right inverses of a.
- $F = \langle \gamma, \delta \rangle$ is a free submonoid of M with rank 2 with basis $\{\gamma, \delta\}$.

Note that:

$$\begin{aligned} aaa\gamma\delta\gamma &= 1 \\ aa\gamma\delta\gamma &= \gamma \notin \langle a \rangle \\ aaaa\gamma\delta\gamma &= a \in \langle a \rangle \end{aligned}$$

Let $d_1 = \gamma\delta$ and $d_2 = \delta\delta\gamma\delta$. We can see that $|d_1| \leqslant |d_2|$ as follows:
Let $c \in \langle a \rangle$ such that $cd_2 = 1$. Then

$$cd_2 = 1 \Rightarrow c = aaaa \Rightarrow |c| = |d_2|$$

and

$$cd_1 = aaa\gamma\delta = a \in \langle a \rangle \Rightarrow |d_1| \leqslant |c|.$$

A positive result

A case where a reduction to the group of units is possible is when every letter in the defining relator is invertible.

Theorem (Garreta and RDG (2019))

Let M be the monoid defined by $\langle A \mid w = 1 \rangle$ and let G be the group of units of M. Suppose that every letter in w is invertible in M. If the Diophantine problem is decidable in G then it is decidable in M.

- Proved using a result of Diekert & Lohrey (2008) showing that for monoids that satisfy a certain cancellation condition, decidability of the existential theory of word equations is preserved under graph products.

First-order theory

Proposition (Diekert and Lohrey (2008)) The bicyclic monoid $B \cong \langle b, c \mid bc = 1 \rangle$ has decidable first-order theory.[2]

It follows from this that all of the following are decidable in the bicyclic monoid:

- the Diophantine problem, the positive universal theory (i.e. identity checking), the positive AE-theory, ...

Theorem (Garreta and RDG (2019))

Let $M = \langle A \mid r = 1 \rangle$ and let $\Delta \subseteq A^*$ be the set of minimal invertible pieces of r. Suppose that:

(C1) no word from Δ is a proper subword of any other word from Δ, and

(C2) there exist distinct words $\gamma, \delta \in \Delta$ with a common first letter, say a.

Then the positive AE-theory of M is undecidable. In particular, M has undecidable first-order theory.

- Uses the result Durnev (1995), Marchenkov (1982) that the positive AE-theory with coefficients of free monoids is undecidable.

[2] They show the theory of the B can be reduced to Presburger arithmetic.

Open problems

Problem

If the word $w \in A^*$ has no self overlaps, i.e. there is no non-empty word which is both a proper prefix of w and a proper suffix of w, then is the Diophantine problem for the one-relator monoid $\langle A \mid w = 1 \rangle$ decidable?
In particular:

- Does $\langle a, b, c \mid abc = 1 \rangle$ have decidable Diophantine problem?
- Does $\left\langle b, c \mid b^2c = 1 \right\rangle$ have decidable Diophantine problem?

Problem

Do one-relator monoids $\langle A \mid w^n = 1 \rangle$, with $n > 1$, have decidable Diophantine problem?

Another direction

Investigate the Diophantine problem for non-special one-relator monoids for which the word problem is known to be decidable e.g.

- $\langle A \mid u = v \rangle$ where $|u| = |v|$ - homogeneous presentations.
- $\langle A \mid u = v \rangle$ where u and v have distinct initial letters and distinct terminal letters $\Rightarrow$ monoid is group embeddable.