The prefix membership problem for one-relator groups, and its semigroup-theoretical cousins

Igor Dolinka

dockie@dmi.uns.ac.rs

Department of Mathematics and Informatics, University of Novi Sad

The eNBSAN Online Meeting 2020

CyberSpace, 24 June 2020

Starring

Robert D. Gray
(Uni of East Anglia, Norwich)

Lt. Col. Frank Slade
(US Army, retired)

Also starring

UEA campus bunnies
(providing the much-required positivity...)

Intro & Some History

The word problem (in groups, monoids,...)

Assume we have given a (finitely generated) group $G = \langle X \rangle$ (e.g. by a presentation, etc.). So, elements of G are represented by words over $\overline{X} = X \cup X^{-1}$.

For starters, we'd very much like to know if two words represent the same element of G, and, in addition, is there an algorithm (think: *computer program*) which decides this.

The word problem for G:

INPUT: A word $w \in \overline{X}^*$.

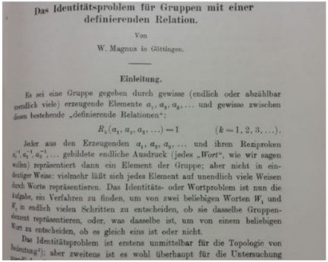
QUESTION: Does w represent the identity element 1 in G?

Similarly, one can ask about the word problem for monoids / inverse monoids / ..., with the difference being that the input requires two words u, v, and then we're keen to decide if $u = v$ holds in the corresponding monoid.

The beginning of the story: Back to the Great Depression

The beginning of the story: back to the Great Depression

The beginning of the story: back to the Great Depression



Das Identitätsproblem für Gruppen mit einer definierenden Relation.

Von

W. Magnus in Göttingen.

Einleitung.

Es sei eine Gruppe gegeben durch gewisse (endlich oder abzählbar unendlich viele) erzeugende Elemente $a_1, a_2, a_3, \ldots$ und gewisse zwischen diesen bestehende „definierende Relationen":

$$R_k(a_1, a_2, a_3, \ldots) = 1 \qquad (k = 1, 2, 3, \ldots).$$

Jeder aus den Erzeugenden $a_1, a_2, a_3, \ldots$ und ihren Reziproken $a_1^{-1}, a_2^{-1}, a_3^{-1}, \ldots$ gebildete endliche Ausdruck (jedes „*Wort*", wie wir sagen wollen) repräsentiert dann ein Element der Gruppe; aber nicht in eindeutiger Weise: vielmehr läßt sich jedes Element auf unendlich viele Weisen durch Worte repräsentieren. Das Identitäts- oder Wortproblem ist nun die Aufgabe, ein Verfahren zu finden, um von zwei beliebigen Worten W_1 und W_2 in endlich vielen Schritten zu entscheiden, ob sie dasselbe Gruppenelement repräsentieren, oder, was dasselbe ist, um von einem beliebigen Wort zu entscheiden, ob es gleich eins ist oder nicht.

Das Identitätsproblem ist erstens unmittelbar für die Topologie von Bedeutung[1]); aber zweitens ist es wohl überhaupt für die Untersuchung

Gimme some old time rock'n'roll

Theorem (W. Magnus, 1932)

Every one-relator group has decidable word problem.

Theorem (Magnus, 1930, "Der Freiheitssatz")

$w \in \overline{X}^*$ & $A \subset X$:

- *cyclically reduced;*
- *contains an occurrence of a letter not in A;*

$\Longrightarrow$ *the subgroup of* $\mathrm{Gp}\langle X \mid w = 1\rangle$ *generated by A is free.*

"Da sind Sie also blind gegangen!"

Max Dehn (Magnus' PhD advisor)

Theorem (Shirshov, 1962)

Every one-relator Lie algebra has decidable word problem.

The one-relator monoid Riddle

Open Problem (still! – as of 2020)

Is the word problem decidable for all one-relator monoids $\mathrm{Mon}\langle X \mid u = v \rangle$?

Theorem (Adyan, 1966)

The word problem for $\mathrm{Mon}\langle X \mid u = v \rangle$ *is decidable if either:*

- *one of* u, v *is empty (e.g.* $u = 1$ *– special monoids), or*
- *both* u, v *are non-empty, and have different initial letters and different terminal letters.*

Lallement (1977) and L. Zhang (1992) provided alternative proofs for the result about special monoids. The proof of Zhang is particularly compact and elegant.

NB. RIP S. I. Adyan (1 January 1931 – 5 May 2020).

The connection to the inverse realm

Adyan & Oganessyan (1987): The word problem for one-relator monoids can be reduced to the special case of

$$\mathrm{Mon}\langle X \mid asb = atc \rangle$$

where $a, b, c \in X$, $b \neq c$ and $s, t \in X^*$ (and their duals).

So, where do (one-relator) inverse monoids come into the picture?

Theorem (Ivanov, Margolis & Meakin, 2001)

If the word problem is decidable for all special inverse monoids $\mathrm{Inv}\langle X \mid w = 1 \rangle$ *— where* w *is a reduced word over* $\overline{X}$ *— then the word problem is decidable for every one-relator monoid.*

This holds basically because $M = \mathrm{Mon}\langle X \mid asb = atc \rangle$ embeds into $I = \mathrm{Inv}\langle X \mid asbc^{-1}t^{-1}a^{-1} = 1 \rangle$.

The plot thickens

	$\mathrm{Gp}\langle X \mid w = 1\rangle$	$\mathrm{Mon}\langle X \mid w = 1\rangle$	$\mathrm{Inv}\langle X \mid w = 1\rangle$
decidable WP	✓ (Magnus, 1932)	✓ (Adyan, 1966)	? ✗ (Gray, 2019)

Conjecture (Margolis, Meakin, Stephen, 1987)

Every inverse monoid of the form $\mathrm{Inv}\langle X \mid w = 1\rangle$ has decidable word problem.

Theorem (RD Gray, 2019; Invent. Math., March 2020)

There exists a one-relator inverse monoid $\mathrm{Inv}\langle X \mid w = 1\rangle$ *with undecidable word problem.*

Inverse monoid basics (1): Definitions & FIM

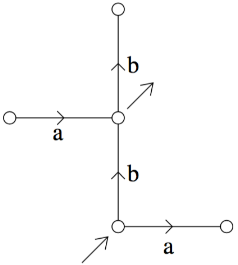
Inverse monoid = a monoid M such that for every $a \in M$ there is a unique $a^{-1} \in M$ such that $aa^{-1}a = a$ and $a^{-1}aa^{-1} = a^{-1}$.

Inverse monoids form a class of unary monoids defined by the laws

$$xx^{-1}x = x, \qquad (x^{-1})^{-1} = x, \qquad (xy)^{-1} = y^{-1}x^{-1},$$

$$xx^{-1}yy^{-1} = yy^{-1}xx^{-1}.$$

Free inverse monoid $FIM(X)$: Munn, Scheiblich (1973/4)



Elements of $FIM(X)$ are represented as Munn trees = birooted finite subtrees of the Cayley graph of $FG(X)$. The Munn tree on the left illustrates the equality

$$aa^{-1}bb^{-1}ba^{-1}abb^{-1} = bbb^{-1}a^{-1}ab^{-1}aa^{-1}b.$$

Inverse monoid basics (2): The E-unitary property

E-unitary inverse semigroups = the well-behaved, "nice guys".
For example, here are several (equivalent) definitions:

- For any $e \in E(S)$ and $x \in S$,
  $e \leq x$ (in the natural inverse semigroup order) $\Rightarrow x \in E(S)$.
- The minimum group congruence σ on S is idempotent-pure, which means that $E(S)$ constitutes a single σ-class.
- $\sigma = \sim$, where $\sim$ is the compatibility relation defined by
  $a \sim b \;\Leftrightarrow a^{-1}b, ab^{-1} \in E(S)$.
- ...

Theorem (Ivanov, Margolis & Meakin, 2001)

If w is cyclically reduced, then $M = \mathrm{Inv}\langle X \mid w = 1\rangle$ is E-unitary.

The key role of the prefix monoid

Consider a one-relator group G given by $\mathrm{Gp}\langle X \mid w = 1\rangle$.

P_w = the submonoid of G generated by all the prefixes of w.
This is the prefix monoid of G.
(Caution: depends on the presentation!)

Prefix membership problem for $G = \mathrm{Gp}\langle X \mid w = 1\rangle$ = membership problem for P_w within G.

Theorem (Ivanov, Margolis & Meakin, 2001)

If $M = \mathrm{Inv}\langle X \mid w = 1\rangle$ is E-unitary, then

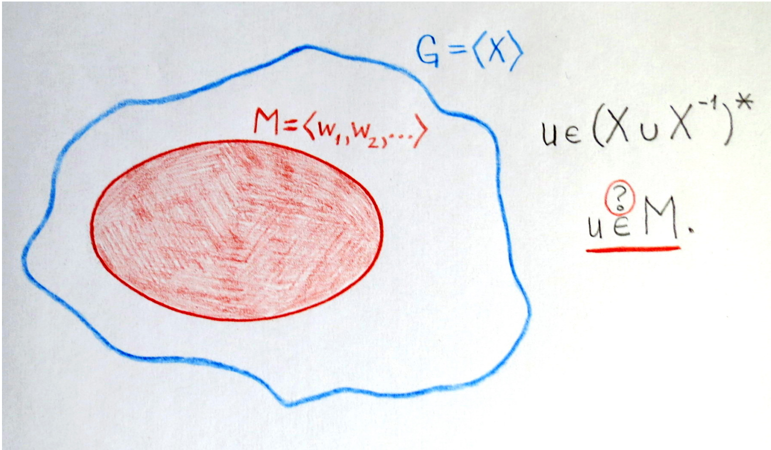
word problem for M = prefix membership problem for $G = \mathrm{Gp}\langle X \mid w = 1\rangle$.

Remark

$G = \mathrm{Gp}\langle X \mid w = 1\rangle$ is the maximum group image of $M = \mathrm{Inv}\langle X \mid w = 1\rangle$.

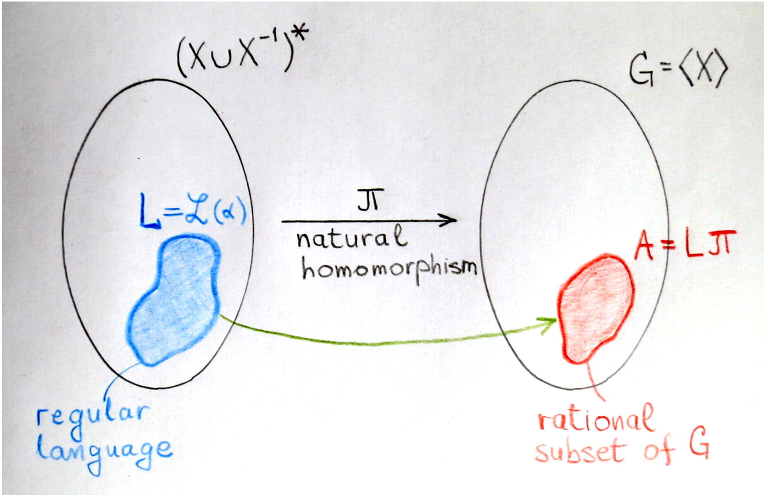
A Glimpse into the Toolbox

Membership problem (for a submonoid M of a group G)



Submonoid membership problem for G: Is there an algorithm which, given $u, w_1, w_2, \dots \in \overline{X}^*$, decides if $u \in \mathrm{Mon}\langle w_1, w_2, \dots \rangle$?

Rational subsets in groups



RSMP + Benois

Rational subset membership problem for a group $G = \langle X \rangle$:

INPUT: A word $w \in \overline{X}^*$ and a regular expression α over $\overline{X}$.

QUESTION: $w \in A_\alpha$?

(Here $A_\alpha \subseteq G$ is the image of $\mathscr{L}(\alpha)$, as in the previous pic.)

Theorem (Benois, 1969)

Every finitely generated free group has decidable RSMP. Consequently, rational subsets of f.g. free groups are closed for intersection and complement.

Factorisations

In this slide we consider factorisations $w \equiv w_1 \dots w_m$.

It is unital w.r.t. $M = \mathrm{Inv}\langle X \mid w = 1\rangle$ if each piece w_i represents an invertible element (i.e. unit, $aa^{-1} = a^{-1}a = 1$) of M.

Lemma

Unital fact. $\Longrightarrow P_w \leq G = \mathrm{Gp}\langle X \mid w = 1\rangle$ *is generated by* $\bigcup_{i=1}^{m} \mathrm{pref}(w_i)$.

In fact, for any factorisation of w we can consider the submonoid $M(w_1, \dots, w_m)$ of G generated by $\bigcup_{i=1}^{m} \mathrm{pref}(w_i)$. In G, we have

$$P_w \subseteq M(w_1, \dots, w_m).$$

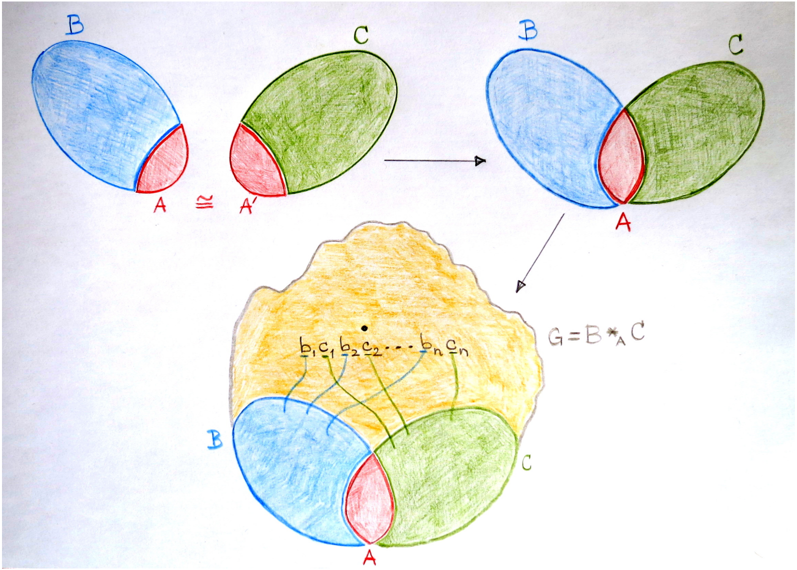
If $=$ holds, the considered factorisation is called conservative.

Theorem

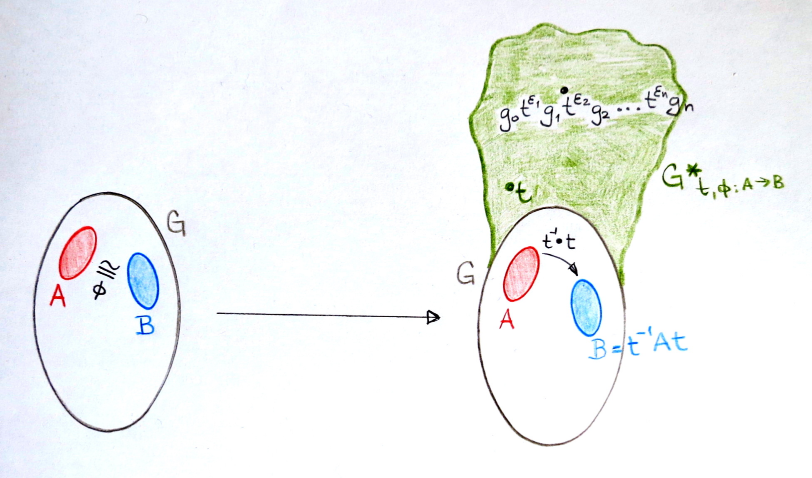
(i) *Any unital factorisation is conservative. (aka previous Lemma)*

(ii) *If* $M = \mathrm{Inv}\langle X \mid w = 1\rangle$ *is E-unitary then every conservative factorisation if unital.*

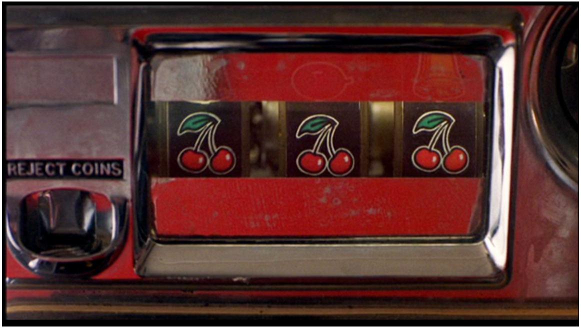
Amalgamated free product of groups $B *_A C$



HNN extension of a group $G*_{t,\phi:A\to B}$



The Results



Theorem A

$G = B *_A C$ (A, B, C finitely generated):

- B, C have decidable word problems;
- the membership problem for A is decidable in both B and C.

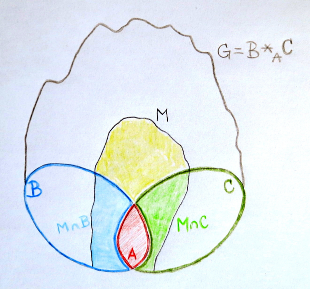
Let M be a submonoid of G with the following properties:

(i) $A \subseteq M$;

(ii) $M \cap B$ and $M \cap C$ are f.g. and $M = \mathrm{Mon}\langle (M \cap B) \cup (M \cap C) \rangle$;

(iii) the membership problem for $M \cap B$ in B is decidable;

(iv) the membership problem for $M \cap C$ in C is decidable.



Then the membership problem for M in G is decidable.

Rational intersections

$H \leq G$ closed for rational intersections:

$$R \in \mathrm{Rat}(G) \Longrightarrow R \cap H \in \mathrm{Rat}(G)$$

$H \leq G$ effectively closed for rational intersections:
there is an algorithm which does the following

INPUT: A regular expression for $R \in \mathrm{Rat}(G)$.
OUTPUT: Computes a regular expression for $R \cap H$.

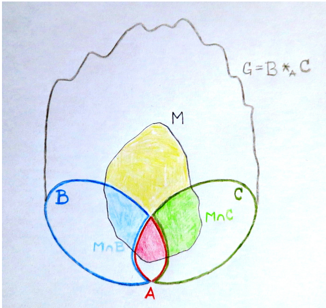
Theorem B

$G = B *_A C$ (A, B, C finitely generated):

- B, C have decidable rational subset membership problems;
- $A \leq B$ is effectively closed for rational intersections;
- $A \leq C$ is effectively closed for rational intersections.

Let M be a submonoid of G such that $M \cap B$ and $M \cap C$ are f.g. and

$$M = \mathrm{Mon}\langle (M \cap B) \cup (M \cap C) \rangle.$$



Then the membership problem for M in G is decidable.

Application #1: Unique marker letters

Theorem

- $G = \mathrm{Gp}\langle X \mid w = 1\rangle$
- $w \equiv u(w_1, \ldots, w_k)$ – *a conservative factorisation of* w
- $\forall i \in [1, k]$: *there is a letter* x_i *appearing exactly once in* w_i *and not appearing in any* w_j, $j \neq i$

$\Longrightarrow$ *G has decidable prefix membership problem.*

Example

The group

$$= \mathrm{Gp}\langle a, b, x, y \mid axbaybaybaxbaybaxb = 1(axb)(ayb)(ayb)(axb)(ayb)(axb) =$$

has decidable prefix membership problem $\Longrightarrow$ the inverse monoid

$$M = \mathrm{Inv}\langle a, b, x, y \mid axbaybaybaxbaybaxb = 1\rangle$$

has decidable WP.

Chicago O'Hare International Airport (IATA code: ORD)

While waiting for a connecting flight at ORD sometime in the 1980s, Stuart Margolis and John Meakin came up with the following example, the (in)famous O'Hare (inverse) monoid:

$$\mathrm{Inv}\langle a, b, c, d \mid (abcd)(acd)(ad)(abbcd)(acd) = 1 \rangle$$

Application #2: O'Hare-type examples

Proposition

Let $M = \mathrm{Inv}\langle Y, a, d \mid (au_{i_1}d)\dots(au_{i_m}d) = 1\rangle$, *where* a, d *do not appear in* u_{i_j}*'s. Assume further that:*

- *some of the* u_{i_j}*'s is the empty word;*
- *for each* $x \in Y$ *we have* $x \equiv \mathrm{red}(u_{i_r}u_{i_s}^{-1})$ *for some* r, s*;*
- *each* $au_{i_j}d$ *represents a unit of* M*.*

Then $G = \mathrm{Gp}\langle Y, a, d \mid (au_{i_1}d)\dots(au_{i_m}d) = 1\rangle$ *has decidable prefix membership problem, and so* M *as decidable WP.*

Consequently, the WP for the O'Hare monoid is decidable – just as announced at the WOW workshop in January 2018 by this fine gentleman:

Application #3: Disjoint alphabets

Theorem

- $G = \mathrm{Gp}\langle X \mid w = 1 \rangle$, *w is cyclically reduced*
- $w \equiv u(w_1, \ldots, w_k)$ *– a conservative factorisation of* w
- $i \neq j \;\Rightarrow\; w_i$ *and* w_j *have no letters in common*

$\Longrightarrow$ *G has decidable prefix membership problem, and thus* $M = \mathrm{Inv}\langle X \mid w = 1 \rangle$ *has decidable WP.*

Example

The group

$$G = \mathrm{Gp}\langle a, b, c, d \mid (abab)(cdcd)(abab)(cdcd)(cdcd)(abab) = 1 \rangle$$

has decidable prefix membership problem $\Longrightarrow$ the inverse monoid

$$M = \mathrm{Inv}\langle a, b, x, y \mid ababcdcdababcdcdcdcdabab = 1 \rangle$$

has decidable WP.

Application #4: Cyclically pinched presentations

Theorem

The prefix membership problem is decidable for one-relator groups defined by cyclically pinched presentations:

$$G = \mathrm{Gp}\langle X \cup Y \mid uv^{-1} = 1\rangle$$

where u, v are reduced words over disjoint X, Y, respectively.

Example

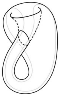
This implies decidability of the prefix membership problem for surface groups:

- orientable (known)

$$\mathrm{Gp}\langle a_1, \dots, a_n, b_1, \dots, b_n \mid [a_1, b_1] \dots [a_n, b_n] = 1\rangle,$$

- non-orientable (new)

$$\mathrm{Gp}\langle a_1, \dots, a_n \mid a_1^2 \dots a_n^2 = 1\rangle.$$



Theorem C

$G^* = G*_{t,\phi:A\to B}$ (G, A, B finitely generated):

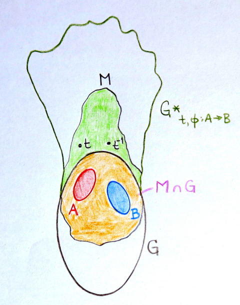
- G has decidable word problem;
- the membership problems for A and B are decidable in G.

Let M be a submonoid of G^* with the following properties:

(i) $A \cup B \subseteq M$;

(ii) $M \cap G$ is f.g. and
$$M = \mathrm{Mon}\langle (M\cap G) \cup \{t, t^{-1}\}\rangle;$$

(iii) the membership problem for $M \cap G$ in G is decidable.



Then the membership problem for M in G^* is decidable.

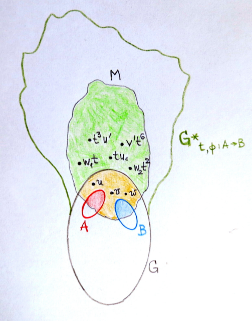
Theorem D

$G^* = G*_{t,\phi:A\to B}$ (G, A, B finitely generated):

- G has decidable rational subset membership problem;
- $A \leq G$ is effectively closed for rational intersections.

For some finite $W_0, W_1, \ldots, W_d, W_1', \ldots, W_d' \subseteq G$ let

$$M = \mathrm{Mon}\langle W_0 \cup W_1 t \cup W_2 t^2 \cup \cdots \cup W_d t^d \cup tW_1' \cup \cdots \cup t^d W_d' \rangle$$



Then the membership problem for M in G^* is decidable.

Application #5: Exponent sum zero result

$G = \mathrm{Gp}\langle X \mid w = 1\rangle$: some $t \in X$ has exponent sum zero in w.

By general theory ("Magnus' method", also Lyndon & McCool), G is $\cong$ an HNN extension of

$$H = \mathrm{Gp}\langle X' \mid \rho_t(w) = 1\rangle$$

where $|\rho_t(w)| < |w|$, w.r.t. to free associated subgroups A, B (will show this in a minute on a concrete example).

Theorem

Suppose that:

- $\rho_t(w)$ *is cyclically reduced;*
- H *has decidable rational subset membership problem;*
- $A \leq H$ *is effectively closed for rational intersections;*
- w *is either prefix t-positive or prefix t-negative.*

$\Longrightarrow$ G *has decidable prefix membership problem.*

Application #5: Exponent sum zero result (example)

$$w \equiv t^{-1}bcbt^{-8}bbct^{6}ct^{3}at^{-3}bt^{3}at^{-3}ct^{2}cta$$

$$\downarrow$$

$$\rho_t(w) \equiv b_1c_1b_1b_9b_9c_9c_3a_0b_3a_0c_3c_1a_0$$

$G = \mathrm{Gp}\langle X \mid w = 1\rangle$ is $\cong$ an HNN extension of

$H = \mathrm{Gp}\langle a_0, b_1, \ldots, b_9, c_1, \ldots, c_9 \mid \rho_t(w) = 1\rangle$ (free of rank 18)

w.r.t. $A = \mathrm{Gp}\langle b_1, \ldots, b_8, c_1, \ldots, c_8\rangle$ and $B = \mathrm{Gp}\langle b_2, \ldots, b_9, c_2, \ldots, c_9\rangle$ (which are free by Freiheitssatz);

$\Longrightarrow$ G has decidable prefix membership problem.
$+$ w is cyclically reduced $\Longrightarrow$ $M = \mathrm{Inv}\langle X \mid w = 1\rangle$ has decidable WP.

Further examples:

- large classes of Adyan-type presentations;
- conjugacy pinched presentations $\mathrm{Gp}\langle X, t \mid t^{-1}utv^{-1} = 1\rangle$ ($u, v \in \overline{X}^*$ reduced), including Baumslag-Solitar groups:

$$B(m, n) = \mathrm{Gp}\langle a, b \mid b^{-1}a^m ba^{-n} = 1\rangle.$$

The grand finale & an open problem

By modifying slightly the ideas from Bob's *Inventiones* paper, we obtain

Theorem

There exists a reduced word w over a 3-letter alphabet X such that $G = \mathrm{Gp}\langle X \mid w = 1\rangle$ has undecidable prefix membership problem.

Open Problem

Characterise the words $w \in \overline{X}^*$ such that the prefix membership problem for $\mathrm{Gp}\langle X \mid w = 1\rangle$ is decidable.
In particular, what about cyclically reduced words?

Thank you!

Questions and comments to:

dockie@dmi.uns.ac.rs

Further information may be found at:

http://people.dmi.uns.ac.rs/∼dockie