THE MEMBERSHIP PROBLEM FOR SUBMONOIDS OF FREE NILPOTENT GROUPS OF CLASS 2

Vitaly Roman'kov

OMSK, October 8, 2020

Rational subsets

Let G be a group. Rat(G) is the smallest collection of subsets of G containing the finite subsets and closed under the following rational operations:

- union: $X, Y \to X \cup Y$;
- product: $X, Y \to XY = \{xy : x \in X, y \in Y\}$;
- generation of submonoids $X \to X^*$.

Some properties of rational subsets

- Kleeny theorem: Let G be a finitely generated group, generated by a finite set X. A subset $R \subseteq G$ is rational if and only if there is a finite automaton $\mathcal{A}$ over X such that R is the output of $\mathcal{A}$.
- Anissimov-Seifert theorem: A subgroup $H \leq G$ belongs to Rat(G) iff H is finitely generated.
- Each finitely generated submonoid is rational, but rational submonoids need not be finitely generated.
- Rational subsets are not in general closed under complement and intersection

Membership problems

In this talk, we discuss the rational subset membership problem.
The rational subset membership problem for a finitely generated group G is the decision problem, where for a given rational subset R of G and a group element g it is asked whether $g \in G$.
We present some results for the case when R is a finitely generated submonoid.

Questions

Problem

Question 1 ([1, Open problem 24], [2]). Is there a finitely generated nilpotent group with an undecidable submonoid membership problem?

Question 2 ([1, Open problem 36], [2]). Does there exist a group with decidable submonoid membership and undecidable rational subset membership?

1. Marcus Lohrey, The rational subset membership problem for groups: a survey, University of St Andrews, Scotland, Publisher: Cambridge University Press, P. 368-389.

2. Benjamin Steinberg, The Submonoid Membership Problem for Groups, City College CUNY Seminar, 22 June 2013, http://www.sci.ccny.cuny.edu/ benjamin/ (Encompasses joint work with Mark Kambites, Markus Lohrey, Pedro Silva and Georg Zetzsche).

Some known results

Positive results.

- Benois, 1969. Rational subset membership is decidable for free groups.
- Eilenberg, Schutzenberger,1969: Rational subset membership in an abelian group is decidable.
- Grunschlag, 1999. Decidability of rational subset membership is a virtual property.
- Nedbay, 2000. The decidability of rational subset membership passes through free products.

Brief history

Negative results.

- Roman'kov, 1999. For every $c \geq 2$, there is an $r >> 1$ so that the free nilpotent. group of class c and rank r has undecidable rational subset membership.
- Lohrey, Steinberg, 2011. The free metabelian group M_2 of rank 2 contains a fixed finitely generated submonoid with an undecidable membership problem.

Positive elements

Definition

Let G be a finitely generated group with generators $x_1, \ldots, x_r$. An element u from G written as a word in the given generators is called *positive* if no x_i occurs in u to a negative exponent. An element u is called *potentially positive* if $\alpha(u)$ is positive for some automorphism α of the group G.

A criterion for potential positivity in free abelian groups

Let $A_r \simeq \mathbb{Z}^r$ be a free abelian group of rank r.

Definition

A subset $B = \{b_1, ..., b_m\}$ of A_r is said to be *positively independent* if an equation $\sum_{i=1}^{m} \alpha_i b_i = 0$ for $\alpha_i \geq 0, i = 1, ..., m$, implies that $\alpha_i = 0, i = 1, ..., m$.

Theorem

O.A. Yurak, 2006. A subset of non-trivial elements $B = \{b_1, ..., b_m\}$ of A_r is potentially positive if and only if it is positively independent.

A criterion for potential positivity in free nilpotent groups of class 2

Now $N_r, r \geq 2$, is the free nilpotent group of class 2 and $A_r = N_r/N_r'$ be the free abelian group For each element $g \in N_r$, by $\bar{g}$ we denote the image of g under the standard homomorphism $N_r \to A_r$.

Theorem

A subset of non-trivial elements $B = \{b_1, ..., b_m\}$ of N_r is potentially positive in N_r if and only if the set $\bar{B} = \{\bar{b}_1, ..., \bar{b}_r\}$ is positively independent in A_r.

Generators of $M = \text{mon}(A_r)$: positive G and negative F

Now $A_r \simeq \mathbb{Z}^r$. Let $1 \neq M = \text{mon}(Y)$, where $Y = \{g_1, \dots, g_k, f_1, \dots, f_l\}$. Here $G = \{g_1, \dots, g_k\}$ is a maximal positively independent subset of Y. Obviously, $G \neq \emptyset$. We can assume that G is positive for a basis $E_r = \{e_1, \dots, e_r\}$ of A_r. Then each subset $G \cup \{f_j\}$ is positively dependent. There are $\beta, \alpha_i \geq 0, i = 1, \dots, k, \beta_j \neq 0$ such that $\sum_{i=1}^k \alpha_i g_i = -\beta_j f_j$, $j = 1, \dots, l$. Then each f_j is negative for E_r. Denote $F = \{f_1, ..., f_l\}$.

$$\uparrow g_1 \uparrow g_2 \dots \uparrow g_k$$

$$\downarrow f_1 \downarrow f_2 ... \downarrow f_l$$

Generators of M in A_r: positive G_1, G_2, negative F and subgroup H

Denote $M_1 = \text{mon}(G)$ and $M_2 = \text{mon}(F)$. For each $f \in M_2$ there is a positive integer t for which $-tf \in M_1$. Then
$H = \{h \in M_2 : \exists(-h) \in M_1\}$ is a subgroup of A_r.
Let $E(1) = \{e_1, \ldots, e_s\}$ be a (minimal) part of E_r which generates a subgroup $A(1)$ containing H. Let $G_1 = \{g_1, \ldots, g_{k_1}\} \subseteq A(1)$. Then
$G_2 = \{g_{k_1+1}, \ldots, g_k\} = G \setminus G_1$.

$$H$$

$$\uparrow g_1 \uparrow g_2 \cdots \uparrow g_{k_1} \qquad \uparrow g_{k_1+1}, \ldots \uparrow g_k$$

$$\downarrow f_1 \downarrow f_2 \ldots \downarrow f_l$$

$$H$$

Generators of M in N_r: positive G_2, semisubgroup H and U

A finitely generated submonoid M of N_r is generated by G_1, G_2, F, U where $U \subseteq N_r'$, and G_1, G_2, F corresponds to the image $\bar{M}$ in A_r. For each $h \in H$ there is $h^- \in H$ such that $hh^- \in N_r'$.

Submonoid membership in N_r: positive results

Theorem

In the following cases the submonoid membership problem for N_r is algorithmically solvable:

- $F = \emptyset$.
- $G_2 = \emptyset$.

Submonoid membership in N_r: negative result

Theorem

For a sufficiently large r, the submonoid membership problem for N_r is algorithmically unsolvable. More exactly: for any Diophantine equation $D = v, v \in \mathbb{N}$ with fixed D there is a finitely generated submonoid M and subset of elements K of N_r such that $k = k(v) \in K$ lies in M if and only if $D = v$ is solvable in non-negative integers. By Matiyasevich theorem, there is D such that the class $D = v, v \in \mathbb{N}$, is unsolvable.

Simplest examples

1. Group: N_4.
Equation: $\zeta = 7$. Basis: $\{x_1, x_2, x_3, x_4\}$.
Monoid: $M = \mathrm{mon}(m_1, m_1^-, m_2)$;
$m_1 = x_1[x_2, x_1][x_4, x_3], m_1^- = x_1^{-1}, m_2 = x_2$.
Element: $g = x_2[x_4, x_3]^7$.
$m_1 m_2 = [x_2, x_1][x_3, x_4] \in M$. $(m_1 m_2)^7 = [x_2, x_1]^7[x_4, x_3]^7 \in M$. But we need in $[x_4, x_3]^7$ only.
Right solution:

$$m_1^7 m_2 (m_1^-)^7 = x_1^7[x_2, x_1]^7[x_4, x_3]^7 x_2 x_1^{-7} =$$

$$x_1^7[x_2, x_1]^7[x_4, x_3]^7 x_1^{-7} x_2 [x_2, x_1]^{-7} = x_2[x_4, x_3]^7.$$

$$7 \longleftrightarrow m_1^7.$$

Simplest examples

2. Group: N_{12}. Basis: $\{x_1, \dots, x_7, y_1, y_2, y_3, y_4, y_5, w, v\}$.
Equation: $\zeta_1^2 + \zeta_2^2 = \upsilon$ is equivalent to
$\zeta_3 = \zeta_1, \zeta_4 = \zeta_2, \zeta_1\zeta_3 = \zeta_5, \zeta_2\zeta_4 = \zeta_6, \zeta_5 + \zeta_6 = \zeta_7, \zeta_7 = \upsilon.$
Monoid:

$$m_1 = x_1[y_1, x_1][y_2, x_3][v, x_1], m_1^- = x_1^{-1}, m_2 = x_2[y_1, x_2][y_2, x_4][v, x_2],$$

$$m_2^- = x_2^{-1}, m_3 = x_3[y_1, x_3], m_3^- = x_3^{-1}, m_4 = x_4[y_1, x_4][w, x_4], m_4^- = x_4^{-1},$$

$$m_5 = x_5[y_1, x_5][x_1, x_3][w, x_5], m_6 = x_6[y_1, x_6][x_2, x_4][w, x_6],$$

$$m_7 = x_7[y_1, x_7][y_5, y_6][w, x_7], \textit{all } [x_i, x_j]^{\pm} \textit{ except} [x_1, x_3] \textit{ and } [x_2, x_4]$$

and all commutators that do not appear above except commutators with w, y_1, y-s, v. We can assume that all these commutators are trivial.
Element: $g = wy_3y_2y_1v[y_5, y_4]^{\upsilon}$. Presentation g in M:

$$m_7^{\zeta_7} ... m_4^{\zeta_4} w m_3^{\zeta_3} m_1^{\zeta_1} y_3 y_2 y_1 (m_3^-)^{\zeta_3} (m_4^-)^{\zeta_4}$$

$$v(m_1^-)^{\zeta_1} (m_2^-)^{\zeta_2} m_5^-)^{\zeta_5} (m_6^-)^{\zeta_6} (m_7^-)^{\zeta_7}$$

THANKS FOR YOUR ATTENTION!