Algorithmic undecidability of recognizing a non-Markovian group property

V G Durnev$^1$ and A I Zetkina$^{1,2}$

$^1$P. G. Demidov Yaroslavl' University, 150003, Sovetskaya str. 14, Yaroslavl', Russia
$^2$Voronezh State University, 394018, University Sq. 1, Voronezh, Russia

E-mail: durnev@uniyar.ac.ru

Abstract. We prove algorithmic undecidability of the following group property: “the positive theory of a group $G$ coincides with the positive theory of a free non-Abelian group” or (which is equivalent) “the positive theory of a group $G$ coincides with the positive theory of the class of all groups”. This group property is non-Markovian, therefore its algorithmic undecidability does not follow from the fundamental Adyan–Rabin theorem.

Keywords: algorithmic decidability, positive theories, non-Markovian group properties

1. Introduction

Study of group properties is of interest not only from the point of view of the abstract theory of algorithms, but also for various application in the information technologies such as machine learning tools. For example, an important problem in logical analysis of data (LAD) is justification of classification rules, e. g. as the rules computed by nearest neighbor classification algorithms or decision trees [1]. These rules are, in fact, extensions of a partially defined Boolean function and are referred to as a “theory” in the sense of combinatorial group theory [2].

We recall that a group property, $\alpha$, is called invariant when, if the property $\alpha$ holds for a group $G$ which is isomorphic to a group $H$, then the property $\alpha$ holds also for the group $H$.

An invariant group property, $\alpha$, is called Markovian, if there exists a finitely defined group, $G^+_\alpha$, for which the property $\alpha$ holds, and there exists a finitely defined group, $G^-\alpha$, which cannot be embedded to any finitely defined group for which the property $\alpha$ would hold. There exist a number of interesting examples of Markovian properties. For example,

- “$G$ is unit group”,
- “$G$ is a finite group”,
- “$G$ as a periodic group”,
- “$G$ is a cyclic group”,
- “$G$ is a Abelian group”,
- “$G$ is a nilpotent group”,
- “$G$ is a solvable group”,
- “a non-trivial identity holds on $G$”,
- “$G$ is a simple group”,

- “$G$ is a non-Abelian group”,
• "G is a finitely approximable group",
• "the identity problem is decidable in the group G" [3, 4],
• "G is a free group",
• "G is a torsion-free group",
• "G is Ǝ-equivalent to a free non-Abelian group",
• "G is ∀-equivalent to a free non-Abelian group",

and so on. Therefore, the following Adyan–Rabin fundamental theorem [5–7] is of a special interest:

**Theorem 1** (Adyan–Rabin). Any Markovian group property is algorithmically undecidable.

It is interesting to note that, according to Adyan–Rabin theorem, even the “simplest” (apparently) question, “whether a group G is isomorphic to one-element group”, is algorithmically undecidable given the definition of the group G.

There exist interesting examples of non-Markovian properties, both algorithmically decidable and algorithmically undecidable. For example, the following properties are non-Markovian: (i) "group G coincides with its derived group" and (ii) "group G is a Hopfian group". The first property is algorithmically decidable, whereas the second is algorithmically undecidable. Indeed, Collings [8] proved that recognizing the Hopfian property is algorithmically undecidable for finitely defined groups. Miller III and Schupp [9] proved that any finitely defined group can be embedded in some Hopfian finitely defined group, therefore the Hopfian property is not Markovian.

Elementary theory, Th(G), of a group G (with constants) is the set of all closed (i.e. those not containing free occurrences of variables) formulas Φ of the type

\[(Q_1 x_1)(Q_2 x_2) \ldots (Q_n x_n) \Psi,\]

where \( \Psi = \bigvee_{i=1}^k \left( \left( \&_{j \in A_i} w_{ij} = u_{ij} \right) \& \left( \&_{t \in B_i} v_{it} \neq z_{it} \right) \right), \)

\( w_{ij}, u_{ij}, v_{it}, z_{it} \) are words in the alphabet \( \{x_1, \ldots, x_n\} \cup G, \)

\( A_i \) and \( B_i \) are sets (possibly empty), \( Q_1, \ldots, Q_n \) being ∀ or ∃ quantifiers,

which are true on the group G.

Let us call \((Q_1 x_1)(Q_2 x_2) \ldots (Q_n x_n) \) the quantifier prefix of the formula Φ, and \( Q_1 Q_2 \ldots Q_n \) being called the type of quantifier prefix, and \( \Psi \) being called the quantifier-free part of the formula Φ.

A formula Φ is called positive if its quantifier-free part, Ψ, does not contain negation sign, i.e. if it has the form:

\[ \bigvee_{i=1}^k \left( \&_{j \in A_i} w_{ij} = u_{ij} \right). \]

The positive theory, \( Th^+(G) \), of a group G is the set of all closed positive formulas Φ which are true on the group G.

For example, a free non-cyclic group is simply infinite cyclic group and therefore it is Abelian group. The Abelian property means that the following positive formula Φ is true:

\[(\forall x)(\forall y)x \cdot y = y \cdot x.\]

On the contrary, the cyclic property ("group G contains an element of order of n") cannot be expressed by positive formulas, but can be expressed using the negation sign:

\[(\exists x)(x^n = 1 \& x^{n-1} \neq 1 \& x^{n-2} \neq 1 \& \ldots \& x^2 \neq 1)\]

On the other hand, if we restrict ourselves by formulas from the first-order language (i.e. the quantifiers are applied only to the group elements, not to sets of them) then the property
“group $G$ contains a non-unit element of a finite order” cannot be expressed by any formula at all.

By a way similar to the above, we define the concepts of elementary theory without constants, $Th(G)$, of a group $G$ and positive theory without constants, $Th^+(G)$, of a group $G$.

2. Setting of the problem and Methods

Here we study the non-Markovian property “positive theory (without constants) of a group $G$ coincides with the positive theory of a free non-cyclic group”. This property is not Markovian since for any group $G$, by Sacerdote’s theorem [10], the group $G \ast F_2$ is positively equivalent to a free non-cyclic group. The same is true not only for $G \ast F_2$, but also for any group having a homomorphic image of the type $A \ast B$, where $A$ and $B$ are not one-element groups and at least one of them contains not less than 3 elements.

**Theorem 2.** Given an arbitrary finitely defined group, $G$, there is no algorithm to decide whether its positive theory coincides with the positive theory of a free non-cyclic group.

According to Merzlyakov’s theorem [11], the positive theories of any two free non-cyclic group coincide with each other, and therefore they coincide with the positive theory of the class of all groups. In other words, a positive formula $\Phi$ holds on a free non-cyclic group if and only if it holds on any group. It means that no group can be distinguished from a free non-cyclic free group using any property $\Phi$ which does not contain negation signs.

From the above mentioned Merzlyakov’s result we obtain the following corollary:

**Corollary 1.** Given an arbitrary finitely defined group, $G$, there is no algorithm to decide whether its positive theory coincides with the positive theory of the class of all groups.

Thus the following theorems hold:

**Theorem 3.** Given an arbitrary finitely defined group, $G$, there is no algorithm to decide whether its positive $\forall \exists^2$-theory coincides with the positive $\forall \exists^2$-theory of a free non-cyclic group (with the positive $\forall \exists^2$-theory of the class of all groups).

**Theorem 4.** Given an arbitrary finitely defined group, $G$, there is no algorithm to recognize whether its positive $\forall \exists^2$-theory is decidable.

**Corollary 2.** Given an arbitrary finitely defined group, $G$, there is no algorithm to recognize whether its positive theory is decidable.

Let us denote by $F_2(\mathfrak{N}_2)$ the free nilpotent group of rank 2 and nilpotency class 2. As a free group of the manifold, $\mathfrak{N}_2$, of nilpotent groups with nilpotency class $\leq 2$, it is defined by the relation

$$\langle\langle a, b | [[x, y], z] = 1 \rangle\rangle.$$

It is important to note that the group $F_2(\mathfrak{N}_2)$ is finitely defined by the relation

$$\langle\langle a, b | [[a, b], a] = 1, [[a, b], b] = 1 \rangle\rangle,$$

where $[a, b] = a^{-1}b^{-1}ab$ is the commutator of the elements $a$ and $b$.

The following statement is a direct corollary from the fundamental Davis–Robinson–Putnam–Matiyasevich result [12]:

**Given an arbitrary recursively enumerable set, $U$, of natural numbers, there exist a formula $\Phi_U(x_1)$ of the type**

$$(\exists x_2 \ldots x_p)\Psi,$$

**where**

$$\Psi = \bigwedge_{i=1}^{m} \varphi_i$$
where each formula $\varphi_i$ has one of the following types:

\[ x_i + x_j = x_i, \quad x_i \cdot x_j = x_i, \quad x_i = c_i, \quad c_i \text{ is integer,} \]

such that the following equivalency holds for any natural $n$:

\[ n \in U \quad \text{if and only if} \quad \Phi_U(n) \text{ holds on the ring of integers, } \mathbb{Z} \]

(i.e. $\mathbb{Z} \models \Phi_U(n)$).

Maltsev [13] considered the predicate

\[ R(x_1, x_2, x_3) = (\exists z_1 z_2) \Psi, \quad \text{where} \]

\[ \Psi = (\& \sum_{i=1}^{2} [a_i, z_i] = x_i \& [z_1, a_2] = 1 \& [z_2, a_1] = 1 \& [z_1, z_2] = x_3) \]

and showed that for arbitrary integers $t, s$ and $r$:

- a formula $R(c^t c^s c^r)$, where $c = [a_2, a_1] = a_2^{-1} a_1^{-1} a_2 a_1$ is the commutator of the elements $a_1$ and $a_2$, holds on the group $F_2(\mathfrak{N}_2)$ if and only if $r = ts$.

Recall some well-known facts about the $F_2(\mathfrak{N}_2)$ group.

(i) Its center coincides with its derived group.

(ii) This center is an infinite free cyclic group generated, for example, by the commutator $c = [a_2, a_1] = a_2^{-1} a_1^{-1} a_2 a_1$.

(iii) For any three elements, $u, v$ and $w$ of the group $F_2(\mathfrak{N}_2)$ the following equalities hold:

\[ [u v, w] = [u, v] [v, w] \quad \text{and} \quad [w, u v] = [w, u] [w, v]. \]

(iv) For any integer $n$ and $m$ the following equalities hold:

\[ [a_2^n, a_1^m] = [a_2, a_1]^{nm} = [a_2, a_1^n] = [a_2, a_1^m] = [a_1, a_2]^{-nm} = [a_1^{-nm}, a_2] = [a_1, a_2^{-nm}]. \]

(v) Therefore for any element $g \in F_2(\mathfrak{N}_2)$ the following equivalences hold:

- $g$ is a power of the element $c$ $\iff$ $g$ is in the derived group of $F_2(\mathfrak{N}_2)$ $\iff$
  - the formula $(\exists u) g = [u, a_1]$ is true on $F_2(\mathfrak{N}_2)$ $\iff$
  - the formula $(\exists u) g = [u, a_2]$ is true on $F_2(\mathfrak{N}_2)$ $\iff$
  - the formula $(\exists u) (\exists v) g = [u, v]$ is true on $F_2(\mathfrak{N}_2)$ $\iff$
  - $g$ is in the center of $F_2(\mathfrak{N}_2)$ $\iff$
  - the formula $\sum_{i=1}^{2} [x, a_i] = 1$ is true on $F_2(\mathfrak{N}_2)$.

Let $\mathbb{Z}(x)$ denote, for example, the formula $\sum_{i=1}^{2} [x, a_i] = 1$ or the formula $(\exists u)(\exists v)x = [u, v]$. Then for an arbitrary element $g$ of the group $F_2(\mathfrak{N}_2)$ the following equivalence holds:

- $g$ is a power of the element $c$ $\iff$ the formula $\mathbb{Z}(g)$ holds on the group $F_2(\mathfrak{N}_2)$.
3. Results and discussion

Let $U$ be an arbitrary recursively enumerable set of natural numbers. Let us transform a formula, $\Phi_U(x_1)$, related to the ring of integers, $\mathbb{Z}$, into the formula $\Phi_U^{(1)}(x_1)$, related to the $F_2(N_2)$ group. To do this, we assume

$$\Phi_U^{(1)}(x_1) = (\exists x_2 \ldots x_p)(\Psi_1, \&_{i=2}^p \mathbb{Z}(x_i)),$$

where $\Psi_1$ is obtained from $\Psi$ by the following substitutions:

- each sub-formula $\varphi$ of the type $x_i + x_s = x_r$ is substituted by the subformula $x_i x_s = x_r$;
- each sub-formula $\varphi$ of the type $x_i x_s = x_r$ is substituted by the subformula $R(x_i, x_s, x_r)$;
- each sub-formula $\varphi$ of the type $x_i = m_s$ is substituted by the subformula $x_i = c^{m_s}$;
- the sub-formulas of the type $x_i = x_s$ are left unchanged.

Then the following equivalence holds for an arbitrary natural $n$:

$$n \in U \text{ if and only if the formula } \Phi_U^{(1)}(c^n) \text{ is true on the } F_2(N_2) \text{ group (i.e. } F_2(N_2) \models \Phi_U^{(1)}(c^n)).$$

Then we reduce the formula $\Phi_U^{(1)}(x_1)$ to pre-normal form, substitute $x_1$ with $x$ and re-enumerate the variables to obtain the formula, $\Phi_U^{(2)}(x)$ of the type

$$(\exists x_1 \ldots x_k)(\&_{i=1}^m w_i(x, x_1, \ldots, x_k, a_1, a_2) = 1)$$

such that the following equivalence holds for an arbitrary natural $n$:

$$n \in U \text{ if and only if the formula } \Phi_U^{(2)}(c^n) \text{ is true on the } F_2(N_2) \text{ group (i.e. } F_2(N_2) \models \Phi_U^{(2)}(c^n)).$$

If we assume

$$\Phi_U(x) = (\forall z_1 z_2)(\exists x_1 \ldots x_k)(\&_{i=1}^m w_i(x, x_1, \ldots, x_k, a_1, a_2) = 1),$$

then the following equivalence holds for an arbitrary natural $n$:

$$n \in U \text{ if and only if the formula } \Phi_U(c^n) \text{ is true on the } F_2(N_2) \text{ group (i.e. } F_2(N_2) \models \Phi_U(c^n)).$$

Taking the set $U$ to be recursively enumerable set (but not recursive set), we obtain that the positive $\forall^2\exists^k$-theory of the $F_2(N_2)$ group is algorithmically undecidable for some $n$.

Since the following equivalences hold:

- the formula $(\exists x_1 \ldots x_k)(\&_{i=1}^m w_i(x_1, \ldots, x_k, a_1, a_2) = 1)$ is true on the group $F_2(N_c) \iff$ the formula $(\exists x_1 \ldots x_k)(\&_{i=1}^m w_i(x_1, \ldots, x_k, a_1, a_2), a_j = 1)$ is true on the group $F_2(N_{c+1}) \iff$
- the formula $(\exists x_1 \ldots x_n)(\&_{i=1}^m w_i(x, x_1, \ldots, x_n, a_1, a_2) = 1)$ is true on the group $F_2(N_c) \iff$

for any $p \geq 2$ the formula $(\exists x_1 \ldots x_k)(\&_{i=1}^m w_i(x_1, \ldots, x_k, a_1, a_2) = 1)$ is true on $F_p(N_c)$,
then it is easy to obtain by induction that for some $k$, the positive $\forall^2 \exists^k$-theory of the $F_p(\mathfrak{N})$ group is algorithmically undecidable at any $p \geq 2$ and $c \geq 2$.

However, there are some obstacles to further strengthening the proven statements. Since the formula of the type
\[
(\forall z_1)(\exists x_1 \ldots x_n)(\bigwedge_{i=1}^m w_i(x_1, \ldots, x_n, z_1) = 1)
\]
is true on the group $F_m(\mathfrak{N})$ if and only if the formula
\[
(\exists x_1 \ldots x_n)(\bigwedge_{i=1}^m w_i(x_1, \ldots, x_n, a_1) = 1),
\]
is true on the infinite cyclic group $F_1 = \langle \langle a_1 \rangle \rangle$, then for any $n$, the positive $\forall \exists^n$-theory of the $F_p(\mathfrak{N})$ group is algorithmically decidable at any $p$ and $c$.

Since the formula of the type
\[
(\exists x_1 \ldots x_n)(\bigwedge_{i=1}^m w_i(x_1, \ldots, x_n, a_1, \ldots, a_p) = 1),
\]
is true on this group, then the question whether the formula of the type
\[
(\forall z_1)(\forall z_2)(\exists x_1 \ldots x_n)w(x_1, \ldots, x_n, z_1, z_2) = 1
\]
is true on the group $F_2(\mathfrak{N})$ is reduced to the question whether formulas of the type
\[
(\exists x_1 \ldots x_n) w(x_1, \ldots, x_n, a_1, a_2) = 1
\]
are true on this group. In other words, the above question is reduced to solvability of a single equation in the group $F_2(\mathfrak{N})$. The latter problem is algorithmically decidable. Indeed, the elements of the group $F_2(\mathfrak{N})$ have unique representation of the type $a_1^u a_2^v c^z$, where $u$, $v$ and $z$ are integer. Therefore, the latter problem can be reduced to the question whether the system of two linear and one quadratic equations with integer coefficients has an integer solution. But the latter question is algorithmically decidable.

Using the results by Merzlyakov [11], Makanin [14] proved that the positive theory (with constants) for a free group of any rank is decidable, as well as the same theory for the class of all groups.

In the following consideration, we use the construction developed by Miller [15]. Let $G$ be a group finitely defined by the following generators and relations
\[
G = \langle \langle a_1, \ldots, a_n \mid R_1 = 1, \ldots, R_m = 1 \rangle \rangle,
\]
and $w$ be an arbitrary words in the alphabet of the group $G$. Following to Miller [15], we denote by $G_w$ the group finitely defined by
\[
G_w = \langle \langle a_1, \ldots, a_n \mid R_1 = 1, \ldots, R_m = 1, a^{-1}ba = (bc)^{-1}c(bc), (ba^{-1})^{-1}a(ba^{-1}) = (bc^{-1})^{-1}c(bc^{-1})\rangle \rangle
\]
\[
a^{-3}[w, b^i]a^3 = c^{-3}bc^3, a^{-(3+i)} a b a^{3+i} = c^{-(3+i)} b c^{(3+i)} (i = 1, 2, \ldots, n)
\]
where $a$, $b$ and $c$ are new characters.

Then the following statements hold:
(i) The group $G_w$ is generated by the elements $b$ and $ca^{-1}$.
(ii) If $w = 1$ in the group $G$, then $G_w$ is one-element group.
(iii) If $w \neq 1$ in the group $G$, then $G$ is a subgroup of the group $G_w$.

The group $G_w*F_2(\Omega_2)$ has a finite definition which contain 4 generators and $(m+2)$ relations.
If the initial group $G$ is a Borisov-type group [16] with 12 relations, then the group $G_w*F_2(\Omega_2)$ has the finite definition of the following type:

$$\langle \langle a, b \mid R_1 = 1, \ldots, R_{14} = 1 \rangle \rangle$$

Therefore we obtain the following alternative:

(i) If $w = 1$ in the group $G$, then for some $k$, the positive $\forall^2 \exists^k$-theory of the group $G_w*F_2(\Omega_2) = F_2(\Omega_2)$ is algorithmically undecidable (does not coincide with the positive $\forall^2 \exists^k$-theory of a free non-cyclic group, and does not coincide with the positive $\forall^2 \exists^k$-theory of the class of all groups)
(ii) If $w \neq 1$ in the group $G$, then, by Sacerdote theorem [10], the positive theory of the $G_w*F_2(\Omega_2)$ group coincides with the positive theory of a free non-cyclic group, as well as with the positive theory of the class of all groups. Therefore, by Makanin’s theorem [14], the positive theory of the $G_w*F_2(\Omega_2)$ group is algorithmically decidable

4. Conclusion
We prove algorithmic undecidability of the following non-Markovian property: “group $G$ is positively equivalent to a free non-cyclic group”. We also prove that there exists such natural $k$, for which the following non-Markovian properties are algorithmically undecidable: (i) “group $G$ is positively $\forall^2 \exists^k$-equivalent to a free non-cyclic group” and “positive $\forall^2 \exists^k$-theory of the group $G$ coincides with the positive $\forall^2 \exists^k$-theory of a free non-cyclic group”.

Acknowledgments
A.Z. acknowledges the support from the Russian Science Foundation (Project No.19-12-00095).

References
[1] Boros E, Crama Y, Hammer P L, Ibaraki T, Kogan A and Makino K 2011 Ann. Oper. Res. 188(1) 33–61
[2] Chikalov I, Lozin V, Lozina I, Moshkov M, Nguyen H S, Skowron A and Zielosko B 2013 Logical Analysis of Data: Theory, Methodology and Applications (Intelligent Systems Reference Library vol 41) (Berlin, Heidelberg: Springer) pp 147–192
[3] Novikov P S 1958 J. Symbol. Logic 23(1) 50–52
[4] Boone W W 1959 Ann. Math. 70 207–265
[5] Adyan S I 1955 Dokl. Akad. Nauk SSSR 103 533–535 in Russian
[6] Adyan S I 1957 Trans. Moscow Math. Soc. 6 231–298 in Russian
[7] Rabin M O 1958 Ann. Math. 67 172–194
[8] Collins D J 1969 Arch. Math. 20(3) 235–240
[9] Miller C F and Schupp P E 1971 J. Algebra 17 171–176
[10] Sacerdote G S 1973 J. Algebra 27 475–485
[11] Merzlyakov Y I 1966 Algebra i logika 5 25–42 in Russian
[12] Matijasevič J V 1970 Sov. Math. Doklady 11 354–358
[13] Mal’tsev A I 1965 Trans. Amer. Math. Soc., Ser. 2 45 221–231
[14] Makanin G S 1985 *Math. USSR Izv.* **25** 75–88

[15] Miller C F 1992 Decision problems for groups — survey and reflections *Algorithms and Classification in Combinatorial Group Theory* (Math. Sci. Res. Inst. Publ. vol 23) ed Baumslag G and Miller C F (New York, NY: Springer) pp 1–59

[16] Borisov V V 1969 *Math. Notes* **6** 768–775