On the equations with constraints in free groups

V G Durnev, O V Zetkina and A I Zetkina
P. G. Demidov Yaroslavl' University, 150003 Yaroslavl', Russia
E-mail: ovzetkina@yandex.ru

Abstract. We establish algorithmic undecidability of the problem of recognizing solubility for some type of equations with constraints in free $F_2$ and $F_3$ groups. Finite inapproximability is proven for explicit (resolved with respect to the unknowns) equations with 6 unknowns in free groups. We also prove existence of a polynomial algorithm to recognize solubility of some equations in words and lengths. The derived (commutator) subgroup of a free non-cyclic group is not a definable subgroup that solves a A. I. Maltsev’s problem from the “Kourovka Notebook”.

1. Introduction
Study of the equations with constraints is an important problem in algebra and algorithm theory. Recall that the Hilbert’s tenth problem is the question of existence of an algorithm which can decide whether the equation with constraints of the type

$$F(x_1, \ldots, x_n) = 0 \& \bigwedge_{i=1}^n x_i \in \mathbb{Z},$$

where $F(x_1, \ldots, x_n)$ is a polynomial over the ring of integers $\mathbb{Z}$, has a solution. It is well-known that this problem has a negative answer obtained in combined work of Martin Davis, Julia Robinson, Hilary Putnam and Yuri Matiyasevich [1]. Another problem, which is equivalent to the above one, has a negative answer as well: there exists no algorithm to decide whether an arbitrary equation with constraints of the type

$$F(x_1, \ldots, x_n) = 0 \& \bigwedge_{i=1}^n x_i \in \mathbb{K},$$

has a solution in natural numbers (e.g for $\mathbb{K} = \mathbb{N}$).

Note that the existence of an algorithm to decide whether the equation with constraints of the type (2) has a solution in rational numbers (e.g for $\mathbb{K} = \mathbb{Q}$) is currently an open problem, while for real numbers ($\mathbb{K} = \mathbb{R}$) this issue was positively solved by Tarski long ago. Note also that the solubility problem for the equation with constraints of the type (2) with $\mathbb{K} = \{0, 1\}$ is NP-complete.

Let $F_m$ be a free group of rank $m$ with free generators $a_1, \ldots, a_m$. For $m = 2$ we will use $a$ and $b$ instead of $a_1$ and $a_2$, respectively.

Recall some definitions related to equations in free groups.
Systems of equations with unknowns $x_1, \ldots, x_n$ in a free group $F_m$ is an expression of the type
\[ \sum_{i=1}^{k} w_i(x_1, \ldots, x_n, a_1, \ldots, a_m) = u_i(x_1, \ldots, x_n, a_1, \ldots, a_m), \tag{3} \]
where $w_i(x_1, \ldots, x_n, a_1, \ldots, a_m)$ and $u_i(x_1, \ldots, x_n, a_1, \ldots, a_m)$ are words in the alphabet
\[ \{ x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}, a_1, a_1^{-1}, \ldots, a_m, a_m^{-1} \}. \]
A set $\langle g_1, \ldots, g_n \rangle$ of the elements of the group $F_m$ is the solution of the system (3), if for all $i$ ($i = 1, \ldots, k$) the equality
\[ w_i(g_1, \ldots, g_n, a_1, \ldots, a_m) = u_i(g_1, \ldots, g_n, a_1, \ldots, a_m) \]
is valid in group $F_m$. Two systems of equations with the same unknowns are equivalent, if they have the same set of solutions.

With the help of the equation
\[ [x, a] = ([x, b] y^2)^2, \]
which has only the trivial solution $x = 1, y = 1$ in a free group $F_m$ for all $m \geq 2$, any system of equations (3) can be substituted by one equivalent equation.

Two main problems are traditionally considered for the equations in free groups: availability of a solution and description of the set of all solutions.

In connection with the problem of decidability of elementary theories of free groups addressed by A. Tarski [2], studies of decidability of equations in free groups started in the end of 1950s (see, e.g. [3–7]).

G. S. Makanin [8] proposed an enumeration algorithm to recognise solubility of equations in a free group. He proved that if a given equation of notational length $d$ has a solution in a free group, then length of each component of the minimal (with respect to maximal length of the components) solution does not exceed $\Phi(d)$, where $\Phi(x)$ is some recursive function.

In the course of the above mentioned A. Tarski’s problem of decidability of elementary theory of an arbitrary free group, it is interesting to study algorithmic nature of this theory. The main results in this field were obtained by G. S. Makanin. On the way established in [8] he proved decidability of existential (universal) and positive theory for any free group [9]. In his proof of decidability of positive theory, G. S. Makanin used the method to eliminate quantifiers from positive sentences related to free groups proposed by Yu. I. Merzlyakov [10].

A. A. Razborov [11] gave the description of the solution set for an arbitrary compatible system of equations in a free group.

2. Methods

After G. S. Makanin [8] had built the deciding algorithm for a system of equations in a free group $F_m$, a special attention was paid to the question of existence of analogous algorithms for equations with various “not so complex” constraints in free groups.

Yu. I. Merzlyakov [10] reduced the question on decidability of the positive theory of a free group to the following problem:

does there exist an algorithm which would allow to recognize whether an arbitrary given equation
\[ w( x_1, \ldots, x_n, a_1, \ldots, a_m ) = 1 \]
in a free group of a countable rank has a solution, $g_1, \ldots, g_n$, such that
\[ g_1 \in F_{m_1}, g_2 \in F_{m_2}, \ldots, g_t \in F_{m_t}. \]
where $m_1 \leq m_2 \leq \ldots \leq m_t$, $F_{m_t}$ is a free group with the generators $a_1, \ldots, a_{m_t}$.

G. S. Makanin [9] built the desired algorithm and thereby proved decidability of the positive theory of a free group.

It is well-known that the question of exactness of the Gassner matrix representation of the colored braid group [12, 13] is equivalent to the question of absence of nontrivial solution of the equation

$$x_1a_1x_1^{-1} \cdot x_2a_2x_2^{-1} \cdots x_ma_mx_m^{-1} = a_1 \cdot a_2 \cdots a_m,$$

in a free group $F_m$ satisfying the condition

$$x_1 \in F_m^{(2)}, \ldots, x_n \in F_m^{(2)};$$

where $F_m^{(2)}$ is the commutator (derived) subgroup of the free group $F_m$. Recall that, for an arbitrary group $G$, its second derived subgroup is denoted as $G^{(2)}$, i.e. $G^{(2)} = [G^{(1)}, G^{(1)}]$, where $G^{(1)} = [G, G]$ is the derived subgroup of $G$. Moreover, the following relations hold for arbitrary $t$: $G^{(t+1)} = [G^{(t)}, G^{(t)}]$ and $G^{(0)} = G$.

Generalizing these problems, G. S. Makanin raised the following problem for equations in free groups in “Kourovka Notebook” [14]:

“9.25. Find an algorithm which recognizes, by an equation

$$w(x_1, \ldots, x_n, a_1, \ldots, a_m) = 1$$

in a free group $F_m$ and by a list of finitely generated subgroups $H_1, \ldots, H_n$ of $F_m$, whether there is a solution of this equation satisfying the condition

$$x_1 \in H_1, \ldots, x_n \in H_n.”$$

The first positive results in solving this problem were obtained by A. Sh. Malkhasyan (see, e.g., [15]).

V. Diekert [16] demonstrated the decidability and PSPACE-hardness of the following problem: given an arbitrary equation

$$w(x_1, \ldots, x_n, a_1, \ldots, a_m) = 1$$

in a free group $F_m$, and a list $H_1, \ldots, H_n$ of regular subsets (“languages”) of $F_m$, recognize whether there exist a solution of this equation satisfying the condition

$$x_1 \in H_1, \ldots, x_n \in H_n.$$

Since the finitely generated subgroups are regular subsets, thereby the above G. S. Makanin’s problem is solved.

Of interest is the further studying of various generalizations of this problem for free groups which could be produced by weakening the constraints imposed on the subgroups $H_1, \ldots, H_n$.

One of reasons to deal with finitely generated subgroups in formulation of the above problem 9.25 is that for finitely generated subgroups of a free group, the membership problem is decidable.

At the same time, the membership problem is also decidable for a number of infinitely generated subgroups of a free group, e.g. for the first, $F_m^{(1)}$, and second, $F_m^{(2)}$, derived subgroups of a free group $F_m$, the membership problem is solved very easily (essentially easily as for some finitely generated subgroups). Therefore the following generalization of the problem 9.25 seems to be quite natural:

“9.25a. Does there exist an algorithm which recognizes, by an equation

$$w(x_1, \ldots, x_n a_1, \ldots, a_m) = 1$$

in a free group $F_m$ and by a list its subgroups $H_1, \ldots, H_n$ with decidable membership problems, whether there is a solution of this equation satisfying the condition $x_1 \in H_1, \ldots, x_n \in H_n$?”.

3
3. Results and discussion

The following result was obtained in [17].

**Theorem 1.** In a free group $F_2$ with the free generators $a$ and $b$ one can construct an equation

$$w(x, x_1, \ldots, x_n, a, b) = 1$$

with unknowns $x_1, x_2, \ldots, x_n$, constants $a, b$ and parameter $x$, such that there exists no algorithm to recognize for an arbitrary $k \in \mathbb{N}$, whether the equation

$$w(a^k, x_1, \ldots, x_n, a, b) = 1,$$

has a solution satisfying the condition

$$x_1 \in [F_2, F_2], \ldots, x_t \in [F_2, F_2],$$

where $t$ is some fixed integer between 1 and $n$.

In what follows we shall strengthen this result substantially. To some extent, this strengthening is close to that finally possible.

Several works [6, 7, 18–21] studied the equations of the type

$$w(x_1, \ldots, x_n) = g(a_1, \ldots, a_m),$$

where $w(x_1, \ldots, x_n)$ is a word in the alphabet of unknowns $x_1, x_2, \ldots, x_n$ (i.e. free of $a_1, \ldots, a_m$ constants), and $g(a_1, \ldots, a_m)$ word in the alphabet of constants $a_1, \ldots, a_m$ (i.e. free of unknowns). Such equations are called explicit equations (resolved with respect to the unknowns, or equations with the right-hand-side). The problem of decidability of such equations is also known as substitution problem.

Let $[u, v]$ denote the commutator of $u$ and $v$ elements, i.e. $[u, v] = uvu^{-1}v^{-1}$.

**Theorem 2.** In a free group $F_2$ with the free generators $a$ and $b$ one can construct a family of explicit equations

$$w(x^k, x_1, \ldots, x_n) = [a, b],$$

where $w(x^k, x_1, \ldots, x_n)$ is a word in the alphabet of unknowns $x, x_1, x_2, \ldots, x_n$, such that there exists no algorithm to recognize for an arbitrary $k \in \mathbb{N}$, whether the equation

$$w(x^k, x_1, \ldots, x_n) = [a, b],$$

has a solution satisfying the condition

$$x_1 \in [F_2, F_2], \ldots, x_t \in [F_2, F_2],$$

where $t$ is some fixed integer between 1 and $n$.

**Theorem 3.** There exists no algorithm to recognize, whether an arbitrary equation

$$w(x_1, \ldots, x_n) = [a, b]$$

in a free group $F_2$ has a solution $g_1, \ldots, g_n$ satisfying the condition

$$g_1 \in F_2^{(2)}.$$
Note that the the word $[a,b]$ in the right-hand-side of the equations in this theorem has the length 4. The following theorem shows that it is impossible to decrease the length of the right-hand-side.

**Theorem 4.** For an arbitrary explicit equation of the type

$$w(x_1, \ldots, x_n) = g(a, b),$$

where $w(x_1, \ldots, x_n)$ is a word in the alphabet of unknowns $x_1, x_2, \ldots, x_n$, and $g(a, b)$ is an element of length less than 4 in a free group $F_2$ with the free generators $a$ and $b$, there exists a polynomial algorithm to recognize whether this equation has a solution satisfying the condition

$$x_1 \in F_2^{(s)}, \ldots, x_t \in F_2^{(s)},$$

where $t$ is some fixed integer between 1 and $n$.

For the equations with one unknown the situation is different.

Let $G(r)$ be either $r$-th derived subgroup $F_n^{(r)}$ of the free group $F_r$ or $r$-th term $(F_m)_r$ of its lower central series.

**Theorem 5.** For an arbitrary explicit equation with one unknown

$$w(x_1, a_1, \ldots, a_n) = 1$$

in a free group $F_n$, there exists a polynomial algorithm to recognize whether this equation has a solution such that $x_1 \in G(r)$.

3.1. Equations with constraints in free group

Let $\varphi_i$ denote the following endomorphism of the free group $F_m$ of rank $m$ with the generators $a_1, \ldots, a_m$

$$\varphi_i(a_j) = a_j \quad \text{for} \quad j \neq i, \quad \varphi_i(a_i) = 1.$$

Similarly to the braid group, let the endomorphism $\varphi_i$ be called “endomorphism of pulling out the $i$-th generator”.

Let us assume

$$P^{(i)}_n = \text{Ker} \varphi_i \quad P_m = \bigcap_{i=1}^{m} P^{(i)}_m$$

and let $P^{(i)}_m$ be its subgroup of $i$-clear elements, and $P_m$ its subgroup of clear or smooth elements.

It is obvious that $P_m$ is normal subgroup of the $F_m$ group which is included in its derived subgroup $F_m^{(1)}$ ($P_m \subseteq F_m^{(1)}$) and $P_2 = F_2^{(1)}$, but $P_m \neq F_m^{(1)}$ for $m \geq 3$.

**Theorem 6.** For $m \geq 3$ there exists no algorithm to recognize whether an arbitrary equation in group $F_m$

$$w(x_1, \ldots, x_n, a_1, \ldots, a_m) = 1$$

has a solution $x_1, \ldots, x_n$ such that $x_1 \in P_m$. 
3.2. On finite approximability for equations in free groups

It is well known that a free group $F_n$ is finitely approximable. This means that for any non-identity element $g$ of the group $F_n$, there exists a finite factor-group, $F_n/N$, in which the image of $g$ is distinct from identity element. A. I. Maltsev [22] noted the importance of the properties of finite approximability with respect to various predicates: these properties imply decidability of the corresponding algorithmic problems.

Let $G$ be a group, $\rho$ be a predicate defined on the group $G$ and on its homomorphic images. Group $G$ is said to be finitely approximable with respect to $\rho$, if for any elements of the group $G$, on which the predicate $\rho$ is false, there exists a finite factor-group $G/N$ such that the predicate $\rho$ is false for the images $G/N$ of these elements.

Finite approximability (in particular, of free groups) was studied in several works with respect to various predicate, such as conjugacy or extractability of $n$-th power root etc. G. Baumslag [23] established finite approximability of free groups with respect to conjugacy or extractability of the primitive-power root, i.e., with respect to decidability of the equations of the type $x^{-1}hx = g$ and $x^p = g$, where $h$ and $g$ are the elements of a free group. In [24] the finite approximability of the free groups was established with respect to decidability of the equations of the type $[x,y] = g$ and $x^n = g$. Coulibois and Khelfi [25] gave an equation of the type $w(x_1, \ldots, x_4, a_1, a_2) = 1$ which had no solution in a free group $F_2$ with the free generators $a_1$ and $a_2$, while the equation $w(x_1, \ldots, x_4, \bar{a}_1, \bar{a}_2) = 1$ has a solution in any finite factor-group $F_2/N$, where $\bar{a}_1$ and $\bar{a}_2$ are the images of the free generators $a_1$ and $a_2$ in the factor-group $F_2/N$ under the natural homomorphism.

Here we report on strengthening of that result, i.e., we give an explicit equation possessing an analogous property. This equation has the form $w(x_1, \ldots, x_m) = g$, where $g$ is some fixed element of the group $F_2$, and the word $w(x_1, \ldots, x_m)$ is free of constants i.e. it depends on the unknowns only.

**Theorem 7.** For any $n \geq 2$ and any non-negative $m$, $p$ and $q$ the equation

$$((x^2u)^{2+p}(z^{-1}y^2vz)^{2+q}t^{2m+3})^4[u,v] = [a_1, a_2]$$

has no solution in the free group $F_n$, while the equation

$$((x^2u)^{2+p}(z^{-1}y^2vz)^{2+q}t^{2m+3})^4[u,v] = [\bar{a}_1, \bar{a}_2]$$

has a solution in any finite factor-group $F_n/N$, where $\bar{a}_1$ and $\bar{a}_2$ are the images of free generators $a_1$ and $a_2$ in the factor-group $F_n/N$ under the natural homomorphism.

The equation considered in the above theorem has the form $w(x_1, \ldots, x_6) = [a_1, a_2]$. Of interest is the possibility of decreasing the number of unknowns in its left-hand-side. This number is clearly not less than two, for at $m = 1$ the equation $w(x_1, \ldots, x_m) = g$ takes the form $x^n = g$, and, as it was shown in [25], this equation has a solution in the free group $F_2$ if and only if it has a solution in any finite factor-group $F_2/N$.

3.3. NP-hardness of the decidability problem for equations with a simple right-hand-side in a free group

**Theorem 8.** The problem of recognizing the decidability of the equations of type $w(x_1, \ldots, x_n) = [a, b]$ in a free group $F_2$, where $w(x_1, \ldots, x_n)$ is a word in the alphabet of unknowns and $[a, b]$ is the commutator of the free generators $a$ and $b$ of the group $F_2$, is NP-hard problem.

Note that the word $[a, b]$ in the right-hand-side has the length 4. For the words $g$ of the length less than 4, the situation is principally different, as it is shown by the following theorem.
Theorem 9. The problem of recognizing the decidability of the equations of type \( w(x_1, \ldots, x_n) = g \) in a free group \( F_2 \), where \( w(x_1, \ldots, x_n) \) is a word in the alphabet of unknowns \( \{x_1, \ldots, x_n\} \), and \( g \) is a word of the length less than 4 in the alphabet \( \{a, b\} \) of the free generators \( a \) and \( b \) of the group \( F_2 \), is polynomially-decidable problem.

3.4. On a A. I. Maltsev’s question from the “Kourovka Notebook”
Yu. L. Ershov included into the “Kourovka Notebook” [14, no. 1.19] the following A. I. Maltsev’s question on elementarily definable subgroups and subsets of a free group. The final part of this question is written as follows: “is the derived subgroup first order definable (relatively elementarily definable) in a free group?”
Here we show that the negative answer to this part of the question no. 1.19 can be obtained from the authors’s result [17] and from decidability of elementary theory of an arbitrary free group established by O. G. Kharlampovich and A. G. Myasnikov [26].

Theorem 10. For any \( m \geq 2 \) it is impossible to give a formula \( CF_m(x) \) (which contains one free variable, \( x \)) of the first-order language with equality of group signature (which contains the group operation, \( \cdot \), the inverse, \( ^{-1} \), and constant symbols for the generators, \( a_1, \ldots, a_m \)) such that for any element, \( g \), of the free group \( F_m \) the following equivalence holds:

\[ CF_m(g) \] is true on the group \( F_m \) if and only if the element \( g \) belongs to the derived (commutator) group, \( F_m^{(1)} \), of the group \( F_m \).

3.5. On automorphic reducibility for sets of elements in a free group
The problem of automorphic reducibility for sets of elements in a free group was formulated and solved by topological methods by J. H. C. Whitehead [27]. The solution with the combinatory group theory methods was proposed by E. S. Rapaport [28] and (in a simpler form) by P. J. Higgins and R. C. Lyndon [29].
Recall here the formulation of the problem of automorphic reducibility:

Given two arbitrary sets, \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_n)\), of elements in a free group, how to recognize whether exists an automorphism, \( \varphi \), of this group such that \( \prod_{i=1}^n \varphi(u_i) = v_i \)?

If we change the meaning of \( \varphi \) from automorphism to endomorphism in the above the formulation of the problem of automorphic reducibility, we obtain the problem of endomorphic reducibility for sets of elements in the group.
We show that the problem of automorphic reducibility for sets of elements in a free group \( F_2 \) of rank 2 can be reduced the the problem of decidability of an explicit equation with five unknowns in this group. Then the results of G. S. Makanin [9] can be applied for the solution of this problem.

Theorem 11. Given two arbitrary sets, \((u_1, \ldots, u_n)\) and \((v_1, \ldots, v_n)\), of elements in a free group \( F_2 \) with the free generators \( a \) and \( b \), it is possible to give an explicit equation of the type \( W(x, y, u, v, z) = [a, b] \) which is solvable in the group \( F_2 \) if and only if there exists an automorphism \( \varphi \) of the group \( F_2 \) such that \( \prod_{i=1}^n \varphi(u_i) = v_i \).

Let us prove beforehand an auxiliary lemma.

Lemma 1. An equation \( w(x_1, \ldots, x_n, a, b) = 1 \) has a solution in a free group \( F_2 \) if and only if the following equation is solvable in this group:

\[ w^4(x_1, \ldots, x_n, u, v)[u, v] = [a, b]. \]
Proof. If the equation \( w(x_1, \ldots, x_n, a, b) = 1 \) has the solution \( g_1, \ldots, g_n \) in a free group \( F_2 \), then \( g_1, \ldots, g_n, a, b \) is the solution of the equation

\[
w^4(x_1, \ldots, x_n, u, v) [u, v] = [a, b].
\]

Conversely, let \( g_1, \ldots, g_n, \alpha, \beta \) be a solution of the equation

\[
w^4(x_1, \ldots, x_n, u, v) [u, v] = [a, b].
\]

A. A. Vdovina [30] proved, in particular, that the equality \( [u, v] [s, t] = w^4 \) in a free group \( F_2 \) implies the equality \( w = 1 \). Therefore the equality

\[
w^4(g_1, \ldots, g_n, \alpha, \beta) [\alpha, \beta] = [a, b]
\]

implies the equalities \( w(g_1, \ldots, g_n, \alpha, \beta) = 1 \) and \( [\alpha, \beta] = [a, b] \).

Then, by A. I. Maltsev’s theorem [18], \( \alpha \) and \( \beta \) are the free generators of the free group \( F_2 \), therefore there exists an automorphism, \( \varphi \), of the free group \( F_2 \) such that \( \varphi(\alpha) = a \) and \( \varphi(\beta) = b \).

Applying the automorphism \( \varphi \) to the equality \( w(g_1, \ldots, g_n, \alpha, \beta) = 1 \), we obtain

\[
w(\varphi(g_1), \ldots, \varphi(g_n), a, b) = 1.
\]

It means that the equation \( w(x_1, \ldots, x_n, a, b) = 1 \) has a solution. \( \square \)

Proof of the theorem 11. A. I. Maltsev [18] proved that

\( U \) and \( V \) are free generators of the free group \( F_2 \) with the free generators \( a \) and \( b \) if and only if the following formula is true on the group \( F_2 \):

\[
(\exists z)[z[U, V]z^{-1} = [a, b] \lor z[U, V]z^{-1} = [a, b]^{-1}.
\]

Therefore, for two sets, \( (u_1(a, b), \ldots, u_n(a, b)) \) and \( (v_1(a, b), \ldots, v_n(a, b)) \), of the free group \( F_2 \) elements, there exists an automorphism \( \varphi \) such that

\[
\& \varphi(u_i(a, b)) = v_i(a, b)
\]

if and only if the following formula is true on the group \( F_2 \):

\[
(\exists x, y, z) \& \ u_i(x, y) = v_i(a, b) \& \ \lor \ \ \in \{-1, 1\} \ z[x, y]z^{-1} = [a, b]^z.
\] (4)

G. A. Gurevich [9] gave a group word, \( D(x, y, a, b) \), such that the equivalence \( D(g, h, a, b) = 1 \) is true for two arbitrary elements, \( g \) and \( h \), of a free group \( F_2 \) if and only if \( g = 1 \lor h = 1 \).

A. I. Maltsev and G. A. Gurevich [9] gave several examples of group words, \( C(x, y, a, b) \), such that the equivalence \( C(g, h, a, b) = 1 \) is true for two arbitrary elements, \( g \) and \( h \), of a free group \( F_2 \) if and only if \( g = 1 \& h = 1 \).

Using the above words, \( D(x, y, a, b) \) and \( C(x, y, a, b) \), and removing the disjunction, \( \lor \), and conjunction, \( \& \), signs from the Eq. (4) we obtain the formula of the type

\[
(\exists x, y, z)U(x, y, z, a, b) = 1
\]

such that for given sets, \( (u_1(a, b), \ldots, u_n(a, b)) \) and \( (v_1(a, b), \ldots, v_n(a, b)) \), of the free group \( F_2 \) elements, there exists an automorphism \( \varphi \) such that

\[
\& \varphi(u_i(a, b)) = v_i(a, b)
\]
if and only if the following formula is true on the group $F_2$:

$$(\exists x, y, z) U(x, y, z, a, b) = 1.$$ 

Using the lemma 1, we obtain that for given sets, $(u_1(a, b), \ldots , u_n(a, b))$ and $(v_1(a, b), \ldots , v_n(a, b))$ of the free group $F_2$ elements, there exists an automorphism $\varphi$ such that

$$\forall i \leq n \varphi(u_i(a, b)) = v_i(a, b)$$

if and only if the following equation is solvable:

$$U^4(x, y, z, u, v)[u, v] = [a, b].$$

Let $F_5$ denote a free group of rank 5 whose free generators, for convenience, are denoted as $a, b, c, d$ and $e$.

The equation of the type

$$W(x, y, z, u, v) = g(a, b)$$

has a solution in the group $F_2$ if and only if it is solvable in the group $F_5$. Moreover, the equation of the above type has a solution in the group $F_5$ if and only if there exists an endomorphism, $\psi$, of this group, such that

$$\psi(W(a, b, c, d, e)) = g(a, b).$$

**Corollary 1.** The problem of automorphic reducibility for sets of elements in a free group $F_2$ of rank 2 can be brought to the problem of endomorphic reducibility for elements in a free group $F_5$ of rank 5.

### 3.6. On the equations in words and lengths

Let $\Pi_m$ denote a free semigroup of rank $m$ with an empty word as neutral element and free generators $a_1, \ldots , a_m$. Let $X = \{x_1, \ldots , x_n, \ldots \}$ denote an alphabet of unknowns.

G. S. Makanin [31] built an algorithm to recognize decidability of an arbitrary system of equations in words

$$\forall i \leq k w_i = u_i,$$  

in the semigroup $\Pi_m$. In the Eq. (5), $w_i$ and $u_i$ ($i = 1, \ldots , k$) are words in the alphabet $\{a_1, \ldots , a_m\} \cup X$.

The question of algorithmic decidability of the problem of consistency of equations in words and lengths, i.e. of the systems of the type

$$\forall i \leq k w_i = u_i \& \forall \{i, j\} \in A |x_i| = |x_j|$$  

has been remaining as an open problem for almost a half of century.

The systems of the type (6) with additional conditions were studied e.g. in [17, 32, 33].

V. Diekert proposed studying systems of inequalities of the type

$$\forall i \leq k w_i(x_1, \ldots , x_n, a_1, \ldots , a_m) \leq u_i(x_1, \ldots , x_n, a_1, \ldots , a_m)$$  

(7)
in free semigroups, where \( w \leq u \) means that for the words, \( w \) and \( u \), in the alphabet of the free generators the sequence of letters in \( w \) is a subsequence of letters in \( u \), i.e. there exist a number \( n \leq |w| \) and words, \( w_1, \ldots, w_n, u_1, \ldots, u_n, u_{n+1} \), such that

\[
w = w_1 \ldots w_n, \quad u = u_1 w_1 u_2 \ldots u_n w_n u_{n+1}.
\]

The systems of inequalities (7) can be considered as a generalization of the system of equations (5), because

\( w = u \) if and only if \( w \leq u \) & \( u \leq w \).

The relationship \( w \leq u \) is a partial order relationship in the semigroup \( \Pi_m \), i.e. it is transitive and antisymmetric. This is another reason to study the systems of inequalities of the type (7).

The algorithmic decidability of the problem of consistency of systems of inequalities (7) is an open question up to now. However, adding the predicate of equality of the lengths to the relation \( w \leq u \) makes this problem algorithmically undecidable.

**Theorem 12.** There exist no algorithm to recognize whether the system of inequalities of the type

\[
\land_{i=1}^k w_i \leq u_i & \land_{\{i,j\} \in A} |x_i| = |x_j|
\]

has a solution.

Note that \( \exists \)-theory of the equality relationship, \( = \), is algorithmically decidable in the semigroup \( \Pi_m \). This follows from the fundamental G. S. Makanin’s theorem [31] since the negation of equality can be removed from all the formulas with the help of the positive \( \exists \)-formula.

At the same time, \( \exists \)-theory of the partial order relationship, \( \leq \), is algorithmically undecidable in the semigroup \( \Pi_m \). This can be proven in a same way as the theorem 12.

4. Conclusion

Here we list the results provided in this paper.

(i) We prove the algorithmic undecidability of the problem of solubility of systems of equations with constraints of the type

\[
w(x_1, \ldots, x_n) = [a, b] \land_{i=1}^l x_i \in F_2^{(1)}
\]

and

\[
w(x_1, \ldots, x_n) = [a, b] \land x_1 \in F_2^{(2)},
\]

in a free group \( F_2 \) of rank 2 with free generators, \( a \) and \( b \), where \( w(x_1, \ldots, x_n) \) is a word in the alphabet of unknowns, \( \{x_1, \ldots, x_n\} \), \( [a, b] \) is the commutator of the free generators, \( a \) and \( b \), \( F_2^{(1)} \) is the derived (commutator) subgroup of \( F_2 \) group, and \( F_2^{(2)} \) is its second derived subgroup.

(ii) We establish existence of a polynomial algorithm to recognize whether an arbitrary explicit (resolved with respect to the unknowns) equation of the type

\[
w(x_1, \ldots, x_n) = g(a, b),
\]

where \( w(x_1, \ldots, x_n) \) is a group word in the alphabet of unknowns, \( g(a, b) \) is an element of length less than 4 in a free group \( F_2 \), has a solution satisfying the constraint

\[
x_1 \in F_2^{(s)}, \ldots, x_l \in F_2^{(s)},
\]
where \( t \) is an arbitrary fixed number between 1 and \( n \), and \( F_2^{(s)} \) is \( s \)-th derived subgroup of \( F_2 \).

The algorithmic decidability of analogous problems for equations with one unknown is also established.

(iii) We prove finite inapproximability for explicit equations with 6 unknowns of the type

\[
((x^2u)^2+p(z^{-1}y^2vz)^2+qt^{2m+3})^4[u,v] = [a_1,a_2], \quad n \geq 2, \quad m,p,q \geq 0
\]

in free groups.

(iv) We establish \( \text{NP} \)-hardness of the problem of solubility of equations of the type

\[ w(x_1, \ldots, x_n) = [a,b] \]

in a free group \( F_2 \).

(v) We prove polynomial decidability of the problem of solubility of equations of the type

\[ w(x_1, \ldots, x_n) = g, \]

where \( g \) is a group word of length less than 4 in the alphabet, \{a,b\}, of free generators of the group \( F_2 \).

(vi) We show that the derived (commutator) subgroup of a free non-cyclic group is not a definable subgroup that solves a A. I. Maltsev’s problem from the “Kourovka Notebook”

(vii) We prove that the problem of automorphic reducibility for sets of elements in a free group \( F_2 \) of rank 2 with free generators, \( a \) and \( b \), can be brought to the problem of solubility of a proper equation \( W(x,y,u,v,z) = [a,b] \) in \( F_2 \), where \( W(x,y,u,v,z) \) is a word of the unknowns \( x,y,u,v,z \), which is to be found according to the initial sets of elements. We also prove that the problem of automorphic reducibility for sets of elements in a free group \( F_2 \) of rank 2 can be brought to the problem of endomorphic reducibility for elements in a free group \( F_3 \) of rank 5.

(viii) We prove the algorithmic undecidability of a compatibility problem for some systems of equations and inequalities in words and word lengths on free non-cyclic semigroup \( \Pi_m \).

The above mathematical results fall into a general problem of “establishing a boundary between the algorithmically decidable and the algorithmically undecidable problems”. In our opinion, these results make a contribution into understanding where does “the boundary lie” between two mathematical domains: “Decidable (solvable) mathematical problems” and “Undecidable (unsolvable) mathematical problems”. And, more widely, where does “the boundary lie” between two domains: “Possible” and “Impossible”. In the present paper we investigate the question: which conditions (constraints) can be added to the description of an algorithmically decidable problem so that it becomes algorithmically undecidable? We believe these questions also help (to some extent) understanding the potential abilities of computers.

References

[1] Davis M, Matijasevič Y and Robinson J 1976 Proceedings of symposia in pure mathematics (Mathematical developments arising from Hilbert problems vol 28) ed Browder F E (Providence, R. I.: American Mathematical Society) pp 323–78 URL http://www.ams.org/books/pspum/028.2/

[2] Tarski A, Mostowski A and Robinson R M 1953 Undecidable Theories Studies in logic and the foundations of mathematics (Amsterdam: North-Holland)

[3] Lyndon R C 1960 Trans. Amer. Math. Soc. 96 445–457

[4] Lorenz A A 1968 Sov. Math. Doklady 9

[5] Appel K I 1968 Proc. Amer. Math. Soc. 19 912–918

[6] Hmelevskii J I 1971 Math. USSR Izv. 5 1245–1276

[7] Hmelevskii J I 1972 Math. USSR Izv. 6 109–180
[8] Makanin G S 1983 *Math. USSR Izv.* 21 483–546
[9] Makanin G S 1985 *Math. USSR Izv.* 25 75–88
[10] Merzlyakov Y I 1966 *Algebra i logika* 5 25–42 in Russian
[11] Razborov A A 1984 *Math. USSR Izv.* 48 115–162
[12] Gassner B J 1961 *Abh. Math. Semin. Univ. Hambg.* 25 10–22
[13] Birman J S 1974 *Braids, Links, and Mapping Class Groups* Annals of Mathematics Studies (Princeton University Press)
[14] Mazurov V D and Khukhro E I 2014 Unsolved Problems in Group Theory. The Kourovka Notebook. No. 18 (English version) ArXiv e-prints arXiv:1401.0300 [math.GR] (Preprint 1401.0300) URL http://arxiv.org/abs/1401.0300
[15] Malkhasyan A S 2014 *Math. Notes Acad. Sci. USSR* 95 520–529
[16] Diekert V 1998 Makanin’s algorithm for solving word equations with regular constraints Tech. Rep. 1998/02 Fakultat für Informatik. Universität Stuttgart
[17] Durnev V G 1974 *Math. Notes Acad. Sci. USSR* 16 1024–1028
[18] Maltsev A I 1962 *Algebra i logika* 1 45–50 in Russian
[19] Schupp P E 1969 *Proc. Amer. Math. Soc.* 23 421–423
[20] Edmunds C C 1975 *Comm. Algebra* 3 1–20
[21] Durnev V G 1996 *Math. Notes* 59 601–610
[22] Maltsev A I 1958 *Uchen. Zap. Ivanovsk. Ped. Inst.* 18 49–60 also in “Selected Papers”, Vol. 1, Algebra, 1976, 450462, in Russian
[23] Baumslag G 1965 *J. Algebra* 2 271–282
[24] Khelif A 2004 *J. Algebra* 281 407–412
[25] Coulbois T and Khelif A 1999 *Proc. Amer. Math. Soc.* 127 963–965
[26] Kharlampovich O and Myasnikov A 2006 *J. Algebra* 302 451–552
[27] Whitehead J H C 1936 *Ann. Math.* 37 782–800
[28] Rapaport E S 1958 *Acta Math.* 99 138–163
[29] Higgins P J and Lyndon R C 1974 *J. London Math. Soc.* s2-8 254–258
[30] Kharlampovich O, Mohajeri A, Taam A and Vdovina A 2017 *Trans. Amer. Math. Soc.* 369 6207–6238
[31] Makanin G S 1977 *Math. USSR-Sb.* 32 129–198
[32] Kossovski N K 1972 *Zap. nauch. sem. LOMI* 32 21–28 in Russian
[33] Kossovski N K 1974 *Zap. nauch. sem. LOMI* 33 24–29 in Russian