Siberian Mathematical Journal, Vol. 36, *No.* 5, 1995

UNDECIDABILITY OF THE POSITIVE $\forall\exists^3$-THEORY OF A FREE SEMIGROUP[†)]

V. G. Durnev

UDC 512.543.12;512.54.03

Let Π_n denote a free semigroup of rank n with free generators $a_1, \dots, a_n$.

As observed in the survey [1], "great progress is achieved in the study of decidability of the elementary theory of a free semigroup. As far back as in 1946 W. V. Quine [2] proved undecidability of this theory. In 1973 V. G. Durnev [3] essentially strengthened the result by proving undecidability for the fragment of the elementary theory which consists of the formulas without negation and with a prefix of type $\exists x \forall y \exists z_1 \exists z_2 \exists z_3$." In the article [4] S. S. Marchenkov proved undecidability of the positive $\forall\exists^4$-theory of a free semigroup, essentially improving the result of [3] as regards the number of quantifier blocks in the formulas under consideration; however, the total number of quantifiers in use is the same in [3] and [4].

In the first half of the present article, the results of the articles [3] and [4] are improved as follows: *the algorithmic undecidability is proven for the positive $\forall\exists^3$-theory of Π_n for $n \geq 2$.*

The proof of this result is carried out along the lines of the article [4] with necessary correctives.

Theorem 1. *For $n \geq 2$ the positive $\forall\exists^3$-theory of Π_n is algorithmically undecidable.*

PROOF. As in the article [4], the proof of the theorem is based on the existence of operator algorithms with nonrecursive domain [5]; however, in contradistinction to [4] we make use of operator algorithms with "simpler" commands.

Let $\mathfrak{A}$ be an *operator algorithm with nonrecursive domain* whose program consists of only commands of the following type (existence of such algorithms is proven, for instance, in [5]):

[×2] "*multiply the given number by* 2 *and proceed to execute the next command*";

[×3] "*multiply the given number by* 3 *and proceed to execute the next command*";

[: 6; i] "*if the given number is divisible by* 6, *then divide it by* 6 *and proceed to execute the command with number i; otherwise, retain the given number unchanged and proceed to execute the next command*";

[stop].

As in [4], we assume that the operator algorithm $\mathfrak{A}$ contains m commands that are enumerated by the numbers from 1 to m; moreover, the initial command has number 1 and the sole command [stop] has number m.

Recall that, given an input x, the work of the operator algorithm $\mathfrak{A}$ begins with executing the command with number 1, producing the number x_1 together with the number i_1 of the next executable command; given x_1, the command with number i_1 produces the number x_2 and the number i_2 of the next command; and so forth. The calculation with the input x terminates when m, the number of the command [stop], is generated at some step of the execution of the algorithm.

Obviously, *the operator algorithm $\mathfrak{A}$ is applicable to a number x if and only if there is a sequence*

$$(x_0, i_0), (x_1, i_1), \dots, (x_t, i_t) \tag{1}$$

(with denotations of [4]) *such that $x_0 = x$, $i_0 = 1$, $i_t = m$, and for every s $(1 \leq s \leq t)$ the application of the command with number i_{s-1} to x_{s-1} produces the number x_s and the number i_s of the next command.*

†) This research was partially supported by the International Science Foundation (ISF) (Grant MUV 000).

Yaroslavl′. Translated from *Sibirskiĭ Matematicheskiĭ Zhurnal*, Vol. 36, No. 5, pp. 1067–1080, September–October, 1995. Original article submitted November 22, 1994.

For convenience, as in [4], we prefer to use 0 and 1 instead of a_1 and a_2.

In the article [4], it is the element

$$0^{x_0+1}1^{i_0}0^{x_1+1}1^{i_1}0^{x_2+1}1^{i_2}\dots 0^{x_t+1}1^{m}$$

of Π_n that is associated with sequence (1). Here we associate the following element of the semigroup Π_n with sequence (1):

$$0^{x_0+1}1^{i_0+\varepsilon_0 m}0^{x_1+1}1^{i_1+\varepsilon_1 m}0^{x_2+1}1^{i_2+\varepsilon_2 m}\dots 0^{x_t+1}1^{i_t+\varepsilon_t m}, \tag{2}$$

with $\varepsilon_i \rightleftharpoons 0$ if x_i is divisible by 6 and $\varepsilon_i \rightleftharpoons 1$ otherwise $(i = 0, \dots, t)$.

Now, proceeding as in [4], we construct a positive quantifier-free formula $\Phi(x, w, s, u, v)$ such that the following equivalence holds for every natural k:

the formula

$$(\forall w)(\exists s, u, v)\,\Phi(0^{k+1}, w, s, u, v)$$

is true on Π_n if and only if the operator algorithm $\mathfrak{A}$ is not applicable to k.

To this end, it suffices to make the formula $(\exists s, u, v)\,\Phi(0^{k+1}, w, s, u, v)$ to assert in essence that w is not of the kind of (2).

We take as Φ the disjunction of the following formulas (1)–(9):

(1) The word w is empty: $ww = w$.

(2) In the word w there is an occurrence of some letter a_i with $3 \le i \le n$: $\bigvee_{i=3}^{n} w = ua_iv$.

(3) The word w begins with neither $x10$ nor $x1^{1+m}0$:

$$\bigvee_{\substack{i,j=1\\ i\neq j}}^{n} (x = ua_is \,\&\, w = ua_jv) \vee x = wu \vee w = x0u$$
$$\vee (w = xu \,\&\, 1u = u1) \vee \bigvee_{2\le i\le m} w = x1^i0u \vee w = x1^{m+2}u.$$

(4) The word w terminates with neither 01^m nor 01^{m+m}:

$$w1 = 1w \vee \Bigl(\bigvee_{0\le i<m} w = u01^i\Bigr) \vee \Bigl(\bigvee_{1\le i<m} w = u01^{i+m}\Bigr) \vee w = u1^{2m+1}.$$

(5) The word w includes 1^{2m+1} as a subword: $w = u1^{2m+1}v$.

(6) The word w contains 1^m or 1^{2m} not at the end: $w = u01^m0v \vee w = u01^{2m}0v$.

Observe that if a word w satisfies none of the conditions (1)–(6) with the replacement of x by 0^{x+1}, then w has the form

$$0^{x+1}1^{j_0}0^{x_1+1}1^{j_1}0^{x_2+1}1^{j_2}\dots 0^{x_t+1}1^{j_t}$$

for some nonnegative integers $x, x_1, \dots, x_t$ and some naturals $j_1, j_2, \dots, j_t$; moreover, $1 \le j_k \le 2m$ $(0 \le k \le t)$, j_t is m or $2m$, j_k for $k < t$ differs both from m and $2m$, and j_0 is either 1 or $1 + m$.

(7) Recall that if x_k is divisible by 6 then $1 \le j_k \le m$, while $m + 1 \le j_k \le 2m$ otherwise. This condition is violated by means of the following formula:

$$s0 = 0s \,\&\Bigl(w = 0s^6 1^{1+m}u \vee \bigvee_{1\le\varepsilon\le5}\ \bigvee_{0\le i\le m} w = 00^{\varepsilon}s^6 1^i 0u \vee w = u10s^6 1^{m+m}$$
$$\vee \bigvee_{1\le\varepsilon\le5} w = u100^{\varepsilon}s^6 1^m \vee \bigvee_{1\le i\le m} w = u10s^6 1^{i+m}0v$$
$$\vee \bigvee_{1\le\varepsilon\le5}\ \bigvee_{1\le i\le m} w = u100^{\varepsilon}s^6 1^i 0v\Bigr).$$

(8) With each i that is the number of a command of type $[\times d]$ with $d = 2, 3$, we associate some formula which essentially asserts that *somewhere in the word* w *a "failure" happened due to improper execution of a command; i.e., either the result of the command is computed wrongly or a wrong number is indicated as the number of the next command.*

As such a formula, we take the formula of the form $s0 = 0s \& (\Psi_1 \vee \Psi_2)$, where *the formula* Ψ_1 *essentially asserts that the result of a command of type* $[\times d]$ *is computed wrongly, whereas the formula* Ψ_2 *asserts that the result of the application of the command* $[\times d]$ *is computed correctly but the number of the next command is indicated wrongly* (on condition that s is the degree of 0).

We let Ψ_1 be the following formula:

$$\Big(\bigvee_{\varepsilon=0,1} w = 0s1^{i+\varepsilon m}0s^d0u\Big) \vee \Big(\bigvee_{\varepsilon=0,1}\bigvee_{1\le l\le d-1} w = v01^{i+\varepsilon m}0s^d0^l1u\Big)$$
$$\vee\Big(\bigvee_{\varepsilon=0,1} w = v00s1^{i+\varepsilon m}0s^d1u\Big) \vee \Big(\bigvee_{\varepsilon=0,1} w = v1s01^{i+\varepsilon m}0s^d0u\Big)$$
$$\vee\Big(\bigvee_{\varepsilon=0,1}\bigvee_{1\le l\le d-1} w = v01^{i+\varepsilon m}0s^d0^l1u\Big) \vee \Big(\bigvee_{\varepsilon=0,1} w = v00s1^{i+\varepsilon m}0s^d1u\Big).$$

As Ψ_2 we take the formula

$$\bigvee_{\varepsilon=0,1}\bigvee_{l=0,1}\bigvee_{j\ne i+1} (w = 0s1^{i+\varepsilon m}0s^d1^{j+lm}0u \vee w = v10s1^{i+\varepsilon m}0s^d1^{j+lm}0u$$
$$\vee w = v10s1^{i+\varepsilon m}0s^d1^{j+lm} \vee w = 0s1^{i+\varepsilon m}0s^d1^{j+lm}).$$

(9) With each i that is the number of a command of type $[: 6; j]$, we associate some formula which essentially asserts that *somewhere in the word* w *a "failure" occurs due to improper execution of the command; i.e., either the result of the command is computed wrongly or a wrong number is indicated as the number of the next command*:

$$s0 = 0s\&\Big(w = 0s^61^i0s0u \vee w = v00s^61^i0s1u \vee w = v10s^61^i0s0u$$
$$\vee w = v00s^61^i0s1u \vee \bigvee_{\varepsilon=0,1}\bigvee_{t\ne j}((w = 0s^61^i0s1^{t+\varepsilon m}0u$$
$$\vee w = 0s^61^i0s1^{t+\varepsilon m}) \vee (w = v10s^61^i0s1^{t+\varepsilon m}0u \vee w = v10^61^i0s1^{t+\varepsilon m}))$$
$$\vee(w = s01^{i+m}s00u \vee w = v00s1^{i+m}0s1u) \vee (w = v1s01^{i+m}s00u$$
$$\vee w = v00s1^{i+m}0s1u) \vee \bigvee_{\varepsilon=0,1}\bigvee_{t\ne i+1} (w = 0s1^{i+m}0s1^{t+\varepsilon m}0u$$
$$\vee w = 0s1^{i+m}0s1^{t+\varepsilon m} \vee w = v10s1^{i+m}0s1^{t+\varepsilon m}0u \vee w = v10s1^{i+m}0s1^{t+\varepsilon m})\Big).$$

Let us make some comments on the last formula: the first four rows relate to the case in which the number to which the ith command $[: 6; j]$ applies is divisible by 6; moreover, the first two rows assert that the result is computed wrongly; i.e., it is not the result of division of the preceding number by 6 and the next two rows assert that the result is computed correctly but the number of the next command is indicated wrongly. Analogously, the last four rows relate to the case in which the number to which the ith command $[: 6; j]$ applies is not divisible by 6; moreover, the first two rows assert that the result is computed wrongly (i.e., the number to which the command applies is changed, although it must be preserved) and the last two rows assert that the result is computed correctly but the number of the next command is indicated wrongly. □

We apply Theorem 1 to studying *Diophantine sets* in free semigroups.

For the sake of convenience, we denote the free generators of Π_2 by a and b.

DEFINITION. A subset S of the set Π_2^p is called *Diophantine* if there are words u and v in the alphabet

$$\{a, b, x_1, \dots, x_p, y_1, y_2, \dots\}$$

such that the equivalence

$$\langle g_1, \dots, g_p \rangle \in S \Leftrightarrow \Pi_2 \models (\exists y_1, \dots, y_n)\, u(g_1, \dots, g_p, y_1, \dots, y_n, a, b) = v(g_1, \dots, g_p, y_1, \dots, y_n, a, b)$$

holds for all elements $g_1, \dots, g_p$ in Π_2. In this case, each such pair of words $\langle u, v\rangle$ is referred to as the *record of the Diophantine set* S.

The intersection and the union of two Diophantine sets are themselves Diophantine sets: it is well known that in Π_2 the conjunction $x_1 = y_1 \& x_2 = y_2$ of equalities is equivalent to the sole equality $x_1ax_2x_1bx_2 = y_1ay_2y_1by_2$; on the other hand, as proven in [6, 7], there are words u and v in the alphabet $\{a, b, x_1, x_2, y_1, y_2, z_1, z_2, z_3, z_4\}$ such that

$$\Pi_2 \models (\forall x_1, x_2, y_1, y_2)((x_1 = x_2 \vee y_1 = y_2) \Leftrightarrow (\exists \bar{z})\, u(\bar{x}, \bar{y}, \bar{z}, a, b) = v(\bar{x}, \bar{y}, \bar{z}, a, b)),$$

where $\bar{x}$ denotes x_1, x_2; $\bar{y}$ denotes y_1, y_2; $\bar{z}$ denotes z_1, z_2, z_3, z_4; and

$$u = u(x_1, x_2, y_1, y_2, z_1, z_2, z_3, z_4, a, b), \quad v = v(x_1, x_2, y_1, y_2, z_1, z_2, z_3, z_4, a, b).$$

We shall show below that it is possible to restrict ourselves just to the new variables z_1 and z_2.

Every singleton set and its complement are Diophantine, which ensues from the following fact: in the articles [6–9], for every $n \geq 2$ the formula

$$P_n(x, y) = (\exists u, v_1, v_2)\left(\bigvee_{\substack{i,j=1\\ i\neq j}}^{n} (x = ua_iv_1 \& y = ua_jv_2) \vee \left(\bigvee_{i=1}^{n} (x = ya_iv_1 \vee y = xa_iv_1)\right)\right)$$

was constructed and there was proven that the equivalence $g \neq h \Leftrightarrow \Pi_n \models P_n(g, h)$ holds for arbitrary two elements g and h of Π_n. Therefore, every finite set and its complement are Diophantine.

N. K. Kosovskiĭ [6] constructed the first examples of recursive sets in Π_2 which are not Diophantine; such is for instance the set S consisting of all symmetric words, i.e. the words of the form

$$a^{\alpha_1}b^{\beta_1}\dots a^{\alpha_t}b^{\beta_t}b^{\beta_t}a^{\alpha_t}\dots b^{\beta_1}a^{\alpha_1}.$$

Observe that, in view of G. S. Makanin's theorem [10], every Diophantine set and its complement therewith are recursive. For this reason, it is of interest, in our opinion, to construct an example of a Diophantine set whose complement is not Diophantine.

To construct such an example from the operator algorithm $\mathfrak{A}$ with nonrecursive domain, this domain denoted by $R(\mathfrak{A})$, we as above construct some formula $\Phi(x, w, s, u, v)$ of the form

$$\bigvee_{i=1}^{k} \mathop{\&}_{j=1}^{l} W_{ij}(x, w, s, u, v, a, b) = U_{ij}(x, w, s, u, v, a, b)$$

for which the equivalence

$$r \notin R(\mathfrak{A}) \Leftrightarrow \Pi_2 \models (\forall w)(\exists s, u, v)\Phi(aa^r, w, s, u, v)$$

holds for every natural number r.

Eliminating the signs & and $\vee$ from the formula Φ and renaming the variables, we obtain a formula $F(x, z, x_1, \dots, x_n)$ of the form

$$u(x, z, x_1, \dots, x_n, a, b) = v(x, z, x_1, \dots, x_n, a, b)$$

for which the following equivalence holds:

$$r \notin R(\mathfrak{A}) \Leftrightarrow \Pi_2 \models (\forall z)(\exists \bar{x})\, u(aa^r, z, \bar{x}, a, b) = v(aa^r, z, \bar{x}, a, b)$$

or

$$r \in R(\mathfrak{A}) \Leftrightarrow \Pi_2 \models (\exists z)\neg(\exists \bar{x})\, u(aa^r, z, \bar{x}, a, b) = v(aa^r, z, \bar{x}, a, b).$$

We now demonstrate that the complement of the Diophantine set

$$D \rightleftharpoons \{\langle g, h\rangle \mid (\exists \bar{x})\, u(g, h, \bar{x}, a, b) = v(g, h, \bar{x}, a, b)\}$$

is not Diophantine. Indeed, in the opposite case there would exist words u_1 and v_1 in the alphabet $\{x, z, y_1, \dots, y_n, a, b\}$ such that

$$\neg(\exists \bar{x})\, u(x, z, \bar{x}, a, b) = v(x, z, \bar{x}, a, b) \Leftrightarrow (\exists \bar{y})\, u_1(x, z, \bar{y}, a, b) = v_1(x, z, \bar{y}, a, b).$$

Then, however, the equivalence

$$r \in R(\mathfrak{A}) \Leftrightarrow \Pi_2 \models (\exists z)(\exists \bar{y})\, u_1(aa^r, z, \bar{y}, a, b) = v_1(aa^r, z, \bar{y}, a, b)$$

would hold and, by G. S. Makanin's theorem [10], the set $R(\mathfrak{A})$ would be recursive, contradicting the choice of the operator algorithm $\mathfrak{A}$.

We will discuss some algorithmic questions concerning the determination of the number of elements of a Diophantine set or its complement.

The following theorem is a simple corollary to G. S. Makanin's result [11]:

Theorem 2. *There is an algorithm allowing us, given an arbitrary pair $\langle u, v\rangle$ of words defining a Diophantine set S and an arbitrary natural number k, to determine whether S contains no less than k elements, or no more than k elements, or exactly k elements.*

PROOF. Let a Diophantine set S has record

$$\langle g_1, \dots, g_p\rangle \in S \Leftrightarrow \Pi_2 \models (\exists y_1, \dots, y_n)\, u(g_1, \dots, g_p, y_1, \dots, y_n, a, b) = v(g_1, \dots, g_p, y_1, \dots, y_n, a, b).$$

Denote the claim "*S contains no less than (no more than, exactly) k elements*" by $|S| \geq k$ ($|S| \leq k, |S| = k$) and denote by Φ_k the formula

$$(\exists x_1^{(1)}, \dots, x_p^{(1)}, y_1^{(1)}, \dots, y_n^{(1)}, \dots, x_1^{(k)}, \dots, x_p^{(k)}, y_1^{(k)}, \dots, y_n^{(k)})\Psi,$$

where Ψ has the form

$$\mathop{\&}_{i=1}^{k} u(x_1^{(i)}, \dots, x_p^{(i)}, y_1^{(i)}, \dots, y_n^{(i)}, a, b)$$
$$= v(x_1^{(i)}, \dots, x_p^{(i)}, y_1^{(i)}, \dots, y_n^{(i)}, a, b) \mathbin{\&} \mathop{\&}_{1\leq i<j\leq k} \left(\bigvee_{t=1}^{p} x_t^{(i)} \neq x_t^{(i)}\right).$$

Then

$$|S| \geq k \Leftrightarrow \Pi_2 \models \Phi_k,$$

and the question of validity of the $\exists$-formula Φ_k on Π_2 is algorithmically decidable by G. S. Makanin's theorem [10]. To complete the proof, it suffices to observe that

$$|S| \leq k \Leftrightarrow \neg(|S| \geq k+1), \quad |S| = k \Leftrightarrow |S| \geq k \& |S| \leq k. \ \square$$

The following question remains open: *Is there an algorithm allowing us, given an arbitrary record of a Diophantine set S, i.e., given the corresponding pair $\langle u, v\rangle$ of words, to determine whether S is a finite set?*

The conjectural answer is positive: in our opinion, it could be reached by proving that the equation

$$u(x_1, \dots, x_q, a, b) = v(x_1, \dots, x_q, a, b)$$

having a solution $g_1, \dots, g_p$ in Π_2 such that g_1 is a "very long" word in comparison with the length of the words u and v admits infinitely many solutions with different first components.

Observe that if the set S is finite then the answer can be obtained by resolving the question of the form "$\Pi_2 \models \Phi_k$?"; difficulties arise in the case of an infinite S.

The following theorem sheds some light on the source of the difficulties:

Theorem 3. *For every fixed k, there is no algorithm allowing us, given an arbitrary pair $\langle u, v\rangle$ of words defining a Diophantine set S, to determine whether the complement of S contains k elements (no less than k elements for $k > 0$, or no more than k elements).*

PROOF. As described above, given the operator algorithm $\mathfrak{A}$ with nonrecursive domain, we construct some formula $\Phi_{\mathfrak{A}}(x)$ of the form

$$(\forall y)(\exists z_1, \dots, z_n)\, w(x, y, \bar{z}, a, b) = u(x, y, \bar{z}, a, b)$$

such that the equivalence

$$r \notin R(\mathfrak{A}) \Leftrightarrow \Pi_2 \models \Phi_{\mathfrak{A}}(aa^r)$$

holds for every natural r.

Denote by $S_{x,w,u}$ the following Diophantine set:

$$\{y \mid \Pi_2 \models (\exists \bar{z})\, w(aa^x, y, \bar{z}, a, b) = u(aa^x, y, \bar{z}, a, b).$$

If $r \notin R(\mathfrak{A})$ then $S_{r,w,u} = \Pi_2$; however, if $r \in R(\mathfrak{A})$ then the complement of the set $S_{r,w,u}$ consists of the only element y_0 (if the commands of the operator algorithm $\mathfrak{A}$ are enumerated by the numbers from 1 to m, the initial command has number 1, and the terminal command has number m, then in the case $r \in R(\mathfrak{A})$ there is a unique sequence of pairs of natural numbers $(x_0, i_0), (x_1, i_1), \dots, (x_t, i_t)$ such that $x_0 = r$, $i_0 = 1$, $i_l = m$, and for every s $(1 \leq s \leq l)$ the application of the command with number i_{s-1} to x_{s-1} gives the number x_s and the number of the next command is i_s); with these notations,

$$y_0 = a^{x_0+1} b^{i_0+\varepsilon_0 m} a^{x_1+1} b^{i_1+\varepsilon_1 m} a^{x_2+1} b^{i_2+\varepsilon_2 m} \dots a^{x_t+1} b^{i_t+\varepsilon_t m},$$

where $\varepsilon_i \rightleftharpoons 0$ if x_i is divisible by 6 and $\varepsilon_i \rightleftharpoons 1$ otherwise $(i = 0, \dots, t)$.

We obtain the following equivalences:

$$\begin{aligned} r \in R(\mathfrak{A}) &\Leftrightarrow |\Pi_2 \setminus S_{r,w,u}| = 1, & r \in R(\mathfrak{A}) &\Leftrightarrow |\Pi_2 \setminus S_{r,w,u}| \geq 1, \\ r \in R(\mathfrak{A}) &\Leftrightarrow \Pi_2 \setminus S_{r,w,u} \neq \varnothing, & r \notin R(\mathfrak{A}) &\Leftrightarrow \Pi_2 \setminus S_{r,w,u} = \varnothing, \\ r \notin R(\mathfrak{A}) &\Leftrightarrow |\Pi_2 \setminus S_{r,w,u}| = 0, & r \notin R(\mathfrak{A}) &\Leftrightarrow |\Pi_2 \setminus S_{r,w,u}| \leq 0. \end{aligned}$$

Let $b_1, \dots, b_k$ be different degrees of the element a; put

$$T_{x,w,u} \rightleftharpoons S_{x,w,u} \setminus \{b_1, \dots, b_k\}.$$

It is easily seen that $T_{r,w,u}$ is a Diophantine set.

If $r \notin R(\mathfrak{A})$ then $S_{r,w,u} = \Pi_2$, and therefore

$$\Pi_2 \setminus T_{r,w,u} = \{b_1, \dots, b_k\}, \quad |\Pi_2 \setminus T_{r,w,u}| = k.$$

However, if $r \in R(\mathfrak{A})$ then $\Pi_2 \setminus S_{r,w,u}$ consists of the only element y_0 which is not a degree of a; hence, $|\Pi_2 \setminus T_{r,w,u}| = k + 1$. We obtain the equivalences

$$r \in R(\mathfrak{A}) \Leftrightarrow |\Pi_2 \setminus T_{r,w,u}| = k + 1, \quad r \in R(\mathfrak{A}) \Leftrightarrow |\Pi_2 \setminus T_{r,w,u}| \geq k + 1.$$

Observe that we always have $|\Pi_2 \setminus T_{r,w,u}| \geq k$; therefore,

$$|\Pi_2 \setminus T_{r,w,u}| = k + 1 \Leftrightarrow \neg(|\Pi_2 \setminus T_{r,w,u} \leq k). \ \Box$$

The following question remains open: *Is there an algorithm allowing us, given an arbitrary record of a Diophantine set S, i.e., given the corresponding pair $\langle u, v\rangle$ of words, to determine whether the complement of the set S is finite?*

We now discuss the question of eliminating the signs & and $\vee$ from the formulas pertinent to free groups and semigroups.

It is well known that in free groups and semigroups the sign & can be eliminated from formulas by methods that are in a sense of the same type: in free groups this is carried out by means of A. I. Mal′tsev's equation $x_1^2a_1x_1^2a_1^{-1} = (x_2a_2x_2a_2^{-1})^2$ (see [12]) that has only the trivial solution $x_1 = 1 \& x_2 = 1$, and the conjunction $x_1 = y_1 \& x_2 = y_2$ in Π_n is equivalent to the equality $x_1a_1x_2x_1a_2x_2 = y_1a_1y_2y_1a_2y_2$ [13].

Although the disjunction sign $\vee$ too can be eliminated from formulas pertinent to free groups and semigroups, this is carried out by several different methods: as was shown by G. A. Gurevich (see [12]), in a free group F_n ($n \geq 2$) the disjunction of the equations $x_1 = 1 \vee x_2 = 1$ is equivalent to the conjunction of the four equations

$$\underset{\varepsilon,\delta=\pm 1}{\&}\left[x_1a_1^{\varepsilon}x_1a_1^{-\varepsilon},\, x_2a_2^{\delta}x_2a_2^{-\delta}\right] = 1.$$

In the case of Π_n N. K. Kosovskiĭ [6, 7] constructed words

$$w(x, y, z, v, x_1, \dots, x_k, a_1, a_2), \quad u(x, y, z, v, x_1, \dots, x_k, a_1, a_2)$$

in variables $x, y, z, v, x_1, \dots, x_k$ and constants a_1 and a_2 such that the equivalence

$$(A = B \vee C = D) \Leftrightarrow \Pi_n \models (\exists \bar{x})\, w(A, B, C, D, \bar{x}, \bar{a}) = u(A, B, C, D, \bar{x}, \bar{a})$$

holds for all elements A, B, C, and D of Π_n, where $\bar{x}$ denotes $x_1, \dots, x_k$ and $\bar{a}$ denotes a_1, a_2; moreover, in the articles [6, 7] $k = 4$. An analogous formula was constructed in the article [14]. In [14] k is much greater than in [6, 7] (near 40), although the authors of [14] point out that it is possible to diminish k to 3 by using rather involved analysis, with the reference to the dissertation [15] that is practically inaccessible to the Russian reader.

We demonstrate that it is possible to construct a rather simple formula with $k = 2$.

As a preliminary, we prove some lemma about solutions to one simple equation in a free semigroup.

Lemma. *If the equality $A^mB^mC^m = D^m$ holds in the free semigroup Π_n ($n \geq 2$) for $m \geq 6$ with $|A| = |B|$ or $|B| = |C|$, then A, B, C, and D are degrees of the same element of Π_n, where $|W|$ is the length of a word W in Π_n.*

PROOF is based on Lemma 2.3 of S. I. Adyan's monograph [16]: *if $A^tA' = B^rB'$, where the word A' is an initial fragment of A, B' is an initial fragment of B, and $|A^tA'| \geq |AB|$; then it is possible to indicate a word D such that $A = D^k$ and $B = D^s$ for some k and s.* It is easily seen that the following assertion is true along with this lemma: *if $A'A^t = B'B^r$, where the word A' is a terminal fragment of A, B' is a terminal fragment of B, and $|A'A^t| \geq |BA|$, then it is possible to indicate a word D such that $A = D^k$ and $B = D^s$ for some k and s.* The last assertion, as well as the former, will be referred to as S. I. Adyan's lemma.

We examine the case in which $|A| = |B|$. The case in which $|B| = |C|$ is treated similarly.

If $A^m = D^kD_1$, where D_1 is an initial fragment of D and $|A^{m-1}| \geq |D|$, then $|A^m| \geq |AD|$, and therefore by S. I. Adyan's lemma there is a word E such that $A = E^s$ and $D = E^t$ for some s and t. Thus, we obtain the equality $E^{sm}B^mC^m = E^{tm}$ which implies the equality $B^mC^m = E^{m(t-s)}$.

If $t - s = 0$ then B and C are empty words and the assertion under proof is valid.

However, if $t - s \geq 1$ then by the Lyndon-Schützenberger theorem [17] B, C, and E are degrees of the same element S, and hence A, B, C, and D are degrees of S.

If $C^m = D_1D^k$ and $|C^{m-1}| \geq |D|$, where D_1 is a terminal fragment of D, then the analogous consideration shows that A, B, C, and D are degrees of the same element.

We are left with settling the case in which $|A^{m-1}| < |D|$ and $|C^{m-1}| < |D|$. Since $m \geq 6$ then $|A^m| < |D^2|$ and $|S^m| < |D^2|$. By assumption, $|A| = |B|$; therefore, $|B^m| < |D^2|$. Hence, $|A^mB^mC^m| < |D^6|$, but $A^mB^mC^m = D^m$, and consequently $|D^m| < |D^6|$, $m < 6$, contradicting the hypothesis of the lemma. $\square$

We turn to constructing a formula $\Phi(x, y, z, v)$ of the form

$$(\exists x_1, x_2)\, w(x, y, z, v, x_1, x_2, a_1, a_2) = u(x, y, z, v, x_1, x_2, a_1, a_2)$$

such that the equivalence $(A = B \vee C = D) \Leftrightarrow \Pi_n \models \Phi(A, B, C, D)$ holds for all elements A, B, C, and D of the group Π_n . Since $(A = B \vee C = D) \Leftrightarrow (AD = BD \vee BC = BD)$, it suffices to construct a formula $F(x, y, z)$ such that $(g = h \vee f = h) \Leftrightarrow \Pi_n \models F(g, f, h)$.

Let $\Psi(x, y, z, x_1, x_2)$ denote the following system of equalities:

$$[(x^k a)^k (x^k b)^k]^k [(y^k a)^k (y^k b)^k]^k = x_1 [(z^k a)^k (z^k b)^k]^k x_2 \& x_1 [(x^k a)^k (x^k b)^k] = [(x^k a)^k (x^k b)^k] x_1 \& x_2 [(y^k a)^k (y^k b)^k] = [(y^k a)^k (y^k b)^k] x_2 \& x_1 x_2 = x_2 x_1.$$

Assume $k \geq 6$.

Theorem 4. *For arbitrary elements g, h, and f of the free group Π_n $(n \geq 2)$ we have*

$$(g = h \vee f = h) \Leftrightarrow \Pi_n \models (\exists x_1, x_2) \Psi(g, f, h, x_1, x_2).$$

PROOF. First of all, we demonstrate that $(x^k a)^k (x^k b)^k$ is a prime element of Π_n for every prime element x of Π_n.

Assume the contrary. Let $(x^k a)^k (x^k b)^k = S^m$ and $m \geq 2$; then by the Lyndon-Schützenberger theorem [17] $x^k a$ and $x^k b$ commute; i.e., $x^k a x^k b = x^k b x^k a$, which is impossible.

If $g = h \vee f = h$ then, obviously, $\Pi_n \models (\exists x_1, x_2) \Psi(g, f, h, x_1, x_2)$.

Conversely, let $\Pi_n \models (\exists x_1, x_2) \Psi(g, f, h, x_1, x_2)$. Then there are n, $m \geq 0$ such that

$$x_1 = [(x^k a)^k (x^k b)^k]^n \& x_2 = [(y^k a)^k (y^k b)^k]^m.$$

Demonstrate that $nm = 0$ or $x = y = z$.

If $nm \neq 0$ then the equality $x_1 x_2 = x_2 x_1$ implies that the elements $(x^k a)^k (x^k b)^k$ and $(y^k a)^k (y^k b)^k$ commute and are consequently degrees of the same element. Since they are prime elements, it follows that $(x^k a)^k (x^k b)^k = (y^k a)^k (y^k b)^k$. But then

$$(x^k a)^k = (y^k a)^k \& (x^k b)^k = (y^k b)^k, \quad x^k a = y^k a \& x^k b = y^k b, \ x^k = y^k, x = y.$$

Hence, the following equality holds:

$$[(x^k a)^k (x^k b)^k]^{2k} = [(x^k a)^k (x^k b)^k]^n [(z^k a)^k (z^k b)^k]^k [(x^k a)^k (x^k b)^k]^m.$$

It is clear that $2k \geq n+m$; therefore, the preceding equality implies the equality $[(x^k a)^k (x^k b)^k]^{2k-n-m} = [(z^k a)^k (z^k b)^k]^k$. Since the elements $(x^k a)^k (x^k b)^k$ and $(z^k a)^k (z^k b)^k$ are prime, we obtain the equality $(x^k a)^k (x^k b)^k = (z^k a)^k (z^k b)^k$ which implies the desired equality $x = z$.

If $nm = 0$ then we examine the case $n = 0$ (the case $m = 0$ is settled similarly). In this case

$$[(x^k a)^k (x^k b)^k]^k [(y^k a)^k (y^k b)^k]^k = [(z^k a)^k (z^k b)^k]^k [(y^k a)^k (y^k b)^k]^m.$$

For $m \geq k$, we obtain

$$[(x^k a)^k (x^k b)^k]^k = [(z^k a)^k (z^k b)^k]^k [(y^k a)^k (y^k b)^k]^{m-k}.$$

If $m - k \geq 2$ then, by the Lyndon-Schützenberger theorem [17] and in view of the fact that the elements $(x^k a)^k (x^k b)^k$ and $(z^k a)^k (z^k b)^k$ are prime, we obtain the equalities $x = y = z$. If $m - k = 0$ then we obtain the equality $x = z$; however, if $m - k = 1$ then we obtain the equality

$$[(z^k a)^k (z^k b)^k]^k (y^k a)^k (y^k b)^k = [(x^k a)^k (x^k b)^k]^k.$$

Since $|y^k a| = |y^k b|$, by the Lemma $y^k a$ and $y^k b$ are degrees of the same element, which is impossible as they have different terminal fragments.

For $m < k$ we obtain the equality

$$[(x^k a)^k (x^k b)^k]^k [(y^k a)^k (y^k b)^k]^{k-m} = [(z^k a)^k (z^k b)^k]^k,$$

whence for $k - m \geq 2$ we again infer the equality $x = z$ by using the Lyndon-Schützenberger theorem [17], while for $k - m = 1$, the equality

$$[(x^k a)^k (x^k b)^k]^k (y^k a)^k (y^k b)^k = [(z^k a)^k (z^k b)^k]^k$$

which by the Lemma leads to a contradiction. □

It was already proven in the article [8] that, to eliminate the disjunction sign from the formulas pertinent to free semigroups is impossible without the existential quantifier. Since the access to the article [8] is very limited, we expose a simplified proof of this fact.

Theorem 5. *For any $n \geq 2$, there are no words*

$$w(x, y, z, v, a_1, \dots, a_n), \quad u(x, y, z, v, a_1, \dots, a_n)$$

in variables x, y, z, and v and constants $a_1, \dots, a_n$ for which the equivalence

$$(g = h \vee p = f) \Leftrightarrow w(g, h, p, f, \bar{a}) = u(g, h, p, f, \bar{a})$$

holds for all elements g, h, p, and f of Π_n.

PROOF. Assume the contrary; i.e., there is an equation

$$w(x, y, z, v, a_1, \dots, a_n) = u(x, y, z, v, a_1, \dots, a_n)$$

whose solutions are the various collections (g, g, p, f) and (g, h, p, p) and only them.

In the words w and u, we distinguish maximal nonempty subwords in the alphabet of the unknowns $\{x, y, z, v\}$:

$$w(x, y, z, v, \bar{a}) \doteq A_1 X_1 A_2 \dots A_t X_t A_{t+1}, \quad u(x, y, z, v, \bar{a}) \doteq B_1 Y_1 B_2 \dots B_k Y_k B_{k+1},$$

where Y_j and X_i are nonempty words in the alphabet of the unknowns $\{x, y, z, v\}$, A_m and B_s are nonempty words in the alphabet $\{a_1, \dots, a_n\}$ (with a possible exception of the cases $m = 1$, $m = t+1$, $s = 1$, and $s = k + 1$), and $\doteq$ is the sign of lexicographic equality of words.

Consider the following formulas:

$$\Phi_1 \rightleftharpoons (\forall x, z, v) w(x, x, z, v, \bar{a}) = u(x, x, z, v, \bar{a}),$$
$$\Phi_2 \rightleftharpoons (\forall x, y, z) w(x, y, z, z, \bar{a}) = u(x, y, z, z, \bar{a}).$$

Since the formulas Φ_1 and Φ_2 are true in the subgroup Π_n and since $n \geq 2$, by Yu. I. Merzlyakov's theorem [18] they are true in every free group F_m with $m \geq n$; in particular, in the group F_{n+3}. Therefore, the equalities

$$w(a_{n+1}, a_{n+1}, a_{n+2}, a_{n+3}, \bar{a}) \doteq u(a_{n+1}, a_{n+1}, a_{n+2}, a_{n+3}, \bar{a}),$$
$$w(a_{n+1}, a_{n+2}, a_{n+3}, a_{n+3}, \bar{a}) \doteq u(a_{n+1}, a_{n+2}, a_{n+3}, a_{n+3}, \bar{a})$$

hold in the group F_{n+3}. Put

$$X_i^{(1)} \rightleftharpoons X_{i[x,y,z,v]}[a_{n+1}, a_{n+1}, a_{n+2}, a_{n+3}],$$
$$Y_j^{(1)} \rightleftharpoons Y_{j[x,y,z,v]}[a_{n+1}, a_{n+1}, a_{n+2}, a_{n+3}],$$
$$X_i^{(2)} \rightleftharpoons X_{i[x,y,z,v]}[a_{n+1}, a_{n+2}, a_{n+3}, a_{n+3}],$$
$$Y_j^{(2)} \rightleftharpoons Y_{j[x,y,z,v]}[a_{n+1}, a_{n+2}, a_{n+3}, a_{n+3}],$$

where $W_{[x,y,z,v]}[A,B,C,D]$ is the word obtained from the word W by the simultaneous replacement of each occurrence of the variable x with the word A, the variable y with the word B, the variable z with the word C, and the variable v with the word D. Then the following equalities hold for $s = 1, 2$:

$$A_1 X_1^{(s)} A_2 \dots A_t X_t^{(s)} A_{t+1} \equiv B_1 Y_1^{(s)} B_2 \dots B_k Y_k^{(s)} B_{k+1}.$$

Since A_j and B_i are words in the alphabet $\{a_1, \dots, a_n\}$ and $X_j^{(s)}$ and $Y_i^{(s)}$ are words in the alphabet $\{a_{n+1}, a_{n+2}, a_{n+3}\}$, the preceding equality implies that $t = k$ and

$$\mathop{\&}_{i=1}^{t+1} A_i \equiv B_i, \quad \mathop{\&}_{s=1}^{2} \mathop{\&}_{i=1}^{t} X_i^{(s)} \equiv Y_i^{(s)}.$$

It is easily seen that the system of the equalities

$$\mathop{\&}_{s=1}^{2} \mathop{\&}_{i=1}^{t} X_i^{(s)} \equiv Y_i^{(s)}$$

implies the system of the equalities

$$\mathop{\&}_{i=1}^{t} X_i \equiv Y_i.$$

Therefore, $w(x,y,z,v,\bar{a}) \equiv u(x,y,z,v,\bar{a})$. Hence, the identity

$$(\forall x,y,z,v)\, w(x,y,z,v,\bar{a}) = u(x,y,z,v,\bar{a})$$

holds on Π_n, contradicting the assumption that was made at the beginning of the proof. □

The following natural question arises: *Is it possible to construct words $w(x,y,z,v,t,\bar{a})$ and $u(x,y,z,v,t,\bar{a})$ such that the equivalence*

$$(g = h \vee p = f) \Leftrightarrow (\exists t)\, w(g,h,p,f,t,\bar{a}) = u(g,h,p,t,\bar{a})$$

holds for all elements g, h, f, and p of Π_n?

The conjectural answer is negative.

As was already pointed out above, in the articles [7–9] the formula

$$P_n(x,y) = (\exists u, v_1, v_2)\left(\bigvee_{\substack{i,j=1\\ i\neq j}}^{n} (x = ua_iv_1 \& y = ua_jv_2) \vee \left(\bigvee_{i=1}^{n} (x = ya_iv_1 \vee y = xa_iv_1)\right)\right)$$

was constructed for every $n \geq 2$ and there was proven that the equivalence

$$g \neq h \Leftrightarrow \Pi_n \models P_n(g,h)$$

holds for arbitrary two elements g and h of Π_n. Therefore, G. S. Makanin's theorem [10] on the algorithmic decidability of the compatibility problem for systems of equations in the free semigroup Π_2 readily implies the algorithmic decidability of the existential and universal theories of every semigroup Π_n.

It was proven in the article [9] that the universal and, consequently, existential theories of a semigroup Π of countable rank are algorithmically decidable. However, the proof in [9] uses the not generally accepted notion of the $\exists$-*quantifier with respect to a generator* and its elimination.

We now demonstrate that *the decidability of the universal theory of a free semigroup of countable rank is a direct corollary to the decidability of the universal theory of an arbitrary free semigroup of finite rank.*

Indeed, assume Φ to be a formula of the form $(\forall x_1, \ldots, x_p)\Psi$ and let Ψ be its matrix (quantifier-free part). Let us show that if Ψ contains as constants only $a_1, \ldots, a_n$, then $\Pi \models \Phi \Leftrightarrow \Pi_{n+1} \models \Phi$. Since Π_m is a subsemigroup of Π for every m, it follows from $\Pi \models \Phi$ that $\Pi_m \models \Phi$ for every $m \geq n$.

Conversely, assume that $\Pi_{n+1} \models \Phi$. Denote by H the subsemigroup of Π_{n+1} which is generated by the elements

$$a_1, \ldots, a_n, a_{n+1}a_1a_{n+1}, \ldots, a_{n+1}^k a_1 a_{n+1}^k, \ldots.$$

Then $H \models \Phi$. However, the semigroup H is isomorphic to the semigroup Π; moreover, we can take such an isomorphism φ for which the following equalities hold:

$$\varphi(a_i) = a_i \quad \text{if} \quad 1 \leq i \leq n, \quad \varphi(a_i) = a_{n+1}^{i-n} a_1 a_{n+1}^{i-n} \quad \text{if} \quad i > n.$$

Therefore, $\Pi \models \Phi$. □

The formulas considered in the articles [3, 4] and in the beginning of the present article have a quite simple prefix. At the same time, their matrices include a good many occurrences of the disjunction sign $\vee$. Of course, using the method indicated above, we could eliminate the sign $\vee$ but this would lead to a considerable increase of the number of existential quantifies in the prefix.

In this connection, in our opinion, the question is of interest whether it is possible to simultaneously simplify the prefix and the matrix of a formula; moreover, the simplest matrix should look like a formula of the form $w = u$, where w and u are words in the alphabet of the variables and generators of the semigroup.

As some advancement in this direction, we propose the following theorem:

Theorem 6. *It is possible to construct a formula $\Phi(x)$ that has one free generator x, is of the form*

$$(\exists w)(\forall y)(\exists x_1, \ldots, x_{11})u = v,$$

where u and v are words in the alphabet $\{x, w, y, x_1, \ldots, x_{11}, a_1, a_2, a_3\}$, and is such that there is no algorithm allowing us, given an arbitrary element g of Π_2, to determine whether the formula $\Phi(g)$ is true on Π_3.

PROOF. Denote by $H(w, z, x_1, x_2, x_3)$ the formula

$$\bigvee_{\substack{i,j=1,\\ i \neq j}}^{3} (w = x_1 a_i x_2 \& z = x_1 a_j x_3) \vee z = w x_1.$$

It is easy to see that the following equivalence holds for arbitrary elements g and h of Π_3:

$$\Pi_3 \models (\exists x_1, x_2, x_3)\, H(g, h, x_1, x_2, x_3) \Leftrightarrow \text{“}h \textit{ is not an initial fragment of } g\text{”}.$$

Denote by Π a semigroup that has presentation $\langle a_1, a_2 \| A_1 = B_1,\ A_2 = B_2,\ A_3 = B_3\rangle$ and for which the problem of equality to a fixed word g_0 is algorithmically undecidable [19]; moreover, the words A_i and B_i are nonempty for every i. Put $A_{3+j} \rightleftharpoons B_j$ and $B_{3+j} \rightleftharpoons A_j$ for $j = 1, 2, 3$. Denote by $F(x)$ the following formula:

$$(\exists w)(\forall y)(\exists x_1, x_2, x_3)\Psi(x, w, y, x_1, x_2, x_3),$$

where

$$\Psi(x, w, y, x_1, x_2, x_3) \rightleftharpoons H(a_3 g_0 a_3 w, y a_3, x_1, x_2, x_3)$$
$$\vee \left(\bigvee_{i=1}^{6} a_3 g_0 a_3 w a_3 g a_3 = y a_3 x_1 A_i x_2 a_3 x_1 B_i x_2 a_3 x_3 \right).$$

Demonstrate that the equivalence

$$\Pi_3 \models F(g) \Leftrightarrow \text{“}g \textit{ equals } g_0 \textit{ in } \Pi\text{”}$$

holds for an arbitrary nonempty word g of Π_2 which differs from g_0.

If g is a nonempty word of Π_2 distinct from g_0 and g equals g_0 in Π, then in Π_2 there is a sequence $g_0, g_1, \dots, g_m$ such that $g_m \rightleftharpoons g$; moreover, for every i $(0 \le i \le m-1)$, there are a j and words X_1 and X_2 such that $g_i \rightleftharpoons X_1 A_j X_2$ and $g_{i+1} \rightleftharpoons X_1 B_j X_2$; furthermore, we may assume $m \ge 2$.

We put

$$W_0 \rightleftharpoons g_1 a_3 g_2 a_3 \dots a_3 g_{m-1}.$$

It is easy to show that the formula

$$(\forall y)\,(\exists x_1, x_2, x_3)\Psi(g, W_0, y, x_1, x_2, x_3)$$

is true on Π_3. Therefore, $\Pi_3 \models F(g)$.

Conversely, let $\Pi_3 \models F(g)$ and let W_0 be an element of Π_3 such that

$$\Pi_3 \models (\forall y)\,(\exists x_1, x_2, x_3)\Psi(g, W_0, y, x_1, x_2, x_3).$$

First of all, it is easy to demonstrate that a_3^2 does not occur in the word $a_3 g_0 a_3 W_0 a_3 g a_3$ and, for that reason, in Π_2 there are nonempty words $h_m, h_{m-1}, \dots, h_0$ $(m \ge 2)$ such that

$$h_m \rightleftharpoons g_0, \quad h_0 \rightleftharpoons g, \quad a_3 g_0 a_3 W_0 a_3 g a_3 \rightleftharpoons a_3 h_m a_3 h_{m-1} a_3 \dots a_3 h_0 a_3.$$

We now show that h_t equals h_0 in Π by inducting on t.

Assume that $m \ge t > 0$ and assume that h_i equals h_0 in Π for every i such that $t > i \ge 0$.

Put $Y \rightleftharpoons a_3 h_m a_3 h_{m-1} a_3 \dots a_3 h_{t+1}$ for $m > t$ and $Y \rightleftharpoons \Lambda$ for $m = t$, where Λ is the empty word. Then $a_3 g_0 a_3 W_0 \rightleftharpoons Y a_3 Z$ for some Z, and therefore there are words X_1, X_2, and X_3 and a number i such that

$$a_3 g_0 a_3 W_0 a_3 g a_3 \rightleftharpoons Y a_3 X_1 A_i X_2 a_3 X_1 B_i X_2 a_3 X_3.$$

1. If the letter a_3 does not occur in the words X_1 and X_2 then $h_t \rightleftharpoons X_1 A_i X_2$ and $h_{t-1} \rightleftharpoons X_1 B_i X_2$, implying that h_t equals h_{t-1} in Π. Since h_{t-1} equals h_0 in Π, it follows that h_t equals h_0 in Π.

2. If the letter a_3 occurs in X_1 then there is $l < t$ such that $h_t \rightleftharpoons h_l$, implying again that h_t equals h_0 in Π.

3. If the letter a_3 does not occur in X_1 but $X_2 \rightleftharpoons X_{2l} a_3 X_{2r}$ and a_3 does not occur in X_{2l} then there is $l < t$ such that $h_t \rightleftharpoons X_1 A_i X_{2l}$ and $h_l \rightleftharpoons X_1 B_i X_{2l}$, which again implies that h_t equals h_0 in Π.

Eliminating the sign $\vee$ from the matrix of the formula $F(x)$ by the above-described method, we obtain a sought formula $\Phi(x)$ of the form

$$(\exists w)(\forall y)(\exists x_1, \dots, x_{11})\, u = v.$$

REMARK. Clearly, the prefix of the formula $\Phi(x)$ is of higher complexity than that of the formula in the articles [3, 4]; however, this circumstance is to some extent outweighed by the simple form of the matrix of the formula. Moreover, the study of formulas of the indicated type reduces in a certain sense to the study of solution sets for equations in 13 unknowns and sheds more light on the source of difficulties that appear in attempts to describe the solution sets for the equations having the number of unknowns greater than 3.

In conclusion, the author expresses his deep gratitude to S. I. Adyan for support and unfailing interest in the article.

References

1. S. I. Adyan and S. G. Makanin, "Study on algorithmic questions of algebra," in: Algebra, Mathematical Logic, Number Theory, and Topology [in Russian], Collection of Survey Articles. Vol. 1: To the 50 Years of the Institute, Nauka, Moscow, 1984, pp. 197–217. (Trudy Mat. Inst. Steklov.; **167**.)
2. W. V. O. Quine, "Concatenation as a basis for arithmetic," J. Symbolic Logic, **11**, 105–114 (1946).
3. V. G. Durnev, "On the positive theory of a free semigroup," Dokl. Akad. Nauk SSSR, **211**, No. 4, 772–774 (1973).
4. S. S. Marchenkov, "Undecidability of the positive $\forall\exists$-theory of a free semigroup," Sibirsk. Mat. Zh., **23**, No. 1, 196–198 (1982).
5. A. I. Mal′tsev, Algorithms and Recursive Functions [in Russian], Nauka, Moscow (1965).
6. N. K. Kosovskiĭ, "Some properties of solutions to equations in a free semigroup," Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), **32**, 21–28 (1972).
7. N. K. Kosovskiĭ, Elements of Mathematical Logic and Its Applications to the Theory of Subrecursive Algorithms [in Russian], Leningrad. Univ., Leningrad (1981).
8. V. G. Durnev, "On the positive theory of a free semigroup," Uchen. Zap. Mat. Kafedry Tul′sk. Ped. Inst., No. 2, 215–241 (1970).
9. A. D. Taĭmanov and Yu. I. Khmelevskiĭ, "Decidability of the universal theory of a free semigroup," Sibirsk. Mat. Zh., **21**, No. 1, 228–230 (1980).
10. G. S. Makanin, "The decidability problem for equations in a free semigroup," Dokl. Akad. Nauk SSSR, **233**, No. 2, 287–290 (1977).
11. Makanin G. S. "The decidability problem for equations in a free semigroup," Mat. Sb., **103**, No. 2, 147–236 (1977).
12. G. S. Makanin, "Decidability of the universal and positive theory of a free semigroup," Izv. Akad. Nauk SSSR Ser. Mat., **48**, No. 4, 735–749 (1984).
13. Yu. I. Khmelevskiĭ, "Equations in a free semigroup," Trudy Mat. Inst. Steklov. (LOMI), **107**, 21–28 (1971).
14. J. R. Büchi and S. Senger, "Coding in the existential theory on concatenation," Arch. Math. Logic, **26**, No. 1–2, 101–106 (1986/1987).
15. S. Senger, The Existential Theory of Concatenation, Ph. D. Dissertation, Purdue University (1982).
16. S. I. Adyan, The Burnside Problem and Identities in Groups [in Russian], Nauka, Moscow (1975).
17. R. C. Lyndon and M. P. Schützenberger, "The equation $a^M = b^N c^P$ in a free group," Michigan Math. J., **9**, 289–298 (1962).
18. Yu. I. Merzlyakov, "Positive formulas on free groups," Algebra i Logika, **5**, No. 4, 25–42 (1966).
19. Yu. V. Matiyasevich, "Simple examples of undecidable associative calculi," Dokl. Akad. Nauk SSSR, **173**, No. 6, 1264–1266 (1967).

TRANSLATED BY K. M. UMBETOVA