ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 4, Pages 101–108
S 1079-6762(98)00047-X (December 14, 1998)

# TARSKI'S PROBLEM ABOUT THE ELEMENTARY THEORY OF FREE GROUPS HAS A POSITIVE SOLUTION

OLGA KHARLAMPOVICH AND ALEXEI MYASNIKOV

(Communicated by Efim Zelmanov)

Abstract. We prove that the elementary theories of all nonabelian free groups coincide and that the elementary theory of a free group is decidable. These results answer two old questions that were raised by A. Tarski around 1945.

The object of this announcement is to sketch proofs of the following two theorems.

**Theorem 1.** *The elementary theories of all nonabelian free groups coincide.*

**Theorem 2.** *The elementary theory of a free group is decidable.*

These theorems answer two old questions that were raised by A. Tarski around 1945. We recall that the *elementary theory $Th(G)$* of a group $G$ is the set of all first order sentences in the language of group theory which are true in $G$. Notice that in the language of group theory every sentence is equivalent to a sentence of the following type:

$$\Phi = \forall X_1 \exists Y_1 \ldots \forall X_k \exists Y_k \bigvee_{p=1}^{r} \Big( \bigwedge_{i=1}^{s} u_{pi}(X_1, Y_1, \ldots, X_k, Y_k) = 1 \\ \bigwedge_{j=1}^{t} v_{pj}(X_1, Y_1, \ldots, X_k, Y_k) \neq 1 \Big). \tag{1}$$

A discussion of this problem can be found in several textbooks on model theory (see, for example, C. Chang and H. Keisler [5] or Yu. Ershov and E. Palutin [8]) as well as in several textbooks on group theory (see, for example, R. Lyndon and P. Schupp [22]).

Our solution of Tarski's problem takes on the strongest possible, positive form, namely: *the free group $F(a_1, \ldots, a_n)$ freely generated by $a_1, \ldots, a_n$ is an elementary subgroup of $F(a_1, \ldots, a_n, \ldots, a_{n+p})$ for every $n \geq 2$ and $p \geq 0$.* Moreover, we prove also that: *the elementary theory $Th(F)$ of a free group $F$ even with constants from $F$ in the language is decidable.*

Observe, by comparison, that it is relatively easy to prove that free abelian groups of finite rank are elementarily equivalent if and only if their ranks coincide. The same is true for free nilpotent groups of finite rank and for free semigroups

Received by the editors May 25, 1998.
1991 *Mathematics Subject Classification.* Primary 20E05, 20F10; Secondary 03B25, 03C68.
*Key words and phrases.* Free group, elementary theory, Tarski.

of finite rank. Notice also that the elementary theory of any free abelian group of finite rank is decidable [35], but that the elementary theory of a free nilpotent nonabelian group of finite rank is undecidable [25]. Moreover, the elementary theory of a finitely generated free semigroup of rank at least two is also undecidable [29].

During the last 50 years Tarski's problem for free groups has proved to be, on the one hand, very challenging, and on the other hand, rather fruitful. Here we mention just a few results from group theory which have been inspired by Tarski's problem.

Around 1959, R. Vaught asked whether the sentence

$$\forall x \forall y \forall z (x^2 y^2 z^2 = 1 \to xy = yx \ \& \ xz = zx \ \& \ yz = zy)$$

holds in all free groups. Shortly afterwards, R. Lyndon proved that, for each solution $x, y, z$ of the quadratic equation $x^2y^2z^2 = 1$ in a free group, the elements $x, y, z$ commute pairwise [17]. This little theorem launched the whole theory of equations over free groups. The first general results in this area are due to R. Lyndon [18], A. Lorenc [16] and K. Appel [1], where they described the solution set of an arbitrary equation of one variable over a free group. In 1966 A. Mal'tsev described the solution set of the equation $[x, y] = [a, b]$ over the free group $F(a, b)$. This has a nontrivial implication for the elementary theory of a free group of rank 2, namely that the set of all (free) bases of $F(a, b)$ can be defined by a first order formula in the language of group theory: *the elements $u, w \in F(a, b)$ form a basis in $F(a, b)$ if and only if they satisfy the following formula (with constants $a, b$):*

$$\exists z([u, w] = z^{-1}[a, b]z \vee [u, w] = z^{-1}[b, a]z).$$

The focus of investigation subsequently turned to quadratic equations over free groups, i.e., equations in which every variable occurs exactly twice (for example, Mal'tsev's equation above). In the papers of C. Edmund and L. Commerford [7], [6] and R. Grigorchuck and P. Kurchanov [10], [9] the solution sets of standard quadratic equations over arbitrary free group were described. This finished off the quadratic case, because it follows from the work of A. Hoar, A. Karras and D. Solitar [12], [13] that every quadratic equation is automorphically equivalent to a standard one.

In 1982 G. Makanin [24] proved the crucial result about the algorithmic decidability of Diophantine problem over free groups. He proved that if a given equation over a free group $F$ has a solution in $F$, then this equation has a solution of bounded length (and this bound can be effectively computed from the equation itself). In his paper G. Makanin developed an extremely powerful technique to deal with equations over free groups (as well as over free semigroups). We will have more to say about this later. G. Makanin's work then made it possible for A. Razborov to describe the solution set of an arbitrary system of equations over $F$ [31], [30].

Shortly afterwards G. Makanin [23] extended his results, proving that the universal theory $Th_\forall(F)$ of $F$ is algorithmically decidable. Recall that given a group $G$, the universal theory $Th_\forall(G)$ consists of all universal sentences that are true in $G$ (a sentence is termed universal if it is equivalent to one of the type (1) in which only universal quantifiers occur). Notice that any two finitely generated nonabelian free groups have exactly the same universal theory; this follows readily from the fact that any two such groups are embeddable into each other and the fact that any universal sentence which is true in a group is also true in every subgroup of this group. Since the theory $Th(F)$ is complete (i.e., for every sentence either the sentence or its negation lies in $Th(F)$), it follows immediately that any two free nonabelian groups satisfy exactly the same boolean combinations of universal formulas.

Now, denote by $Th_+(G)$ the positive theory of the group $G$, i.e., the set of all positive sentences from $Th(G)$ (a sentence is called positive if it is equivalent to one of the type (1) that does not contain inequalities). In 1966 Yu. Merzlyakov proved the remarkable theorem that any two nonabelian free groups of finite rank have the same positive theory [26]. Combining results on the decidability of $Th_\forall(F)$ with the above-mentioned theorem, G. Makanin showed that the positive theory $Th_+(G)$ is decidable [23].

Another part of the elementary theory which was shown to be the same for any two nonabelian free groups of finite rank consists of all so-called $\forall\exists$-sentences or, sometimes, $\Pi_2$-sentences (a $\forall\exists$-sentence is a sentence which is equivalent to a sentence of the type $\forall X \exists Y \phi(X,Y)$, where formula $\phi$ does not contain quantifiers, and $X$ and $Y$ are arbitrary tuples of variables). The corresponding part of $Th(F)$ is denoted by $Th_{\forall\exists}(F)$. That result is due to G. Sacerdote [34]. He used Merzlyakov's ideas and the small cancellation technique in Van-Kampen diagrams for group presentations. Again, it follows from his theorem that free nonabelian groups of finite rank satisfy the same boolean combinations of $\forall\exists$-sentences.

So, two important pieces of Tarski's conjecture, $Th_+(F)$ and $Th_{\forall\exists}(F)$, have already been proved to be true. In order to understand more of $Th(F)$ some new ingredients were needed. The new tools in our investigation of $Th(F)$ are algebraic geometry over groups, the theory of exponential groups, a technique involving what is termed discrimination, an implicit function theorem (over free groups) and a description of irreducible algebraic varieties (over free groups) in terms of trianglular quasi-quadratic systems. It is to these topics that we need to turn now.

It was clear from the beginning that to deal with the Tarski problem one needed a precise description of solution sets of equations (and inequations) over free groups. In the classical case, algebraic geometry has been shown to be very useful in dealing with polynomial equations over fields. An analog of algebraic geometry over groups has been developed by G. Baumslag, A. Myasnikov and V. Remeslennikov in [2]. It provides the necessary topological machinery as well as a method for transcribing geometric notions into the language of pure group theory. Following [2] and [14] we can use standard algebraic geometry notions such as algebraic sets, the Zariski topology, Noetherian domains, irreducible varieties, radicals and coordinate groups to organize an approach to finding a solution of Tarski's problem. Some of these ideas go back to R. Bryant [4], V. Guba [11], B. Plotkin [28] and E. Rips.

Another essential ingredient in our treatment of the Tarski problem is the theory of exponential groups. This area starts with results of P. Hall, A. Mal'tsev, G. Baumslag and R. Lyndon. R. Lyndon was the first who recognized the importance of exponential groups for solving equations over groups. He found that the solution set of any equation with one variable over a free group $F$ can be obtained from finitely many "parametric" words by specializing their parameters into the ring of integers [18]. More precisely, a parametric word over $F$ with parametrs in the polynomial ring $Z[t_1, \ldots, t_n]$ is a formal expression that can be obtained from a basis of $F$ by finitely many concatenations and exponentiations by elements from $Z[t_1, \ldots, t_n]$. If one specializes the parameters $t_1, \ldots, t_n$ into integers (i.e., one substitutes some particular integers in place of the $t_i$'s), then this gives rise to a specialization of a given parametric word into an element of the group $F$. What R. Lyndon proved is that for any equation with one variable (and, perhaps, constants from $F$) one can effectively find a finite set of parametric words with parameters from the ring $Z[t_1, \ldots, t_n]$, such that any solution of this equation can be obtained by some specialization of one of these words. Later K. Appel refined this result, proving that the solution set of an equation in one variable over a free group can be parametrized by finitely many words of the type $fg^th$, where $f, g, h \in F$ and $t$ is a parameter (from $Z[t]$) [1]. This led R. Lyndon to introduce the notion of a group with parametric exponents in an associative unitary ring $A$. In particular, he described and studied the free exponential group $F^{Z[t]}$ over the ring $Z[t]$. One of the crucial results of this study was that the group $F^{Z[t]}$ is discriminated by $F$, i.e., for any finitely many nontrivial elements in $F^{Z[t]}$ there exists a homomorphism $\phi : F^{Z[t]} \to F$, which is the identity on $F$, such that all the images under $\phi$ of the given elements are also nontrivial. In 1989 V. Remeslennikov established a surprising connection between residual properties of groups and their universal theories, namely, that a finitely generated group $H$ can be discriminated by a nonabelian free group $F$ if and only if $H$ has exactly the same universal theory as $F$ [33]. It follows then immediately from Lyndon's result that all finitely generated subgroups of $F^{Z[t]}$ have the same universal theory as $F$. This emphasized once more the role of $F^{Z[t]}$ in the investigation of $Th(F)$.

A modern treatment of exponential groups is contained in the paper by A. Myasnikov and V. Remeslennikov [27]. In particular, they proved that the group $F^{Z[t]}$ can be obtained starting from $F$ by an infinite chain of HNN-extensions of a very specific type, so-called extensions of centralizers. If $G$ is a group and $C$ is the centralizer of a nontrivial element in $G$, then the following HNN-extension:

$$G(C, s) = \langle G, s \mid s^{-1}cs = c \quad (c \in C)\rangle$$

is called a *free extension of the centralizer* $C$ *by* $s$. Thus, to construct $F^{Z[t]}$ one needs to extend each centralizer sufficiently many times until every proper centralizer is isomorphic to a free abelian group of infinite rank (i.e., the additive group of $Z[t]$). This implies that any finitely generated subgroup of $F^{Z[t]}$ is actually a subgroup of a group which can be obtained from $F$ by finitely many extensions of centralizers, and for such groups one can apply the techniques of H. Bass and J.-P. Serre to describe the structure of these subgroups.

In the same paper [27] the authors put forward the following conjecture: *a finitely generated group is discriminated by a nonabelian free group $F$ if and only if it is embeddable into $F^{Z[t]}$*. A positive solution of this conjecture would provide a description of finitely generated groups which are discriminated by $F$ as well as a description of all finitely generated groups which have the same universal theory as $F$.

This conjecture was positively solved by O. Kharlampovich and A. Myasnikov in a series of two papers [14] and [15]. Our present work is a continuation of these two papers and makes use of the results and methods developed there. In the first of these papers we proved the following result: the coordinate group $F_{Rad(S)}$ of the algebraic set $V_F(S)$ defined by a quadratic equation $S = 1$ with coefficients in $F$ is embeddable into a group obtained from $F$ by finitely many extensions of centralizers (and hence is a subgroup of $F^{Z[t]}$). This implies that the variety $V_F(S)$ is irreducible in the Zariski topology over $F^n$. Moreover, we completely described the radical $Rad(S)$. It turns out that the radical $Rad(S)$ coincides (with a few special classes of exceptions) with the normal closure of $S$ in the group $F * F(X)$. This embedding theorem has its roots in G. Baumslag's paper [3], where he considered discrimination of surface groups, which are exactly (with few exceptions) the coordinate groups of the standard quadratic equations without coefficients. For quadratic equations with coefficients the embeddings are not easy to construct. We need to use a particular form of such embeddings in order to prove a so-called implicit function theorem over free groups, which we will discuss in due course. In the second paper [15] we refined the Makanin–Razborov process to get much simpler descriptions of solution sets of arbitrary systems of equations with coefficients over free groups. To explain what this means, we need the following definition.

Let $G$ be a group and let $X_1, \ldots, X_m$ be disjoint tuples of variables. A system (with coefficients from $G$)

$$\begin{aligned} S_1(X_1, \ldots, X_m) \quad &= 1 \\ S_2(X_2, \ldots, X_m) \quad &= 1 \\ \ddots \quad & \\ S_m(X_m) \quad &= 1 \end{aligned}$$

is said to be *triangular quasi-quadratic* if for every $i$ the equation $S_i(X_i, \ldots, X_m) = 1$ is quadratic in the variables from $X_i$.

Such a system is said to be *nondegenerate* if the equation $S_i(X_i, \ldots, X_m) = 1$ over the coordinate group

$$G_{i+1} = G[X_{i+1}, \ldots X_m]/Rad(S_{i+1}(X_{i+1}, \ldots, X_m), \ldots, S_m(X_m)), \quad G_m = G$$

(with elements from $X_i$ considered as variables and elements from $X_{i+1}, \ldots, X_m$ as coefficients from $G_{i+1}$) has a solution in $G_{i+1}$ for each $i$.

Notice that to solve a nondegenerate triangular quasi-quadratic system over $G$ one needs to solve the last quadratic equation $S_m(X_m) = 1$ over $G$, then the previous one (which is again quadratic!) $S_{m-1}(X_{m-1}, X_m) = 1$ over the coordinate group $G_{m-1}$, and continue the process going up along the triangular system until the first equation $S_1(X_1, \ldots, X_m) = 1$ has been solved in the group $G_1$. Now, to get solutions of this system in the initial group $G$, one needs to specialize the solutions obtained into $G$ (in this case to specialize means to take an arbitrary homomorphism from $G_1$ into $G$ and apply it to the obtained set of solutions in $G_1$). Now, the following crucial result from [15] describes the solution set in $F$ of an arbitrary system $S(X) = 1$ with coefficients from $F$: for any such $S(X) = 1$ one can effectively find a finite family of nondegenerate triangular quasi-quadraitc systems $U_1(Y_1) = 1, \ldots, U_n(Y_n) = 1$ (here $Y_i$'s are disjoint tuples of variables of, possibly, different length) and word mappings $p_1(Y_1), \ldots, p_n(Y_n)$ such that

$$V_F(S) = p_1(V_F(U_1)) \cup \cdots \cup p_n(V_F(U_n)).$$

The possibility of some weak form of such description of solution sets was conjectured by A. Razborov in [32] and also by E. Rips.

The main technical result needed in this work is the following "implicit function theorem" for quadratic equations over $F$, which is interesting in its own right.

*Let*

$$S(x_1, \ldots, x_n, c_1, \ldots, c_k) = 1$$

*be a "nonexceptional" quadratic equation in variables* $X = (x_1, \ldots, x_n)$ *with constants* $c_1, \ldots, c_k$ *in* $F$ *(roughly speaking, "nonexeptional" means that the radical of*

*$S$ coincides with the normal closure of $S$ and $S$ is not an equation of one of few very specific types). Suppose now that for each solution of the equation $S(X) = 1$ some other equation*

$$T(x_1, \ldots, x_n, y_1, \ldots, y_m, c_1, \ldots, c_k) = 1$$

*has a solution in $F$; then $T(X, Y) = 1$ has a solution $Y = (y_1, \ldots, y_m)$ in the coordinate group $F_{Rad(S)}$ of the equation $S(X) = 1$.*

This implies that locally (in terms of Zariski's topology), i.e., in the neighbourhood defined by the equation $S(X) = 1$, the implicit functions $y_1, \ldots, y_m$ can be expressed as an explicit word in variables $x_1, \ldots, x_n$ and constants from $F$, say $Y = P(X)$. This result allows one to eliminate a quantifier from the following formula:

$$\Phi = \forall X \exists Y (S(X) = 1 \quad \to \quad T(X, Y) = 1).$$

Indeed, the sentence $\Phi$ is equivalent in $F$ to the following one:

$$\Psi = \forall X (S(X) = 1 \quad \to \quad T(X, P(X)) = 1).$$

The following theorem then holds.

**Theorem 3.** *Let $F = F(a_1, \ldots, a_n, \ldots, a_{n+p})$, $n \geq 2, p \geq 0$, be a free group with a basis $a_1, \ldots, a_{n+p}$. There exists an algorithm which, given a first order sentence $\Psi$ in the language of group theory with constants $a_1, \ldots, a_n$, finds a finite boolean combination $\Psi^*$ of universal sentences in the same language, such that $\Psi$ is true in $F$ if and only if $\Psi^*$ is true in $F$. Moreover, this boolean combination $\Psi^*$ does not depend on $p$.*

We are very thankful to V. Remeslennikov and E. Rips for numerous discussions. In 1991–1992 V. Remeslennikov suggested a new approach for finding a system of axioms for the elementary theory $Th(F)$. In 1995, in several talks in New York and Montreal, E. Rips acquainted the authors with some methods due to Yu. Merzlyakov and G. Makanin and also with an interesting scheme for eliminating quantifiers for arbitrary formulas in free groups to obtain Diophantine formulas. We used a different approach, but it seems that the methods presented here might help to carry out their projects.

We also would like to mention that in our research we made use of the software package "Magnus" developed at CCNY of CUNY (which can be found on their home page at http://zebra.sci.ccny.cuny.edu/web ). This software enabled us to solve some awkward equations over free groups and henceforth to find particular embeddings of some groups into $F^{Z[t]}$.

## References

[1] K. I. Appel, *One-variable equations in free groups*, Proc. Amer. Math. Soc. **19** (1968), 912–918. MR **38:**1149

[2] G. Baumslag, A. Myasnikov, and V. Remeslennikov, *Algebraic geometry over groups*, 1996, submitted to Invent. Math., 1998.

[3] G. Baumslag, *On generalised free products*, Math. Zeitschr. **78** (1962), 423–438. MR **25:**3980

[4] R. Bryant, *The verbal topology of a group*, Journal of Algebra **48** (1977), 340–346. MR **56:**12131

[5] C. C. Chang and H. J. Keisler, *Model theory*, North-Holland, London and New York, 1973. MR **53:**12927

[6] L. P. Comerford jr. and C. C. Edmunds, *Quadratic equations over free groups and free products*, Journal of Algebra **68** (1981), 276–297. MR **82k:**20060

[7] ———, *Solutions of equations in free groups*, Walter de Gruyter, Berlin and New York, 1989. MR **90a:**20067

[8] Yu. L. Ershov and E. A. Palutin, *Mathematical logic*, Walter de Gruyter, Berlin and New York, 1989. MR **88i:**03002

[9] R. I. Grigorchuk and P. F. Kurchanov, *Some questions of group theory connected with geometry*, Algebra, 7, Itogi Nauki i Tekhniki, VINITI AN SSSR, Moscow, 1989. (Russian) MR **92e:**20002

[10] ———, *On quadratic equations in free groups*, Contemp. Math., vol. 131 (1), pp. 159–171, Amer. Math. Soc., Providence, RI, 1992. MR **94m:**20074

[11] V. Guba, *Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems*, Mat. Zametki **40** (1986), 321–324. (Russian) MR **88d:**20060

[12] A. Hoare, A. Karrass, and D. Solitar, *Subgroups of finite index of Fuchsian groups*, Math. Z. **120** (1971), 289–298. MR **44:**2837

[13] ———, *Subgroups of infinite index of Fuchsian groups*, Math. Z. **125** (1972), 59–69. MR **45:**2029

[14] O. Kharlampovich and A. Myasnikov, *Irreducible affine varieties over a free group. 1: Irreducibility of quadratic equations and Nullstellensatz*, J. of Algebra **200** (1998), 472–516. CMP 98:09

[15] ———, *Irreducible affine varieties over a free group. 2: Systems in triangular quasi-quadratic form and description of residually free groups*, J. Algebra **200** (1998), 517–570. CMP 98:09

[16] A. A. Lorenc, *The solution of systems of equations in one unknown in free groups*, Dokl. Akad. Nauk SSSR **148** (1963), 262–266. (Russian) MR **32:**1285

[17] R. C. Lyndon, *The equation $a^2b^2 = c^2$ in free groups*, Michigan Math. J. **6** (1959), 155–164. MR **21:**1999

[18] ———, *Equations in free groups*, Trans. Amer. Math. Soc. **96** (1960), 445–457. MR **27:**1488

[19] ———, *Groups with parametric exponents*, Trans. Amer. Math. Soc. **96** (1960), 518–533. MR **27:**1487

[20] ———, *Length functions in groups*, Math. Scand. **12** (1963), 209–234. MR **29:**1246

[21] ———, *Equations in groups*, Bol. Soc. Bras. Mat. **11** (1980), 79–102. MR **82j:**20070

[22] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Springer, Berlin and New York, 1977. MR **58:**28182

[23] G. S. Makanin, *Decidability of the universal and positive theories of a free group*, Izv. Akad. Nauk SSSR, Ser. Mat., **48(1)** (1985), 735–749; English transl. in Math. USSR Izv. **25** (1985). MR **86c:**03009

[24] ———, *Equations in a free group*, Izv. Akad. Nauk SSSR, Ser. Mat., **46** (1982), 1199–1273; English transl. in Math. USSR Izv. **21** (1983). MR **84m:**20040

[25] A. I. Mal'tsev, *On some correspondence between rings and groups*, Mat. Sbornik **50** (1960), 257–266. (Russian) MR **22:**9448

[26] Yu. I. Merzlyakov, *Positive formulae on free groups*, Algebra i Logika **5(4)** (1966), 25–42. (Russian) MR **36:**5201

[27] A. G. Myasnikov and V. N. Remeslennikov, *Exponential groups 2: Extension of centralizers and tensor completion of csa-groups*, Interntional Journal of Algebra and Computation **6(6)** (1996), 687–711. MR **97j:**20039

[28] B. Plotkin, *Varieties of algebras and algebraic varieties. Categories of algebraic varieties*, Preprint, Hebrew University, Jerusalem, 1996.

[29] W. Quine, *Concatenation as a basis for arithmetic*, J. of Symb. Logic **11** (1946), 105–114. MR **8:**307b

[30] A. Razborov, *On systems of equations in a free group*, Math. USSR Izvestiya **25(1)** (1985), 115–162. MR **86c:**20033

[31] ———, *On systems of equations in a free group*, PhD Thesis, Steklov Math. Institute, Moscow, 1987.

[32] ———, *On systems of equations in free groups*, Combinatorial and geometric group theory (Edinburgh, 1993), pp. 269–283, Cambridge University Press, 1995. MR **96c:**20039

[33] V. N. Remeslennikov, *$\exists$-free groups*, Siberian Math. J. **30** (1989), 998–1001. MR **91f:**03077

[34] G. S. Sacerdote, *Elementary properties of free groups*, Trans. of the AMS **178** (1973), 127–138. MR **47:**8686

[35] W. Szmielew, *Elementary properties of Abelian groups*, Fund. Math. **41** (1955), 203–271. MR **17:**233e

[36] J. R. Stallings, *Finiteness properties of matrix representations*, Ann. Math. **124** (1986), 337–346. MR **88b:**20105

Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. West, Montreal, QC, Canada H3A 2K6
*E-mail address*: olga@Math.McGill.CA

Department of Mathematics, City College, Convent Ave. & 138th St., New York, NY 10031
*E-mail address*: Alexei@rio.sci.ccny.cuny.edu