On Systems of Equations in Free Groups

Alexander A. Razborov
Steklov Mathematical Institute
Vavilova 42, 117966, GSP–1, Moscow, RUSSIA

Abstract

The main purpose of this presentation is to introduce non-specialists into recent developments in the study of systems of equations in free groups and, at a very intuitive level, into the related techniques.

0.1 Introduction

The most important class of algebraic systems for which the question of the algorithmic decidability of their elementary theories was left open after the remarkable breakthrough in the area achieved in the 60's, is the class of free groups. It is also open whether the elementary theories of non-abelian free groups with different number of generators coincide or not; both these questions are usually attributed to Tarski.

The natural approach to these questions is to begin with first-order formulae from a restricted class. The simplest nontrivial class is made by existential formulae i.e. those of the form

$$\exists x_1 \ldots \exists x_n \; A(x_1, \ldots, x_n), \tag{0.1}$$

where A is open. And it turns out that even for this class Tarski's first problem becomes very hard, and the second becomes non-trivial.

In fact, if we additionally require the formula A in (0.1) to be positive (that is to contain no negations) then already this case bears all the difficulties of the case of arbitrary existential formulae (see e.g. [20]). And, with this additional requirement, the formula (0.1) is equivalent to a finite disjunction of systems of equations in free groups. The latter objects are the main target of this presentation.

The two natural questions about systems of equations in free groups are:

(i) *Is it algorithmically decidable whether a given system has at least one solution?*
(ii) *How to describe the solution set?*

Both these questions have been answered in affirmative by now. The machinery involved in settling them is, however, extremely complicated. In this presentation we try to explain it at a very rough and intuitive level.

The paper is organized as follows. Section 0.2 contains necessary definitions. In Section 0.3 we address Question (i), and in Section 0.4 – Question (ii).

The reader who has got that far will undoubtedly have been convinced in the extreme importance of so-called quadratic equations for the whole theory. In Section 0.5 we present a result which indicates that those equations make a proper hierarchy. An informal implication of this is that one can not hope to get a drastic simplification of the description from Section 0.4.

The paper is concluded with a brief overview in Section 0.6.

0.2 Notations and Definitions

We will denote the free group with basis $x_1, \ldots, x_n$ by $\langle x_1, \ldots, x_n \rangle$. The symbol $=$ will stand for the group equality, and $A_1 \ldots A_r \mathrel{\overset{\circ}{=}} B_1 \ldots B_s$, by definition, will mean that both left- and right-hand sides are reduced and equal to each other. $\partial\,(A)$ is the length of the word A.

Vectors of letters like $\phi_1, \ldots, \phi_m$ or $X_1, \ldots, X_n$ etc. will be denoted by $\bar{\phi}, \bar{X}, \ldots$ When we need to consider simultaneously several vectors of the same type, we use superscripts: $\bar{X}^{(1)}, \ldots, \bar{X}^{(h)}, \ldots$

We fix the following group alphabets:

$$\Sigma_0 \rightleftharpoons \{x_1, \ldots, x_n, \ldots, x_1^{-1}, \ldots, x_n^{-1}, \ldots\} \quad - \quad \text{the alphabet of } \textit{variables},$$

$$\Sigma_1 \rightleftharpoons \{a_1, \ldots, a_\omega, \ldots, a_1^{-1}, \ldots, a_\omega^{-1}, \ldots\} \quad - \quad \text{the alphabet of } \textit{coefficients}.$$

Let F_0 and F_1 be free groups with the set of generators Σ_0, Σ_1 respectively. A *system of equations in a free group* is a system of equalities of the form

$$\left\{ \begin{array}{c} \phi_1(\bar{x}, \bar{a}) = 1, \\ \cdots \\ \phi_m(\bar{x}, \bar{a}) = 1, \end{array} \right. \tag{0.2}$$

where $\phi_1, \ldots, \phi_m$ are words over $\Sigma_0 \cup \Sigma_1$. A system is *trivial* if all its equations have the form $1 = 1$. A system is *coefficient-free* if its equations do not contain coefficients. A *solution* of the system (0.2) is a vector $\bar{X} \in F_1$ such that $\phi_i(\bar{X}, \bar{a}) = 1$ for all $1 \leq i \leq m$. We denote by $\mathrm{Sol}(\bar{\phi})$ the set of all solutions of the system (0.2).

The *length* of a solution $\bar{X} = (X_1, \ldots, X_n)$ [of a system $\bar{\phi} = (\phi_1, \ldots, \phi_m)$] is $\partial\left(\bar{X}\right) \rightleftharpoons \sum_{i=1}^{n} \partial\,(X_i)$ $[\partial\left(\bar{\phi}\right) \rightleftharpoons \sum_{i=1}^{m} \partial\,(\phi_i)$, respectively]. A solution $\bar{X}$ of a system $\bar{\phi}$ is *minimal* if $\partial\left(\bar{X}\right) \leq \partial\left(\bar{X}'\right)$ for every $\bar{X}' \in \mathrm{Sol}(\bar{\phi})$. Obviously, any system which has at least one solution, also has a minimal solution.

A system is *quadratic* if every variable which occurs in the system, occurs there exactly twice. It is very easy to see that quadratic systems can always be reduced to single quadratic equations. However, for the sake of uniformity, we often will prefer to talk of arbitrary quadratic systems rather than of single equations.

0.3 Algorithmic Decidability

The algorithm for deciding whether $\mathrm{Sol}(\bar{\phi}) = \emptyset$ was given by Makanin [19, 20]†. It is appropriate, however, to give a short survey of preceding results before elucidating some ideas of that work.

The case of quadratic equations is easy. All the necessary ideas for solving this case can be extracted already from [8, 22] and [10, Sections 1.6, 1.7].

Lyndon [9] constructed an algorithm for solving equations in one variable, and Lorents [17] noticed that his algorithm can also be applied to *systems* of equations in one variable.

Khmelevskiĭ [28, 29] established the algorithmic decidability for systems in which every equation contains at most two variables and, moreover, has either the form $\phi(x, \bar{a}) = \psi(y, \bar{a})$ or $W(x, y) = A(\bar{a})$, where all letters which may appear in ϕ, ψ, W, A are explicitly displayed. Ozhigov [24] was able to handle equations in two variables.

As we mentioned above, the algorithm for solving arbitrary systems in free groups was given by Makanin [19, 20].

In fact, all these results (with the important exception [9, 17]) use the same idea of simplifying the pair $(\bar{\phi}, \bar{X})$, where $\bar{X} \in \mathrm{Sol}(\bar{\phi})$ by applying to $\bar{\phi}$ some elementary transforms. It is the kind of allowed transforms and the requirements on the arrangement of equations in the systems which make the difference between different approaches. In this paper, however, we consider things only at a very intuitive level, and the easiest way to explain the basic idea is to start with the toy-like case of quadratic systems.

So, assume that we have a non-trivial quadratic system

$$\bar{\phi}(x_1, \ldots, x_n, a_1, \ldots, a_\omega),$$

and imagine for a moment that $\bar{X}$ is its solution. As $\bar{\phi}\left(\bar{X}, \bar{a}\right) = 1$, the vector $\left(\bar{X}, \bar{a}\right)$ is *not* Nielsen reduced and hence can be simplified by an

† the original proof in [19] contained a gap shortly after fixed in [20]

elementary Nielsen transformation. This transformation may have one of the following forms:

$$X_i \text{ is crossed out since } X_i = 1, \tag{0.3}$$

$$X_i^\epsilon \longrightarrow X_i^\epsilon U, \tag{0.4}$$

where $U \in \left\{X_1^{\pm 1}, \ldots, X_n^{\pm 1}, a_1^{\pm 1}, \ldots a_\omega^{\pm 1}\right\}$. What is important, in case (0.4) the transformation is *attached to* the system $\bar{\phi}$ (cf. [10, Section 1.6]) that is $x_i^\epsilon u$ is a subword of one of its equations. Here $u = U$ if $U \in \Sigma_1$ and $u = x_j^\delta$ if $U = X_j^\delta$. Denote by $\left(\bar{X}', \bar{a}\right)$ the vector resulted from this transformation.

Let $\bar{\phi}'(\bar{x}', \bar{a})$ be the system obtained from $\bar{\phi}$ by the substitution $x_i \longrightarrow 1$ in case (0.3), and by the substitution $x_i^\epsilon \longrightarrow x_i^\epsilon u^{-1}$ in case (0.4). Then $\bar{X}'$ is its solution.

Let's now forget about the imaginary solution $\bar{X}$ and see what we can do without it. We still can apply to $\bar{\phi}$ all elementary transformations (0.3) and those transformations (0.4) which are attached to it. This results in a list of systems

$$\bar{\phi}^{(1)}(\bar{x}^{(1)}, \bar{a}) = 1, \ldots, \bar{\phi}^{(r)}(\bar{x}^{(r)}, \bar{a}) = 1$$

and group homomorphisms

$$\pi_1 : \langle \bar{x}, \bar{a} \rangle \longrightarrow \langle \bar{x}^{(1)}, \bar{a} \rangle, \ldots, \pi_r : \langle \bar{x}, \bar{a} \rangle \longrightarrow \langle \bar{x}^{(r)}, \bar{a} \rangle$$

such that $\pi_i(a_j) = a_j$ and

$$\mathrm{Sol}(\bar{\phi}) = \bigcup_{i=1}^{r} \left\{ \pi_i(\bar{X}^{(i)}) \;\middle|\; \bar{X}^{(i)} \in \mathrm{Sol}(\bar{\phi}^{(i)}) \right\}. \tag{0.5}$$

Here $\pi_i \left(\bar{X}^{(i)}\right)$ means that we interpret $\bar{X}^{(i)}$ as a homomorphism

$$\langle \bar{x}^{(i)}, \bar{a} \rangle \longrightarrow F_1$$

and compose this with π_i to get a vector $\bar{X}$.

The effective transforms of one system $\bar{\phi}$ into a finite set of systems $\bar{\phi}^{(1)}, \ldots, \bar{\phi}^{(r)}$ with the characteristic property (0.5) is the core of almost all known approaches. This is what we called above *elementary transforms*; (0.5) basically means that we have reduced the system $\bar{\phi}$ to $\bar{\phi}^{(1)}, \ldots, \bar{\phi}^{(r)}$.

We can iterate the elementary transforms and get a tree (see Figure 0.1).

Now we once again bring in consideration a solution $\bar{X}$ and note that the elementary Nielsen transformations can not be applied to $\left(\bar{X}, \bar{a}\right)$

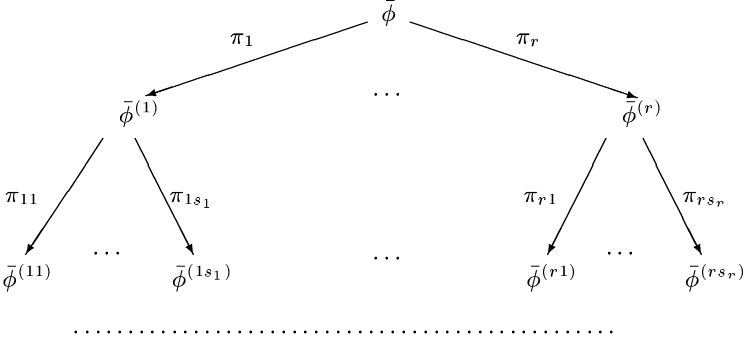

Fig. 0.1. The tree made of elementary transforms

forever. Instead, they terminate at some point, and the only way it may happen is when we arrive at a trivial system. This means that $\mathrm{Sol}(\bar{\phi}) \neq \emptyset$ *if and only if the tree on Figure 0.1 contains a trivial system.* The main problem (which, once again, is characteristic) is that this tree is in general infinite.

The remedy in the case of quadratic systems is very simple. Namely, $\partial\left(\bar{\phi}^{(i)}\right) \leq \partial\left(\bar{\phi}\right)$. This is obvious for singular transformations $x_i \longrightarrow 1$, and if we apply a regular transformation $x_i^\epsilon \longrightarrow x_i^\epsilon u^{-1}$ attached to $\bar{\phi}$ then the length indeed increases by two but then it is restored to at least its original value as $u^{-1}u$ gets canceled. Hence the tree on Figure 0.1 in fact contains only finitely many different systems, and the algorithm for solving $\bar{\phi}$ looks as simple as that.

Start constructing the tree crossing out all repetitions of the same system (the subtrees rooted at such systems are isomorphic so we may consider only one of them). When the process is over, look at the result. The original system $\bar{\phi}$ has at least one solution if and only if the tree contains at least one trivial system.

For the general case this naive approach immediately breaks apart. We can not guarantee any longer that the tree contains only finitely many different systems, hence we do not have a weapon against the potential infinity. In later works this is circumvented by a much more careful choice of the class of systems, their solutions, elementary transforms etc. allowed in the tree. Let us briefly sketch along these lines some ideas from the culminating work of Makanin [19, 20].

The first step (which is very easy) is to reduce our original system

$\bar{\phi}(\bar{x}, \bar{a})$ to finitely many systems of the form

$$\begin{cases} \psi_1(\bar{x}, \bar{a}) \circeq \theta_1(\bar{x}, \bar{a}), \\ \quad\quad \cdots \\ \psi_u(\bar{x}, \bar{a}) \circeq \theta_u(\bar{x}, \bar{a}). \end{cases} \tag{0.6}$$

This is done simply by writing down all possible ways in which the words $\phi_i\left(\bar{X}, \bar{a}\right)$ may get canceled.

The next step is to arrange the resulted systems (0.6) into a special form which Makanin, somewhat ironically, called *generalized equations*. We omit the exact definition.

Then we (similarly to the case of quadratic systems but in a much more sophisticated way) define elementary transforms for generalized equations so that the analogue of the crucial property (0.5) still takes place. These elementary transforms are designed to control as many parameters of generalized equations as possible, like Nielsen elementary transformations controlled the length of the quadratic systems.

Next we construct the analogue of the tree on Figure 0.1. Makanin's elementary transforms never increase the length of the solution, and those transforms which preserve it can be applied along any branch only finitely often. Which means that, once again, $\mathrm{Sol}(\bar{\phi}) \neq \emptyset$ iff the tree contains the trivial generalized equation.

The problem with the potential infinity of the tree is this time much more elaborate. We still can cross out the repetitions in the tree but what remains still may contain infinite branches along which generalized equations get more and more complicated. Makanin showed, however, that if the original solution $\bar{X}$ was *minimal* then it is possible to find a *recursive* bound on the number of elementary transforms leading from $\left(\bar{\phi}, \bar{X}\right)$ to the trivial generalized equation. One of the crucial properties of minimal solutions necessary (but not sufficient) for this purpose is the following Bulitko's Lemma [15]: *if* $(X_1, \ldots, X_n)$ *is a minimal solution of a system* $\bar{\phi}$ *then* X_i *may not contain* $P^{\gamma(\bar{\phi})}$ *as a subword, where* P *is non-empty and* $\gamma(\bar{\phi})$ *is an explicit integer-valued recursive function.* If we are interested only in the *solvability* of the system $\bar{\phi}$, it is good enough, and we can terminate the construction of the tree at a point which is specified by a *recursive* function given in advance.

We conclude this section with a brief survey of known partial results related to Tarski's problems.

For the second problem (that is whether the elementary theories of non-abelian free groups with different number of generators coincide or not) the strongest results were obtained by Merzlyakov [23] and Sacerdote [13]. Namely, Merzlyakov showed that the set of positive formulae which are true on a non-abelian free group is indeed independent of its rank. Sacerdote established the same thing for the class of $\forall \dots \forall \exists \dots \exists$-formulae that is for formulae of the form

$$\forall x_1 \dots \forall x_n \exists y_1 \dots \exists y_m \ A(x_1, \dots, x_n, y_1, \dots, y_m)$$

with A open. These results do *not* use Makanin's technique.

Makanin's algorithm immediately gives raise to an algorithm recognizing the set of true positive existential formulae. Based upon ideas of Merzlyakov, Makanin [20] noticed that it can be also used for recognizing true formulae *either* from the class of positive formulae *or* from the class of existential formulae. The latter result was strengthened by him in [21], where the decidability for the class of $\forall \exists \dots \exists$-formulae was established (notice that we have here only *one* universal quantifier, not a block).

0.4 Description of the Solution Set

There are three known languages for describing $\mathrm{Sol}(\bar{\phi})$.

The first, logical language is based upon the notion of *parametric functions.* Very good examples are provided by Lyndon's parametric words [9] and Nielsen-Knmelevskiĭ function [28, 29]. Lyndon used his parametric words for describing the solution set of equations in one variable, and this description was extended to the case of one-variable systems and considerably simplified by Lorents [17]. The final result proved independently by Appel [1] and Lorents [18] says that for any such system $\bar{\phi}$,

$$\mathrm{Sol}(\bar{\phi}) = \bigcup_{i=1}^{h} \{ A_i B_i^{\mu} C_i \mid \mu \in \mathbf{Z} \}, \tag{0.7}$$

and this representation can be constructed effectively. Khmelevckiĭ [28, 29] proved that the solution set of those systems for which he established the algorithmic decidability (see Section 0.3) can be always represented in terms of Lyndon's parametric words and Nielsen-Khmelevskiĭ functions.

The second approach is that of *fundamental sequences* which was suggested in [25]. It has more algebraic flavour and is based upon the well-known observation that $\mathrm{Sol}(\bar{\phi})$ is actually isomorphic to the set of coefficient-preserving homomorphisms from $\mathrm{Hom}\left(H(\bar{\phi}), F_1\right)$. Here

$H(\bar{\phi})$ is the finitely presented group $\langle x_1, \ldots, x_n, a_1, \ldots, a_\omega \mid \phi_1(\bar{x}, \bar{a}) = 1, \ldots, \phi_m(\bar{x}, \bar{a}) = 1\rangle$. One advantage of this approach is that it allows us to combine into one scheme both the representation of $\mathrm{Sol}(\bar{\phi})$ and *the proof* that all vectors $\bar{X}$ obtained from this representation are indeed in $\mathrm{Sol}(\bar{\phi})$.

At this conference, however, the most appropriate language is geometric. Before we continue, let me stress that the differences between all three languages are actually very minor.

Once again, we begin with the case of quadratic equations. Let us once more consider the tree on Figure 0.1 but instead of removing repetitions in that tree, we factor it by the corresponding equivalence relation. Then we delete from the resulting finite graph all systems from which no paths lead to trivial systems (as follows from the discussion in the previous section, they do not have solutions anyway).

We end up with a finite directed graph whose nodes are marked with systems of equations in a free group, and every edge of the form

$$e : \bar{\phi}^{(1)}\left(\bar{x}^{(1)}, \bar{a}\right) \longrightarrow \bar{\phi}^{(2)}\left(\bar{x}^{(2)}, \bar{a}\right)$$

is marked by a coefficient-preserving homomorphism

$$\pi_e : \langle \bar{x}^{(1)}, \bar{a}\rangle \longrightarrow \langle \bar{x}^{(2)}, \bar{a}\rangle.$$

This graph has one input node marked by the original system $\bar{\phi}$, and all sink nodes are marked by trivial systems. The main property of this graph (compare with (0.5)) is that

$$\mathrm{Sol}(\bar{\phi}) = \left\{\pi_p\left(\bar{X}'\right) \mid p \text{ is a path from the input node to a sink node, and } \bar{X}' \text{ is an arbitrary vector}\right\}.$$

In connection with this, note that trivial systems usually have "dummy" variables, but their solution set is also trivial and consists of all possible vectors whatsoever. π_p is defined in the natural way.

A graph with this properties is called the *solution graph* for the system $\bar{\phi}$. In order to better understand its structure, we recall that two nodes u and v lie in the same *strong component* iff there exists a loop containing both of them. This is an equivalence relation, and, factoring by it the solution graph, we get an *acyclic* graph. Now, we can separate all I/O paths in the factor graph and come up with a tree. All this means that we can represent the solution graph as on Figure 0.2. Here $\bar{\phi}$ is the original system, $\bar{\psi}^{(1)}, \ldots, \bar{\psi}^{(h)}$ are all trivial, and circles correspond to strong components. Although it is not clear a priori, in all known constructions

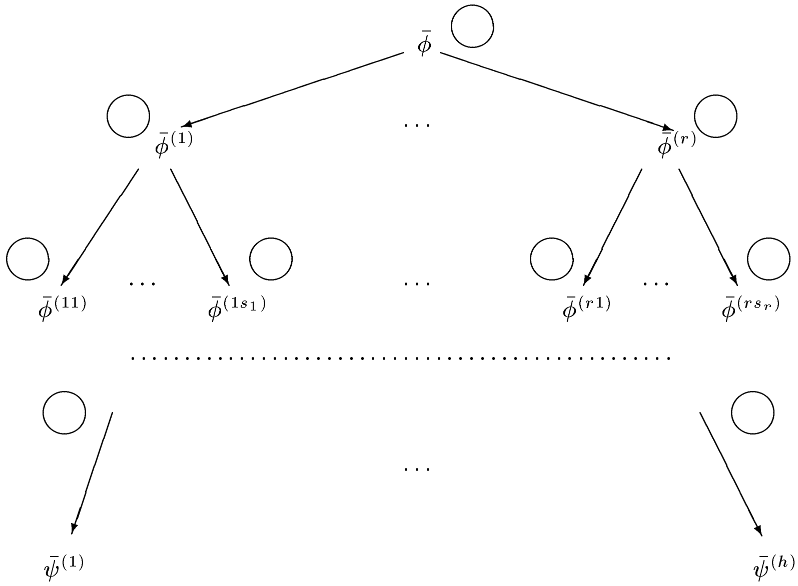

Fig. 0.2. The solution graph

the edges lying within a strong component can be inverted. Hence we may assume that every strong component consists of a single node, and that the set of all loops within that component possesses the group structure. Moreover, this group actually consists of automorphisms of a certain group $G(\bar{\phi})$ associated with the system $\bar{\phi}$ sitting at that node. This observation lies in the heart of the algebraic approach to describing $\mathrm{Sol}(\bar{\phi})$ mentioned at the beginning of this section.

Coming back to the case of quadratic equations, I want to mention a remarkable result proved independently by Comerford and Edmonds [3] and by Grigorchuk and Kurchanov [6] (some partial results in that direction were obtained in [8, 22, 14, 28, 29, 4, 11]). Namely, for that case the general picture on Figure 0.2 can be simplified as shown on Figure 0.3. Another way of stating their result is that, while transforming an arbitrary solution $\bar{X}$ along the tree on Figure 0.1, we can apply first a sequence of regular transforms (0.4) alone (this give us the circle on Figure 0.3) followed by a sequence of singular transforms (0.3).

Now we turn to the general case. Makanin's algorithm alone does not suffice since it essentially uses the minimality of the solution $\bar{X}$. This

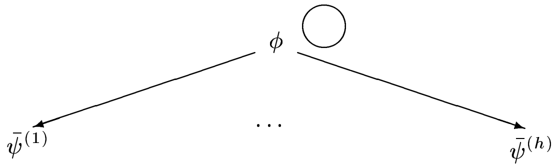

Fig. 0.3. The solution graph for quadratic equations

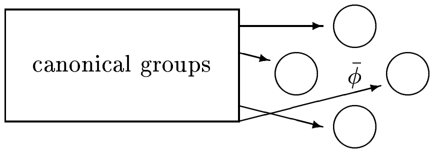

Fig. 0.4. The structure of strong components

difficulty was overcome in two steps by Razborov [25, 27]. The key idea is to bring into consideration transforms which are inverse to Makanin's elementary transforms. When we meet a situation which is not liked by Makanin's algorithm then, instead of the minimality assumption, we use a combination of original and inverse transforms in order to "shrink" our solution while retaining the generalized equation. A number of new difficulties arises on this way, e.g. the fact that inverse transforms may in general increase the length of the solution. All these difficulties are, however, tractable. The final result [27] says that for every system $\bar{\phi}$ we can effectively construct a finite solution graph describing $\mathrm{Sol}(\bar{\phi})$.

It is clear already from Figure 0.2 that it is the strong components which make the most essential part of this description (as this is the only place where the potential infinity comes in). And something can be additionally said about their structure. Namely, every strong component can be assumed to have the form as shown on Figure 0.4, where the petals correspond to so-called *canonical groups of automorphisms* [27] closely related to quadratic equations. We address the reader to [27, 16] for the precise definition and confine ourselves here to one typical example.

Assume that the system $\bar{\phi}$ on Figure 0.4 has the special form

$$\begin{cases} \bar{\psi}(\bar{z},\bar{a}) = 1 \\ \prod_{i=1}^{n} w_i^{-1} U_i(\bar{z},\bar{a}) w_i \cdot \prod_{j=1}^{g} [v_{2j-1}, v_{2j}] = U_0(\bar{z},\bar{a}). \end{cases} \tag{0.8}$$

Let P be the pointwise stabilizer of the set

$$\left\{u_1, \ldots, u_n, \prod_{i=1}^{n} w_i^{-1} u_i w_i \cdot \prod_{j=1}^{g} [v_{2j-1}, v_{2j}]\right\}$$

in $\mathrm{Aut}(\bar{u}, \bar{v}, \bar{w})$. Then every automorphism $\sigma \in P$ gives raise, in a natural way, to an automorphism $\sigma' \in \mathrm{Aut}(\bar{a}, \bar{z}, \bar{v}, \bar{w})$ preserving $\bar{a}, \bar{z}$ and the equations of the system (0.8). We take a finite system of generators $\sigma_1, \ldots, \sigma_\ell$ of P (it can be found effectively e.g. by the general result of McCool, see [10, Chapter 1.6]) and form one petal on Figure 0.4 by including to it ℓ edges marked $\sigma_1', \ldots, \sigma_\ell'$.

Very loosely speaking, the result from [25, 27] reduces arbitrary systems of equations in a free group to a finite number of auxiliary *quadratic* equations. One application of this result was given in [25], namely the solution of the so-called rank problem: the rank of a coefficient-free system of equations in a free group is algorithmically computable. Here the *rank* of a system is, by definition, the maximal possible rank of subgroups generated by its solutions. Some of the techniques from [27] were also useful in the study of group actions on $\mathbf{R}$-trees (see [2, 5]).

0.5 The Hierarchy of Quadratic Equations

In view of the description given in the previous section, it is important to study quadratic equations in a free group. Another good reason for this is their close connection to the Poincaré Conjecture (see e.g. [10, Section 4.4] or [16, §2.2]). One natural question is whether their hierarchy is proper or, more generally, isn't it possible to start with a *finite* number of *arbitrary* systems $\bar{\phi}^{(1)}, \ldots, \bar{\phi}^{(\ell)}$ so that for any other system $\bar{\phi}$, $\mathrm{Sol}(\bar{\phi})$ can be "decomposed" on the base of $\mathrm{Sol}\left(\bar{\phi}^{(1)}\right), \ldots, \mathrm{Sol}\left(\bar{\phi}^{(\ell)}\right)$. The intuitive answer is "no". The proof, however, is a more complicated story, and it was given in [12] (this result was originally announced in [26]).

For the purposes of this section the geometric language becomes somewhat awkward and does not let us to formulate the result in its full generality. So, we switch to the more general language of parametric functions.

Fix one more group alphabet

$$\Sigma_2 \rightleftharpoons \{u_1, \ldots, u_n, \ldots, u_1^{-1}, \ldots, u_n^{-1}, \ldots\}$$

of *free word variables.* Let $P^{(1)}, P^{(2)}, \ldots, P^{(m)}, \ldots$ be some sets of absolutely arbitrary nature. We associate with each $P^{(i)}$ countably many *parameter variables* $p_1^{(i)}, \ldots, p_k^{(i)}, \ldots$

A *parametric function of rank* r is an arbitrary mapping

$$F(p_1^{(i_1)}, \ldots, p_l^{(i_l)}) : P^{(i_1)} \times \cdots \times P^{(i_l)} \longrightarrow \{u_1^{\pm 1}, \ldots, u_r^{\pm 1}\}^*.$$

We can think alternatively of F as of the mapping

$$F : P^{(i_1)} \times \cdots \times P^{(i_l)} \times \underbrace{\Sigma_1^* \times \cdots \times \Sigma_1^*}_{r} \longrightarrow \Sigma_1^* \tag{0.9}$$

which takes $\boldsymbol{p}_1^{(i_1)} \in P^{(i_1)}, \ldots, \boldsymbol{p}_l^{(i_l)} \in P^{(i_l)}$ and $U_1, \ldots, U_r \in \Sigma_1^*$ to the result of substituting into $F(\boldsymbol{p}_1^{(i_1)}, \ldots, \boldsymbol{p}_l^{(i_l)})$ the words $U_1, \ldots, U_r$ for the free word variables $u_1, \ldots, u_r$. We consider F as a function symbol $F(p_1^{(i_1)}, \ldots, p_l^{(i_l)}, u_1, \ldots, u_r)$ in the first order many-sorted logic with the interpretation provided by (0.9).

Given a family $\mathcal{L}$ of parametric functions, we define *parametric terms over* $\mathcal{L}$ merely as those terms in the many-sorted signature $\langle \Sigma_1, ^{-1}, \cdot, \mathcal{L} \rangle$ which take values in Σ_1^*. See [12] for more details.

Let now $\bar{\phi}(x_1, \ldots, x_n, \bar{a})$ be a system of equations, and $T_i^{(j)}(\bar{p}, \bar{u})$ $(1 \leq i \leq n,\ 1 \leq j \leq h)$ be a matrix of parametric terms over some $\mathcal{L}$. We say that this matrix *represents* $\mathrm{Sol}(\bar{\phi})$ *over* $\mathcal{L}$ if

$$\left\{ \bar{T}^{(j)} \left(\bar{\boldsymbol{p}}, \bar{U} \right) \,\middle|\, 1 \leq j \leq h,\ \boldsymbol{p}_k^{(\nu)} \in P^{(\nu)},\ \bar{U} \in \Sigma_1^* \right\} = \mathrm{Sol}(\bar{\phi}).$$

The connection with the geometric language from the previous section is clear. If we have a solution graph represented as on Figure 0.2, then for every internal node marked by $\bar{\phi}'(x_1, \ldots, x_r, a_1, \ldots, a_\omega) = 1$ we introduce the parametric functions

$$F_1(p, u_1, \ldots, u_{r+\omega}), \ldots, F_r(p, u_1, \ldots, u_{r+\omega}),$$

where p runs over the fundamental group of the corresponding strong component. Namely, $F_i(p, u_1, \ldots, u_{r+\omega})$ is the result of substituting into $\pi_p(x_i)$ letters $u_1, \ldots, u_{r+\omega}$ for $x_1, \ldots, x_r, a_1, \ldots, a_\omega$. Then for every leaf $\bar{\psi}^{(j)}$ in the tree we can define parametric terms $\bar{T}^{(j)}(\bar{p}, u_1, \ldots, u_{r_j})$ representing exactly those solutions which terminate at $\bar{\psi}^{(j)}$. The free word variables $u_1, \ldots, u_{r_j}$ are in one-to-one correspondence with the set of (dummy) variables of $\bar{\psi}^{(j)}$.

Of course, the definition of parametric functions is quite general. For example, if we have the canonical coefficient-free equation

$$\prod_{i=1}^{g} [x_i, y_i] = 1 \tag{0.10}$$

then it is very easy to represent its solution set by parametric functions of rank g. We merely enumerate all its solutions in $< u_1, \ldots, u_g >$.

However, being not quite adequate for positive results, this language is perfect to state the following theorem:

Theorem 0.5.1 *Let $g \geq 3$. Then the solution set of the equation* (0.10) *cannot be represented over the language consisting of* **all** *parametric functions of rank at most* $(g-1)$.

As a corollary, we obtain that no *finite* language $\mathcal{L}$ suffices to represent the solution set of all canonical quadratic equations (0.10).

As we noticed in the beginning of this section, this result is not unexpected. In fact, the main motivation for pursuing the proof was to see which kind of techniques do we need to prove things like that. We conclude this section with mentioning one concept discovered on this way as it may be of independent interest.

The following hierarchy $\mathcal{H}(d, r)$ of words over Σ_2 lies in the heart of the proof:

$$\mathcal{H}(0, r) \rightleftharpoons \Sigma_2,$$
$$\mathcal{H}(d+1, r) \rightleftharpoons \cup \{ \mathrm{Gp}(A_1, \ldots, A_r) \mid A_1, \ldots, A_r \in \mathcal{H}(d, r) \}.$$

The members of this hierarchy majorize the sets of values of parametric terms. And what we basically need for the proof is to establish "lower bounds" for it that is to show that some explicit words do not belong to certain members of this hierarchy. Such a machinery is indeed developed in [12].

0.6 Discussion and Open Problems

As in the previous sections, we begin with the case of quadratic equations. Here the situation is rather well understood, and the results from [3, 6] mentioned in Section 0.4 show that studying quadratic equations (or systems) is in fact more or less equivalent to studying mapping class groups of 2-manifolds. Of course, the latter area is still rich in important open problems, but this is already another story.

Turning to the general case, it should be noticed first that Makanin's algorithm is of purely existential nature. Indeed, Kościelski and Pacholsky [7] noticed that it is not even primitively recursive. This would be extremely interesting to reduce the complexity of the algorithm or (which, to my feeling, is the problem of the same sort) to become able to apply it to at least some concrete interesting systems.

Now, disregarding the complexity questions, the problem of describing $\mathrm{Sol}(\bar{\phi})$ for arbitrary $\bar{\phi}$ is reduced to solving finitely many auxiliary quadratic equations. I feel, however, that this reduction is incomplete since every strong component of the solution graph still may contain several "canonical petals" (see Figure 0.4). It would be very nice to show that actually only one such petal per node is sufficient. This would immediately imply that every system $\bar{\phi}$ can be reduced to a "triangular" system of quadratic equations. I feel that this question might be solved by refining the technique from [27].

Turning to Tarski's first problem, the next interesting class of formulae to be considered is made by $\forall\ldots\forall\exists\ldots\exists$-formulae. As we noticed in Section 0.3, Makanin solved the partial case when there is only one universal quantifier. Attempts to generalize his result to a sequence of universal quantifiers immediately lead to several natural questions about the description of $\mathrm{Sol}(\bar{\phi})$. One of them was already mentioned in the previous paragraph. Another natural thing to ask along these lines is the following.

Can we assume that the number of dummy (= free word) variables in every trivial system appearing in the solution graph is strictly less than the number of variables in the original system (unless the latter is itself trivial)? Note for comparison that it is true for systems in one variable, that is the Lyndon-Lorents description (0.7) does not involve free word variables. It is this circumstance which allowed Makanin to solve the case with one universal quantifier. If the conjecture above is true then for the case of arbitrary $\forall\ldots\forall\exists\ldots\exists$-formulae we might try to apply induction on the number of universal quantifiers.

An upper bound on the number of free word variables was noticed in [27] but it is only quadratic and, which is worse, is given in terms of the *length* of $\bar{\phi}$, not in terms of the number of variables. Somewhat curiously, the main problem with resolving this conjecture lies in the obvious transition from the original system to (0.6) since we apparently must introduce new variables for pieces resulting from the process of cancellation.

0.7 Acknowledgement

This work was supported by the grant # 93-011-16015 of the Russian Foundation for Fundamental Research.

Bibliography

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

[2] M. Bestvina and M. Feighn. Stable actions of groups on real trees. Manuscript, 1992.

[3] L. P. Comerford and C. C. Edmunds. Solutions of equations in free groups. In *Group Theory, Proceedings of the Singapore Group Theory Conference held at the National University of Singapore, June* 8-19,1987, pages 347–356. Walter de Gruyter, 1989.

[4] M. Culler. Using surfaces to solve equations in free groups. *Topology*, 20:133–145, 1981.

[5] D. Gaboriau, G. Levitt and F. Paulin. Pseudogroups of isometries and Rips' theorem on free actions on **R**-trees. Manuscript, 1992.

[6] R. I. Grigorchuk and P. F. Kurchanov. On quadratic equations in free groups. *Contemporary Mathematics*, 131:159–171, 1992. (Part 1).

[7] A. Kośćielski and L. Pacholski. Complexity of unification in free groups and free semi-groups. In *Proceedings of the* 31*st IEEE FOCS*, pages 824–829, 1990.

[8] R. C. Lyndon. The equation $a^2b^2 = c^2$ in free groups. *Michigan Math. J.*, 6:89–95, 1959.

[9] R. C. Lyndon. Equations in free groups. *Trans. Amer. Math. Soc.*, 96:445–457, 1960.

[10] R. C. Lyndon and P. E. Shupp. *Combinatorial Group Theory.* Springer-Verlag, New York/Berlin, 1977. рус. пер.: Р. Линдон, П. Шупп, Комбинаторная теория групп, М.: Мир, 1980.

[11] D. Piollet. Solutions d'une equation quadratique dans le groupe libre. *Discrete Math.*, 59:115–123, 1986.

[12] A. Razborov. On the parameterization of solutions for equations in free groups. *International Journal of Algebra and Computation*, 3:251-273, 1993.

[13] G. S. Sacerdote. Elementary properties of free groups. *Trans. Amer. Math. Soc.*, 178:127–138, 1972.

[14] H. Zieschang. Alternierende produkte in freien gruppen. *Abh. Math. Sem. Univ. Hamburg*, 27:13–31, 1964.

[15] В. К. Булитко. Об уравнениях и неравенствах в свободной группе и свободной полугруппе. *Ученые записки мат. кафедр. Тульский гос. пед. ин-т*, 2:242–253, 1970. V. K. Bulitko,

On equations and inequalities in a free group and in a free semigroup, *Proceedings of the math. dep. Tula State Institute for Elementary School*, 2(1970), 242-253.

[16] Р. И. Григорчук и П. Ф. Курчанов. Некоторые вопросы теории групп, связанные с геометрией. In *Итоги науки и техники. Современные проблемы математики, фундаментальные направления,* 58. ВИНИТИ, 1990. R. I. Grigorchuk and P. F. Kurchanov, Some Questions of Group Theory Related to Geometry, to appear in *EMS*, 58.

[17] А. А. Лоренц. Решение систем уравнений с одним неизвестным в свободных группах. *Докл. АН СССР*, 148(6):1253–1256, 1963. A. A. Lorenc, The solution of systems of equations in one unknown in free groups, *Soviet Math. Dokl.*, 4(1963), 262-266.

[18] А. А. Лоренц. О представлении множеств решений систем уравнений с одним неизвестным в свободных группах. *Докл. АН СССР*, 178(2):290–292, 1968. A. A. Lorenc, On the representation of solution sets of systems of equations with one unknown in a free group, *Soviet Math. Dokl.*, 9(1968).

[19] Г.С. Маканин. Уравнения в свободной группе. *Изв. АН СССР, сер. матем.*, 46(6):1199–1273, 1982. G. S. Makanin, Equations in a free group, *Math. USSR Izv.*, 21(1983), 483-546.

[20] Г. С. Маканин. Разрешимость универсальной и позитивной теорий свободной группы. *Изв. АН СССР, сер. матем.*, 48(4):735–749, 1984. G. S. Makanin, Decidability of universal and positive theories of a free group, *Math. USSR Izv.*, 1984.

[21] Г. С. Маканин. Об одном разрешимом фрагменте элементарной теории свободной группы. In С. И. Адян, editor, Вопросы кибернетики. Сложность вычислений и прикладная математическая логика, pages 103–114. ВИНИТИ, Москва, 1988. G. S. Makanin, On one decidable fragment of the elementary theory of a free group. In *Problems of Cybernetics. Complexity Theory and Applied Mathematical Logic*, ed.: S. I. Adian. Moscow, 1988, pages 103-114.

[22] А. И. Мальцев. Об уравнении $zxyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ в свободной группе. *Алгебра и логика*, 1(5):45–50, 1962. A. I. Malcev, On the equation $zxyx^{-1}y^{-1}z^{-1} = aba^{-1}b^{-1}$ in a free group, *Algebra i Logika*, 1, 45-50 (1962).

[23] Ю. И. Мерзляков. Позитивные формулы на свободных группах. *Алгебра и логика*, 5(4):25–42, 1966. Yu. I. Merzlyakov, Positive formulae over free groups, *Algebra i Logika*, 5(4):25-42 (1966).

[24] Ю. И. Ожигов. Уравнения с двумя неизвестными в свободной группе. *Докл. АН СССР*, 268(4):808–814, 1983. Yu. I. Ozhigov, Equations with two unknowns in a free group, *Soviet Math. Dokl.*, 27(1983).

[25] А. А. Разборов. О системах уравнений в свободной группе. *Изв. АН СССР, сер. матем.*, 48(4):779–832, 1984. A. A. Razborov, On systems of equations in a free group, *Math. USSR Izvestiya*, 25(1):115-162, 1985.

[26] А. А. Разборов. Об уравнениях в свободной группе, общие решения которых не представимы в виде суперпозиции

конечного числа параметрических функций. In *Тезисы 9 всесоюзного симпозиума по теории групп*, page 54, Москва, 1984. A. A. Razborov, An equation in a free group whose set of solutions does not allow a representation as a superposition of a finite number of parametric functions. In *Proceedings of the 9th All-Union Symposium on the Group Theory*, Moscow, 1984, p. 54.

[27] А. А. Разборов. О системах уравнений в свободной группе. PhD thesis, МГУ, 1987. A. A. Razborov, On systems of equations in a free group, Moscow State University, 1987.

[28] Ю. И. Хмелевский. Системы уравнений в свободной группе, I. *Изв. АН СССР, сер. матем.*, 35(6):1237–1268, 1971. Yu. I. Khmelevskiĭ, Systems of equations in a free group, *Math. USSR Izv.*, 5(1971).

[29] Ю. И. Хмелевский. Системы уравнений в свободной группе, II. *Изв. АН СССР, сер. матем.*, 36(1):110–179, 1972. Yu. I. Khmelevskiĭ, Systems of equations in a free group, *Math. USSR Izv.*, 6(1972).