*Submitted exclusively to the London Mathematical Society*
DOI: 10.1112/S0000000000000000

# FINITELY GENERATED GROUPS AND FIRST-ORDER LOGIC

A. MOROZOV, A. NIES

Abstract

We prove that the following classes of finitely generated (f.g.) groups have $\Pi^1_1$–complete first–order theories: all f.g. groups, the $n$–generated groups, and the strictly $n$–generated groups ($n \geqslant 2$). Moreover, all those theories are distinct. Similar techniques show that quasi-finitely axiomatizable (QFA) groups have a hyperarithmetical word problem, where a f.g. group is QFA if it is the only f.g. group satisfying an appropriate first–order sentence [8]. The Turing degrees of word problems of QFA groups form a cofinal set in the Turing degrees of hyperarithmetical sets.

Given a first order theory, two fundamental tasks are to determine its computational complexity and its expressivity. The *theory* $\mathrm{Th}(\mathcal{E})$ of a class $\mathcal{E}$ of groups is the set of first–order sentences which are true in all the members of $\mathcal{E}$. We determine the complexity for various theories $\mathrm{Th}(\mathcal{E})$. Our main results in this direction are:

- The theory $T$ of the class of finitely generated (f.g.) groups is $\Pi^1_1$-complete.
- For $n \geq 2$, the theories $T_n$ of all $n$-generated groups, and the theories $T^!_n$ of all strictly $n$-generated groups are $\Pi^1_1$-complete.

Here a group is *strictly $n$-generated* if it is $n$-generated but not $(n-1)$-generated. An example of a $\Pi^1_1$-complete set from arithmetic is the set of all sentences of the form $\forall X \phi(X)$ which hold in $\mathbb{N}$, for any $\Sigma_1$-formula $\phi$ involving the arithmetical operations and expressions "$t \in X$" for some term $t$. For another related example, the set of (indices for) recursive subtrees of $\omega^{<\omega}$ which have no infinite path is $\Pi^1_1$-complete. We first verify that all those theories are in $\Pi^1_1$. Then we prove that it is as hard as it could possibly be to determine whether a first–order sentence $\phi$ holds in all f.g. groups, and similarly for the other classes: the theories are $\Pi^1_1$-complete.

Theories of classes of groups and their complexity have been studied for a long time. A. Tarski [16] was the first to prove undecidability of the theory of groups in 1949. Many other results on decidability and undecidability of theories of classes of groups were obtained by A. I. Mal'cev and Yu. L. Ershov in the 1960's (see [17] for details and bibliography) and later. Szmielev [15] proved that the theory of all abelian groups is decidable, and O. Kharlampovich and A. Myasnikov announced that the theory of a free groups is decidable [3]. Other theories, while being undecidable, have a comparatively low complexity, like the theory of all groups, which is in $\Sigma^0_1$, or the theory of finite groups, which is in $\Pi^0_1$. Nies [8, Cor 5.5] showed that the theory of many classes of groups have the same complexity as true arithmetic $\mathrm{Th}(\mathbb{N}, +, \times)$, for example the class of finitely presented groups, or the class of f.g. groups of nilpotency class $c$ ($c \geq 2$ fixed). In one case the theory of a class of

---

2000 *Mathematics Subject Classification* 03D35 (primary), 03D40, 20A15, 20F10 (secondary).

The first author was partially supported by binational NSF grant DMS-0075899 and by RFBR (Russian Fund for Basic Research) grant No. 02-01-00593. The second author was partially supported by binational NSF grant DMS-0075899.

groups was shown to be $\Pi^1_1$–complete. A.S.Morozov proved this for the class of all subgroups of the group of computable permutations [6].

Fragments of theories have been considered as well. The universal theory of the f.p. groups is undecidable by the unsolvability of the word problem. Slobodskoi [14] showed that the universal theory of finite groups is undecidable.

Besides the complexity, one wants to determine the expressive power of first order theories. Kharlampovich and Myasnikov [3] also announced that all non-abelian free groups have the same first–order theory, thereby answering a long–open question of Tarski. The result was later confirmed by Sela [12]. This exposes a weakness in the expressiveness of first–order logic for free groups. On the other hand, Nies [8] shows that many natural classes of groups have distinct theories, for instance the classes of finite, finitely presented (f.p.), f.g., and of all groups (or, equivalently, all countable groups). In this paper we also show that all the theories $T, T_n$ and $T^!_n$ introduced above are distinct. Thus all the inclusions in the diagram below are proper:

$$\begin{array}{ccccccccccc} & & & & T^!_{n+1} & & T^!_n & & & & T^!_2 \\ & & & & \cup & & \cup & & & & \cup \\ T & \subset & \ldots & \subset & T_{n+1} & \subset & T_n & \subset & \ldots & \subset & T_2 \end{array}$$

The class of f.g. groups is very rich; for instance, it has uncountably many isomorphism types. Thus, at first sight it may seem that all consistent first-order properties of groups are already realized in a f.g. group. However, Kueker gave an example of a sentence which holds in the Prüfer group $\mathbf{C}_{2^\infty}$, but fails in any f.g. group (we thank G. Sabbagh for pointing out this example to us). The sentence expresses that the group is abelian, divisible by 2, and has an element of order 2. For the non-abelian case, in [8] Nies obtains a sentence which holds in Hall's universal locally finite group $H$ [2], the unique countable locally finite group which embeds every finite group and has the further property that any two isomorphic finite subgroups are conjugate. Nies shows that $H$, but no f.g. group, satisfies a first-order property related to definability with parameters of finite subsets in this group. By our result that $T$ is $\Pi^1_1$ complete, $T$ is, in fact, vastly different from the theory of all groups, which is merely $\Sigma^0_1$. The reason for this difference is that, if $G$ is f.g., we have a way to recognize standardness of a copy of $\mathbb{Z}$ which is coded within $G$ via first-order formulas with parameters. Consider a $\Pi^1_1$–complete set $A \subseteq \omega$ given by some condition

$$n \in A \Leftrightarrow \langle \mathbb{Z}, +, \times \rangle \models \forall X \, \varphi(n, X) \tag{0.1}$$

where $\varphi(n, X)$ is a first order formula in an appropriate language. For instance, let $\varphi(n, X)$ express that (under suitable encodings) the function encoded by $X$ is not a path on the $n$-th recursive subtree of $\omega^{<\omega}$. (We can ensure that $\varphi$ is $\Sigma_1$.)

*The concrete case.* For each $X \subseteq \omega$ we construct a group $G$, first-order encoding a model $\widetilde{G}$ including a copy $\widetilde{\mathbb{Z}}$ of $\langle \mathbb{Z}, +, \times \rangle$. Some elements of $G$ will encode the set $X$ (in what way will be described below). Here we make extensive use of permutation groups, refining methods from Morozov [6]. The groups $G$ are 2-generated permutation groups on $\mathbb{Z}$, and $\widetilde{G}$ is in fact a two-sorted model also including $G$ and its natural action on $\widetilde{\mathbb{Z}}$: $G$ "mirrors itself". In this way, we have the full expressive power of arithmetic to talk about our permutations within the language of $G$.

*The abstract case.* We also write a finite list of first-order axioms satisfied by each

$G_X$, in a way that, if an abstract group $G$ is f.g. and satisfies those axioms, then it can be viewed as a group $G_X$ for some $X$. Since we can require basic axioms of arithmetic and of the action in a first-order way, the main problem will be to ensure that the $\mathbb{Z}$-component of $\widetilde{G}$ is in fact a copy of the standard integers $\mathbb{Z}$. The principal non-technical idea of this paper is how to use being f.g. in order to achieve this (see details in the beginning of Section 2). Now we obtain a reduction of the set $A$ to $T$: $n \in A$ iff for all f.g. groups $G$ satisfying the axioms, an effective translation of $\phi$ into $\widetilde{G}$ holds.

The argument above proves in fact that $T \cap \Sigma_k$ is $\Pi^1_1$-complete for some $k$ (depending on the fixed collection of formulas we use to define $\widetilde{G}$).

In [8] Nies defined a f.g. group to be quasi-finitely axiomatizable (QFA) if it is the only *finitely generated* group satisfying an appropriate first–order sentence. He showed that the restricted wreath product $\mathbb{Z}_p \wr Z$ ($p$ any prime) and $\mathrm{UT}^3_3(\mathbb{Z})$ are QFA. Given classes $\mathcal{C} \subset \mathcal{D}$ of f.g. groups closed under isomorphism, a good way to separate their theories is to find a QFA group $H$ in $\mathcal{D} - \mathcal{C}$ (if $H$ is axiomatized by $\phi$, then $\neg\phi \in \mathrm{Th}(\mathcal{C}) - \mathrm{Th}(\mathcal{D})$. For instance, via $H = \mathbb{Z}_p \wr \mathbb{Z}$ he separates the theories of $\mathcal{C}$ ="f.p." from $\mathcal{D}$="f.g.". We will call this type of separation a *QFA-separation* of theories. Via permutation groups, we obtain many new examples of QFA-groups: there is a strictly $n$-generated QFA group with solvable word problem, for each $n \geq 3$ ($\mathbb{Z}_p \wr \mathbb{Z}$ does the case $n = 2$). This implies that most inclusions of theories in the diagram above can in fact be QFA-separated.

We also analyze the complexity of word problems: for each recursive ordinal $\alpha$, there is a QFA group whose word problem is Turing equivalent to $\varnothing^{(\alpha)}$. On the other hand, we prove each such word problem is hyperarithmetical (that is, Turing below some such iterate of the jump). Thus, we obtain a group theoretic characterization of hyperarithmetical sets: $X$ is hyperarithmetical iff $X \leq_T W$ for some word problem $W$ of a QFA group.

*Notation.* We use standard primitive recursive coding $s = \langle a_0, \ldots, a_{k-1} \rangle$ of sequences of natural numbers together with the primitive recursive predicate $\mathrm{seq}(x)$ which distinguishes numbers of sequences, the primitive recursive function $\mathrm{lh}(x)$ that gives the length of a sequence coded by $x$ if $\mathrm{seq}(x)$, and a primitive recursive function $(x)_i$ that yields an $i$th member of a sequence coded by $x$ in case $\mathrm{seq}(x)$ (see [13]).

The set of all integers will be denoted by $\mathbb{Z}$. Let $\widehat{z}$ be the successor function on $\mathbb{Z}$. (Note that $z \mapsto \widehat{z}$ is a permutation on $\mathbb{Z}$.)

## 1. $\Pi^1_1$–*complete theories*

PROPOSITION 1. *The theories $T$, $T_n$ and $T^!_n$ are in $\Pi^1_1$.*

*Proof.* Note that each subset $X \subseteq \omega$ codes a ternary relation $\{\langle (x)_0, (x)_1, (x)_2 \rangle \mid x \in X\}$. If this relation defines a group operation then this relation is the diagram of the uniquely defined group, denoted by $G_X$.

Informally,

(i) a sentence $\varphi$ is true in all f.g. groups if and only if

$$\forall X \, \forall m \, ((X \text{ codes the diagram of an } m\text{–generated group}) \to G_X \models \varphi);$$

(ii) a sentence $\varphi$ is true in all $n$–generated groups if and only if

$$\forall X\,((X \text{ codes the diagram of an } n\text{–generated group}) \to G_X \models \varphi).$$

(iii) a sentence $\varphi$ is true in all strictly $n+1$–generated groups if and only if

$$\forall X\,(X \text{ codes the diagram of a strictly } (n+1)\text{–generated group} \to G_X \models \varphi).$$

Let $\ulcorner\varphi\urcorner$ be the Gödel number of a formula $\varphi$. We will translate the statements in the right hand side of each of these equivalences into the form

$$\forall X \exists x \forall y \Psi(\ulcorner\varphi\urcorner, x, y, X)$$

uniformly in $n$ and $\varphi$ (in the first case $n$ is redundant), which proves all these problems to be in $\Pi^1_1$.

It is clear how to write a predicate that says "$X$ codes a group" in the language of arithmetic extended by a unary predicate for $X$, and we omit this step.

To express the property "to be $n$–generated", we need to code group terms in generators $x_1, \ldots, x_n$. For a term $x_{i_1}^{\varepsilon_{i_1}} \cdot \ldots \cdot x_{i_k}^{\varepsilon_{i_k}}$, $i_1, \ldots, i_k \in \{1, 2, \ldots, n\}$, $\varepsilon_{i_1}, \ldots, \varepsilon_{i_k} \in \{1, -1\}$ we let

$$\mathrm{code}(x_{i_1}^{\varepsilon_{i_1}} \cdot \ldots \cdot x_{i_k}^{\varepsilon_{i_k}}) = \langle \langle i_1, \varepsilon_{i_1} + 1\rangle, \ldots, \langle i_k, \varepsilon_{i_k} + 1\rangle \rangle .$$

The property "$y$ is a code of a term of first $n$ variables $x_1, \ldots x_n$" can be expressed by the following formula in the language of arithmetic:

$$\mathrm{seq}(y) \;\&\; \forall j < \mathrm{lh}(y)[1 \leqslant ((y)_j)_0 \leqslant n \;\&\; (((y)_j)_1 = 0 \vee ((y)_j)_1 = 2)].$$

Our next predicate in this language is "$m$ codes a term and $y$ is its value on $x_1 = (x)_1, x_2 = (x)_2, \ldots, x_k = (x)_k, \ldots$". We just say that there exists a $v$ which codes the sequence of intermediate results of computations of terms $x_{i_1}^{\varepsilon_{i_1}}$, $x_{i_1}^{\varepsilon_{i_1}} x_{i_2}^{\varepsilon_{i_2}}$, $x_{i_1}^{\varepsilon_{i_1}} x_{i_2}^{\varepsilon_{i_2}} x_{i_3}^{\varepsilon_{i_3}}, \ldots$:

$$(m \text{ codes a term}) \;\&\; \exists v\,[(((m)_0)_1 = 2 \;\&\; (v)_0 = (x)_{((m)_0)_0} \vee$$

$$((m)_0)_1 = 0 \;\&\; (v)_0 = ((x)_{((m)_0)_0})^{-1} \text{ in the group coded by } X) \;\&$$

$$\forall j < \mathrm{lh}(m) - 1\,[((m)_{j+1})_1 = 2 \;\&\; \left\langle (v)_j, (x)_{((m)_j)_0}, (v)_{j+1} \right\rangle \in X \vee$$

$$((m)_{j+1})_1 = 0 \;\&\; \left\langle (v)_{j+1}, (x)_{((m)_j)_0}), (v)_j \right\rangle \in X]].$$

The condition "$G_X$ is an $n$–generated group" is expressed by:

> there exists an $x$ such that for all $j \in \{1, \ldots, n\}$ $(x)_j \in (X)_0$; and for each $y \in (X)_0$ there exists an $m$ which codes a term of $x_1, \ldots, x_n$ whose value on $(x)_1, \ldots, (x)_n$ equals $y$,

which can be rewritten as a formula in the language of arithmetic extended by a unary symbol for $X$.

The condition $G_X \models \varphi$ can be uniformly in $\varphi$ translated into a formula of arithmetic extended by a unary predicate for $X$.

In each case (1)–(3) we can write a formula of kind $\forall X \Phi_\varphi(X)$ where $\Phi_\varphi(X)$ is in the language of arithmetic extended by a unary predicate for $X$ uniformly in parameters $\varphi$ and $n$. Using standard quantifier techniques (for instance, from [**10**, Chapters 15, 16]) in each of the cases above, we can construct a formula

$\Psi(m, x, y, X)$ such that

$$\forall X \Phi_\varphi(X) \Leftrightarrow \forall X \exists x \forall y \Psi(\ulcorner \varphi \urcorner, x, y, X).$$

THEOREM 1.

(I) *The theory $T$ of all f.g. groups is $\Pi^1_1$–complete.*
(II) *The theory $T_n$ of all $n$–generated groups is $\Pi^1_1$–complete for each $n > 1$.*
(III) *The theory $T^!_n$ of all strictly $n$–generated groups is $\Pi^1_1$–complete for each $n > 1$.*
(IV) *All the theories $T, T_n, T^!_n$, $n > 1$, are distinct.*

*Proof.* After Proposition 1, it suffices to show that some $\Pi^1_1$-complete set $A$ is many-one reducible to each of the theories. We rely on the following.

LEMMA 1 (Main Lemma). *There exists a formula* $\mathrm{Standard}(x, y, z)$ *in the first order language of groups such that the following conditions are satisfied:*

(i) *(Concrete case) For each group $G \leqslant \mathrm{Sym}(\mathbb{Z})$ which possesses an $f$ such that each $g \in G$ is $T$–reducible to $f$ and which contains all finitary permutations and the permutation $\widehat{z}(x) = x + 1$,*

$$G \models \mathrm{Standard}(\widehat{z}, (0, 1), (0, -1)).$$

(ii) *(Abstract case) Assume $G$ is a f.g. group and $z, \tau_0, \tau_1$ are elements such that $G \models \mathrm{Standard}(z, \tau_0, \tau_1)$. Then the two–sorted model*

$$\widetilde{G} = \langle G, \mathbb{Z}; +, \times, s, <, 0, \mathrm{ap} \rangle$$

*is elementary definable in $G$ with parameters $z, \tau_0, \tau_1$ via a fixed collection of formulas, where*

(a) *$\mathbb{Z}$ is the set of standard integers and $+, \times, s$ are usual addition, multiplication, and successor operations, $<$ is the usual ordering on $\mathbb{Z}$, $0$ is the usual zero element;*
(b) *$\mathrm{ap}(h, x)$ is the application operation which takes each pair $(h, x)$ to the result $\mathrm{ap}(h, x)$. If $\widetilde{h}$ is the function $x \to \mathrm{ap}(h, x)$ $(x \in \mathbb{Z})$, then $\widetilde{f} = \widetilde{g}$ implies $f = g$. In this way, $G$ can be viewed as a subgroup of $\mathrm{Sym}(\mathbb{Z})$;*
(c) *Viewing the elements of $G$ as permutations, there exists a permutation $f$ such that any permutation $g \in G$ is Turing–reducible to $f$.*

(iii) *For each $n > 0$, there exist a sentence $\theta_n$ such that for each f.g. group $G$, $G \models \exists x \exists y \exists z\ \mathrm{Standard}(x, y, z)$, the following holds.*

$$G \models \theta_n \Leftrightarrow G \text{ is } n\text{–generated.}$$

If the elements $\zeta, \tau_0, \tau_1$ satisfy $G \models \mathrm{Standard}[\zeta, \tau_0, \tau_1]$ then they are called *standard parameters*. We defer the proof of this Lemma to Section 2.

Since the formulas which establish the interpretation in this Lemma do not depend on the group, we can effectively transform a formula $\psi(u_0, \ldots, u_k)$ in the language of $\widetilde{G}$ where all the variables have type $G$ into an equivalent formula $\psi^*(u_0, \ldots, u_k, \zeta, \tau_0, \tau_1)$ in the language of groups. That is, for all triples of standard parameters $\zeta, \tau_0, \tau_1$ and for all $g_0, \ldots, g_k \in G$ the following is true:

$$\widetilde{G} \models \psi(u_0, \ldots, u_k) \ \Leftrightarrow\ G \models \psi^*(u_0, \ldots, u_k, \zeta, \tau_0, \tau_1).$$

(I). We code subsets $X$ of $\omega$ by permutations $f$ as follows (saying *$f$ $\alpha$-codes $X$*):
any permutation $f$ on $\mathbb{Z}$ defines a set

$$X = \{n \mid 3(n+1) \xrightarrow{f} 3(n+1)+1 \xrightarrow{f} 3(n+1)+2 \xrightarrow{f} 3(n+1)\}.$$

On the other hand, each set $X \subseteq \omega$ can be $\alpha$-coded by some $f$, the product of 3–cycles:

$$f = f_X = \prod_{k \in X} (3(k+1), 3(k+1)+1, 3(k+1)+2). \tag{1.1}$$

We have chosen this particular way of coding because in what follows we will need some groups to be 2–generated.

The formula $\widehat{\varphi}(n, f)$ is obtained from $\varphi(n, X)$ by replacing all subformulas of the kind $X(t)$ by the formula which says $t$ is in the set $\alpha$-coded by $f$.

The $\Pi^1_1$-complete set $A$ was introduced in (0.1). We claim that

$$n \in A \Leftrightarrow \forall f \, \forall z, a_0, a_1 (\text{Standard}(z, a_0, a_1) \to \widehat{\varphi}^*(s^n(0), f, z, a_0, a_1)) \in T \tag{1.2}$$

The implication ($\Rightarrow$) follows from the "abstract case", (ii) of the Main Lemma. For the implication ($\Leftarrow$), take an arbitrary $X \subseteq \omega$ and consider the group $G$ generated by the following two permutations: $\widehat{z}$ (the successor on $\mathbb{Z}$) and $h = f_X \cdot (0,1)$. This group contains elements $\widehat{z}$, $(0,1) = h^3$. Therefore it contains all permutations of finite support. So, by the "concrete case" (i) of the Main Lemma it has standard parameters $\widehat{z}$, $a_0 = (0,1)$, $a_1 = (0,-1)$. Taking $f = f_X$ and $\widehat{z}$, $a_0$, $a_1$ as values under the quantifiers in this formula, we obtain that $\widehat{\varphi}^*(s^n(0), f, \widehat{z}, a_0, a_1)$ holds, and thus $\varphi(n, X)$. Since $X$ was arbitrary, $\forall X \, \varphi(n, X)$ holds, as required.

Thus, there exists a computable sequence $(\psi_n)_{n<\omega}$ of first order group formulas such that $n \in A \Leftrightarrow \psi_n$ is true on each f.g. group., which establishes $\Pi^1_1$–completeness of $T$.

(II). If we restrict the class of groups we are considering while keeping the ones from the concrete case, then the proof goes through as before. Thus, since the group generated by $\widehat{z}$ and $(0,1) \cdot f_X$ is 2–generated, we have also proved $\Pi^1_1$–completeness of the theories $T_n$, $n > 1$.

(III). First assume that $n = 2$. $T^!_2$ is the theory of 2-generated groups, so by the last remark, the proof goes through. However, if $n \geq 3$, we need to modify the proof in order to make sure that the permutation groups used in the concrete case are strictly $n$-generated. We introduce a more elaborate way of coding sets by permutations. A permutation $f$ on $\mathbb{Z}$ *$\beta$-codes a set* $X$ if

$$\begin{aligned} X = \{n \in \omega \mid &\text{ the } 2n\text{th prime } p_{2n} \text{ is the minimal} \\ &\text{prime divisor of some } x \text{ with the property } \widehat{z}(x) = f(x)\} \end{aligned} \tag{1.3}$$

and

$$\begin{aligned} \omega \setminus X = \{n \in \omega \mid &\text{ the } (2n+1)\text{th prime } p_{2n+1} \text{ is the minimal} \\ &\text{prime divisor of some } x \text{ with the property } \widehat{z}(x) = f(x)\}. \end{aligned}$$

Note that $X$ is Turing reducible to $f$, since $X$ and $\omega \setminus X$ are r.e. in $\pi_1$.

If $f$ $\beta$-codes $X$, we write $X = X^f$. One verifies that the relations "$x \in X^f$" and "$f$ $\beta$-codes a set" are first order definable in any model $\widetilde{G}$ defined by standard parameters in $G$. Moreover, each set $X \subseteq \omega$ has the form $X^f$ for some $f \in G$.

As before, we need to check the equivalence

$$n \in A \Leftrightarrow \forall f \forall z, a_0, a_1\, [(\text{Standard}(z, a_0, a_1)\ \&\ (f\ \beta\text{-codes a set}) \rightarrow$$
$$\rightarrow \tilde{\varphi}\,'(s^n(0), f, z, a_0, a_1))] \tag{1.4}$$
$$\text{is true in all strictly } n\text{—generated groups}$$

where $\tilde{\varphi}(n, f)$ is obtained from $\varphi(n, X)$ by replacing all subformulas of kind $X(t)$ with the formula which expresses $t \in X^f$.

The implication $(\Rightarrow)$ in (1.4) follows as before from the abstract case (ii) of the Main Lemma. For the other direction, we replace groups generated by $\widehat{z}$ and $f_X \cdot (0,1)$ by groups $G_{n,X}$ introduced next.

LEMMA 2. *For each $X \subseteq \omega$ and for each $n \geq 3$, there exists a strictly $n$–generated group $G = G_{n,X} \leqslant \mathrm{Sym}(\mathbb{Z})$ such that*

(i) $\widehat{z},\ (0,1) \in G$;

(ii) *For some $g \in G$, all elements of $G$ are Turing reducible to $g$;*

(iii) *$G$ contains some $f$ which $\beta$-codes $X$.*

The proof will be given in Section 3

(IV). The sentences $\theta_n$ were introduced in (iii) of Lemma 1. For $n \geq 2$ let $\Phi_n$ be the sentence

$$\theta_n\ \&\ \neg\theta_{n-1}\ \&\ \exists x, y, z\ \ \text{Standard}(x, y, z).$$

Then, for each f.g. group $G$ such that $G \models \exists x, y, z\, \text{Standard}(x, y, z)$,

$$G \models \theta_n \Leftrightarrow\ \text{“ the least possible number of generators of } G \text{ is } n\text{”}.$$

Note that a sentence $\phi$ is consistent with a theory $S = \mathrm{Th}(\mathcal{E})$ if not $S \vdash \neg\phi$, that is, $G \models \phi$ for some $G \in \mathcal{E}$. The theories in the list $T$, $(T_n)_{n\geq 2}$ and $(T_n^!)_{n\geq 2}$ can be distinguished as follows.

– The theory $T_n$ of $n$–generated groups $(n > 1)$ is the only theory in this list such that the sentences $\Phi_2, \ldots, \Phi_n$ are consistent with it and all other sentences $\Phi_{n+1}$, $\Phi_{n+2}$, ... are not consistent with it.

– The theory $T_n^!$ of strictly $n$–generated groups $(n \geq 2)$ is the only theory in this list such that the sentence $\Phi_n$ is consistent with it and all other sentences $\Phi_i$, $i \in \{2, 3, \ldots\} \setminus \{n\}$ are not consistent with it.

## 2. *Proof of the Main Lemma*

The formula Standard$(x, y, z)$ will be a conjunction of a finite family of formulas, called *axioms,* which describe properties of triples $x, y, z$. We will at the same time investigate properties of abstract f.g. groups which satisfy the axioms we formulated, and we check that all these axioms are true in the concrete case, namely in a group satisfying the following:

$(*)$ $G \leq \mathrm{Sym}(\mathbb{Z})$; $G$ contains the successor $\widehat{z}$ and at least one 2–cycle $(a, b)$; $G$ contains an $f$ such that $g \leqslant_T f$ for all $g \in G$.

Our overall goal is to introduce a finite family of group axioms which will enable us to consider elements of these groups as permutations on a copy of the integers

defined in the group, and then use this structure of integers to express some facts about their computability, working with terms, tuples of permutations, etc. The most difficult thing here will be to ensure that this copy of the integers is actually the standard integers. Of course, by Löwenheim–Skolem type results it is impossible to do so in general case. Here we use the extra condition that the group is f.g., which is of course not a first-order property. We use that, if $G$ is f.g., then each element can be expressed by a *standard* term in some (finite) generating set. So we can formulate the concept of standardness of integers defined in the group in first–order logic by looking at the minimal lengths of such terms. Since our axioms ensure that $G$ is infinite, the lengths of these terms will form a set cofinal in $\mathbb{N}$, which will enable us to distinguish standard integers.

In the concrete case, we want to define the action of $G \leq \mathrm{Sym}(\mathbb{Z})$ on $\mathbb{Z}$ within $G$. The idea is to distinguish 2–cycles in $G$ (we call them *transpositions*) and then to consider elements $x \in \mathbb{Z}$ as associated with pairs of transpositions of the kind $(a, x)$, $(x, b)$, $a \neq b$. We will say that this pair *holds* an element $x$. One can easily check that two transpositions $\tau_0$, $\tau_1$ hold some element if and only if they do not commute. Thus, elements of $x \in \mathbb{Z}$ can be associated with families of pairs of non–commuting transpositions that hold $x$. It is possible to define the action of $G$ on elements of $\mathbb{Z}$ coded by families of these pairs, etc.; see details below.

Now we start presenting the axioms. Some properties we postulate as axioms could be derived from the axioms we enumerated so far. When it is convenient, we do not prove and just postulate them.

**Axiom 0.** In [5, Lemma 0], R. McKenzie has proven that if a group $G \leq \mathrm{Sym}(\mathbb{Z})$ contains all permutations with finite support, then its transpositions are distinguished by the formula

$$\mathrm{tr}(x) = \neg(x = 1) \ \&\ (x^2 = 1) \ \&\ \forall y \left([x, y]^6 = 1\right).$$

Our first axiom says that *there is at least one pair of non–commuting transpositions:*

$$\exists x \, \exists y \, (\mathrm{tr}(x) \ \&\ \mathrm{tr}(y) \ \&\ [x, y] \neq 1).$$

**Axiom 1.** One checks that the formula

$$E(x_0, x_1, y_0, y_1) = \bigwedge_{i,j \in \{0,1\}} (x_i y_j)^3 = 1 \ \&$$

$$\bigwedge_{i,j \in \{0,1\}} (x_i = y_j \ \&\ x_{1-i} \neq y_{1-j} \to x_{1-i} \neq x_i^{-1} y_{1-j} x_i)$$

is true for transpositions $\pi_0, \pi_1, \tau_0, \tau_1$ such that $[\pi_0, \pi_1] \neq 1$ & $[\tau_0, \tau_1] \neq 1$ if and only if the elements held by the pairs of transpositions $\langle \pi_0, \pi_1 \rangle$, $\langle \tau_0, \tau_1 \rangle$ are equal. This axiom says that *the relation*

$$\langle \pi_0, \pi_1 \rangle \sim \langle \tau_0, \tau_1 \rangle \overset{df}{\Leftrightarrow} E(\pi_0, \pi_1, \tau_0, \tau_1)$$

*is an equivalence on the set*

$$\{\langle x_0, x_1 \rangle \mid G \models \mathrm{tr}(x_0) \ \&\ \mathrm{tr}(x_1) \ \&\ [x_0, x_1] \neq 1\}.$$

**Axiom 2.** Clearly, if a pair of transpositions $\langle \tau_0, \tau_1 \rangle$ holds the element $x$ and $f \in \mathrm{Sym}(\mathbb{Z})$ then the pair $\langle f\tau_0 f^{-1}, f\tau_1 f^{-1} \rangle$ holds $f(a)$. This enables us to define a faithful action of the group $G$ on classes $\langle \tau_0, \tau_1 \rangle /_\sim$ as follows:

$$(\langle \tau_0, \tau_1 \rangle /_\sim)^f = \langle f\tau_0 f^{-1}, f\tau_1 f^{-1} \rangle /_\sim.$$

This axiom says that *this action is defined correctly and is faithful and transitive, and each transposition moves exactly two elements, and that for each two elements there exists a transposition which permutes them.*

Remark. If a group $G$ satisfies the axioms (0)–(2) then it can be considered as a subgroup of the symmetric group of the set

$$Z_G = \{\langle x_0, x_1 \rangle \mid G \models \mathrm{tr}(x_0)\ \&\ \mathrm{tr}(x_1)\ \&\ [x_0, x_1] \neq 1\}/_\sim.$$

In the concrete case, i.e., $G$ satisfying $(*)$, the set $Z_G$ can be identified with the set of integers.

In developing the next group of axioms, we try to define on the group $G$ along with $Z_G$ a structure of model of integers and postulate some of its properties.

Since any group $G$ with distinguished element $z$ which satisfies the axioms (0)–(2) can be viewed as a subgroup of $\mathrm{Sym}(Z_G)$, we may introduce the notion of *support of* $f$ as

$$\mathrm{sp}(f) = \{x \in Z_G \mid f(x) \neq x\}.$$

First we will define the structure of $\mathbb{Z}$ in any group $G$ which satisfies $(*)$. The so obtained formulas will serve in the next axioms we will formulate. The very possibility to define the structure of $\mathbb{Z}$ in this way proves everything we formulate to be compatible with the class of f.g. groups.

The next thing we have to do is to define the order relation $x < y$ on $\mathbb{Z} = Z_G$ with parameter $z$ provided $G$ satisfies $(*)$. At first glance, it would seem enough to say that

$$\begin{aligned} x < y \Leftrightarrow \exists f \in G[\, & x, y \in \mathrm{sp}(f)\ \& \\ & x \text{ is the only element such that } z^{-1}(x) \notin \mathrm{sp}(f)\ \& \\ & y \text{ is the only element such that } z(y) \notin \mathrm{sp}(f)\,]. \end{aligned}$$

Denote the subformula $\exists f \in G[\ldots]$ in the right hand part of the equivalence above by $R(x, y, f, z)$ and observe that in a group satisfying $(*)$ it may happen that for some $f, f' \in G$ both conditions $R(x, y, f, z)$ and $R(y, x, f', z)$ are satisfied, for instance, when $x = 0$, $y = 2$, $\mathrm{sp}(f) = \{0, 1, 2\}$, $\mathrm{sp}(f') = \{0, -1, -2, \ldots\} \cup \{2, 3, \ldots\}$. Thus the definition above does not work and we should be more careful.

The idea is that there are two types of $\mathrm{sp}(f)$ such that $R(x, y, f, z)$, but just one of them is finite. The finite support can be mapped by a finitary permutation into any other support $\mathrm{sp}(f')$ for which $R(x, y, f', z)$.

The following definition will work:

$$\begin{aligned} x < y \Leftrightarrow \exists f[ & R(x, y, f)\ \& \\ & \forall f'[(R(x, y, f') \vee R(y, x, f')) \to \exists h \in G(\mathrm{ap}(h, \mathrm{sp}(f)) \subseteq \mathrm{sp}(f'))]]. \end{aligned}$$

This gives us a first order definition for $x < y$. Actually, this definition contains $z$ as a parameter, and it would be correct to use notation $<_z$, but we will omit indices like this when it will be clear what is meant.

Exploiting the definition for $<$, we can easily write a first order definition for the successor function $s$, which depends on the parameter $z$. We will sometimes denote it by $s_z$.

Now we need to pick the zero in $Z_G$. It could be done by taking a pair $a_0, a_1$ of two non–commuting transpositions as new parameters which hold the element we suppose to be zero. For groups satisfying $(*)$, we can take $a_0 = (0, 1)$, $a_1 = (0, -1)$.

For an abstract group satisfying axioms (0)–(2) and transpositions $a_0$, $a_1$, $a_0 a_1 \neq a_1 a_0$, we define the zero element $0_{z,a_0,a_1}$ as their common element.

Now we define addition $+_{z,a_0,a_1}$ and multiplication $\cdot_{z,a_0,a_1}$ on the set of "natural numbers" $N_{z,a_0,a_1} = \{x \in Z_G \mid x > 0_{z,a_0,a_1}\}$. We will sometimes omit subscripts in these notations for operations.

One can check that

- $x + y = t$ if and only if there exists an $f \in G$ such that it takes 0 to $x$, $y$ to $t$ and for each $u$ which satisfies the condition $0 \leqslant u < y$ it is true that $f(s(u)) = s(f(u))$.
- $x \cdot y = t$ if and only if there exists an $f \in G$ which takes 0 to 0, $y$ to $t$ and for each $u$ which satisfies the condition $0 \leqslant u < y$ it is true that $f(s(u)) = x + f(u)$, where $+$ is defined above.

These properties can be expressed in first-order logic, and may be taken as definitions of the operations $+$ and $\cdot$.

**Axiom 3.** *$s$, $+$, and $\cdot$ are total operations on $N_{z,a_0,a_1}$.*

Fix a family $Q$ of axioms for arithmetic which suffices to represent all computable functions and predicates. We use the one mentioned in [13], in which this theory is called $N$. Here is the list of axioms of $Q$:

1) $s(x) \neq 0$;
2) $s(x) = s(y) \to x = y$;
3) $x + 0 = x$;
4) $x + s(y) = s(x + y)$;
5) $x \cdot 0 = 0$;
6) $x \cdot s(y) = (x \cdot y) + x$;
7) $\neg(x < 0)$;
8) $x < s(y) \leftrightarrow x < y \vee x = y$;
9) $x < y \vee x = y \vee y < x$.

It will be important that this theory derives the equivalence:

$$\forall i < s^m(0)\ \varphi(i, \ldots) \leftrightarrow \varphi(0, \ldots)\ \&\ \varphi(s(0), \ldots)\ \&\ \ldots \varphi(s^{m-1}(0), \ldots). \tag{2.1}$$

**Axiom 4.** *The so defined operations $0_{z,a_0,a_1}$, $s_{z,a_0,a_1}$, $+_{z,a_0,a_1}$, $\cdot_{z,a_0,a_1}$ on $N_{z,a_0,a_1}$ satisfy the finite set of axioms $Q$ and $<_z$ has neither maximal nor minimal elements.*

**Axiom 5.** It says that the "positive" and "negative" parts of $Z_G$ are symmetric, namely,

(i) for each $x < 0$ there exists the unique $x' > 0$ and a group element $f$ which isomorphically maps the model $\langle \{t \mid x \leqslant t \leqslant 0\}, < \rangle$ onto the model $\langle \{t \mid 0 \leqslant t \leqslant x'\}, <^{-1} \rangle$.
(ii) for each $x > 0$ there exists the unique $x' < 0$ and a group element $f$ which isomorphically maps the model $\langle \{t \mid 0 \leqslant t \leqslant x\}, < \rangle$ onto the model $\langle \{t \mid x' \leqslant t \leqslant 0\}, <^{-1} \rangle$.

Note that if the axioms listed so far are satisfied then $Z_G$, with the operations $+_{z,a_0,a_1}$, $\cdot_{z,a_0,a_1}$, $s_z$, and relation $<_z$, looks like this: it contains a standard "middle part" surrounding zero which is isomorphic to usual integers and maybe some nonstandard elements.

Denote for each $x$ its unique $x'$ which exists by Axiom 5 by $-x$.

The following axioms are needed to recognize (in f.g. groups) those triples of parameters $z, a_0, a_1$ for which the set $N_{z,a_0,a_1}$ with the operations $+_{z,a_0,a_1}, \cdot_{z,a_0,a_1}$, $s_z$, $0_{z,a_0,a_1}$ is a standard model of arithmetic. First we need a way to deal with (maybe nonstandard-) finite families of permutations.

Before we formulate the axiom, recall that Turing reducibility is an arithmetical relation on sets, since for some computable function $\rho$

$$A \leq_T B \Leftrightarrow \exists n \forall x, y \left(\chi_A(x) = y \leftrightarrow \exists u_+ u_- \left(\langle x, y, u_+, u_- \rangle \in W_{\rho(n)} \right.\right.$$
$$\left.\left. \& \; D_{u_+} \subseteq B \;\&\; D_{u_-} \subseteq \overline{B}\right)\right).$$

(Here $W_n$ denotes $n$th computably enumerable set and $D_n$ denotes $n$th standard finite set, see [10]) If $n$ is a witness in the right hand part of this equivalence, we say that the *index $n$ reduces $A$ to $B$*. If $m$ reduces a function $f$ to a function $g$, we write $g = \{m\}^f$.

**Axiom 6.** Here we want to say that $G$ contains a Turing complete element, i.e., there exists $f \in G$ such that $g \leqslant_T f$, for all $g \in G$. A slight difficulty is that instead of natural numbers we have integers. But we may select some computable way to code integers by natural numbers, for instance, let $2m$ be the code of $m \geqslant 0$ and $2(-m) - 1$ be the code for $m < 0$ and, as a part of this axiom, we state that *this coding is one–to one*. We denote code of $a$ as $\zeta(a)$. Clearly, the fact $\zeta(a) = b$ is first order definable in the model $\langle Z_G, +_{z,a_0,a_1}, \cdot_{z,a_0,a_1}, s_z, <_z, 0_{z,a_0,a_1}\rangle$. Now we understand the reducibility $f \leqslant_T g$ for $f, g \in G$ as the reducibility $\zeta f \zeta^{-1} \leqslant_T \zeta g \zeta^{-1}$.

The next part of the axiom states that *"There exists $f$ such that for each permutation $g$ there is an index that $T$–reduces $g$ to $f$"*.

The set of axioms obtained so far is still consistent, since it is true in any group satisfying $(*)$ with parameters $z(x) = x + 1$, $(0, 1)$, $(0, -1)$. In view of the above axiom, the property *to be a Turing-complete permutation* is first order definable in such groups by formulas with parameters $z, a_0, a_1$ in any model. If $m$ is an index which reduces $g$ to a permutation $f$, we will say *$g$ has $f$–index $m$*.

**Axiom 7.** Fix formulas which represent functions $(x)_i$, $\mathrm{lh}(x)$, $\mathrm{seq}(x)$, $p_n$ ($n$th prime) in the theory $Q$.

This axiom says

- *these formulas define total functions on $N_{z,a_0,a_1}$*;
- $\forall x, m, k \in N_{z,a_0,a_1} \exists x' (\forall i < m((x)_i = (x')_i) \;\&\; (x')_m = k)$;
- $\forall s \forall m \exists s' (\mathrm{lh}(s') = m \;\&\; \forall i < m((s)_i = (s')_i))$.

This axiom is needed since we wish to deal with nonstandard natural numbers. We need to be sure we can code all finite sequences of elements of $Z_G$.

Now everything is ready to express the property "to be standard". The idea is to describe a formula which says $n = \langle n_1, \ldots, n_k\rangle$ codes a tuple of $f$–indices of elements of $G$ and $m$ is the minimal length of a term $\tau(\{n_1\}^f, \ldots, \{n_k\}^f)$ whose value is $x$. If $n \in \omega \subseteq \mathbb{Z}$, $n = \langle n_1, \ldots, n_k\rangle$ is the code of a finite tuple of generators $\{n_1\}^f, \ldots, \{n_k\}^f$ of $G$ then the set $M_n$ of such $m$'s for different $x$'s is cofinal in

$\omega$ and thus its downward closure $\widehat{M_n} = \{y \in \omega \mid \exists m \in M_n (y \leqslant m)\}$ equals $\omega$. If $n$ does not code a tuple of generators then the corresponding set $\widehat{M_n}$ can happen to be finite either can contain a nonstandard element of $\mathbb{Z}_G$. Anyway, if $G$ is f.g. then the intersection of all possible sets $\widehat{M_n}$ having no maximal element equals $\omega$, i.e., the set of all standard non-negative elements of $\mathbb{Z}$. This intersection can be defined by a formula. In carrying out the details, we must be careful because of the presence of nonstandard integers.

We first need to define some more formulas. We say that $m \in N_{z,a_0,a_1}$ *codes a family of elements of* $G$ if the set

$$\{\{(m)_i\}^f \mid i < \mathrm{lh}(m)\}$$

consists of permutations given by elements of $G$. This is expressed by the following formula:

$$\texttt{CodFamily}\,(m, f, z, a_0, a_1) = \forall i < \mathrm{lh}(m) \exists g \forall x \left[\mathrm{ap}(g, x) = \{(m)_i\}^f(x)\right].$$

Note that by Axiom 7, each finite series of elements of a group has a code.

The property "$t$ codes a term" is expressed by the following formula:

$$\texttt{CodTerm}\,(t, f, z, a_0, a_1) = \forall i < \mathrm{lh}(t)\,[((t)_i)_1 \in \{0, 2\}]\,.$$

The property "$t$ codes a term, $n$ codes a series of elements, and the maximal number of a variable is less than the length of a sequence coded by $n$" that expresses an opportunity to compute this term with values given by $n$ can be expressed by the formula:

$$\begin{aligned}\texttt{CanCompute}\,(t, n, f, z, a_0, a_1) = {} & \texttt{CodTerm}\,(t, f, z, a_0, a_1)\ \& \\ & \texttt{CodFamily}\,(m, f, z, a_0, a_1)\ \& \\ & \forall i < \mathrm{lh}(t)\ (((t)_i)_0 < \mathrm{lh}(n))\,.\end{aligned}$$

Express now by a formula the property that a term whose code is $t$ can be computed on the following values of its variables: $x_0 = \{(n)_0\}^f,\ x_1 = \{(n)_1\}^f, \ldots$ and that the value of this computation is $y$:

$$\texttt{Val}\,(t, n, y, f, z, a_0, a_1)\ =\ \texttt{CanCompute}\,(t, n, f, z, a_0, a_1)\ \&$$

$$\exists s(((((t)_0)_1 = 2\ \&\ (s)_0 = (n)_0) \vee (((t)_0)_1 = 0\ \&\ \{(s)_0\}^f \cdot \{(n)_0\}^f = \mathrm{id}))\ \&$$

$$\forall i < \mathrm{lh}(t) - 1\,[(((t)_{i+1})_1 = 2\ \&\ \{(s)_{i+1}\}^f = \{(s)_i\}^f \cdot \{(n)_{i+1}\}^f) \vee$$

$$(((t)_{i+1})_1 = 0\ \&\ \{(s)_{i+1}\}^f = \{(s)_i\}^f \cdot (\{(n)_{i+1}\}^f)^{-1})]\ \&\ y = \{(s)_{\mathrm{lh}(t)-1}\}^f).$$

Let $G$ be a f.g. group which has elements satisfying all axioms listed so far and let $z, a_0, a_1$ be its parameters whose properties are described in these axioms. Fix a series of generators $g_0, \ldots, g_k$ and an element $f \in G$ which satisfies the formula saying it is Turing maximal, and fix standard $f$–indices of the generators: $\{n_0\}^f = g_0$, $\{n_1\}^f = g_1, \ldots, \{n_k\}^f = g_k$. By Axiom 7, there exists a standard element $n$ such that $\mathrm{lh}(n) = k + 1$ and $(n)_i = n_i$, for all $i = 0, \ldots, k$. Denote by $L(g, n, f, z, a_0, a_1)$ the minimal length of a term which generates $g$ from $g_0, \ldots, g_k$. It is of course standard.

Let $l$ be any standard natural number. We check that

$$L(g, n, f, z, a_0, a_1) = l \Leftrightarrow \exists t(\texttt{Val}\,(t, n, g, f, z, a_0, a_1)\ \&\ \mathrm{lh}(t) = l\ \&$$

$$\forall t'(\texttt{Val}\,(t', n, g, f, z, a_0, a_1) \to \mathrm{lh}(t') \geqslant l)).$$

This is not so obvious because we consider this formula over a nonstandard model!

($\Leftarrow$) Take a witness $t$ in the right hand part of the equivalence. We see that $\mathrm{lh}(t) = s^l(0)$ is standard. Making use the property (2.1) of $Q$, replace all quantifiers bounded by $\mathrm{lh}(t)$ or by $\mathrm{lh}(t) - 1$ by finite conjunctions. We see then that the so obtained formula expresses the fact that $g$ is really the value of a term of $g_0, \ldots, g_k$ of length $l$. Assume this $l$ is not a minimal possible length of a term, i.e., there exists a shorter term $\tau$ of $g_0, \ldots, g_k$ whose value is $g$. By Axiom 7, this term possesses a code, say $t'$. To prove $\texttt{Val}\,(t', n, g, f, z, a_0, a_1)$ is true, take a required $s$ that codes a sequence of $f$–indices of intermediate results in computation of $\tau(g_0, \ldots, g_k)$. Such $s$ exists by Axiom 7. Again making use the property (2.1) of $Q$, $\texttt{Val}\,(t', n, g, z, a_0, a_1)$ is true. Then $\mathrm{lh}(t') \geqslant l$, which contradicts the fact that the term coded by $t'$ is shorter than that of $t$.

($\Rightarrow$) Similarly, we use the fact that $l$ is standard and apply (2.1).

Let

$$L^*(n, f, z, a_0, a_1) = \{x \in N_{z,a_0,a_1} \mid \exists l \exists g\,(x \leqslant L(g, n, f, z, a_0, a_1))\}.$$

Thus, the standard natural numbers can be defined as the set:

$$N^*_{f,z,a_0,a_1} = \bigcap\{L^*(n, f, z, a_0, a_1) \mid L^*(n, f, z, a_0, a_1) \neq \varnothing\ \&$$
$$L^*(n, f, z, a_0, a_1) \text{ has no } <_z\text{–maximal element}\}.$$

Clearly, this set is first order definable from the parameters $z, a_0, a_1$.

**Axiom 8.** Each element in $N_{z,a_0,a_1}$ is in $N^*_{f,z,a_0,a_1}$ (i.e., is standard).

Denote the conjunction of the axioms (0)–(8) and of the property that $z, a_0, a_1$ are standard parameters by Standard$(a, z)$.

(iii) follows since to be $n$–generated can be expressed by a first order formula in the model $\widetilde{G}$.

This complete the proof of the Main Lemma.

## 3. *Proof of Lemma 2*

First note that the free group $F_n$ of rank $n$ is strictly $n$–generated, see [4, Proposition 2.7].

It suffices to prove the following.

Claim 1. *For arbitrary $m \in \mathbb{N}$, there exists a f.g. group $G$ which is not $m-1$-generated and satisfies the properties in Lemma 2, i.e. $\widehat{z}$, $(0,1) \in G$; for some $g \in G$, all elements of $G$ are Turing reducible to $g$; and $G$ contains some $f$ which $\beta$-codes $X$.*

If so, let us fix a desired number of generators $n$, $n \geqslant 3$. By the Claim, there is such a group $G$ which is strictly $k$-generated for some $k \geqslant n$. We start with the subgroup of $G$ generated by $z, (0,1)\cdot h$, where $h$ $\beta$-codes $X$, and an $f$ which has greatest Turing degree among elements of $G$. This group is either 2–generated or 3–generated. Then we add one by one the members of an arbitrary family of generators of the group $G$. After each such step, the minimal number of generators is increased by at most one (it may also decrease). Thus, in the process of introducing new generators, there exists a step when the group with these generators is strictly $n$-generated.

We prove the Claim by constructing, for each $m \in \omega$ and $X \subseteq \omega$, permutations $\pi_1, \ldots, \pi_{m-1}$ such that $\pi_1$ $\beta$-codes $X$, $\widehat{z}, \pi_2, \ldots, \pi_{m-1} \leqslant_T \pi_1$, and $\widehat{z}, \pi_1, \ldots, \pi_{m-1}$ satisfy no nontrivial relations. To prove the groups is not $m-1$-generated, consider the canonical homomorphism from the group $G = ((0,1), \widehat{z}, \pi_1, \ldots, \pi_m)$ onto its quotient modulo the normal subgroup Fin of all permutations with finite support. The images of elements $\widehat{z}, \pi_1, \ldots, \pi_{m-1}$ are free generators of the quotient, because if there was a nontrivial relation $r = r(\widehat{z}/_{\mathrm{Fin}}, \pi_1/_{\mathrm{Fin}}, \ldots, \pi_{m-1}/_{\mathrm{Fin}}) = 1$ on these images, then $r(\widehat{z}, \pi_1, \ldots, \pi_{m-1}) \in \mathrm{Fin}$. Hence $r(\widehat{z}, \pi_1, \ldots, \pi_{m-1})^l = 1$ for some nonzero natural number $l$, which is only possible in case $r(\widehat{z}, \pi_1, \ldots, \pi_{m-1}) = 1$. Thus, the elements $\widehat{z}, \pi_1, \ldots, \pi_{m-1}$ satisfy a nontrivial relation as well, contradiction. The group $G = ((0,1), \widehat{z}, \pi_1, \ldots, \pi_m)$ has an epimorphic image which is not $m-1$-generated, and hence is not generated by fewer than $m$ elements itself.

We construct the permutations $\pi_1, \ldots, \pi_{m-1}$ in stages. At each stage we define a finite part of the permutations. We fix an effective numbering $\tau_0, \tau_1, \ldots$ of non–reducible group terms in $z, \pi_1, \ldots, \pi_m$. In step 1 of stage $t$, we make the term $\tau_t$ nontrivial, by finding a $q$ such that $\tau(q)$ is defined and does not coincide with $q$. In step 2 we extend $\pi_1$ in order to code more of $X$. In step 3, we extend $\pi_1, \ldots, \pi_m$ so they will become permutations.

STAGE $t$

*Step 1.* We make the term

$$\tau_t = (\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1})(\widehat{z}^{\alpha_2}\pi_{i_2}^{\beta_2}) \ldots (\widehat{z}^{\alpha_s}\pi_{i_s}^{\beta_s})\widehat{z}^{\alpha_{s+1}}$$

nontrivial, where $s, \beta_1, \beta_2, \ldots, \beta_s \neq 0$ and if $i_l = i_{l+1}$ then $\alpha_{l+1} \neq 0$, for $l = 1, \ldots, s-1$. (We write $af$ instead of $f(a)$.) We need to extend the $\pi_i$'s so that there exists an $m$ with

$$m(\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1})(\widehat{z}^{\alpha_2}\pi_{i_2}^{\beta_2}) \ldots (\widehat{z}^{\alpha_s}\pi_{i_s}^{\beta_s})\widehat{z}^{\alpha_{s+1}} > m. \tag{3.1}$$

Consider the following cases:

*Case 1.* ($i_1 \neq i_2$ and $\beta_1 > 0$) or ($i_1 = i_2$ and $\beta_1, \beta_2 > 0$).

Take an $m$ so that $m\widehat{z}^{\alpha_1} \notin \mathrm{dom}(\pi_{i_1})$. Define $m\widehat{z}^{\alpha_1}\pi_{i_1}$ so that for the new $\pi_{i_1}$ $m\widehat{z}^{\alpha_1}\pi_{i_1} \notin \mathrm{dom}(\pi_{i_1})$, then define $m\widehat{z}^{\alpha_1}\pi_{i_1}\pi_{i_1}$ so that $m\widehat{z}^{\alpha_1}\pi_{i_1}\pi_{i_1} \notin \mathrm{dom}(\pi_{i_1})$, etc. and finally that $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_i - 1} \notin \mathrm{dom}(\pi_{i_1})$. At last, define $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_i}$ so that $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1}\widehat{z}^{\alpha_2} \notin \mathrm{dom}(\pi_{i_2})$.

*Case 2.* ($i_1 \neq i_2$ and $\beta_1 < 0$) or ($i_1 = i_2$ and $\beta_1, \beta_2 < 0$).

Take an $m$ so that $m\widehat{z}^{\alpha_1} \notin \mathrm{range}(\pi_{i_1})$. Define $m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1}$ so that for the new $\pi_{i_1}$ $m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1} \notin \mathrm{range}(\pi_{i_1})$, then define $m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1}\pi_{i_1}^{-1}$ so that $m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1}\pi_{i_1}^{-1} \notin \mathrm{range}(\pi_{i_1})$, etc. and finally that $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_i+1} \notin \mathrm{range}(\pi_{i_1})$. At last, define $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_i}$ so that $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1}\widehat{z}^{\alpha_2} \notin \mathrm{range}(\pi_{i_2})$.

*Case 3.* $i_1 = i_2$ and $\beta_1 > 0, \beta_2 < 0$. Select an $m$ so that $m\widehat{z}^{\alpha_1} \notin \mathrm{dom}(\pi_{i_1})$. Define $m\widehat{z}^{\alpha_1}\pi_{i_1}$ so that for this new $\pi_{i_1}$ $m\widehat{z}^{\alpha_1}\pi_{i_1} \notin \mathrm{dom}(\pi_{i_1})$. Then define $m\widehat{z}^{\alpha_1}\pi_{i_1}\pi_{i_1}$ so that $m\widehat{z}^{\alpha_1}\pi_{i_1}\pi_{i_1} \notin \mathrm{dom}(\pi_{i_1})$, etc. Eventually, we will have $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1 - 1} \notin \mathrm{dom}(\pi_{i_1})$. Then define $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1-1}\pi_{i_1}$ so that $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1-1}\pi_{i_1}\widehat{z}^{\alpha_2} \notin \mathrm{range}(\pi_{i_1})$. The last extension of $\pi_{i_1}$ is possible since in that case $\alpha_2 \neq 0$.

*Case 4.* $i_1 = i_2$ and $\beta_1 < 0, \beta_2 > 0$. Select an $m$ so that $m\widehat{z}^{\alpha_1} \notin \mathrm{range}(\pi_{i_1})$. Define

$m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1}$ so that for this new $\pi_{i_1}$ $m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1} \notin \mathrm{range}(\pi_{i_1})$. Then define $m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1}\pi_{i_1}^{-1}$ so that $m\widehat{z}^{\alpha_1}\pi_{i_1}^{-1}\pi_{i_1}^{-1} \notin \mathrm{range}(\pi_{i_1})$, etc. Eventually, we will have $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1+1} \notin \mathrm{range}(\pi_{i_1})$. Then define $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1+1}\pi_{i_1}^{-1}$ so that the number $m\widehat{z}^{\alpha_1}\pi_{i_1}^{\beta_1+1}\pi_{i_1}^{-1}\widehat{z}^{\alpha_2} \notin \mathrm{dom}(\pi_{i_1})$. The last extension of $\pi_{i_1}$ is possible since in that case $\alpha_2 \neq 0$.

Then we iterate this procedure for $\pi_{i_2}$, etc.

While processing the last bracket, we are looking for the extension of $\pi_{i_s}$ such that (3.1) holds.

There is one more restriction we must obey here.

RESTRICTION. *While doing this step, we should not change the set $\beta$–coded in $\pi_1$. By this, when carrying this instruction out, we should never add new pairs of kind $\langle a, \widehat{z}(a)\rangle$ to $\pi_1$.*

Since each time we can select an element in an infinite set of possible values, this restriction can be easily obeyed.

*Step 2.* Choose a minimal $m \in \omega$ such that none of the conditions below is true:

(i) There exists a natural number $x$ such that $\pi_1(x) = \widehat{z}(x)$ and $p_{2m}$ is the minimal prime divisor of $x$.

(ii) There exists a natural number $x$ such that $\pi_1(x) = \widehat{z}(x)$ and $p_{2m+1}$ is the minimal prime divisor of $x$.

Take a minimal $k \in \omega$ so that

(i) its minimal prime divisor is greater than $p_{2m}$, $p_{2m+1}$ and

(ii) $p_{2m}k$, $\widehat{z}(p_{2m}k)$, $p_{2m+1}k$, $\widehat{z}(p_{2m+1}k)$ are not in $\mathrm{dom}(\pi_1) \cup \mathrm{range}(\pi_1)$, for current value of $\pi_1$ enumerated so far.

If $m \in X$ then extend $\pi_1$ by letting $\pi_1(p_{2m}k) = \widehat{z}(p_{2m}k)$. If $m \notin X$ then extend $\pi_1$ by letting $\pi_1(p_{2m+1}k) = \widehat{z}(p_{2m+1}k)$.

*Step 3.* Extend all permutations we are constructing by extending their domains and ranges with minimal elements which are not contained in them yet. While doing this, we obey the Restriction above.

This ends STAGE $t$.

Clearly each $\pi_i$, $i = 1, \ldots, m$ is computable in $X$. On the other hand, $X$ is computable in $\pi_1$, as remarked above. Hence all permutations in this group are Turing reducible to $\pi_1$.

This completes the proof of Lemma 2.

## 4. *The complexity of the word problem for QFA–groups*

Recall that $\mathbb{HYP}_\omega$ is the minimal admissible set which contains the model $\langle \omega, < \rangle$ as an element (see Barwise [1]).

THEOREM 2. *The word problem of each QFA–group is hyperarithmetical.*

*Proof.* If a QFA–group $G$ is axiomatized by a first order sentence $\varphi$, then it is determined up to isomorphism by the infinitary sentence

$$\Phi = \varphi \wedge \bigvee_{n \in \omega} \exists x_1 \ldots x_n \forall y \left( \bigvee_{\tau} y = \tau(x_1, \ldots, x_n) \right).$$

Since the sentence $\Phi$ is in the admissible fragment $L_{\mathbb{HYP}_\omega}$ and it has, up to iso-

morphism, only one countable model, by [7], it has a model in $\mathbb{HYP}_\omega$. We give an idea of the proof assuming the reader is familiar with the monograph [1]. The Barwise Completeness Theorem [1, p. 99] together with Löwenheim–Skolem Theorem imply that for each sentence $\psi \in L_{\mathbb{HYP}_\omega}$ it is true that

$$(\vdash \Phi \to \psi) \vee (\vdash \Phi \to \neg\psi),$$

where $\vdash \vartheta$ means "there exists a $\mathbb{HYP}_\omega$–proof of $\theta$". By this, the property $\Phi \vdash \psi$ is a $\Delta$–property. Consider some fragment $L \in \mathbb{HYP}_\omega$ containing the sentence $\Phi$ and a countable family of new constants $(c_i)_{i\in\omega} \in \mathbb{HYP}_\omega$. The usual Henkin construction yields a model of $\Phi$ which is in $\mathbb{HYP}_\omega$. So the word problem of $G$ is hyperarithmetical. □

Next we prove that the degrees of word problems of QFA–groups are cofinal within the degrees of hyperarithmetic sets. Recall that a set $S \subseteq \omega$ is called *arithmetical singleton* if there exists a formula $\varphi(X)$ in the language of arithmetic extended by a new unary predicate symbol $X$ that for each $P \subseteq \omega$, $\varphi(P)$ is true in the standard model of arithmetic if and only if $P = S$. It is well known that each arithmetical singleton is a hyperarithmetical set and that each hyperarithmetical set is Turing reducible to an arithmetical singleton [9, 10, 11], a suitable iterate of the jump $\varnothing^{(\alpha)}$, $\alpha$ a recursive ordinal.

THEOREM 3.

(i) *For each arithmetical singleton $S$, there exists a 2–generated QFA–group $G$ whose word problem $W(G)$ satisfies*

$$S \leqslant_T W(G) \leqslant_T S'.$$

(ii) *For each arithmetical singleton $S$ and for each $n \geqslant 3$ there exists an $n$–generated QFA–group $G$ such that $W(G)$ is Turing equivalent to $S$.*

*Proof.* (i) Consider the group $G$ generated by $\widehat{z}, (0,1) \cdot f$, which is constructed as in the proof (i) of Theorem 1, where $f = f_S$ $\alpha$-codes $S$. Clearly, $f \equiv_T S$.

To prove that this group is QFA, consider a sentence $\varphi$ which says that this group possesses standard parameters, and with respect to the model $\widetilde{G}$ given by these standard parameters, there exists a permutation

$$f = (0,1) \cdot \prod_{m\in S} (3(m+1), 3(m+1)+1), 3(m+1)+2)$$

such that $f, z$ generate the whole group. The latter is expressed by a sentence which says the following:

– the only 2–cycle of $f$ is $(0,1)$;
– if $f$ moves an element $n$ then this $n$ is contained in a 3–cycle of the kind $(3(u+1), 3(u+1)+1, 3(u+1)+2)$;
– the set $\{u \mid f(3(u+1)) = 3(u+1)+1 \;\&\; f(3(u+1)+1) = 3(u+1)+2 \;\&\; f(3(u+1)+2) = 3(u+1)\}$ satisfies $\varphi(X)$.

Clearly, this axiomatizes $G$ amongst the f.g. groups.

We prove $S \leqslant_T W(G)$. Note that each f.g. group $G$ has a $W(G)$–computable copy; so we may consider $G$ as a $W(G)$–computable model. Since all transpositions can be obtained by conjugation from a single transposition, the set of transpositions of $G$ is $W(G)$–computably enumerable. Since the model $\widetilde{G} = \langle G, \mathbb{Z}, \mathrm{ap}\rangle$ is defined over $G$

by means of quantifier–free formulas, there exists a $W(G)$–computable presentation of it. Using this presentation, we can effectively in this presentation recognize the set $S$ using the following property:

$$k \in S \Leftrightarrow f(s^{3(k+1)+1}(0)) \neq s^{3(k+1)+1}(0).$$

Thus, $S \leqslant_T W(G)$.

On the other hand, the word problem of this group is $S'$–computable, since for each term $t$, $t(\widehat{z}, f) = 1 \Leftrightarrow \forall x(\mathrm{ap}(\tau(\widehat{z}, f), x) = x)$. Hence $W(G) \leqslant_T S'$.

To prove (ii), reconsider the group $G$ generated by elements $\widehat{z}, (0,1), \pi_1, \pi_2, \ldots$ as in the proof Lemma 2, where $\pi_1$ $\beta$-codes $S$, and all other $\pi_i$'s are Turing reducible to $\pi_1$. Again, the model $\langle G, \mathbb{Z}, \mathrm{ap}\rangle$ is $W(G)$–computable. The set $S$ can be computed in this model, which follows from the following two equivalences:

$$x \in S \Leftrightarrow \exists x[\widehat{z}(x) = \pi_1(x) \ \&\ \text{the minimal prime which divides } x \text{ is } p_{2x}]$$

$$x \in \omega \setminus S \Leftrightarrow \exists x(\widehat{z}(x) = \pi_1(x) \ \&\ \text{the minimal prime which divides } x \text{ is } p_{2x+1}].$$

By this, $S \leqslant_T W(G)$.

To prove $W(G) \leqslant S$, consider an arbitrary word

$$w = w_1 \tau w_2 \tau w_3 \tau \ldots w_k \tau w_{k+1}$$

on $\tau = (0,1)$, $\pi_1, \ldots, \pi_n$, where $w_i$ do not contain $\tau$. We have

$$\begin{aligned} w &= (w_1 \tau w_1^{-1}) w_1 w_2 \tau w_3 \tau \ldots w_k \tau w_{k+1} = \\ &= (w_1 \tau w_1^{-1})(w_1 w_2 \tau (w_1 w_2)^{-1}) w_1 w_2 w_3 \tau \ldots w_k \tau w_{k+1} = \\ &\text{etc.} \end{aligned}$$

Eventually we arrive at an expression

$$(u_1 \tau u_1^{-1})(u_2 \tau u_2^{-1}) \ldots (u_k \tau u_k^{-1}) v,$$

in which $u_1, u_2, \ldots, u_k, v$ do not contain $\tau$. Then in case $v \neq 1$ we have $w \neq 1$, since as is already noted above, the elements $\pi_1/_{\mathrm{Fin}}, \pi_2/_{\mathrm{Fin}}$ admit no nontrivial relations and $(u_1 \tau u_1^{-1}), (u_2 \tau u_2^{-1}), \ldots, (u_k \tau u_k^{-1}) \in \mathrm{Fin}$. If $v = 1$ then we can effectively in $S$ compute the elements which are moved by transpositions $(u_1 \tau u_1^{-1})$, $(u_2 \tau u_2^{-1})$, $\ldots$, $(u_k \tau u_k^{-1})$ and then check whether this product of transpositions equals 1. Recall that in this case this product equals $w$. Thus, $W(G) \leqslant_T S$.

The group is QFA, since it is axiomatized amongst the f.g. groups by the sentence which expresses, for some fixed $m \in \omega$,

- the group contains standard parameters with respect to which there exists a permutation $f$ which $\beta$–codes the set $S$ and
- the group is generated by permutations $\pi_0 = \{(m)_0\}^S, \pi_1 = \{(m)_1\}^S, \ldots$ together with $\widehat{z}$ and the 2–cycle $(0,1)$,

□

QUESTION. Does (ii) of Theorem 3 hold for $n = 2$?

COROLLARY 1. *For each $n \geq 2$, there is a strictly $n$-generated QFA group with solvable word problem.*

*Proof.* For $n = 2$ this was proved in [8], via the 2-generated group $\mathbb{Z}_2 \wr \mathbb{Z}$. For $n \geq 3$, take the group $G_{n,\varnothing}$. □

We say that an inclusion $S' \supseteq S$ of theories can be *QFA–separated* if there exists a QFA–group $G$ such that $G \models S$ but $G \not\models S'$.

COROLLARY 2. *Let* $2 \leq n < m$.
(i) *The inclusion* $T_n \supset T_m$ *can be QFA-separated.*
(ii) *The inclusion* $T_m^! \supset T_m$ *can be QFA-separated.*

*Proof.* (i). Take $H = G_{m,\varnothing}$. (ii) Let $H$ be a 2-generated group $\mathbb{Z}_p \wr Z$, which is QFA by [8]. □

## *References*


**1.** J. BARWISE, *Admissible Sets and Structures*, (Springer-Verlag, Berlin, Göttingen, Heidelberg, 1975).
**2.** P. HALL, 'Some constructions for locally finite groups.', *J. London Math. Soc.* 34 (1959) 305-319.
**3.** O. KHARLAMPOVICH, A. MYASNIKOV, 'Tarski's problem about the elementary theory of free groups has a positive solution', *Electronic research announcements of the AMS* 4 (1998) 101-108.
**4.** R. C. LYNDON, P. E. SCHUPP, *Combinatorial group theory*, (Springer-Verlag, Berlin-Heidelberg-New York, 1977).
**5.** R. MCKENZIE, 'On elementary types of symmetric groups', *Alg. Universalis* 1 (1971) 13-20.
**6.** A. S. MOROZOV, 'On the theories of classes of recursive permutation groups', *Proc. of the Inst. of Math. of Siberian Branch of the USSR Academy* 12 (1989) 91-104. (Russian), English translation in: *Siberian Advances in Mathematics*, 1 (1991) 138-153.
**7.** A. S. MOROZOV, 'Once more on countably categorical sentences', *Siberian Journ. of Math.* 40 (1999) 374-377.
**8.** A. NIES, 'Separating classes of groups by first-order formulas', *Intern. J. Algebra Computation.* 13, no 3 (2003) 287-302.
**9.** P. ODIFREDDI, *Classical Recursion Theory. The Theory of Functions and Sets of Natural Numbers*, (North–Holland, Amsterdam, New York, oxford, Tokio, 1989).
**10.** H. ROGERS, *Theory of Recursive Functions and Effective Computability*, (McGraw-Hill Book Company, New York, St. Louis, San Francisco, Toronto, London, Sydney, 1967).
**11.** G. E. SACKS *Higher Recursion Theory*, (Springer-Verlag, Heidelberg, 1990).
**12.** Z. SELA, 'Diophantine geometry over groups and the elementary theory of free and hyperbolic groups', *Proceedings of the International congress of mathematicians, Vol II* (2002) 87-92.
**13.** J. R. SHOENFELD, *Mathematical Logic*, (Addison-Wesley, 1967).
**14.** A. M. SLOBODSKOI, 'Undecidability of the universal theory of finite groups', *Algebra i Logika* 20 (1981) 207-230.
**15.** W. SZMIELEW, 'Elementary properties of abelian groups', *Fund. Math.* 41 (1955) 203-71.
**16.** A. TARSKI, 'Undecidability of group theory', *The Journ. of Symb. Logic* 14 (1949) 76-77. Abstracts of invited addresses and contributed papers, 11th Meeting of the Association of Symbolic Logic, Columbus, Ohio, 1948.
**17.** A. D. TAIMANOV, M. A. TAITSLIN, YU. L. ERSHOV and I. A. LAVROV, 'Elementary theories', *Russian Math. Surveys* 20 (1965) 35-105.



*Andrei Morozov*
*Sobolev Institute of Mathematics*
*Koptyug prosp. 4*
*Novosibirsk, 630090*
*Russia*

morozov@math.nsc.ru

*André Nies*
*University of Auckland*
*Auckland, New Zeland*

nies@math.uchicago.edu