J. Group Theory ▮ (2006), 1–15
DOI 10.1515/JGT.2006.▮▮▮

Journal of Group Theory

Comparing quasi-finitely axiomatizable and prime groups

Andre Nies

(Communicated by R. Göbel)

Abstract. An infinite f.g. group G is quasi-finitely axiomatizable (QFA) if there is a first-order sentence φ such that $G \models \varphi$, and if H is a f.g. group such that $H \models \varphi$, then $G \cong H$. The first result is that all Baumslag–Solitar groups of the form $\langle a, d \mid d^{-1}ad = a^m \rangle$ are QFA.

A f.g. group G is a prime model if and only if there is a tuple $g_1, \ldots, g_n$ generating G whose orbit (under the automorphisms of G) is definable by a first-order formula. The second result is that there are continuum many non-isomorphic f.g. groups that are prime models. In particular, not all are QFA.

1 Introduction

To what extent is a finitely generated group determined by its properties that are formalizable in first-order logic? We shall study two classes of groups related to this question, quasi-finitely axiomatizable groups and finitely generated (f.g.) groups that are prime models. The former can be distinguished among the f.g. groups by a single first-order axiom. The latter are determined by being the least model of their theory under elementary embeddings. We give new examples of QFA groups, and show that not every prime group is QFA, answering a question of Oger [10].

The first-order language of groups consists of formulas built up in the expected way from equations $t = s$, using brackets, the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$, and the quantifiers $\exists x$, $\forall x$. A *sentence* is a formula where every variables is in the range of some quantifier. For a group G, $\mathrm{Th}(G)$ is the set of sentences which hold in G. For more terminology from mathematical logic, see Subsection 1.2.

An infinite finitely generated group G is *quasi-finitely axiomatizable* (*QFA*) if there is a single first-order property that, along with the information that the group is f.g., determines G; see [8]. That is, there is a first-order sentence φ such that

- $G \models \varphi$, and
- if H is a f.g. group such that $H \models \varphi$, then $G \cong H$.

The author was partially supported by the Marsden Fund of New Zealand, grant no. 03-UOA-130.

No abelian group is QFA; see [8]. Examples of QFA groups include the Heisenberg group $\mathrm{UT}_3^3(\mathbb{Z})$ (that is, the free class 2 nilpotent group of rank 2) [8], and the subgroup $P_\varnothing$ of $\mathrm{Sym}(\mathbb{Z})$ generated by the transposition $(0,1)$ and successor [5]. The first-order properties characterizing them are complex, and the proofs in [5] and [8] are of a logical nature. Oger and Sabbagh [11] gave an algebraic characterization of being QFA for f.g. nilpotent groups: G is QFA if and only if each central element has a power in the commutator subgroup (or equivalently, no finite index subgroup has $\mathbb{Z}$ as a direct factor). This also gives an alternative, algebraic proof that $\mathrm{UT}_3^3(\mathbb{Z})$ is QFA.

We shall introduce examples of QFA groups of another type: for each $m \geqslant 2$, the group

$$H_m = \mathbb{Z}[1/m] \rtimes \mathbb{Z} = \langle a, d \mid d^{-1}ad = a^m \rangle$$

is QFA. These groups are Baumslag–Solitar groups, introduced in [1]. The proof that they are QFA is purely algebraic.

A more inclusive notion than being QFA is the following: an infinite f.g. group G is *quasi-axiomatizable* if all first-order properties together suffice to single out G among the f.g. groups. That is, if H is f.g. and $\mathrm{Th}(H) = \mathrm{Th}(G)$ then $H \cong G$. It is not sufficient to require that H be countable, by general model theory [2, Theorem 7.3.1.]: if n is the rank of G, then the theory of G has infinitely many $(n+1)$-types and thus cannot be countably categorical, that is, it has non-isomorphic countable models.

Each infinite f.g. abelian group is quasi-axiomatizable. On the other hand, there is a f.g. group which is nilpotent of class 3 and not quasi-axiomatizable (see [6, Section 5]).

The following notion comes from model theory. A group G is said to be a *prime model* (or to be *prime*, for short) if G is an elementary submodel of each group H such that $\mathrm{Th}(G) = \mathrm{Th}(H)$. If a theory has a prime model then the model is unique up to isomorphism. For instance, $(\mathbb{Q}, +)$ and the Prüfer group $\mathbb{Z}(p^\infty)$ for each prime number p are prime models. However, various theories of groups fail to have a prime model, for instance $\mathrm{Th}(\mathbb{Z}, +)$ and $\mathrm{Th}(F_2)$. For the free group, see [7]. Possibly the easiest example of a f.g. prime group is the Heisenberg group $\mathrm{UT}_3^3(\mathbb{Z})$.

By model theory, G is prime if and only if each realized type is principal [2]. This leads to the following, more algebraic characterization of being prime for f.g. groups. For a proof, see [11].

Fact 1.1. Let G be a f.g. group. Then G is prime if and only if there is a generating tuple $g_1, \ldots, g_n$ whose orbit (under the automorphisms of G) is definable by a first-order formula without parameters.

Note that this closely resembles the definition of a QFA group. In fact, the following is an open question of Oger and Sabbagh.

Question 1.2 ([10]). Is each QFA group prime?

All the examples of QFA groups discussed above are prime:

Oger and Sabbagh [11] showed that if G is a nilpotent f.g. group, then G is QFA if and only if G is prime. In particular, $\mathrm{UT}_3^3(\mathbb{Z})$ is prime (this also follows from the proof in [8] that $\mathrm{UT}_3^3(\mathbb{Z})$ is QFA). This equivalence was extended to nilpotent-by-finite groups by Oger [10].

Khelif (personal communication) has shown that the groups H_m are prime. In this case, unlike $\mathrm{UT}_3^3(\mathbb{Z})$, the generating tuple with definable orbit cannot be inferred directly from the QFA proof. Indeed, the author hoped when considering H_m that it would provide a counter-example, thereby answering Oger's question in the negative.

We will see in Corollary 3.8 that the QFA group $P_\varnothing$ introduced above is prime.

Oger [10] also asked if, conversely, each prime group is QFA. As a corollary to the second result of the paper we answer this question in the negative. There is a class of size $2^{\aleph_0}$ of non-isomorphic f.g. groups that are prime. But, of course, there are only countably many QFA groups, up to isomorphism. (However, the whole *class* consists of the f.g. groups satisfying a sentence α.)

While most of the groups above fail to be QFA, all of them are quasi-axiomatizable. We do not know at present if this is necessarily so for each f.g. prime group.

1.1 Basics. *Group-theoretic notation*. We write $\mathrm{Conj}(g, w)$ for the conjugate $w^{-1}gw$. The *commutator* $[x, y]$ is the term $x^{-1}y^{-1}xy$. If G is a group and $X \subset G$, then $\langle X \rangle_{\mathrm{gp}}$ is the subgroup generated by X, and $\mathrm{Ncl}(X)$ is the normal closure of X.

Turing and many-one reducibility. For sets $X, Y \subset \mathbb{N}$, X is Turing reducible to Y (written $X \leqslant_T Y$) if there is an oracle Turing machine computing X when the oracle is Y (see [9] for more details). Here is a special case if many-one reducibility: X is many-one reducible to Y if there is a computable function f such that $X = f^{-1}(Y)$.

For $m, n \in \mathbb{N}$, we write $\langle m, n \rangle = m + (n + m)(n + m + 1)/2$; this defines the Cantor pairing function, a bijection $\mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$.

The *word problem* $W(G)$ for a f.g. group G is the problem of deciding whether $t(x_1, \ldots, x_n) \in N$, where $G \cong F(x_1, \ldots, x_n)/N$ is a fixed presentation of G. It is easy to see that, up to many-one degree, this is independent of the particular presentation.

1.2 First-order logic. Here are some examples what first-order logic can express in groups.

The sentence $\forall x \forall y [x, y] = 1$ expresses that the group is abelian.

The sentence $\forall u, v \exists r, s, t [u, v] = r^2 s^2 t^2$ holds for all groups. (Let $r = u^{-1}v^{-1}$, $s = vuv^{-1}$, $t = v$.)

A first-order language and the notions of theory etc. can be defined for any set of symbols denoting constant, functions, or relations. Such a set of symbols is called a *signature*. For instance, the signature of groups is $\{1, \circ, {}^{-1}\}$, and the signature of ordered rings is $\{<, 0, +, \times)\}$.

The formulas at the bottom are called *atomic relations*. They do not involve quantifiers or connectives. For instance, $u \circ v = v \circ u$ is an atomic relation in the first-order language of groups (in the examples above, we have omitted $\circ$ in the usual way), and $y < x \times x$ is an atomic relation in the first-order language of ordered rings.

If G is a group, $\psi(x_1, \ldots, x_n)$ is a first-order formula with the free variables displayed and $g_1, \ldots, g_n \in G$, then $G \models \psi(g_1, \ldots, g_n)$ denotes that in G, ψ holds for $g_1, \ldots, g_n$. A relation $R \subseteq G^n$ is *first-order definable* if there is a formula $\psi(x_1, \ldots, x_n)$ such that

$$R = \{(g_1, \ldots, g_n) : G \models \psi(g_1, \ldots, g_n)\}.$$

For instance, the formula $\psi(x) \equiv \forall u[x, u] = 1$ defines the center in a group in a first-order way. The commutator subgroup is not in general first-order definable, as arbitrarily long finite products are not part of our language. Sometimes we allow fixed elements from G in ψ: in that case R is called *first-order definable with parameters*. An example is the centralizer of an element d of the group, that is, $C = \{x : [x, d] = 1\}$.

Interpretations via first-order formulas are introduced in [2, Chapter 5]. Roughly speaking, $\mathbf{B}$ is interpretable in $\mathbf{A}$ if the elements in $\mathbf{B}$ can be represented by tuples in a definable relation D on $\mathbf{A}$, in such a way that equality of $\mathbf{B}$ becomes a definable equivalence relation E on $\mathbf{A}$, and the other atomic relations on $\mathbf{B}$ are also definable. A simple example is the difference group construction: $(\mathbb{Z}, +)$ can be interpreted in $(\mathbb{N}, +)$, where the relation D is $\mathbb{N} \times \mathbb{N}$, addition is component-wise and E is the relation given by $(n, m)E(n', m')$ if and only if $n + m' = n' + m$. Further examples include the quotient field construction and $\mathrm{GL}_n(R)$ for fixed $n \geqslant 1$, which can be first-order interpreted in the ring R. A matrix B is represented a tuple of length n^2, D is given by the first-order condition that $\det(B)$ is a unit of R, and E is simply equality of tuples. Multiplication of matrices can be expressed in a first-order way using the ring operations.

For more background, see the survey article [6].

2 New examples of QFA groups

We write $\mathbb{Z}(m)$ for the cyclic group $\mathbb{Z}/m\mathbb{Z}$. For groups G, A, C, recall that $G = A \rtimes C$ (G is a *semidirect product* of A by C) if

$$AC = G, \quad A \lhd G, \quad \text{and} \quad A \cap C = \{1\}.$$

A group G is *metabelian* if its commutator group $G' = \langle \{[x, y] : x, y \in G\} \rangle_{\mathrm{gp}}$ is abelian; that is, if G has solvability length 2. All known examples of solvable non-nilpotent QFA groups are semidirect products $H = A \rtimes C$, where A abelian and C is infinite cyclic. For any such group H, we have

Lemma 2.1. *The set of commutators of H forms a subgroup. In fact, $H' = \{[u, d] : u \in A\}$. In particular $H' \leqslant A$.*

For a proof, see [8, Lemma 2.5 (i)].

We shall give two types of examples of metabelian QFA groups. Both are semidirect products $A \rtimes C$ as above. The ones of the second type are one-relator groups, first studied by Baumslag and Solitar. The ones of the first type from [8] are not even finitely presented.

Theorem 2.2. (i) *For each prime p, the restricted wreath product $\mathbb{Z}(p) \wr \mathbb{Z}$ is QFA.*

(ii) *For each $m \geqslant 2$, the group*

$$H_m = \langle a, d \mid d^{-1}ad = a^m \rangle$$

is QFA.

By definition, $\mathbb{Z}(p) \wr \mathbb{Z}$ is a semidirect product $A \rtimes C$, where $A = \bigoplus_{r \in \mathbb{Z}} \mathbb{Z}(p)^{(r)}$, $\mathbb{Z}(p)^{(r)}$ is a copy of $\mathbb{Z}(p)$, and $C = \langle d \rangle_{\mathrm{gp}}$ with d of infinite order. The element d acts on A by shifting, i.e., the copy $\mathbb{Z}(p)^{(r)}$ is mapped to the copy $\mathbb{Z}(p)^{(r+1)}$.

The group H_m is a semidirect product of $A = \mathbb{Z}[1/m] = \{zm^{-i} : z \in \mathbb{Z}, i \in \mathbb{N}\}$ by $\langle d \rangle$, where the action of d is given by $d^{-1}ud = um$.

Oger [10] has found further examples of this type, using some algebraic number theory. In his examples, A is free abelian of finite rank, while in the ones above, A is not f.g. A typical case is $A = \mathbb{Z}[u]$ where $u = 2 + \sqrt{3}$, and the action of d is given by $a \mapsto au$ for $a \in A$.

Proof. The proofs of (i) and (ii) (and to some extent also Oger's example) follow the same scheme. For the sake of comparison, we also sketch the proof of (i) from [8], in slightly simplified form.

The group A is given by a first-order definition in G. One writes a list $\psi(d) = (\mathrm{P}1) \wedge \cdots \wedge (\mathrm{P}k)$ of first-order properties of an element d in a group G so that the group in question is QFA via the sentence $\exists d \psi(d)$.

Let $C = C(d)$ be the centralizer of d, that is, $C = \{x : [x, d] = 1\}$. In the following,

$$u, v \text{ denote elements of } A \text{ and } x, y \text{ elements of } C.$$

(P1) The commutators form a subgroup.

(P2) A and C are abelian, and $G = A \rtimes C$.

(P3) $C - \{1\}$ acts on $A - \{1\}$ without fixed points. That is, $[u, x] \neq 1$ for all $u \in A - \{1\}$, $x \in C - \{1\}$.

(P4) $|C : C^2| = 2$.

Clearly these conditions can be formulated in the first-order language of groups. By (P1), G' is definable.

(i) To specify $\mathbb{Z}_p \wr \mathbb{Z}$, one uses the definition $A = \{g : g^p = 1\}$, and requires in addition that $|A : G'| = p$ and no element in $C - \{1\}$ has order less than p. The remaining details are as in [8].

(ii) To specify H_m one fixes a prime q not dividing m. One uses the definition

$$A = \{g : g^{m-1} \in G'\}.$$

The remaining conditions are as follows.

(P5) $\forall u\ d^{-1}ud = u^m$.

(P6) The map $u \mapsto u^q$ is 1–1.

(P7) $x^{-1}ux \neq u^{-1}$ for $u \neq 1$.

(P8) $|A : A^q| = q$.

(P9) $\forall g\ g^i \neq d$, for each i, $1 < i \leqslant m$.

We first verify that (H_m, d) satisfies the properties. (P1) holds by Lemma 2.1, and (P2)–(P9) are obviously satisfied, once we show that the first-order definition of A is correct, that is,

$$\mathbb{Z}[1/m] = \{g : g^{m-1} \in H'_m\}.$$

To do this, note that $H'_m \leqslant \mathbb{Z}[1/m]$ since $H_m/\mathbb{Z}[1/m]$ is abelian. First suppose that $g \in \mathbb{Z}[1/m]$. Then $[g, d] = g^{m-1}$, so that $g^{m-1} \in H'_m$. For the other inclusion, it suffices to notice that $\mathbb{Z}[1/m]$ is closed under taking roots, because $H_m/\mathbb{Z}[1/m]$ is torsion-free. Thus, if $g \notin \mathbb{Z}[1/m]$ then $g^{m-1} \notin \mathbb{Z}[1/m]$ and in particular, $g^{m-1} \notin H'_m$.

Now suppose that G is a f.g. group, and $d \in G$ satisfies the properties (P1)–(P9). We first show that d has infinite order. If $d^r = 1$ for $r > 0$, then for each $u \in A$ we have $u = \mathrm{Conj}(u, d^r) = u^{mr}$. So one may choose k minimal such that $A^k = \{1\}$. If the prime q divides k, then the q-primary component $\{g \in A : \exists i\ g^{(q^i)} = 1\}$ is non-trivial, so that the map $u \mapsto u^q$ is not 1–1, contrary to (P6). If q does not divide k, then this map is an automorphism of A, contrary to (P8).

Let $\mathscr{R} = \mathbb{Z}[1/m]$, viewed as a ring. Then A is turned into an $\mathscr{R}$-module by defining $u(zm^{-i}) = \mathrm{Conj}(u^z, d^{-i})$ for $z \in \mathbb{Z}$, $i \in \mathbb{N}$.

Claim 2.3. *A is f.g. and torsion-free as an $\mathscr{R}$-module.*

To prove this, note that C is f.g. and abelian, and C has only one infinite cyclic factor by (P4). Since d has infinite order, one can choose $c \in C$ such that $c^s = d$ for some $s \geqslant 1$, and $\langle c\rangle_{\mathrm{gp}} \times F = C$ where $F = T(C)$ is the torsion subgroup. Since $G = AC$, G has a finite generating set of the form $B \cup \{c\} \cup F$ where $B \subseteq A$. We may assume that B is closed under inverses, and under conjugation by elements of the finite set $F \cup \{c^i : 1 \leqslant i < s\}$. If $u \in A$ then $u = 1$ in G/A, so that u can be written as a product of terms $\mathrm{Conj}(b, xc^z)$, where $x \in F$, $z \in \mathbb{Z}$, $b \in B$, and therefore of terms $\mathrm{Conj}(b, d^w)$, where $w \in \mathbb{Z}$, by the closure properties of B. This shows that A is f.g. as an $\mathscr{R}$-module.

To show that A is torsion-free as an $\mathscr{R}$-module, suppose that

$$u(zm^{-i}) = \mathrm{Conj}(u^z, d^{-i}) = 1 \quad \text{for } u \neq 1,\ i \geqslant 0,\ z \neq 0.$$

Then $u^z = 1$. Conjugation by d is an automorphism of the finite subgroup $\langle u\rangle_{\mathrm{gp}}$, by (P5), and so some power of d has a fixed point, contrary to (P3). This proves the claim.

Since $\mathscr{R}$ is a principal entire ring, we may conclude that A is free (see Lang [3, Theorem XV.2.2]), so that A is isomorphic to the additive group of $\mathscr{R}^k$ for some k. Then $|A : A^q| = q^k$ and hence $k = 1$ by (P8). Next, $F = T(C)$ is trivial by (P7), because the only non-trivial automorphism of finite order of $\mathbb{Z}[1/m]$ is the inversion map. Choose $i \geqslant 1$ such that $c^i = d$ where $\langle c \rangle_{\text{gp}} = C$. Then $i \leqslant m$ because the automorphism $u \mapsto um$ is not an ith power in $\text{Aut}(\mathbb{Z}[1/m])$ for any $i > m$. (However, it may be a proper power, for instance if $m = 9$, in which case $\mathbb{Z}[1/m] = \mathbb{Z}[1/3]$.) So $i = 1$ by (P9), and d generates C. This shows that $G \cong H_m$. □

3 $2^{\aleph_0}$ many non-isomorphic f.g. prime groups

Generalizing the concept of a QFA group, we shall say a class $\mathscr{C}$ of f.g. groups is QFA if there is a first-order axiom φ such that for each f.g. group G,

$$G \in \mathscr{C} \quad \text{if and only if} \quad G \models \varphi.$$

Thus, a group G is QFA if and only if the class $\{G\}$ is. The following theorem establishes a QFA class of prime groups with continuum many non-isomorphic members, via the axiom $\varphi \equiv \exists w, h\ \psi(w, h)$.

Theorem 3.1. *There is a first-order formula $\psi(w, h)$ such that,*

(i) *for each f.g. group P, if $w, h \in P$ and $P \models \psi(w, h)$, then P is prime. In fact, w, h generate P and ψ defines the orbit of w, h within P.*

(ii) *there are 2^ω many non-elementary equivalent such groups P. More precisely, for each non-empty $Y \subseteq \mathbb{N}$, there is a 2-generated group P_Y which is prime model such that Y can be recovered from $\text{Th}(P_Y)$. Moreover, Y is Turing below the word problem of P_Y, which is Turing below Y'.*

The following answers a question of Oger [10].

Corollary 3.2. *There is a f.g. prime group which is not quasi-finitely axiomatizable.*

Proof. Of course this follows from Theorem 3.1, because there are only countably many QFA groups (up to isomorphism). For a somewhat more concrete counterexample, we may use the fact [5, Theorem 2] that each QFA group has a hyperarithmetical word problem. Now choose Y not hyperarithmetical; then the word problem for P_Y is again not hyperarithmetical by the last statement in (ii), and so P_Y is not QFA. □

In order to prove Theorem 3.1, we need to discuss the construction of QFA groups in [5]. In [5], it is shown that for each arithmetical singleton S, there exists a 2-generated QFA group G_S whose word problem $W(G)$ satisfies $S \leqslant_T W(G) \leqslant_T S'$. This construction works for any set S, though only the arithmetical singletons yield a QFA group. A modification of this construction will lead to the prime groups P_Y.

(A set $S \subseteq \omega$ is called an arithmetical singleton if there exists a formula $\varphi(X)$ in the language of arithmetic extended by a new unary predicate symbol X such that for each $P \subseteq \omega$, $\varphi(P)$ is true in the standard model of arithmetic if and only if $P = S$.)

Consider a group G in which a set $\mathbf{Z}_G$ can be interpreted (without parameters), in the sense of Subsection 1.2. Thus $\mathbf{Z}_G = D/E$, where $D \subseteq G^n$ is a first-order definable relation and E is a first-order definable equivalence relation on D. Then G acts on $\mathbf{Z}_G$ by conjugation, and one can require in a first-order way that this action be faithful.

In what we call the 'concrete case' in [5], the QFA groups G are subgroups of $\mathrm{Sym}(\mathbb{Z})$ which contain the successor and $(0, 1)$, and hence all permutations with finite support. D is the set of pairs $\langle u, v\rangle$ of transpositions whose supports share exactly one element (we say that they *hold* this element). In [4] it is shown that D is first-order definable, by the formula

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

Next, two pairs $\langle u, v\rangle \in D$, $\langle u', v'\rangle \in D$ are equivalent modulo E if they hold the same element. Again, this relation is first-order definable in G; see [5]. The groups considered in the 'abstract case' are those f.g. groups H satisfying an axiom α_0, which says that the defined sets behave in the expected way, namely, that the formula for E defines an equivalence relation on the non-empty set D, and the action is faithful. Thus, whenever H is f.g. and $H \models \alpha_0$, then we have a non-empty domain

$$\mathbf{Z}_H = D/E,$$

where D and E are defined without parameters in H via the formulas mentioned above.

To pin G down further in the concrete case, we also interpret a structure with domain $\mathbf{Z}_G$. We use parameters w, s, t to define a copy of $(\mathbb{Z}, <, 0, +, \times)$ on $\mathbf{Z}_G$. The action of the parameter w determines a permutation with only one cycle on $\mathbf{Z}_G$, which becomes the successor relation. The E-equivalence class of the pair $\langle s, t\rangle$ represents 0.

In the concrete case, $w = \hat{z}$ is successor on $\mathbb{Z}$, $s = (-1, 0)$ and $t = (0, 1)$. Using that G contains all permutations with finite support, one can define $<$, as well as $+$, $\times$ on $\mathbf{Z}_G$. In the abstract case, let $\mathbf{Z}_{w,s,t}$ be the structure interpreted in G via these formulas. By a further first-order condition, one can require that the basic axioms of arithmetic hold. However, in general $\mathbf{Z}_{w,s,t}$ may be a non-standard version of $\mathbb{Z}$, that is, there may be elements greater than each natural number. The main idea in [5] is to transform the property of being finitely generated into a first-order condition for standardness: we develop a formula $\mathrm{Standard}(w, s, t)$ which for each f.g. group G ensures that $\mathbf{Z}_{w,s,t}$ is standard, and which holds for the parameters $\hat{z}$, $s = (-1, 0)$, $t = (0, 1)$, in f.g. permutation groups G satisfying some fairly general properties.

This is summarized in the following lemma, stating that if G is f.g. and $G \models \mathrm{Standard}(w, s, t)$, then G can be viewed as a subgroup of $\mathrm{Sym}(\mathbf{Z}_G)$, and we have the full power of arithmetic to describe, within G, properties of the permutations.

Main Lemma 3.3 ([5]). *There exists a formula* $\mathrm{Standard}(w, s, t)$ *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 has an element* f *such that each* $g \in G$ *is Turing-reducible to* f *and which contains all finitary permutations and the permutation* $\hat{z}(x) = x + 1$,

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

(ii) (*Abstract case*) *Assume that* G *is a f.g. group and* w, s, t *are elements such that* $G \models \mathrm{Standard}(w,s,t)$. *Then* $\mathbf{Z}_{w,s,t} = (\mathbf{Z}_G, <_{w,s,t}, 0_{w,s,t}, +_{w,s,t}, \times_{w,s,t})$ *is standard, and* w, *when viewed as a permutation of* $\mathbf{Z}_G$, *becomes the successor function.*

Proof of Theorem 3.1. We begin with some notation. Recall that $\mathrm{Conj}(g,w)$ denotes the conjugate $w^{-1}gw$. The image of an element y under a map f is denoted by yf, and fg denotes the map $x \mapsto (xf)g$. Moreover,

- for $r \in \mathbb{N}$, let $k(r) = 2 + 3r(r+1)/2$. Then $k(r+1) - k(r) = 3(r+1)$. The set $\{2, 5, 11, 20, \ldots\}$ of such numbers is called the set of *coding locations*.
- If $c \in \mathbb{N}$ and $x \in \mathbb{Z}$, let $B_c(x) = \{y : |y - x| \leqslant c\}$.
- Given $Y \subseteq \mathbb{N}$, let

$$\hat{Y} = \{k(\langle x, m\rangle) : x \in Y, m \in \mathbb{N}\}.$$

For each Y, the desired group P_Y is a subgroup of $\mathrm{Sym}(\mathbb{Z})$, namely

$$P_Y = \langle \hat{z}, h_Y \rangle_{\mathrm{gp}},$$

where $\hat{z}$ is successor and

$$h_Y = (0,1) \cdot \prod_{k \in \hat{Y}} (k, k+1, k+2). \tag{1}$$

The group P_Y is a variant of the group G_S from [5], where $S = \hat{Y}$. The main difference is that here a set $Y \subseteq \mathbb{N}$ is coded at locations $k(r)$ which are further and further apart. Clearly, $h_Y \equiv_T \hat{Y}$, and $g \leqslant_T h_Y$ for each $g \in P_Y$, so that the hypothesis in (i) of the Main Lemma 3.3 is satisfied. The formula $\psi(w,h)$ lists first-order properties of elements w, h in a group H, satisfied by $\hat{z}$, h_Y in P_Y, so that the conclusions of Theorem 3.1 can be reached.

(B1) $\mathrm{Standard}(w,s,t)$ *holds, where* $s = h^3$, $t = w^{-1}sw$. We write $\mathbf{Z}_{w,h}$ for the copy $\mathbf{Z}_{w,s,t}$ of $(\mathbb{Z}, <, 0, +, \times)$ defined on $\mathbf{Z}_H$. The elements of H can now be viewed as permutations of $\mathbf{Z}_H$.

(B2) *The elements* w, h *generate the whole group*. This is first-order because we can existentially quantify over free group terms within the model $\mathbf{Z}_{w,h}$. See [5] for details.

(B3) *With respect to* $\mathbf{Z}_{w,h}$, *the only* 2*-cycle of* h *is* $(0,1)$, *and if* h *moves an element* $x \neq 0,1$ *then this* x *is contained in a* 3*-cycle of the kind* $(k, k+1, k+2)$, *where* $k = k(r)$ *for some* r. Let

$$Y_{w,h}$$

be the set of numbers $k(r)$ for which there is such a 3-cycle.

(B4) $Y_{w,h} \neq \varnothing$, *and* $Y_{w,h}$ *has the following* padding property:
(pad) *for all* $x, m, m' \in \mathbb{N}$, *we have* $k(\langle x, m\rangle) \in Y_{w,h}$ *if and only if* $k(\langle x, m'\rangle) \in Y_{w,h}$.
In particular, $Y_{w,h}$ is infinite.

To verify $P_Y \models \psi(\hat{z}, h_Y)$, note that in (B1) each permutation of P_Y is Turing below h_Y. The other properties are obvious.

Next we prove a crucial lemma. Fix a f.g. group H. Then the set $Y_{w,h}$ represented by parameters w, h such that $H \models \psi(w,h)$ is always the same (but it depends on H). From this we will conclude that any two such pairs (w,h) and (w',h') of parameters are automorphic, in fact conjugate in $\mathrm{Sym}(\mathbb{Z})$. Since any such pair generates H, this shows that H is prime, by Fact 1.1.

Lemma 3.4. *Let* H *be f.g. and let* $w, h, w', h' \in H$. *If* $H \models \psi(w,h)$ *and* $H \models \psi(w',h')$, *then* $Y_{w,h} = Y_{w',h'}$.

Proof idea. We view $\mathbf{Z}_{w,h}$ as our '*reference copy*' of $(\mathbb{Z}, <, 0, +, \times)$ within H. Each $g \in H$ is viewed as a permutation of this copy. By (B1) for w', h' and the Main Lemma 3.3, $\mathbf{Z}_{w',h'}$ is a further copy, with the same domain $\mathbf{Z}_H$. Let

$$p : \mathbf{Z}_{w,h} \mapsto \mathbf{Z}_{w',h'}$$

be the unique isomorphism, which is a permutation of $\mathbf{Z}_H$. We want to show that passing from w, h to w', h' does not change the set coded, and in fact $h' = p^{-1}hp$.

(a) The first goal is to show that p is close to the identity, namely

$$|xp - x| \text{ is bounded}$$

(In the following, arithmetical operations like difference, absolute value etc. are always taken in the reference copy $\mathbf{Z}_{w,h}$.) We use that by (B2), $w' = h^j v$ for some $v \in \mathrm{Ncl}(w)$. Then w' is sufficiently similar to w to show that p is close to being the identity. For a while, we have to carry along the case that instead, w' is similar to w^{-1}.

(b) The second goal is to show that h' is sufficiently similar to h that applying (a) we can conclude that $Y_{w,h} = Y_{w',h'}$. We use that $h' = w^j g$ for some $g \in \mathrm{Ncl}(h)$ and $j \in \mathbb{Z}$. Thus $g = t(h,w)$ where t is a product of conjugates of powers of h by powers of w. Then, for sufficiently large x, $xg \neq x$ implies that $xg = xt(C_{k(r)}, h)$, where $k(r) \in Y_{w,h}$ is a coding location close to x. Here C_x denotes the cycle $(x, x+1, x+2)$. Thus, the value xg is determined by a unique cycle $C_{k(r)}$, not by the interaction of

various cycles, because the coding locations $k(r)$ are sufficiently far apart for large enough r. Then $j = 0$.

Details. To reach goal (a), we first show that w' is merely a small perturbation of the successor w in our reference copy, or of its inverse. In the first case, for an appropriate c, $xw' \neq xw$ is only possible if both x and xw' are within c of some coding location.

Claim 3.5. *There is an* '*orientation*' $b = b_{w'} \in \{1, -1\}$ *and* $c \in \mathbb{N}$ *such that*

$$\forall x\ xw' \neq xw^b \Rightarrow \exists r\ x, xw' \in B_c(k(r)). \tag{2}$$

Proof. We use that w' consists of only one cycle. Note that $w' \notin \langle h \rangle_{\mathrm{gp}}$, so that we can write

$$w' = h^j \prod_{i=1}^{n} \mathrm{Conj}(w^{b_i}, h^{t_i}),$$

where $n \geqslant 1$, $b_i \in \{1, -1\}$, $0 \leqslant t_i < 6$ and $0 \leqslant j < 6$. Let $b = \sum_i b_i$. If $xw' \neq xw^b$, then there is a least m such that the application of h affects the mth factor of the product (here h^j is considered the 0th factor). In more detail, let $P_m = h^j \prod_{i=1}^{m-1} \mathrm{Conj}(w^{b_i}, h^{t_i})$; then either $xh \neq x$, or there is an $m \geqslant 1$ such that

$$xP_{m-1} = xw^{\sum_{i<m} b_i} =: z$$

but $zh \neq z$ or $zh^{-t_m} w^{b_m} h \neq zh^{-t_m} w^{b_m}$. By (B3), this implies that $x \in B_{n+2}(k(r))$ for some r.

Clearly $|x - xw'| \leqslant 5n + 2$. So letting $c = 6n + 4$, we have $xw' \in B_c(k(r))$. This shows that (2) holds.

It remains to verify that $b \in \{1, -1\}$. Assume otherwise. Pick x such that

$$k(r) + c < x < k(r+1) - c \quad \text{for some } r \geqslant c.$$

If $b = 0$ there is a trivial cycle, and this is a contradiction. Otherwise, say $b > 1$. Then applying the permutation w' to y yields $y + b$, for each y in the interval $(k(r) + c, k(r+1) - c)$. The cycle of w' can only connect x, $x + 1$ if there is $y > k(r+1) - c$ such that $yw' < k(r) + c$, which is impossible by (2). □

Claim 3.6. *Let* p *be the isomorphism* $\mathbf{Z}_{w,h} \mapsto \mathbf{Z}_{w',h'}$.

(i) *If* $b_{w'} = 1$ *then* $\exists u \in \mathbb{N} \forall x\ |xp - x| < u$.

(ii) *If* $b_{w'} = -1$ *then* $\exists u' \in \mathbb{N} \forall x > 0\ |xp + x| \leqslant u'$.

Proof. Let c be as in Claim 3.5.

(i) If $x < x_0 = k(0) - c$, then $xw' = x + 1$. So $xp - x = x_0 p - x_0$ for each $x < x_0$.

Let $y_r = k(r) + c + 1$. By (2), for each $r \geqslant c$ and each $x \in \mathbf{Z}_H$,

$$x <_{w',h'} y_r \quad \text{if and only if} \quad x <_{w,h} y_r.$$

Hence $y_r p - y_r = y_c p - y_c$ for each $r \geqslant c$. If $x \in [y_r, k(r+1) - c)$ then $xw' = xw^b$ by (2) again. So $xp - x = y_r p - y_r$. While the cycle of w' is within $B_c(k(r))$, $r \geqslant c$, $|xp - x|$ can increase by at most $2c$. The desired bound u is therefore the maximum of $|y_c p - y_c| + 2c$ and $\max(\{|xp - x| : x_0 \leqslant x \leqslant k(c) + c\}$, where $x_0 = k(0) - c$ as above.

(ii) is simpler, since $xh = x$ and hence $xw' = xw^{-1} = x - 1$ for any $x < 0$. Let $x_0 \in \mathbf{Z}_H$ be least such that $x_0 p < 0$, then $(x_0 + r)p = x_0 p - r$ for any $r > 0$. This shows that $|xp + x|$ is bounded for any $x > 0$. $\square$

For $x \in \mathbf{Z}_{w,h}$, recall that C_x denotes the cycle $(x, x+1, x+2)$. Notice that

$$\mathrm{Conj}(C_x, w^s) = C_{x+s} \quad \text{for each } s \in \mathbb{Z}.$$

We have almost reached goal (a), but we do not yet know that $B_{w'} = 1$. For this and also to reach (b), we analyze elements in the normal closure $\mathrm{Ncl}(h)$ of h, i.e. elements of the form

$$g = \prod_{0 \leqslant i < m} h_i, \quad \text{where } h_i = \mathrm{Conj}(h^{t_i}, w^{s_i}),\ 0 \leqslant t_i < 6,\ s_i \in \mathbb{Z}.$$

Let

$$d = 2 + \max_i |s_i|,$$

and let $q = k(d) - d$. We will show in Claim 3.7 below that $\{x : x < q\}$ is closed under application of the maps g and g^{-1}. On the other hand, for $x \geqslant q$, the value xg is determined by a unique cycle $C_{k(r)}$ of h.

To prepare this, suppose that $xh_i \neq x$. Then either $\{x, xh_i\} = \{s_i, s_{i+1}\}$ or $xh_i = xC_{k(r)+s_i}^{t_i}$ for some unique r. Note that

$$x < q \Leftrightarrow r < d \Leftrightarrow h_i(x) < q. \tag{3}$$

(To prove the first equivalence, say, if $r \geqslant d$, then $x \geqslant k(r) + s_i - 2 \geqslant k(d) - d = q$. If $r < d$, then $x < k(d-1) + s_i + 2 < q$, because $k(d) - k(d-1) = 3d$. The second equivalence is similar.)

We write

$$t(v, w) = \prod_{0 \leqslant i < m} \mathrm{Conj}(v^{t_i}, w^{s_i}).$$

Claim 3.7. *Let $g = t(h, w) = \prod_{0 \leqslant i < m} h_i$, where $h_i = \mathrm{Conj}(h^{t_i}, w^{s_i})$, and let d, q as above. Then*

(i) $x < q$ *if and only if* $xg < q$.

(ii) *If* $x \geqslant q$ *and* $xg \neq x$, *then there is* $r \geqslant d$ *such that* x, $xg \in B_d(k(r))$, *and* xg *is obtained by applying* $t(C_{k(r)}, w)$ *to* x.

Proof. (i) is immediate from (3).

(ii) Suppose that $x \geqslant q$ and $xg \neq x$. For $n \leqslant m$, let $g_n = \prod_{0 \leqslant i < n} h_i$ (where g_0 is the identity). By (3), $xg_n \geqslant q$ for each n. Since $B_d(k(r)) \cap B_d(k(r')) = \varnothing$ for distinct $r, r' \geqslant d$, there is a *fixed* $r \geqslant q$ such that, if $xg_i \neq xg_{i+1}$, then the permutation $C_{k(r)+s_i}^{t_i}$ was applied. Thus $xg = xt(C_{k(r)}, w)$. □

To reach goal (b) (showing that h' is similar to h) note that by (B2), there are $j \in \mathbb{Z}$ and $g \in \mathrm{Ncl}(h)$ such that $h' = w^j g$. Applying Claim 3.7 to g, we obtain d and $q = k(d) - d$. We show that $j = 0$. Otherwise say $j > 0$, and choose $y \geqslant k(d)$ such that $[y, y + 6j] \cap B_d(k(r)) = \varnothing$ for each r. As $xg = x$ for each $x \in [y, y + 3j]$ and w is the successor function in our reference copy $\mathbf{Z}_{w,h}$, the permutation $h' = w^j g$ has cycles which are neither 2-cycles nor 3-cycles. This contradicts (B3) for w', h', since the cycle structure remains unchanged under applying the isomorphism p. Thus $j = 0$ and

$$h' = g = \prod_{0 \leqslant i < m} \mathrm{Conj}(h^{t_i}, w^{s_i}).$$

Claim 3.6 completes goal (a) above once we show that $b_{w'} = 1$. Otherwise $b_{w'} = -1$, and by (ii) of Claim 3.6, $|xp + x|$ is bounded for $x > 0$. Since $Y_{w',h'}$ is infinite, with respect to $\mathbf{Z}_{w',h'}$, h' has a cycle $(x, x+1, x+2)$ for arbitrarily large x, and hence with respect to the reference copy $\mathbf{Z}_{w,h}$, h' has a 3-cycle below arbitrarily small (negative) x. On the other hand, if d is as above then $xh' = x$ for any $x \leqslant -d$, since the cycles of h are only on the positive side of $\mathbf{Z}_{w,h}$. This is a contradiction.

For each $t, k \in \mathbb{N}$, let $B'_t(k)$ be the set $B_t(k)$ evaluated in $\mathbf{Z}_{w',h'}$. Recall from (i) of Claim 3.6 that there is a constant u such that $|xp - x| < u$ for all x. Thus $B_l(k) \subseteq B'_{l+u}(k)$ for all $k, l \in \mathbb{N}$.

By Claim 3.7, a non-trivial cycle of $h' = g$ other than its 2-cycle is either completely below q, or is a cycle of $t(C_{k(r)}, w)$, where $k(r) \in Y_{w,h}$. Also, if $r \geqslant d$, then the support of each factor $C_{k(r)+s_i}^{t_i}$ of $t(C_{k(r)}, w)$ is contained in $B_d(k(r)) \subseteq B'_{d+u}(k(r))$, and hence so is the support of $t(C_{k(r)}, w)$.

In the following, we always suppose that $r \geqslant d + u$. By (B3), for w', h',

with respect to $\mathbf{Z}_{w',h'}$, $t(C_{k(r)}, w)$ either equals a 3-cycle $C_{k(r)}$ of h' or is the identity.

Clearly, for each i, $t(C_{i+s}, w)$ is a shift of $t(C_i, w)$ by s, that is,

$$t(C_{i+s}, w) = \mathrm{Conj}(t(C_i, w), w^s).$$

Then, if $t(C_{k(r)}, w)$ were the identity for *some* $k(r)$, this would hold for *all* $k(r)$, and so $Y_{w',h'}$ is finite, contrary to (B4). Thus $t(C_{k(r)}, w)$ is always $C_{k(r)}$ with respect to $\mathbf{Z}_{w',h'}$.

We can now argue that $Y_{w,h} - Y_{w',h'}$ is finite: if $k(r) \in Y_{w,h}$ for $r \geqslant d+u$, then $C_{k(r)}$ is a cycle of h, so that $t(C_{k(r)}, w)$ is a cycle of h', and hence $k(r) \in Y_{w',h'}$.

On the other hand, $Y_{w',h'} - Y_{w,h}$ is finite as well: if $k(r) \notin Y_{w,h}$ where $r \geqslant d+u$, then h' has no 3-cycle at the coding location $k(r)$, so that $k(r) \notin Y_{w',h'}$. Then, by (B4), $Y_{w',h'} = Y_{w,h}$. □

For (i) in Theorem 3.1, it remains to show that there is an automorphism of H taking $\langle w, h\rangle$ to $\langle w', h'\rangle$. Conjugation by the isomorphism $p : \mathbf{Z}_{w,h} \mapsto \mathbf{Z}_{w',h'}$ induces an automorphism of $\mathrm{Sym}(\mathbf{Z}_H)$ taking w to w' and h to h' (as always we identify elements of H with the permutation of $\mathbf{Z}_H$ induced by their action). As H is generated by w, h and by w', h', the restriction of this automorphism to H is as desired.

For (ii), clearly P_Y satisfies $\psi(\hat{z}, h_Y)$. Moreover,

$$n \in Y \text{ if and only if } P_Y \models \exists w, h[\psi(w,h) \wedge \text{`}\mathbf{Z}_{w,h} \models h(k(n)) = k(n)+1\text{'}].$$

So Y can be recovered (via a fixed many-one reduction) from $\mathrm{Th}(P_Y)$. The assertion that the word problem of P_Y is Turing between Y and Y' is verified as in [5]. □

Recall that $P_\varnothing$ is the subgroup of $\mathrm{Sym}(\mathbb{Z})$ generated by $(0,1)$ and successor. Clearly $P_\varnothing = \mathrm{Sym}_{\mathrm{fin}}(\mathbb{Z}) \rtimes \langle d\rangle_{\mathrm{gp}}$ where d is the successor function and its action on $\mathrm{Sym}_{\mathrm{fin}}(\mathbb{Z})$ is given by shifting. Thus $P_\varnothing$ is a permutation groups analog of the examples in Theorem 2.2. As a corollary to the proof of Theorem 3.1, we obtain that the QFA group $P_\varnothing$ is prime.

Corollary 3.8. *The group $P_\varnothing = \mathrm{Sym}_{\mathrm{fin}}(\mathbb{Z}) \rtimes \mathbb{Z}$ is QFA.*

Proof. For technical reasons we required in (B4) that $Y_{w,h} \neq \varnothing$, which precisely excludes $P_\varnothing$. If we require instead of (B3) and (B4) that h is the transposition $(0,1)$, then the proof becomes simpler and shows that $P_\varnothing$ is prime. □

The proof of Theorem 3.1 is mostly algebraic. A somewhat different proof, involving more model theory and in particular the concept of bi-interpretabiity, is sketched in the last subsection of [6].

All examples that we have seen are far from being simple groups.

Question 3.9. Is there a QFA group that is simple? Is there an infinite f.g. prime group that is simple?

References

[1] G. Baumslag and D. Solitar. Some two-generator one-relator non-Hopfian groups. *Bull. Amer. Math. Soc.* **68** (1962), 199–201.
[2] W. Hodges. *Model theory* (Cambridge University Press, 1993).
[3] S. Lang. *Algebra* (Addison-Wesley, 1965).
[4] R. McKenzie. On elementary types of symmetric groups. *Algebra Universalis* **1** (1971), 13–20.

[5] A. Morozov and A. Nies. Finitely generated groups and first-order logic. *J. London Math. Soc*. (2) **71** (2005), 545–562.
[6] A. Nies. Describing groups. *Bull. Symbolic Logic*, to appear. http://www.cs.auckland.ac .nz/~nies/papers/.
[7] A. Nies. Aspects of free groups. *J. Algebra* **263** (2003), 119–125.
[8] A. Nies. Separating classes of groups by first-order formulas. *Internat. J. Algebra Comput*. **13** (2003), 287–302.
[9] P. Odifreddi. *Classical recursion theory*, vol. 1 (North–Holland Publishing Co., 1989).
[10] F. Oger. Quasi-finitely axiomatizable groups and groups which are prime models. *J. Group Theory* **9** (2006), 107–116.
[11] F. Oger and G. Sabbagh. Quasi-finitely axiomatizable nilpotent groups. *J. Group Theory* **9** (2006), 95–106.

Received 15 November, 2005; revised 26 June, 2006

Andre Nies, Department of Computer Science, Office 565, University of Auckland, Private Bag 92019, Auckland, New Zealand