Reverse Mathematics of the Nielsen-Schreier Theorem

Rodney G. Downey
Denis R. Hirschfeldt
Steffen Lempp
Reed Solomon *

School of Mathematical and Computing Sciences
Victoria University of Wellington
Post Office Box 600
Wellington
New Zealand

Department of Mathematics
University of Wisconsin-Madison
Madison, WI 53706
USA

Abstract

The Nielsen-Schreier Theorem states that every subgroup of a free group is free. To formalize this theorem in weak subsystems of second order arithmetic, one has to choose between defining a subgroup in terms of a set of group elements and defining it in terms of a set of generators. We show that if subgroups are defined by sets, then the Nielsen-Schreier Theorem is provable in RCA_0, while if subgroups are defined by generators, the theorem is equivalent to ACA_0.

1 Introduction

The fundamental question in reverse mathematics is to determine which set existence axioms are required to prove particular theorems of ordinary mathematics. In this article, we consider the Nielsen-Schreier Theorem that every subgroup of a free group is free. While this section

*This research was carried out while the first and second authors were visiting the third and fourth authors at the University of Wisconsin. The first and second author's research is partially supported by the Marsden Fund of New Zealand. The third author's research is partially supported by NSF grant DMS-9732526.

provides some background material on reverse mathematics, the reader who is unfamiliar with this area is referred to [4] or [1] for more details.

Reverse mathematics uses subsystems of second order arithmetic to gauge the proof theoretic strength of a theorem. Here, we are concerned with only two subsystems: RCA_0 and ACA_0. RCA_0 contains the ordered semiring axioms for the natural numbers, plus Δ^0_1 comprehension, Σ^0_1 formula induction, and the set induction axiom

$$\forall X\,\big((0 \in X \wedge \forall n(n \in X \to n+1 \in X)\big) \to \forall n(n \in X)\big).$$

The Δ^0_1 comprehension scheme consists of all axioms of the form

$$\forall n\,\big(\varphi(n) \leftrightarrow \psi(n)\big) \to \exists X\,\forall n\,\big(n \in X \leftrightarrow \varphi(n)\big)$$

where φ is a Σ^0_1 formula, ψ is a Π^0_1 formula, and X does not occur freely in either φ or ψ. In this scheme, φ may contain free set variables other than X as parameters. We use $\mathbb{N}$ to denote the set defined by the formula $x = x$. The Σ^0_1 formula induction scheme contains the following axiom for each Σ^0_1 formula φ:

$$\big(\varphi(0) \wedge \forall n\big(\varphi(n) \to \varphi(n+1)\big)\big) \to \forall n\big(\varphi(n)\big).$$

Although it is not contained in the axioms, induction over Π^0_1 formulas also holds in RCA_0.

A model for RCA_0 is a two sorted first order structure $\mathfrak{A}$ which satisfies these axioms. If the first order part of $\mathfrak{A}$ is isomorphic to ω, then $\mathfrak{A}$ is called an ω-model. In this case, $\mathfrak{A}$ is often denoted by the subset of $\mathcal{P}(\omega)$ which specifies the second order part of the model.

The computable sets form the minimum ω-model of RCA_0, and any ω-model of RCA_0 is closed under both Turing reducibility and the Turing join. RCA_0 is strong enough to prove the existence of a set of unique codes for the finite sequences of elements from any set X. We use Fin_X to denote this set of codes. Also, we use $\langle a, b\rangle$, or more generally $\langle x_0, \ldots, x_n\rangle$, to denote pairs, or longer sequences, of elements of $\mathbb{N}$. For any sequences σ and τ, we denote the length of σ by $\mathrm{lh}(\sigma)$, the k^{th} element of σ by $\sigma(k)$, and the concatenation of σ and τ by $\sigma\tau$.

ACA_0 consists of RCA_0 plus the comprehension scheme over all arithmetic formulas. Any ω-model of ACA_0 is closed under the Turing jump, so the arithmetic sets form the minimum ω-model of ACA_0.

We use RCA_0 as our base system, which means that if we cannot find a proof of a theorem T in RCA_0, but do find a proof of T in ACA_0, then we try to show that $\mathrm{RCA}_0 + T$ suffices to prove the extra comprehension axioms in ACA_0. When proving such a reversal, the following well-known result is extremely useful (see [4]).

Theorem 1.1. *(RCA_0) The following are equivalent.*

1. *ACA_0.*
2. *The range of every one-to-one function exists.*

Given the characterizations of the ω-models of RCA_0 and ACA_0 in terms of Turing degrees, it is not surprising that equivalences in reverse mathematics have immediate consequences in computable mathematics. Any theorem provable in RCA_0 is effectively true, while the effective version of any theorem equivalent to ACA_0 does not hold.

The first question one has to decide when developing a branch of mathematics in second order arithmetic is how to define the relevant objects. In most cases the choice is straightforward, but in the case of combinatorial group theory, some variation is possible. It is natural to define a free group in terms of a set of generators and the trivial relations on those generators. The elements of the free group are the reduced words over the set of generators and their inverses, and multiplication is defined by concatenation followed by free reduction.

Moving away from free groups, the choices become more complicated. In combinatorial group theory, a group is often given by a presentation; however, RCA_0 cannot go from a presentation with unsolvable word problem to the set of elements in the group. Therefore, the difference between defining a group in terms of a presentation and defining a group by the set of elements is significant. In this article, we explore the proof theoretic strength of the Nielsen-Schreier Theorem using each of these definitions for a subgroup. If we require that the subgroup be given by a set, the result is provable in RCA_0. However, if we allow the subgroup to be defined by a presentation, the theorem is equivalent to ACA_0.

In Section 2, we give the formalism for free groups in RCA_0 and introduce notation that will be used throughout the article. In Section 3, we use a known proof of the Nielsen-Schreier Theorem to show that whenever a subgroup of a free group is given by its set of elements, RCA_0 suffices to prove that it is free. The proof that ACA_0 is required if a subgroup is defined in terms of its generators is presented in Section 4.

2 Free Groups

Our approach to free groups follows [2]. To define the free group on a set of generators $A \subseteq \mathbb{N}$, it is convenient to think of the elements of A as distinct symbols in some alphabet. Let a^1 stand for the pair $\langle a, 1\rangle$ and a^{-1} stand for the pair $\langle a, -1\rangle$. Here, ϵ will always denote either 1 or -1, and hence a^ϵ is either $\langle a, 1\rangle$ or $\langle a, -1\rangle$.

Definition 2.1. (RCA_0) If $A \subseteq \mathbb{N}$, then the set of **words over A**, denoted by Word_A, is the set of finite sequences of pairs $\langle a, \epsilon\rangle$, where $a \in A$ and $\epsilon \in \{+1, -1\}$. The empty sequence in Word_A is denoted by 1_A.

In keeping with standard mathematical notation, we write $a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$ for the sequence $\sigma \in \mathrm{Word}_A$ with $\sigma(i) = a_i^{\epsilon_i}$ for $1 \leq i \leq k$. We write $w_1 w_2$ for the concatenation of the sequences w_1 and w_2 in Word_A, and we abbreviate the sequence $ww\cdots w$ of length k by w^k.

A sequence $x \in \mathrm{Word}_A$ is called reduced if there is no place in the sequence where a^1 and a^{-1} appear next to each other for any $a \in A$.

Definition 2.2. (RCA_0) The set of **reduced words over A**, denoted by Red_A, contains all $x \in \mathrm{Word}_A$ such that

$$\forall i < (\mathrm{lh}(x) - 1) \ \big(\ \pi_1(x(i)) \neq \pi_1(x(i+1)) \vee \pi_2(x(i)) = \pi_2(x(i+1))\ \big),$$

where π_1 and π_2 are the standard projection functions on pairs.

The definitions of both Word_A and Red_A use Σ^0_0 formulas, so RCA_0 suffices to prove these sets exist. Two words are called 1-step equivalent if either they are the same sequence or one results from the other by deleting a pair of elements a^1 and a^{-1} that appear next to each other.

Definition 2.3. (RCA_0) Two words $x, y \in \mathrm{Word}_A$ are **1-step equivalent**, denoted $x \sim_1 y$, if one of the following conditions holds.

1. $x = y$.
2. $\mathrm{lh}(x) = \mathrm{lh}(y) + 1$ and

$$\exists i < \mathrm{lh}(x) \Big(\forall j < i \, \big(x(j) = y(j)\big) \wedge \\ \wedge \forall j \geq i \, \big(j < \mathrm{lh}(y) \to y(j) = x(j+2) \big) \wedge \\ \wedge \pi_1(x(i+1)) = \pi_1(x(i)) \wedge \pi_2(x(i+1)) + \pi_2(x(i)) = 0 \Big).$$

3. Same as 2 with the roles of x and y switched.

The conditions in this definition are Σ^0_0, so RCA_0 proves the existence of the set of all pairs $\langle x, y\rangle$ with $x \sim_1 y$.

Definition 2.4. (RCA_0) Two words $x, y \in \mathrm{Word}_A$ are **freely equivalent**, denoted $x \sim y$, if there is a finite sequence σ of elements of Word_A such that

1. $\sigma(0) = x$,
2. $\sigma(\mathrm{lh}(\sigma) - 1) = y$, and
3. $\sigma(i) \sim_1 \sigma(i+1)$ for all $i < \mathrm{lh}(\sigma) - 1$.

Notice that the condition in this definition is Σ^0_1. To prove the existence of the set of pairs $\langle x, y\rangle$ with $x \sim y$ in RCA_0, we use the function $\rho : \mathrm{Word}_A \to \mathrm{Red}_A$ defined by recursion: $\rho(1_A) = 1_A$, $\rho(a^\epsilon) = a^\epsilon$ for $a \in A$ and $\epsilon \in \{-1, +1\}$, and if $\rho(u) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$, then

$$\rho(ua^\epsilon) = \begin{cases} a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} a^\epsilon & \text{if } a \neq a_k \text{ or } a = a_k \wedge \epsilon_k + \epsilon \neq 0 \\ a_i^{\epsilon_1} \cdots a_{k-1}^{\epsilon_{k-1}} & \text{if } a = a_k \wedge \epsilon_k + \epsilon = 0. \end{cases}$$

Lemma 2.5. *(RCA_0) The following properties hold of ρ for all words w, w_1 and w_2 in $Word_A$ and all $a \in A$.*

1. *$\rho(w) \in Red_A$.*
2. *$\rho(w) \sim w$.*
3. *$w \in Red_A \to \rho(w) = w$.*
4. *$\rho(w_1 w_2) = \rho(\rho(w_1) w_2)$.*

5. $\rho(wa^{\epsilon}a^{-\epsilon}) = \rho(w)$.

6. $\rho(w_1 a^{\epsilon}a^{-\epsilon}w_2) = \rho(w_1 w_2)$.

Proof. The proofs are all by induction either on the length of w or on the length of w_2. To prove that $\rho(w) \in \mathrm{Red}_A$, we prove $\forall n \varphi(n)$ by induction, where $\varphi(n)$ is the Σ^0_0 formula

$$(w \in \mathrm{Word}_A \wedge \mathrm{lh}(w) = n) \rightarrow \rho(w) \in \mathrm{Red}_A.$$

The only element of Word_A with length 0 is 1_A. Since $\rho(1_A) = 1_A$, we have that $\varphi(0)$ holds. If $\mathrm{lh}(w) = 1$, then $w = a^{\epsilon}$ for some $a \in A$. By the definition of ρ, $\rho(a^{\epsilon}) = a^{\epsilon}$, and so $\varphi(1)$ holds. In the case when $\mathrm{lh}(w) > 1$, we write w as the concatenation $w = ua^{\epsilon}$. By the induction hypothesis, $\rho(u) \in \mathrm{Red}_A$. Assume $\rho(u) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$, and split into two cases.

If $a_k \neq a$, or if $a_k = a$ but $\epsilon_k + \epsilon \neq 0$, then by definition $\rho(w) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} a^{\epsilon}$ and $\rho(w) \in \mathrm{Red}_A$. If $a_k = a$ and $\epsilon_k + \epsilon = 0$, then $\rho(w) = a_1^{\epsilon_1} \cdots a_{k-1}^{\epsilon_{k-1}}$. Again, since $\rho(u) \in \mathrm{Red}_A$, we have $\rho(w) \in \mathrm{Red}_A$. This proves Property 1.

To prove $\rho(w) \sim w$, we use Σ^0_1 induction on $\mathrm{lh}(w)$. Formally, we use induction to show $\forall n \varphi(n)$, where $\varphi(n)$ is the Σ^0_1 formula

$$(w \in \mathrm{Word}_A \wedge \mathrm{lh}(w) = n) \rightarrow \rho(w) \sim w.$$

If $\mathrm{lh}(w) = 0$ or $\mathrm{lh}(w) = 1$, then the argument is the same as for Property 1. Assume $\mathrm{lh}(w) > 1$ and $w = ua^{\epsilon}$ with $u \sim \rho(u) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$. Let σ be the sequence which shows the free equivalence of u and $\rho(u)$. Split into the same two cases as in the proof of Property 1. If $\rho(w) = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} a^{\epsilon}$, then $\tilde{\sigma}$ gives the free equivalence of w and $\rho(w)$, where $\tilde{\sigma}$ is defined from σ by $\tilde{\sigma}(i) = \sigma(i)a^{\epsilon}$. If $\rho(w) = a_1^{\epsilon_1} \cdots a_{k-1}^{\epsilon_{k-1}}$, then $\tilde{\sigma}$ gives the free equivalence of w and $\rho(w)$, where $\tilde{\sigma}$ is defined by

$$\begin{gathered} \forall i < \mathrm{lh}(\sigma)(\tilde{\sigma}(i) = \sigma(i)a^{\epsilon}) \\ \text{and } \tilde{\sigma}(\mathrm{lh}(\sigma)) = \rho(w). \end{gathered}$$

The proofs of the remaining properties involve similar case analysis, except for Property 6, which is a direct consequence of the earlier properties. For more details, see [2]. □

Lemma 2.6. *(RCA_0) If $x \sim y$, then $\rho(x) = \rho(y)$.*

Proof. From the definition of 1-step equivalence and Property 6 of Lemma 2.5, it follows that if $x \sim_1 y$, then $\rho(x) = \rho(y)$. Assume $x \sim y$, and let σ be the sequence that shows $x \sim y$. Since $\sigma(i) \sim_1 \sigma(i+1)$ for all $i < (\mathrm{lh}(\sigma) - 1)$, we have $\rho(\sigma(i)) = \rho(\sigma(i+1))$. Thus, $\rho(\sigma(0)) = \rho(\sigma(\mathrm{lh}(\sigma) - 1))$, and so $\rho(x) = \rho(y)$. □

Proposition 2.7. *(RCA_0) For every $x \in Word_A$, there is a unique $y \in Red_A$ such that $x \sim y$.*

Proof. Since $\rho(x) \in \mathrm{Red}_A$ and $x \sim \rho(x)$, we know that there is at least one $y \in \mathrm{Red}_A$ such that $x \sim y$. It remains to show that if $x \sim y$ and $y \in \mathrm{Red}_A$, then $y = \rho(x)$. Because $x \sim y$ implies that $\rho(x) = \rho(y)$ and $y \in \mathrm{Red}_A$ implies that $\rho(y) = y$, we have $\rho(x) = y$ as required. □

Because free equivalence is an equivalence relation, it follows that if $\rho(x) = \rho(y)$, then $x \sim y$. Together with Lemma 2.6, this shows that $x \sim y$ if and only if $\rho(x) = \rho(y)$. The set of pairs $\langle x, y \rangle$ such that $x \sim y$ can be formed by Σ^0_0 comprehension:

$$\{\langle x, y \rangle \mid x \sim y\} \;=\; \{\langle x, y \rangle \mid \rho(x) = \rho(y)\}.$$

We can now give the formal definition of the free group on the set of generators A.

Definition 2.8. (RCA_0) Let $A \subseteq \mathbb{N}$. The set of elements of the **free group on the set of generators A** is Red_A. The empty sequence 1_A is the identity element, and multiplication is defined by $x \cdot y = \rho(xy)$.

3 Set subgroups of free groups

In this section, we show that RCA_0 proves the Nielsen-Schreier Theorem when the subgroups are defined by sets. Our proof is a slight variation of the one given in [3], originally due to A.J. Weir. The main modifications involve proving the existence of a Schreier transversal in RCA_0 and handling various normal closures in RCA_0, where they must be treated formally as Σ^0_1 objects.

Definition 3.1. Let F be the free group on X. A **set subgroup** of F is a set $G \subset F$ such that G is a subgroup of F. Such a set subgroup is denoted by $G < F$.

Definition 3.2. Let F be the free group on X, and let $\rho : \mathrm{Word}_X \to \mathrm{Red}_X$ be defined as in Section 2. A set subgroup G of F is **free** if there exists $B \subset G$ such that

1. $\forall g \in G\, \exists w \in \mathrm{Red}_B(\rho(w) = g)$, and
2. If $w_1 \neq w_2 \in \mathrm{Red}_B$, then $\rho(w_1) \neq \rho(w_2)$.

Notice that there is a distinction between Red_B and Red_X, but since $B \subset \mathrm{Word}_X$, we can apply ρ to elements of Red_B. In what follows, we frequently consider the right cosets Gw of G in F and use the fact that $Gw = Gu$ if and only if $wu^{-1} \in G$. Notice that RCA_0 suffices to prove that each coset Gw exists, since $Gw = \{u | wu^{-1} \in G\}$.

Definition 3.3. A **transversal** of $G < F$ is a set of unique representatives for the right cosets of G. That is, $T \subset F$ is a transversal for G if for every $t_1 \neq t_2 \in T$, $t_1 t_2^{-1} \notin G$, and for every $x \in F$, there is a $t \in T$ such that $xt^{-1} \in G$. A transversal T is called a **Schreier transversal** if for every $t \in T$, all initial segments of the word t are in T.

For any $G < F$, we can define a transversal for G by choosing the $\mathbb{N}$-least representative of each coset.

Definition 3.4. Let $G < F$ and $D \subset F$ be a finite set. We say that D has the **Schreier property** (with respect to G) if D is a finite approximation to a Schreier transversal. Formally, we require that for all $x \neq y \in D$, $xy^{-1} \notin G$, and if $x \in D$, then all initial segments of x are in D.

Notice that $1_F \in T$ for any Schreier transversal T, and so 1_F represents the identity coset of G. Similarly, if D has the Schreier property, then $1_F \in D$.

Lemma 3.5. *(RCA_0) Let F be the free group on X and $G < F$. There exists a Schreier transversal for G.*

Proof. We define a primitive recursive function $f : F \times \mathrm{Fin}_F \to F \times \mathrm{Fin}_F$, where Fin_F is the set of all finite subsets of F. The idea is that if f is given an input (w, D), where D has the Schreier property, then f returns a pair $(\hat{w}, \hat{D})$ such that $\hat{w} \in \hat{D}$, $D \subset \hat{D}$, $\hat{D}$ has the Schreier property, and $Gw = G\hat{w}$ (that is, $\hat{w}w^{-1} \in G$). Thus, f has extended D to include a representative for Gw.

Formally, $f(w, D)$ is defined by primitive recursion on $\mathrm{lh}(w)$. Let $f(1_F, D) = (1_F, D)$. Assume $w \neq 1_F$ and proceed as follows.

1. If there is a $\hat{w} \in D$ such that $Gw = G\hat{w}$, then $f(w, D) = (\hat{w}, D)$.
2. Otherwise, let $w = vx^\epsilon$ for some $x \in X$. Notice that $\mathrm{lh}(v) < \mathrm{lh}(w)$.
   (a) If $Gw = Gv$, then $f(w, D) = f(v, D)$.
   (b) If $Gw \neq Gv$, then
      i. if $Gv = Gu$ for some $u \in D$, then $f(w, D) = (ux^\epsilon, D \cup \{ux^\epsilon\})$.
      ii. if $Gv \neq Gu$ for all $u \in D$, then $f(w, D) = (\hat{v}x^\epsilon, \hat{D} \cup \{\hat{v}x^\epsilon\})$ where $f(v, D) = (\hat{v}, \hat{D})$.

A simple induction establishes that if D has the Schreier property, $w \in F$, and $f(w, D) = (\hat{w}, \hat{D})$, then $\hat{D}$ has the Schreier property, $D \subset \hat{D}$, $\hat{w} \in \hat{D}$, and $G\hat{w} = Gw$.

We use f to define $T : \mathbb{N} \to \mathrm{Fin}_F$ by primitive recursion. Set $T(0) = \{1_F\}$ and

$$T(n+1) = \begin{cases} T(n) & \text{if } \ n \notin F \\ \pi_2(f(n+1, T(n))) & \text{if } \ n \in F \end{cases}$$

where π_2 is the projection function onto the second component for pairs. Let $T = \cup_{i=1}^{\infty} T(n)$. T exists since for every $w \in F$, there is a $\hat{w} \in T(w)$ such that $Gw = G\hat{w}$, and therefore, $w \in T$ if and only if $w \in T(w)$. It is clear from the definition of $T(n)$ that T is a Schreier transversal for G. ☐

Theorem 3.6. *(RCA_0) Every set subgroup of a free group is free.*

Proof. Let F be free on X, $G < F$, and T be a Schreier transversal for G. Most of this proof works without the assumption that T has the Schreier property, but we will use this property near the end. For any $w \in F$, let $[w]$ denote the element of T such that $Gw = G[w]$. Notice that $[1_F] = 1_F$ since $1_F \in T$, that $[u] = 1_F$ for all $u \in G$, and that for any $u, v \in F$, $[u]v[uv]^{-1} \in G$.

The outline of the proof is as follows. First, we define an auxiliary free group $\hat{F}$ and a homomorphism $\tau : \hat{F} \to G$. Second, we show that τ is onto, and hence G is isomorphic to

$\hat{F}/\ker(\tau)$. Third, we show that $\ker(\tau)$ is generated by a subset of the generators of $\hat{F}$. Hence, G is isomorphic to the free group on the generators of $\hat{F}$ which are not in $\ker(\tau)$.

Let $\hat{F}$ be the free group on $T \times X$, and let y_{ix} denote the generator corresponding to $i \in T$ and $x \in X$. Define $\tau : \hat{F} \to G$ by sending $y_{ix} \mapsto [i]x[ix]^{-1}$ and extending across $\hat{F}$. Notice that $[i] = i$ since $i \in T$.

To verify the required properties of τ, we use the map $f : T \times F \to \hat{F}$ defined below. It is best to think of f as a sequence of maps $f_i : F \to \hat{F}$ for $i \in T$. Define f by primitive recursion on the length of $u \in F$. Set $f(i, 1_F) = 1_{\hat{F}}$, $f(i, x) = y_{ix}$ for $x \in X$, and $f(i, x^{-1}) = y^{-1}_{[ix^{-1}]x}$, also for $x \in X$. For $u \in F$ with $u = vz$, $z \in X \cup X^{-1}$, define $f(i, u) = f(i, v)f([iv], z)$. The maps f_i are not group homomorphisms, but the following three properties can be verified.

$$\forall u, v \in \mathrm{Red}_F\,(f(i, uv) = f(i, u)f([iu], v)). \tag{1}$$
$$\forall v \in \mathrm{Red}_F\,(f(i, v^{-1}) = f([iv^{-1}], v)^{-1}). \tag{2}$$
$$\forall v \in \mathrm{Red}_F \forall i \in T\,(\tau(f(i, v)) = [i]v[iv]^{-1}). \tag{3}$$

Properties (1) and (3) follow by induction on the length of v (for details see [3]), and Property (2) follows from applying Property (1) with $v = u^{-1}$.

Next, we define $\psi : G \to \hat{F}$ by $\psi(u) = f(1_F, u)$. Properties (1) and (2) guarantee that ψ is a group homomorphism, and Property (3) shows that $\tau\psi : G \to G$ is the identity map. Therefore, τ is onto (which was our second goal), and ψ is one-to-one.

It remains to examine $\ker(\tau)$. Let $\chi = \psi\tau : \hat{F} \to \hat{F}$. Since ψ is one-to-one, we have $\ker(\chi) = \ker(\tau)$.

Claim. $\ker(\tau)$ is equal to the normal closure in $\hat{F}$ of $y_{ix}^{-1}\chi(y_{ix})$ for $i \in T$ and $x \in X$.

The normal closure of these elements is defined by a Σ^0_1 formula, so we cannot immediately claim that RCA_0 proves its existence. Formally we define the normal closure using the function $C : \mathbb{N} \times \mathbb{N} \times \hat{F} \to \{0, 1\}$ defined as follows.

$$C(0, m, z) = \begin{cases} 1 & \text{if } \exists i, x \leq m(z = y_{ix}^{-1}\chi(y_{ix})) \\ 0 & \text{otherwise} \end{cases}$$

$$C(n+1, m, z) = \begin{cases} 1 & \text{if } C(n, m, z) = 1 \text{ or} \\ & C(n, m, z^{-1}) = 1 \text{ or} \\ & \exists a, b \leq m(C(n, m, a) = 1 \wedge z = b^{-1}ab) \text{ or} \\ & \exists a, b \leq m(C(n, m, a) = C(n, m, b) = 1 \wedge z = ab) \\ 0 & \text{otherwise} \end{cases}$$

We write $z \in N$ for $\exists n, m(C(n, m, z) = 1)$ until we prove that N exists in RCA_0. RCA_0 proves the following properties of N by direct calculation.

$$\forall z \in N(z^{-1} \in N)$$
$$\forall a, b \in N(ab \in N)$$
$$\forall a \in N\, \forall w \in \hat{F}(w^{-1}aw \in N)$$
$$\forall i \in T\, \forall x \in X(y_{ix}^{-1}\chi(y_{ix}) \in N)$$
$$\forall z \in N\, \forall w \in \hat{F}\, \exists \hat{z} \in N(zw = w\hat{z})$$

To show N exists in RCA_0, we show that $N = \ker(\tau)$. First, to see that $N \subset \ker(\tau)$, recall that $\tau\psi : G \to G$ is the identity map. Therefore, we can cancel $\tau\psi$ inside $\chi^2 = \psi\tau\psi\tau$ to get $\chi^2 = \chi$. The following equalities show that $y_{ix}^{-1}\chi(y_{ix}) \in \ker(\chi)$.

$$\chi(y_{ix}^{-1}\chi(y_{ix})) = \chi(y_{ix})^{-1}\chi^2(y_{ix}) = \chi(y_{ix})^{-1}\chi(y_{ix}) = 1_{\hat{F}}.$$

As mentioned above, $\ker(\chi) = \ker(\tau)$. Therefore, since $\ker(\tau)$ is closed under multiplication and conjugation, it follows by Π^0_1 induction that $z \in N$ implies $z \in \ker(\tau)$.

To prove the claim, it remains to show that $\ker(\tau) \subset N$. First, by induction on the length of $w \in \hat{F}$, we get $w^{-1}\chi(w) \in N$. For the details of this induction, see [3]. Second, if $w \in \ker(\tau)$, then $\chi(w) = 1_{\hat{F}}$. We have $w^{-1}\chi(w) = w^{-1} \in N$, and therefore $w \in N$ as required. This statement finishes the proof that $N = \ker(\tau)$.

Claim. $\ker(\tau)$ is the normal closure of the elements $f(1_F, u)$ for $u \in T \subset F$.

As in the first claim, we formalize this statement by defining a function $D : \mathbb{N} \times \mathbb{N} \times \hat{F} \to \{0, 1\}$ such that $z \in \hat{F}$ is in the normal closure if and only if $\exists n, m D(n, m, z) = 1$. We write $z \in M$ for $\exists n, m D(n, m, z) = 1$, and we show M exists in RCA_0 by proving it is equal to $\ker(\tau)$.

To show that $M \subset \ker(\tau)$, notice that by Property (3) above

$$\tau(f(1_F, u)) = [1_F]u[1_F u]^{-1} = uu^{-1} = 1_G,$$

for $u \in T$. From here, use induction.

To show that $\ker(\tau) \subset M$, it suffices by the first claim to show that $y_{ix}^{-1}\chi(y_{ix}) \in M$ for all $i \in T$ and $x \in X$. Fix $i \in T$ and $x \in X$.

$$\begin{aligned} \chi(y_{ix}) &= f(1_F, \tau(y_{ix})) = f(1_F, [i]x[ix]^{-1}) = f(1_F, [i]x)f([ix], [ix]^{-1}) \\ &= f(1_F, [i])f([i], x)f([ix(ix)^{-1}], [ix])^{-1} = f(1_F, [i])y_{ix}f(1_F, [ix])^{-1}. \end{aligned}$$

Both $f(1_F, [i])$ and $f(1_F, [ix])^{-1}$ are in M. Just as in the first claim, M has the property that

$$\forall z \in M \, \forall w \in \hat{F} \, \exists \hat{z} \in M \, (zw = w\hat{z}).$$

Therefore, $y_{ix}^{-1}\chi(y_{ix}) \in M$ as required. This completes the proof of the second claim.

To finish the proof, we consider the set A of all y_{ix} such that $y_{ix} \in \ker(\tau)$, and we let S denote the normal closure of A in $\hat{F}$. Of course, as above, we use a function to formalize S as a Σ^0_1 defined object. Clearly, $S \subset \ker(\tau)$, but we also make the following claim (which, as above, shows that S is a set in RCA_0).

Claim. $\ker(\tau) = S$.

First, we show why this claim finishes the proof. Let C be the set of y_{ix} which are not in A. Since G is isomorphic to $\hat{F}/\ker(\tau)$, we see that G is isomorphic to the subgroup of $\hat{F}$ generated by C. But, this subgroup is exactly the free group on C, which we denote by H. Hence, there is an isomorphism $\varphi : G \to H$.

To see that this fact implies that G is free in the sense of Definition 3.2, let $B = \varphi^{-1}(C)$ (which exists since φ is an isomorphism). Notice that we cannot apply φ to an arbitrary

$w \in \mathrm{Red}_B$ since w might not be X-reduced, and hence might not be a member of G. However, we can define a map $\beta : \mathrm{Word}_B \to \mathrm{Word}_C$ by

$$\beta(b_1^{\epsilon_1} b_2^{\epsilon_2} \cdots b_n^{\epsilon_n}) = \varphi(b_1)^{\epsilon_1}\varphi(b_2)^{\epsilon_2}\cdots\varphi(b_n)^{\epsilon_n}$$

for any B-symbols $b_1, b_2, \ldots, b_n$. The point is that each B-symbol is an element of G, so φ can be applied to it. The following properties of β follow from the definition of B and the fact that φ is an isomorphism.

$$\forall w \in \mathrm{Red}_B\,(\beta(w) \in \mathrm{Red}_C \wedge \beta(w) = \varphi(\rho(w))) \tag{4}$$
$$\forall u \in \mathrm{Red}_C\,(\beta^{-1}(u) \in \mathrm{Red}_B) \tag{5}$$
$$\forall w_1 \neq w_2 \in \mathrm{Red}_B\,(\beta(w_1) \neq \beta(w_2)) \tag{6}$$

To verify Condition 2 in Definition 3.2, suppose $w_1 \neq w_2 \in \mathrm{Red}_B$, but $\rho(w_1) = \rho(w_2)$. Then, by Property (4) above,

$$\beta(w_1) = \varphi(\rho(w_1)) = \varphi(\rho(w_2)) = \beta(w_2).$$

This statement contradicts Property (6). To verify Condition 1 in Definition 3.2, consider any $g \in G$. We have $\varphi(g) \in \mathrm{Red}_C$, so $\beta^{-1}(\varphi(g)) \in \mathrm{Red}_B$. Let $w = \beta^{-1}(\varphi(g))$. By Property (4), we know $\beta(w) = \varphi(\rho(w))$. From the definition of w, we get $\beta(w) = \varphi(g)$, and hence, since φ is one-to-one, $g = \rho(w)$.

It remains to prove the last claim by showing that $\ker(\tau) \subset S$. By the second claim above, it suffices to show that $f(1_F, u) \in S$ for each $u \in T$. The result then follows by induction. We show $f(1_F, u) \in S$ by induction on the length of u. If $\mathrm{lh}(u) = 1$, then u is either x or x^{-1} for some $x \in X$. Tracing through the definitions, $f(1_F, x) = y_{1_F x}$ and $f(1_F, x^{-1}) = y^{-1}_{[x^{-1}]x}$. In either case, $f(1_F, u) \in \ker(\tau)$, so $y_{1_F x}$ and $y^{-1}_{[x^{-1}]x}$ are in S as required.

If $\mathrm{lh}(u) > 1$, then either $u = vx$ or $u = vx^{-1}$, where $\mathrm{lh}(v) < \mathrm{lh}(u)$ and $x \in X$. Because T is a Schreier transversal, we know that $v \in T$ and so the induction hypothesis applies to v. If $u = vx$, then we have

$$f(1_F, u) = f(1_F, v) f([v], x),$$

which means that

$$f(1_F, u) f(1_F, v)^{-1} = y_{[v]x}.$$

The left side of this equation is in $\ker(\tau)$, so $y_{[v]x} \in \ker(\tau)$, and hence $y_{[v]x} \in S$. By induction, $f(1_F, v) \in S$, so $f(1_F, u) \in S$ as required.

The case for $u = vx^{-1}$ is similar. We have the following equalities.

$$f(1_F, u) = f(1_F, v) f([v], x^{-1}).$$
$$f(1_F, u) f(1_F, v)^{-1} = f([vx^{-1}], x)^{-1} = y^{-1}_{[vx^{-1}]x}.$$

The left side of the bottom equation is in $\ker(\tau)$, so, reasoning as above, $f(1_F, u) \in S$, which finishes the proof. $\square$

4 Presented subgroups of free groups

In this section, we show that ACA_0 is equivalent to the Nielsen-Schreier Theorem when subgroups are defined by generating sets.

Definition 4.1. Let F be the free group on X. Given a set $A \subset F$, the **subgroup presented by** A is

$$\langle A \rangle \ = \ \{ \, g \in F \mid \exists w \in \mathrm{Word}_A(g = \rho(w)) \, \}.$$

$\langle A \rangle$ is **free** if there is a $B \subset F$ such that

1. $\forall b \in B \exists w \in \mathrm{Word}_A(\rho(w) = b)$,
2. $\forall w \in \mathrm{Word}_A \exists \hat{w} \in \mathrm{Word}_B(\rho(w) = \rho(\hat{w}))$, and
3. $\forall w_1 \neq w_2 \in \mathrm{Red}_B(\rho(w_1) \neq \rho(w_2))$.

Such a set B is called a **set of free generators for** $\langle A \rangle$.

Theorem 4.2. *(RCA_0) The following are equivalent.*

1. *ACA_0.*
2. *Every presented subgroup of a free group is free.*

Proof. Case. (1) $\Rightarrow$ (2)

ACA_0 suffices to prove the existence of the set of elements in a presented subgroup. Theorem 3.6 shows that RCA_0 suffices to prove from here that the presented subgroup is free.

Case. (2) $\Rightarrow$ (1)

Let $f : \mathbb{N} \to \mathbb{N}$ be a one-to-one function. By Theorem 1.1, it suffices to code the range of f. Pick an infinite set of generators $X = \{x_i | i \in \mathbb{N}\}$, let F be the free group on X, and let $\rho : \mathrm{Word}_X \to \mathrm{Red}_X$ be as in Section 2. Define A by

$$A = \{x_i^2 | i \in \mathbb{N}\} \cup \{x_i^{2s+1} | f(s) = i\},$$

and let B be a set of free generators for $\langle A \rangle$.

Claim. We can form $\{ \, n \mid x_n \in \langle A \rangle \, \}$ in RCA_0.

For all $n \in \mathbb{N}$, we know that $x_n^2 = \rho(w)$ for some $w \in \mathrm{Red}_B$. Also, $x_n \in \langle A \rangle$ if and only if $x_n = \rho(u)$ for some $u \in \mathrm{Red}_B$. Therefore, if such a u exists, then $w \sim_B u^2$. Our strategy is to give a method (eventually formalized by a Σ^0_0 formula) for determining from w whether there is such a u. To do this, we need limits both on the length of u in terms of B-symbols and on which B-symbols could occur in u.

Assume that $\mathrm{lh}(u) = n$, where the length is measured in B-symbols. We claim that $n < \mathrm{lh}(u^2) \leq 2n$, where by $\mathrm{lh}(u^2)$ we mean the length in B-symbols of the B-reduced word equivalent to u^2. To see this fact, consider first the case in which $\mathrm{lh}(u) = 2m + 1$ for some m. Then

$$uu = (b_1 \cdots b_m b_{m+1} b_{m+2} \cdots b_{2m+1}) \cdot (b_1 \cdots b_m b_{m+1} b_{m+2} \cdots b_{2m+1})$$

At worst, the last m symbols of the first w could cancel with the first m symbols of the second w, leaving us with $b_1 \cdots b_{m+1} b_{m+1} \cdots b_{2m+1}$, which has length $2m + 2 = n + 1$.

Second, consider the case when $\mathrm{lh}(u) = 2m$. If $w = b_1 \cdots b_{2m}$, then the maximum amount of cancellation in u^2 would leave us with $b_1 \cdots b_m b_{m+1} b_m b_{m+1} \cdots b_{2m}$. Because w is reduced, b_m and b_{m+1} do not cancel. Therefore, the shortest possible length for the reduced form of u^2 in B-symbols is $2m + 2 = n + 2$.

If $w \sim_B u^2$ and $w \in \mathrm{Red}_B$, then by this calculation, $\mathrm{lh}(u) < \mathrm{lh}(w)$, so we have our required bound on the length of u. This argument also shows that every symbol which occurs in u occurs in the B-reduced form of u^2. However, the B-reduced form of u^2 is w, so every B-symbol which occurs in u also occurs in w.

We can now form the set $\{n | x_n \in \langle A \rangle\}$ using Σ^0_0 comprehension, because n is in this set if and only if there is a $u \in \mathrm{Red}_B$ such that $\rho(u) = x_n$, $\mathrm{lh}(u) \leq \mathrm{lh}(w)$ (where $w \in \mathrm{Red}_B$ and $\rho(w) = x_n^2$), and every B-symbol in u occurs in w.

The following claim finishes the proof of the theorem.

Claim. The range of f is equal to $\{\, n \,|\, x_n \in \langle A \rangle \,\}$.

From the definition of A, it is clear that if n is in the range of f, then $x_n \in \langle A \rangle$. Before proving the other direction, we introduce some terminology. Assume $w \in F$ and some $x \in X$ occurs in w as a positive symbol (that is, it occurs as x as opposed to as x^{-1}). We say that a particular occurrence of x has the form x^n, for some $n \in \mathbb{N}$, if the maximum block of x's which includes this occurrence of x has length n. Notice that since w is reduced, all occurrences of x in this block must be positive. Similarly, if x occurs in w as x^{-1}, then this occurrence has the form x^{-n} if the maximum block of x^{-1}'s which include this occurrence has length n.

Assume that n is not in the range of f. We need to show that for every $w \in \mathrm{Word}_A$, $\rho(w) \neq x_n$ (recall that ρ represents reduction in F in terms of X-symbols). To accomplish this goal, we prove that for every $w \in \mathrm{Word}_A$, if x_n occurs as an X-symbol in $\rho(w)$ (either as x_n or as x_n^{-1}), then every occurrence of x_n in $\rho(w)$ is of the form x_n^{2k} for some integer k. This fact suffices to finish the proof of the claim, since x_n does not occur an even number of times in x_n, and hence $\rho(w) \neq x_n$.

The proof proceeds by induction on the A-length of w. If $w \in A$, then this statement is clear. Suppose the A-length of w is greater than 1 and $w = va$, with $v \in \mathrm{Word}_A$ and $a \in A$. We have $\rho(va) = \rho(\rho(v)a)$, and by induction, all occurrences of x_n in $\rho(v)$ are of the form x_n^{2k}. If a is not x_n^2, then a does not mention x_n and we are done. If $a = x_n^2$, then split into the case in which $\rho(v)$ ends in x_n^{2k} and the case in which it ends in an X-symbol other than x_n. In either case, the claim holds. □

References

[1] H.M. Friedman, S.G. Simpson and R.L. Smith, *Countable algebra and set existence axioms*, ***Ann. Pure Appl. Logic***, vol. 25 (1983), pp. 141-181.

[2] W. Magnus, A. Karrass and D. Solitar, ***Combinatorial group theory***, Dover, 1976.

[3] D.J. Robinson, ***A course in the theory of groups***, 2^{nd} ed., Springer-Verlag, 1996.

[4] S.G. Simpson, ***Subsystems of second order arithmetic***, Springer-Verlag, 1998.