Ordering Free Products in Reverse Mathematics

Reed Solomon

1 Introduction

This paper is a contribution to Harvey Friedman's project of reverse mathematics in which one tries to classify theorems of ordinary mathematics by the set theoretic axioms required to prove them.[1] All of the result in this paper are formalized in RCA_0, the weakest of the standard systems in reverse mathematics, and concern classical theorems about countable ordered groups. The reader who is not familiar with reverse mathematics is referred to Simpson [8] for the background definitions and to Solomon [9] and [10] for specific information concerning reverse mathematics and ordered groups. We begin with some background definitions before stating our main results.

DEFINITION 1 (RCA_0). A *partially ordered (p.o.) group* is a group G together with a partial order $\leq_G$ on the elements of G such that for any $a, b, c \in G$, if $a \leq_G b$ then $a \cdot_G c \leq_G b \cdot_G c$ and $c \cdot_G a \leq_G c \cdot_G b$. If the order is linear, then $(G, \leq_G)$ is called a *fully ordered (f.o.) group*.

We frequently drop the subscripts on $\cdot_G$ and $\leq_G$ when the ambient group is clear. An order preserving homomorphism between p.o. groups is called an *o-homomorphism*. If an o-homomorphism is onto, it is an *o-epimorphism*, and if it is a bijection, then it is an *o-isomorphism*.

If a subgroup H of G is normal, then the quotient G/H inherits a natural group structure. We form the quotient group G/H in RCA_0 by picking the $\leq_{\mathbb{N}}$-least representative of each coset. Since $aH = bH \leftrightarrow a^{-1}b \in H$, RCA_0 suffices to define the quotient group G/H.

If G is a p.o. group, then we need an additional condition on a normal subgroup H for the order on G to induce an order on G/H. H is *convex* if for any $a, b \in H$ and $g \in G$, we have that $a \leq g \leq b$ implies $g \in H$. If H is a convex normal subgroup, then the *induced order* $\leq_{G/H}$ on G/H is defined for $a, b \in G/H$ by $a \leq_{G/H} b \leftrightarrow \exists h \in H(a \leq_G bh)$. In the general case for a p.o. group G and a convex normal subgroup H, ACA_0 is required to prove

[1]The author thanks two anonymous referees for many helpful suggestions.

the existence of the induced order. (See [9] for a proof.) However, if G is an f.o. group, then RCA_0 is strong enough to form the induced order.

THEOREM 2 (RCA_0). *Let $(G, \leq_G)$ be an f.o. group and H a convex normal subgroup. The induced order $\leq_{G/H}$ on G/H exists.*

Proof. Let $a, b \in G/H$ and $a \neq b$. Because a and b are representatives of different cosets, $ab^{-1} \notin H$.

CLAIM 3. $\exists h \in H\, (a \leq_G bh)$ if and only if $a \leq_G b$.

If $a \leq_G b$ then, because $1_G \in H$, it follows that $\exists h \in H\, (a \leq_G bh)$. For the other direction, suppose for a contradiction that $\exists h \in H (a \leq_G bh)$ and $b <_G a$. Then $b <_G a \leq_G bh$ and so $1_G <_G b^{-1}a \leq_G h$. Since H is convex, $b^{-1}a \in H$. Because H is normal, $bb^{-1}ab^{-1} \in H$, and hence $ab^{-1} \in H$ which is a contradiction. The induced order can now be given by a Σ^0_0 condition: $aH \leq_{G/H} bH$ if and only if $aH = bH$ or $a <_G b$. ■

It is well known that every group G is isomorphic to a quotient group F/N of a free group F by a normal subgroup N. A similar result holds for ordered groups. Every f.o. group $(G, \leq)$ is o-isomorphic to a quotient group $(F/N, \leq_{F/N})$ of a fully ordered free group $(F, \leq_F)$ by a convex normal subgroup N. Classical proofs of this fact can be found in Fuchs [4] and Kokorin and Kopytov [5]. The main result of this paper is to give a proof of this classical theorem in RCA_0. (This result was first announced in Solomon [10].)

THEOREM 4 (RCA_0). *Every countable f.o. group is the o-epimorphic image of a fully ordered free group. Hence, for every f.o. group $(G, \leq_G)$, there is a fully ordered free group $(F, \leq_F)$ and a convex normal subgroup N of F such that $(G, \leq_G)$ is o-isomorphic to $(F/N, \leq_{F/N})$.*

Because Theorem 4 is provable in RCA_0, it follows that for every computably fully ordered computable group $(G, \leq_G)$, there is a computably ordered free group $(F, \leq_F)$ and a computable convex normal subgroup N such that $(G, \leq_G) \cong (F/N, \leq_{F/N})$, which answers an open question from Downey and Kurtz [2]. In this paper, we obtain a proof of Theorem 4 after first proving the following theorem in RCA_0.

THEOREM 5 (RCA_0). *The free product of f.o. groups A and B is fully orderable.*

There are also a number of different classical proofs of Theorem 5. We modify and formalize the classical proof of this theorem contained in Kokorin and Kopytov [5]. Before proving these theorems, we give additional background information about ordered groups in this section and explain how to formalize free groups and free products in RCA_0 in Section 2. In

Section 3, we prove Theorem 4 in RCA_0 using Theorem 5 and an idea from Revesz [7]. In Sections 4 and 5, we prove Theorem 5 in RCA_0. In Section 6, we present proofs of some technical formulas used in previous sections.

It follows from Theorem 5 that RCA_0 proves that the free group on infinitely many generators is fully orderable, and hence that the natural computable presentation of this free group admits a computable order. The standard classical proof that free groups are fully orderable uses the fact that the lower central series of a free group has length ω. In Dabkowska, Dabkowski, Harizanov and Tongha [1], this fact and the Fox calculus (for determining where elements of the free group sit in the lower central series) were used to show that free groups have orders of every Turing degree (including computable orders). Rather than developing properties of the lower central series of free groups in RCA_0, we obtain our effective proof that free groups are fully orderable as a corollary of Theorem 5 using the facts (shown in RCA_0 in Section 2) that the free group on two generators is isomorphic to the free product $\mathbb{Z} * \mathbb{Z}$ and the free group on countably many generators embeds into the free group on two generators.

When working with ordered groups, it is often easier to work with the set of positive elements in the group rather than the order $\leq_G$. Proofs of the following results (which are straightforward formalizations of the standard classical proofs) can be found in Solomon [9].

DEFINITION 6 (RCA_0). The *positive cone* of a p.o. group $(G, \leq_G)$ is the set $P(G) = \{g \in G \mid 1_G \leq_G g\}$.

Because $ab^{-1} \in P(G) \leftrightarrow b \leq_G a$, RCA_0 suffices to define the positive cone from the order and vice versa. There is a classical set of algebraic conditions that determines if an arbitrary subset of a group is the positive cone of some full or partial order. If G is a group and $X \subseteq G$, then $X^{-1} = \{g^{-1} \mid g \in X\}$. X is a *full subset of* G if $X \cup X^{-1} = G$ and X is a *pure subset of* G if $X \cap X^{-1} \subseteq \{1_G\}$.

THEOREM 7 (RCA_0). *A subset P of a group G is the positive cone of some partial order on G if and only if P is a normal pure semigroup with identity. Furthermore, P is the positive cone of a full order if and only if in addition P is full.*

If $(G_i, \leq_{G_i})$, $i \in \mathbb{N}$, is a uniform sequence of f.o. groups, then RCA_0 suffices to lexicographically order the (restricted) direct product $\prod_{i \in \mathbb{N}} G_i$. The elements of the product are represented by finite sequences σ such that $\sigma(i) \in G_i$ and the last element of σ is not the identity. The sequences are multiplied componentwise (removing any trailing identity elements). We order distinct sequences σ and τ in the product by $\sigma < \tau$ if and only if $\sigma(i) <_{G_i} \tau(i)$ for the $\leq_{\mathbb{N}}$-least i such that $\sigma(i) \neq \tau(i)$. (If σ is an initial segment of τ, then $\sigma < \tau$ if and only if $1_{G_j} <_{G_j} \tau(j)$ for the least $j \geq \mathrm{lh}(\sigma)$ such that $\tau(j) \neq 1_{G_j}$, where $\mathrm{lh}(\sigma)$ denotes the length of σ.) When ordering a direct product in RCA_0, it is important that the sequence of orders is given uniformly. In general, the fact that an infinite direct product of fully orderable groups is fully orderable is equivalent to WKL_0. (See Solomon [9].)

2 Free Groups and Free Products

In this section, we give a brief presentation of free groups in second order arithmetic, indicating informally how to define these groups in RCA_0. For a more formal presentation, including proofs of the stated properties, see Downey, Hirschfedlt, Lempp and Solomon [3]. After handling free groups, we give a more formal presentation of free products in RCA_0, although we often omit proofs which are straightforward formalizations of their classical counterparts as contained in [6]. [3] contains the formal versions of these properties for free groups and the modifications required for free products are minimal. Throughout this section, we work in RCA_0. We let Fin_X denote the set of codes for finite sequences of elements of a set X, $\mathrm{lh}(\sigma)$ denote the length of $\sigma \in \mathrm{Fin}_X$, and $x^\frown y$ denote the concatenation of $x, y \in \mathrm{Fin}_X$.

Let $A \subseteq \mathbb{N}$. When defining the free group on the generators A, it is convenient to think of the elements of A as distinct symbols in an alphabet. Let a^1 stand for the pair $\langle a, 1\rangle$ and a^{-1} stand for the pair $\langle a, -1\rangle$. In this section, ϵ will always denote either 1 or -1. The set of *words over A* is $\mathrm{Word}_A = \mathrm{Fin}_{\tilde{A}}$ where $\tilde{A} = \{a^\epsilon \mid a \in A \text{ and } \epsilon = \pm 1\}$. The empty sequence is denoted by 1_A. In keeping with standard mathematical notation, we write $a_0^{\epsilon_0} \cdots a_{k-1}^{\epsilon_{k-1}}$ for the sequence $\sigma \in \mathrm{Word}_A$ with $\mathrm{lh}(\sigma) = k$ and $\sigma(i) = a_i^{\epsilon_i}$.

An element $x \in \mathrm{Word}_A$ is *reduced* if there is no place in the sequence where a^1 and a^{-1} appear next to each other for any $a \in A$. More formally, $x \in \mathrm{Red}_A$ if and only if $x \in \mathrm{Word}_A$ and

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

where π_1 and π_2 are the standard projection functions on pairs. Both Word_A and Red_A have Σ^0_0 definitions, so RCA_0 proves they exist.

To define the group structure on Red_A, we need a function that maps words to reduced words by repeatedly removing symbols a^1 and a^{-1} which occur next to each other. Two words $x, y \in \mathrm{Word}_A$ are *1 step equivalent*, denoted $x \sim_1 y$, if either they are the same sequence or one results from the other by deleting a pair a^1, a^{-1} that appear next to each other. This concept can be formalized by a Σ^0_0 formula, so RCA_0 proves the existence of the set of pairs $\langle x, y\rangle$ such that $x \sim_1 y$. 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 $\sigma(0) = x$, $\sigma(\mathrm{lh}(\sigma) - 1) = y$, and $\sigma(i) \sim_1 \sigma(i+1)$ for $0 \leq i < \mathrm{lh}(\sigma) - 1$. Although formalizing this concepts uses a Σ^0_1 definition, we can capture free equivalence by defining a function ρ by primitive recursion as follows.

$$\rho : \mathrm{Word}_A \to \mathrm{Red}_A$$
$$\rho(1_A) = 1_A$$
$$\rho(a^\epsilon) = a^\epsilon \text{ for } a \in A, \epsilon = \pm 1$$

If $\rho(U) = a_0^{\epsilon_0} \cdots a_{k-1}^{\epsilon_{k-1}}$ then

$$\rho(U^\frown a^\epsilon) = \begin{cases} a_0^{\epsilon_0} \cdots a_{k-2}^{\epsilon_{k-2}} & \text{if } a = a_{k-1} \text{ and } \epsilon_{k-1} + \epsilon = 0 \\ a_0^{\epsilon_0} \cdots a_{k-1}^{\epsilon_{k-1}} a^\epsilon & \text{otherwise} \end{cases}$$

It follows that $x \sim \rho(x)$, $\rho(x) \in \mathrm{Red}_A$, $x \sim y$ if and only if $\rho(x) = \rho(y)$, and

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

DEFINITION 8 (RCA_0). Let $A \subseteq \mathbb{N}$. The *free group on the generators A* consists of the elements Red_A with the identity element 1_A and the multiplication $x \cdot y = \rho(x^\frown y)$.

The definition of the free product of two groups $A * B$ is similar. Instead of using sequences of generators and inverses as elements, we will use sequences whose elements alternate between A and B. For example, if $a_i \in A$ and $b_i \in B$ then strings such as

$$\langle a_1, b_3, a_2\rangle \text{ and } \langle b_2, a_1\rangle$$

are in $A * B$. To form the free product, we start with the set of finite strings over $A \cup B$. Strings are reduced by removing occurrences of 1_A and 1_B and by multiplying elements of the same group which appear next to each other in the string. For example,

$$\langle a_1, 1_A, b_2, b_3\rangle \;\mapsto\; \langle a_1, b_2 \cdot_B b_3\rangle.$$

The definitions and lemmas for free products parallel those given for free groups.

DEFINITION 9 (RCA_0). For groups A and B, we define $\mathrm{Word}_{A*B} = \mathrm{Fin}_{A\cup B}$ and we let 1_{A*B} denote the empty sequence.

DEFINITION 10 (RCA_0). The set of *reduced words* is defined by $x \in \mathrm{Red}_{A*B}$ if and only if $x \in \mathrm{Word}_{A*B}$ and one of the following conditions holds:

1. $x = 1_{A*B}$
2. For all $i < \mathrm{lh}(x)$, $x(i)$ is not 1_A or 1_B, and for all $i < (\mathrm{lh}(x) - 1)$, if $x(i) \in A$ then $x(i+1) \in B$ and if $x(i) \in B$ then $x(i+1) \in A$.

DEFINITION 11 (RCA_0). Two words $x, y \in \mathrm{Word}_{A*B}$ are *1 step equivalent*, $x \sim_1 y$, if and only if $x = y$ or one of the following conditions holds:

1. $\mathrm{lh}(x) = \mathrm{lh}(y) + 1$ and the sequence y is the same as x except one occurrence of 1_A or 1_B is removed (or the symmetric condition with the roles of x and y reversed).
2. $\mathrm{lh}(x) = \mathrm{lh}(y) + 1$ and there is an $i < \mathrm{lh}(y)$ such that $y(j) = x(j)$ for all $j < i$, $y(j) = x(j+1)$ for all $j > i$, and either $x(i), x(i+1) \in A$ and $y(i) = x(i) \cdot_A x(i+1)$, or $x(i), x(i+1) \in B$ and $y(i) = x(i) \cdot_B x(i+1)$ (or the symmetric condition with the roles of x and y reversed).

DEFINITION 12 (RCA_0). Two words $x, y \in \mathrm{Word}_{A*B}$ are *freely equivalent*, $x \sim y$, if there exists a finite sequence σ of elements of Word_{A*B} such that $\sigma(0) = x$, $\sigma(\mathrm{lh}(\sigma) - 1) = y$, and $\forall i < (\mathrm{lh}(\sigma) - 1)\ (\sigma(i) \sim_1 \sigma(i+1))$.

As in the case of free groups, this condition is Σ^0_1, so we use a function $\rho : \mathrm{Word}_{A*B} \to \mathrm{Red}_{A*B}$ to form the set of pairs $\langle x, y \rangle$ with $x \sim y$ in RCA_0.

$$\rho(1_{A*B}) = 1_{A*B}$$

$$\rho(\langle g \rangle) = \begin{cases} 1_{A*B} & \text{if } g = 1_A \vee g = 1_B \\ \langle g \rangle & \text{otherwise} \end{cases}$$

If $\rho(U) = \langle h_1, h_2, \ldots, h_r \rangle$ then

$$\rho(U^\frown \langle g \rangle) = \begin{cases} \langle h_1, \ldots, h_r \rangle & \text{if } g = 1_A \ \vee \ g = 1_B \\ \langle h_1, \ldots, h_{r-1} \rangle & \text{if } g = h_r^{-1} \\ \langle h_1, \ldots, h_r, g \rangle & \text{if } (g \in A \setminus 1_A \wedge h_r \in B) \\ & \quad \vee \ (g \in B \setminus 1_B \wedge h_r \in A) \\ \langle h_1, \ldots, h_{r-1}, h_r \cdot_A g \rangle & \text{if } g \in A \setminus 1_A \ \wedge \ h_r \in A \setminus g^{-1} \\ \langle h_1, \ldots h_{r-1}, h_r \cdot_B g \rangle & \text{if } g \in B \setminus 1_B \ \wedge \ h_r \in B \setminus g^{-1} \end{cases}$$

As in the free group case, we use properties of ρ to show that each word in Word_{A*B} is freely equivalent to a unique reduced word.

LEMMA 13 (RCA_0). *For all $W_1, W_2, W \in Word_{A*B}$:*

1. *$\rho(W) \in Red_{A*B}$ and $\rho(W) \sim W$*
2. *$W \in Red_{A*B} \to \rho(W) = W$*

3. $\rho(W_1^\frown W_2) = \rho(\rho(W_1)^\frown W_2)$

4. $\rho(W_1^\frown\langle 1_A\rangle^\frown W_2) = \rho(W_1^\frown\langle 1_B\rangle^\frown W_2) = \rho(W_1^\frown W_2)$

5. If $g, h \in A$ *then* $\rho(W^\frown\langle g, h\rangle) = \rho(W^\frown\langle g \cdot_A h\rangle)$*, and similarly for* $g, h \in B$

6. If $g, h \in A$ *then* $\rho(W_1^\frown\langle g, h\rangle^\frown W_2) = \rho(W_1^\frown\langle g \cdot_A h\rangle^\frown W_2)$*, and similarly for* $g, h \in B$

The proof of this lemma is a series of inductions formalizing the classical arguments in [6]. (Similar properties in the context of free groups are shown formally in RCA_0 in [3].) It follows from this lemma that RCA_0 can prove that $x \sim y$ if and only if $\rho(x) = \rho(y)$ and that for every $x \in \mathrm{Word}_{A*B}$ there is a unique $y \in \mathrm{Red}_{A*B}$ such that $x \sim y$. Thus, we obtain

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

and hence RCA_0 can form the set of pair $\langle x, y\rangle$ such that $x \sim y$.

DEFINITION 14. (RCA_0) Let A and B be groups. The *free product of* A *and* B, denoted $A * B$, consists of the elements Red_{A*B} with the empty sequence 1_{A*B} as the identity and multiplication given by $x \cdot y = \rho(x^\frown y)$.

Unraveling the definitions, we obtain the connection between free products of $\mathbb{Z}$ and free groups.

PROPOSITION 15 (RCA_0). *The free product* $\mathbb{Z}*\mathbb{Z}$ *is isomorphic to* F_2*, the free group on two generators.*

Proof. Let a, b denote the generators of F_2. We illustrate the isomorphism with an example. Consider the element $\langle a, a, b^{-1}, a, b, b\rangle$ of F_2. For notational convenience, let a also denote 1 in the first copy of $\mathbb{Z}$ and b denote 1 in the second copy of $\mathbb{Z}$. The given element of F_2 corresponds to the element $\langle 2a, -b, a, 2b\rangle$ of $\mathbb{Z}*\mathbb{Z}$. The isomorphism from $\mathbb{Z}*\mathbb{Z}$ to F_2 is built by expanding elements resembling na in sequences in $\mathbb{Z}*\mathbb{Z}$ to n-tuples $\langle a, a, \dots, a\rangle$ in which a appears n times. That is,

$$\langle 2a, -b, a, 2b\rangle \ \mapsto \ \langle a, a, b^{-1}, a, b, b\rangle.$$

Writing this map formally, we obtain the isomorphism. ■

3 Main Result

Having formalized the notions of free group and free product in the last section, we use standard mathematical notation for elements of these groups.

Specifically, if $X = \{x_0, x_1, \ldots\}$ is the set of generators of a free group, then we write an arbitrary element of Word_X as $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$ with $n_i \in \mathbb{Z} \setminus 0$, where $x_i^{n_i}$ refers to x_i^1 or x_i^{-1} repeated $|n_i|$ times. In this section, we prove Theorem 4 (every countable f.o. group is the o-epimorphic image of an f.o. free group) assuming the following theorem (which will be proved in later sections).

THEOREM 16 (RCA_0). *The free product of two f.o. groups is fully orderable.*

Combining Theorem 16 and Proposition 15, we obtain the following corollary.

COROLLARY 17 (RCA_0). *The free group on two generators is fully orderable.*

We use Corollary 17 to show that the free group on countably many generators is fully orderable. Let $\mathbb{N}^+$ denote the set of strictly positive natural numbers.

LEMMA 18 (RCA_0). *Let F be the free group on the two generators x, y. For each $i \in \mathbb{N}^+$ let $\alpha_i = x^i y^i$.*

1. *The word $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ with $i_{j+1} \neq i_j$, $n_j \in \mathbb{Z} \setminus \{0\}$, and $k > 0$ freely reduces to a word ending in $x^\epsilon y^{i_k}$ if $n_k > 0$ and $y^\epsilon x^{-i_k}$ if $n_k < 0$.*
2. *No product $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ with the above restrictions is the identity element.*

Proof. Assuming the first property holds, there is either an x or a y with a nonzero exponent in the reduced form of $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$. Therefore, the second property follows immediately from the first. The first property is proved by induction on k. If $k = 1$ then

$$\alpha_{i_1}^{n_1} = (x^{i_1} y^{i_1})^{n_1}$$

which satisfies the first property. If $k > 1$, then split into cases depending on the signs of n_k and n_{k-1}.

CASE 19. $n_k > 0$ and $n_{k-1} > 0$

By the induction hypothesis, $\alpha_{i_1}^{n_1} \cdots \alpha_{i_{k-1}}^{n_{k-1}}$ reduces to a word ending in $x^\epsilon y^{i_{k-1}}$. Thus $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ reduces to a word ending in $x^\epsilon y^{i_{k-1}} (x^{i_k} y^{i_k})^{n_k}$. Since $n_k > 0$, this word ends in $x^{i_k} y^{i_k}$. The case when $n_k, n_{k-1} < 0$ is similar.

CASE 20. $n_k > 0$ and $n_{k-1} < 0$

By the induction hypothesis, $\alpha_{i_1}^{n_1} \cdots \alpha_{i_{k-1}}^{n_{k-1}}$ reduces to a word ending in $y^\epsilon x^{-i_{k-1}}$. Hence $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ reduces to a word ending in $y^\epsilon x^{-i_{k-1}}(x^{i_k} y^{i_k})^{n_k}$. If $n_k = 1$ then we have a word ending in $y^\epsilon x^{i_k - i_{k-1}} y^{i_k}$. By assumption, $i_k - i_{k-1} \neq 0$ so we have satisfied the first property. If $n_k > 1$, then this word ends in $x^{i_k} y^{i_k}$. The case when $n_k < 0$ and $n_{k-1} > 0$ is similar. ■

PROPOSITION 21 (RCA_0). *The free group on a countable number of generators is fully orderable.*

Proof. Let F and α_i be as in Lemma 18 and let $P(F)$ be the positive cone for some full order on F. Let G be the free group on the generators x_i with $i \in \mathbb{N}^+$. Define the homomorphism $\psi : G \to F$ sending $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \mapsto \alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$. If $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}$ is fully reduced and $x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \neq 1_G$, then $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k}$ satisfies the hypotheses of Lemma 18. Hence $\alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k} \neq 1_F$ so ψ is a monomorphism. The set $P(G) = \{x_{i_1}^{n_1} \cdots x_{i_k}^{n_k} \mid \alpha_{i_1}^{n_1} \cdots \alpha_{i_k}^{n_k} \in P(F)\}$ is the positive cone of a full order on G. ■

We can use a technique from Revesz [7] to give a proof of Theorem 4, which is restated below.

THEOREM 22 (RCA_0). *Every countable f.o. group is the o-epimorphic image of an f.o. free group.*

Proof. Let $(G, \leq_G)$ be an f.o. group, $P(G)$ be the positive cone of $\leq_G$, and $g_0, g_1, \ldots$ be an enumeration of $G \setminus \{1_G\}$. Let F be the free group on the generators $x_0, x_1, \ldots$ and, by Proposition 21, let $P(F)$ be the positive cone of some full order on F. Define the epimorphism $\varphi : F \to G$ by $\varphi(x_{i_1}^{n_1} \cdots x_{i_k}^{n_k}) = g_{i_1}^{n_1} \cdots g_{i_k}^{n_k}$. We produce a new order $\tilde{P}(F)$ on F under which φ is order preserving.

Define an embedding $\psi : F \to G \times F$ by $\psi(a) = \langle \varphi(a), a \rangle$. Order $G \times F$ lexicographically, i.e. by the positive cone

$$\langle a, b \rangle \in P(G \times F) \leftrightarrow (a \in P(G) \wedge a \neq 1_G) \vee (a = 1_G \wedge b \in P(F)).$$

Since ψ is a monomorphism, we define a new positive cone on F by $\tilde{P}(F) = \{a \mid \psi(a) \in P(G \times F)\}$. It remains to show that φ is order preserving under $\tilde{P}(F)$. Rewriting the definition of $\tilde{P}(F)$ we have

$$a \in \tilde{P}(F) \leftrightarrow (\varphi(a) \in P(G) \wedge \varphi(a) \neq 1_G) \vee (\varphi(a) = 1_G \wedge a \in P(F)).$$

Let $\leq_F$ be the order corresponding to $\tilde{P}(F)$. Suppose that $a \leq_F b$. Since $a^{-1}b \in \tilde{P}(F)$, we have $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \in P(G)$ by the definition of $\tilde{P}(F)$ and hence $\varphi(a) \leq_G \varphi(b)$. Now, suppose that $c, d \in G$ and $c <_G d$. Since φ is onto, there are $a, b \in F$ with $\varphi(a) = c$ and $\varphi(b) = d$. Since $c <_G d$, we have that $c^{-1}d \in P(G)$ and $c^{-1}d \neq 1_G$. Because $\varphi(a^{-1}b) = c^{-1}d$ and $c^{-1}d \neq 1_G$, we have (by the definition of $\tilde{P}(F)$) that $a^{-1}b \in \tilde{P}(F)$ and so $a <_F b$. Therefore, φ is an o-epimorphism from $(F, \leq_F)$ onto $(G, \leq_G)$. ■

4 Ordered Rings and Triangular Matrices

In this section, we lay the framework to prove Theorem 16, which we do in the next section. The proof given here is a modification of the proof given in Kokorin and Kopytov [5]. The idea is to embed the free product into a set of infinite upper triangular matrices over a fully ordered ring. In this section, we introduce ordered rings and formalize the spaces of upper triangular matrices in second order arithmetic.

DEFINITION 23 (RCA_0). A *ring* is a set R together with two functions $+_R$, $\cdot_R$ and two constants 0_R, 1_R which satisfy the usual axioms for a commutative ring with identity. (We often drop the subscripts R when there is no chance of confusion.)

In this paper, rings will always be commutative with identity. As with groups, the subscripts will be dropped when the context is clear.

DEFINITION 24 (RCA_0). A *partially ordered (p.o.) ring* is a ring R together with a partial order $\leq_R$ on R such that $a \leq_R b$ implies $a + c \leq_R b + c$ for all $a, b, c \in R$, and $a \leq_R b$ and $c >_R 0_R$ implies $ca \leq_R cb$ and $ac \leq_R bc$. If $\leq_R$ is linear, then $(R, \leq_R)$ is a *fully ordered (f.o.) ring*.

The positive cone of a p.o. ring R is $P(R) = \{r \in R \mid r \geq_R 0_R\}$ and negative cone is $-P(R) = \{-r \mid r \in P(R)\}$. RCA_0 can verify properties of P similar to those for p.o. groups such as $P \cap -P = \{0\}$ and for fully ordered rings $P \cup -P = R$. Classically, positive cones for rings also satisfy $P + P \subseteq P$ and $PP \subseteq P$. Although RCA_0 is not strong enough to prove that the sets $P + P$ and PP exist, it is strong enough to show

$$\forall x, y \in R \; (x \in P \wedge y \in P \rightarrow x + y \in P)$$
$$\forall x, y \in R \; (x \in P \wedge y \in P \rightarrow xy \in P).$$

In the context of RCA_0, we take $P + P \subseteq P$ to stand for the top formula and $PP \subseteq P$ to stand for the bottom formula.

THEOREM 25 (RCA_0). *A subset P of a ring R is the positive cone of a partial order on R if and only if $P \cap -P = \{0\}$, $P + P \subseteq P$ and $PP \subseteq P$. P is the positive cone of a full order if and only if P also satisfies $P \cup -P = R$.*

Proof. It is straightforward to check that any positive cone satisfies these requirements. Conversely, if P is a set with these properties, then the order can be defined by $a \leq b$ if and only if $b - a \in P$. ■

Given a f.o. ring K, we define a class of upper triangular matrices with the rows and columns indexed by the elements of $\mathbb{N}^+$ and with positive invertible elements along the main diagonal. Such a matrix resembles:

$$\begin{pmatrix} k_{11} & k_{12} & k_{13} & k_{14} & \dots \\ 0 & k_{22} & k_{23} & k_{24} & \dots \\ 0 & 0 & k_{33} & k_{34} & \dots \\ \vdots & \vdots & \vdots & \ddots & \ddots \end{pmatrix}$$

where each k_{ii} is in $P(K)$ and has a multiplicative inverse. Since there are an uncountable number of such matrices, we represent them in second order arithmetic as a class of functions.

DEFINITION 26 (RCA_0). Let $(K, \leq_K)$ be a fully ordered ring with positive cone $P(K)$. The function $f : \mathbb{N}^+ \times \mathbb{N}^+ \to K$ is *in the class Tri$_K$*, denoted $f \in \text{Tri}_K$, if and only if it satisfies the following conditions.

1. For all $i > j$, $f(i, j) = 0_K$.
2. For all i, $f(i, i) \in P(K)$ and $\exists x \in K(f(i, i) \cdot x = 1_K)$.

We define an order and a group structure on Tri_K. Given $f, g \in \text{Tri}_K$, we define $f < g$ if and only if for some pair $\langle i, j\rangle \in \mathbb{N}^+ \times \mathbb{N}^+$ with $i \leq j$ the following two conditions hold:

1. $f(i, j) <_K g(i, j)$.
2. $f(k, k + s) = g(k, k + s)$ for all k, s such that $i + s < j$ or $i + s = j$ and $k < i$.

A pair $\langle i, j\rangle$ for which these conditions hold is called a witness for $f < g$. When f and g are viewed as matrices, these conditions say that we compare f and g down the diagonals, starting with the main diagonal, then the diagonal to its right, and so on, until we find the first place that f and g differ. The entries of f and g are compared in the order indicated in this picture:

$$\begin{pmatrix} 1 & \omega & \omega+\omega & \omega+\omega+\omega & \dots \\ \cdot & 2 & \omega+1 & \omega+\omega+1 & \ddots \\ \cdot & \cdot & 3 & \omega+2 & \ddots \\ \cdot & \cdot & \cdot & 4 & \ddots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

That is, we compare f and g by comparing two ordered sequences of elements of K with order type $\omega \cdot \omega$. If $f \neq g$, then the relationship between f and g is determined by the relationship between the elements of K at the first place where these ordered sequences differ. While RCA_0 is strong enough to prove that $\omega \cdot \omega$ is well ordered, we will eventually need a stronger comparability result. Our goal is to embed $A * B$ into Tri_K (for a particular K we construct in the next section) and pull the order back from Tri_K to $A * B$. For this process, we need to be able to determine the order between elements of Tri_K (in the image of the embedding) uniformly. RCA_0 is not strong enough to uniformly compare sequences of length $\omega \cdot \omega$.

To be more specific, let $s_i(x, y)$ (for $i \in \mathbb{N}$) be a sequence of functions. For each i, think of $s_i(x, y)$ as representing an $\omega \cdot \omega$ length sequence in which the $(n \cdot \omega + m)$-th value is $s_i(n, m)$. Assume that for all $i \neq j$, there is at least one pair (n, m) for which $s_i(n, m) \neq s_j(n, m)$. RCA_0 is not strong enough to prove the existence of a function $g(x, y)$ such that for all $i \neq j$, $g(i, j)$ is the least pair (n, m) (in the $\omega \cdot \omega$ order) at which s_i and s_j differ.

In the next section, we define a countable subgroup of Tri_K for which RCA_0 can determine the order. (For this subgroup, we will reduce the length of the well order along which we do our comparisons from $\omega \cdot \omega$ to ω.) For now, our goal is to define the group structure and to prove that the elements of Tri_K satisfy the axioms for a partially ordered group with this order.

Given $f, g \in \mathrm{Tri}_K$, we define the product $f \cdot g$ to be the function

$$f \cdot g : \mathbb{N}^+ \times \mathbb{N}^+ \to K$$
$$(f \cdot g)(i, j) = \sum_{n=1}^{\infty} f(i, n) g(n, j).$$

This definition is the standard definition for matrix multiplication. Since $f(i, n) = 0$ for $n < i$ and $g(n, j) = 0$ for $n > j$, if n is not between i and j, then $f(i, n)g(n, j) = 0$. Therefore, if $i > j$, then the sum is 0, and if $i \leq j$, then the infinite sum reduces to the finite sum $\sum_{n=i}^{j} f(i, n)g(n, j)$. Thus, RCA_0 proves $f \cdot g$ well defined. Since $(f \cdot g)(i, i) = f(i, i)g(i, i)$, $(f \cdot g)(i, i)$ is both positive and invertible, and hence $f \cdot g \in \mathrm{Tri}_K$. The matrix $I \in \mathrm{Tri}_K$ defined by $I(i, i) = 1_K$ and $I(i, j) = 0_K$ for $i \neq j$ plays the role of the identity element in Tri_K. The next two lemmas show that RCA_0 proves the associativity of the multiplication and the existence of inverses.

LEMMA 27 (RCA_0). *For all $f, g, h \in Tri_K$, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$.*

Proof. For $j < i$, both of these products have the value 0 on input (i, j).

For $i \leq j$, direct calculation shows that

$$((f \cdot g) \cdot h)(i,j) = (f \cdot (g \cdot h))(i,j) = \sum_{i \leq n \leq m \leq j} f(i,n)g(n,m)h(m,j).$$

■

LEMMA 28 (RCA_0). *If $f \in Tri_K$, then f has an inverse $g \in Tri_K$, in the sense that $f \cdot g = g \cdot f = I$, given by:*

$$g(i,j) = \begin{cases} 0 & j < i \\ f(i,j)^{-1} & i = j \\ -\frac{f(i,j)}{f(i,i)f(j,j)} + \sum_{i<k_1<j} \frac{f(i,k_1)f(k_1,j)}{f(i,i)f(k_1,k_1),f(j,j)} & \\ \quad - \sum_{i<k_1<k_2<j} \frac{f(i,k_1)f(k_1,k_2)f(k_2,j)}{f(i,i)f(k_1,k_1)f(k_2,k_2)f(j,j)} + \cdots & i < j \\ \quad \cdots + (-1)^{j-i} \frac{f(i,i+1)\cdots f(j-1,j)}{f(i,i)f(i+1,i+1)\cdots f(j,j)} & \end{cases}$$

Since $f(n,n)$ is invertible, we write it in the denominator of a fraction as shorthand for $f(n,n)^{-1}$. The proof of Lemma 28 is presented in Section 6.

It remains to verify that the order interacts in the appropriate way with the group structure. If $f \in \mathrm{Tri}_K$, we say $f \in P(\mathrm{Tri}_K)$ if and only if $I \leq f$ in the order given above. If $f \neq I$ this is equivalent to either

$$\exists i\ [f(i,i) > 1 \wedge \forall j < i(f(j,j) = 1)]$$

or

$$\forall i\ (f(i,i) = 1)\ \wedge\ \exists i,j\ \Big(\ i < j \wedge f(i,j) > 0\ \wedge$$
$$\forall k\ \forall s > 0\ \big((i+s < j \vee (i+s = j \wedge k < i)) \rightarrow f(k,k+s) = 0\big)\Big).$$

The proof of the following lemma is delayed until Section 6.

LEMMA 29 (RCA_0).

1. *If $f, g \in P(Tri_K)$ then $f \cdot g \in P(Tri_K)$.*
2. *If $f \in P(Tri_K)$ and $f \neq I$ then $f^{-1} \notin P(Tri_K)$.*
3. *If $f \in P(Tri_K)$ and $g \in Tri_K$ then $gfg^{-1} \in P(Tri_K)$.*

5 Free Products of Fully Ordered Groups

In this section we prove Theorem 16. The proof has several steps, so we outline them here. Given fully ordered groups A and B, we form a larger group C of which A and B are direct summands. We use the orders on A and B to fully order the group ring $\mathbb{Q}[C]$ and form the ordered matrix group $\mathrm{Tri}_{\mathbb{Q}[C]}$. The free product $A * B$ is embedded in $\mathrm{Tri}_{\mathbb{Q}[C]}$ and we define an order on $A * B$ by pulling back the order from $\mathrm{Tri}_{\mathbb{Q}[C]}$.

Let A and B be fully ordered groups. We first define a larger ordered group C. For each pair $\langle i, j\rangle \in \mathbb{N}^+ \times \mathbb{N}^+$, let x_{ij} and y_{ij} generate copies of $\mathbb{Z}$ ordered such that x_{ij}^n and y_{ij}^n are positive if and only if $n \geq 0$. (Note that we are writing these groups multiplicatively.) For each $i \in \mathbb{N}^+$, let u_i and v_i generate copies of $\mathbb{Z}$ ordered in the same way. The notation $\langle x_{ij}\rangle$ is used for the group generated by x_{ij}, and similarly for $\langle y_{ij}\rangle$, $\langle u_i\rangle$, and $\langle v_i\rangle$.

The group C is the restricted direct product

$$C = A \times B \times \prod_{i,j=1}^{\infty} \langle x_{ij}\rangle \times \prod_{i,j=1}^{\infty} \langle y_{ij}\rangle \times \prod_{i=1}^{\infty}\langle u_i\rangle \times \prod_{i=1}^{\infty}\langle v_i\rangle.$$

Since there is a uniform sequence of orders on the factors of C, C can be lexicographically ordered in RCA_0. As above, note that C is written multiplicatively even though many of the summands are normally written additively. We use x_{ij} to denote the element of C which is the identity in all components of C except the $\langle x_{ij}\rangle$ component and has value x_{ij} in the $\langle x_{ij}\rangle$ component. We abuse notation similarly for $a \in A$, $b \in B$ and the generators u_i, v_i, y_{ij}.

Let $\mathbb{Q}[C]$ be the group ring of C over $\mathbb{Q}$. Formally, the elements of $\mathbb{Q}[C]$ are the finite sums $\sum \alpha_i c_i$ with $\alpha_i \in \mathbb{Q} \setminus \{0\}$, $c_i \in C$ and all the c_i distinct. Addition is defined by:

$$\sum_{i\in I} \alpha_i c_i \;+\; \sum_{j\in J} \beta_j c_j \;=\; \sum_{i\in I\setminus J} \alpha_i c_i \;+\; \sum_{j\in J\setminus I} \beta_j c_j \;+\; \sum_{i\in I\cap J} (\alpha_i+\beta_i) c_i$$

with the stipulation that any terms in the third sum with $\alpha_i + \beta_i = 0$ are removed. Multiplication is defined by:

$$\left(\sum_{i\in I} \alpha_i c_i\right)\left(\sum_{j\in J} \beta_j c_j\right) \;=\; \sum_{i\in I}\sum_{j\in J} (\alpha_i\beta_j) c_i c_j$$

where the terms with the same value from C in this finite sum are collected and any term with coefficient 0 is dropped. The additive identity is the empty sum and the multiplicative identity is the sum with one element $1_{\mathbb{Q}} 1_C$.

In the context of $\mathbb{Q}[C]$, we use x_{ij} to denote the single element sum $1_{\mathbb{Q}} x_{ij}$ (and similarly for y_{ij}, u_i, v_i, $a \in A$ and $b \in B$) and we use 0 (or $0_{\mathbb{Q}[C]}$) and 1 (or $1_{\mathbb{Q}[C]}$) to denote the additive and multiplicative identities.

The positive cone $P(\mathbb{Q}[C])$ is defined by $\sum_{i \in I} \alpha_i c_i \in P(\mathbb{Q}[C])$ if and only if $I = \emptyset$ or $\alpha_j >_{\mathbb{Q}} 0$ where j is such that c_j is the $\leq_C$-least element among the c_i with $i \in I$. Since I is finite there is such a $\leq_C$-least element. RCA_0 suffices to prove that this gives a full order on $\mathbb{Q}[C]$.

Now that we have a fully ordered ring, we can use the machinery of the previous section to work with $\mathrm{Tri}_{\mathbb{Q}[C]}$. The goal is to embed $A * B$ into $\mathrm{Tri}_{\mathbb{Q}[C]}$ and then use our formal ordering of $\mathrm{Tri}_{\mathbb{Q}[C]}$ to order $A * B$. The embedding is given by uniformly associating to each element of $A * B$ a function in $\mathrm{Tri}_{\mathbb{Q}[C]}$. To do this we specify four matrices in $\mathrm{Tri}_{\mathbb{Q}[C]}$ denoted X, Y, U and V.

$$X(i,j) = \begin{cases} 1 & i = j \\ 0 & i > j \\ x_{ij} & i < j \end{cases}$$

$$Y(i,j) = \begin{cases} 1 & i = j \\ 0 & i > j \\ y_{ij} & i < j \end{cases}$$

$$U(i,j) = \begin{cases} u_i & i = j \\ 0 & i \neq j \end{cases}$$

$$V(i,j) = \begin{cases} v_i & i = j \\ 0 & i \neq j \end{cases}$$

As matrices, these functions look like:

$$X = \begin{pmatrix} 1 & x_{12} & x_{13} & \dots \\ 0 & 1 & x_{23} & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$U = \begin{pmatrix} u_1 & 0 & 0 & \dots \\ 0 & u_2 & 0 & \dots \\ 0 & 0 & u_3 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

U is upper triangular and has positive elements on the diagonal since u_i is positive in our order on $\langle u_i \rangle$. Also, since $1_{\mathbb{Q}} u_i \cdot 1_{\mathbb{Q}} u_i^{-1} = 1_{\mathbb{Q}[C]}$, U has invertible elements along the diagonal. Thus, $U \in \mathrm{Tri}_{\mathbb{Q}[C]}$. Similarly, $X, Y, V \in \mathrm{Tri}_{\mathbb{Q}[C]}$.

These matrices are used to define the embedding in several steps. For each $a \in A$, define $\alpha(a) : \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{Q}[C]$ by:

$$\alpha(a)(i,j) = \begin{cases} 1 & i = j \text{ and } i \text{ is odd} \\ a & i = j \text{ and } i \text{ is even} \\ 0 & i \neq j \end{cases}$$

As a matrix, this looks like:

$$\alpha(a) = \begin{pmatrix} 1 & 0 & 0 & \dots \\ 0 & a & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Regardless of whether a is positive or negative in A, $1_{\mathbb{Q}}a$ is positive in $\mathbb{Q}[C]$ since $1_{\mathbb{Q}} > 0_{\mathbb{Q}}$. Also, a is invertible in $\mathbb{Q}[C]$ because $1_{\mathbb{Q}}a \cdot 1_{\mathbb{Q}}a^{-1} = 1_{\mathbb{Q}[C]}$. Hence, $\alpha(a) \in \text{Tri}_{\mathbb{Q}[C]}$.

For each $b \in B$ define $\beta(b) \in \text{Tri}_{\mathbb{Q}[C]}$ similarly:

$$\beta(b)(i,j) = \begin{cases} 1 & i = j \text{ and } i \text{ is odd} \\ b & i = j \text{ and } i \text{ is even} \\ 0 & i \neq j \end{cases}$$

We define two more maps on A and B. For $a \in A$ and $b \in B$, define

$$\alpha'(a) = X^{-1} \cdot \alpha(a) \cdot X \qquad \beta'(b) = Y^{-1} \cdot \beta(b) \cdot Y$$
$$\alpha''(a) = U^{-1} \cdot \alpha'(a) \cdot U \qquad \beta''(b) = V^{-1} \cdot \beta'(b) \cdot V.$$

Later, we will use results from the previous section to produce explicit formulas for the entries in these matrices.

Because RCA_0 proves that $\text{Tri}_{\mathbb{Q}[C]}$ is closed under inverses and products, $\alpha''(a)$ and $\beta''(b)$ are both in $\text{Tri}_{\mathbb{Q}[C]}$. Also, since we have explicit formulas for inverses and products in $\text{Tri}_{\mathbb{Q}[C]}$, $\alpha''(a)$ and $\beta''(b)$ can be given uniformly from A and B. The embedding of $A * B$ into $\text{Tri}_{\mathbb{Q}[C]}$ is given by associating to each word $a_1 b_1 \cdots a_n b_n$ over A and B the product $\alpha''(a_1)\beta''(b_1) \cdots \alpha''(a_n)\beta''(b_n)$ in $\text{Tri}_{\mathbb{Q}[C]}$. The term embedding is being used loosely here since $\text{Tri}_{\mathbb{Q}[C]}$ is not a set. The correspondence is really a uniform construction of a function in $\text{Tri}_{\mathbb{Q}[C]}$ for each word over A, B. That said, we will continue to use the term embedding and will use $\gamma(w)$ to denote the element of $\text{Tri}_{\mathbb{Q}[C]}$ which corresponds to the word w.

We need to describe and check the properties of this embedding. It follows from the definitions that for $a \in A$, $\alpha(a)^{-1} = \alpha(a^{-1})$ and hence that $\gamma(a)^{-1} = \gamma(a^{-1})$. Similarly, $\gamma(b)^{-1} = \gamma(b^{-1})$ for $b \in B$, and $\gamma(w_1^{-1}) = \gamma(w_1)^{-1}$ and $\gamma(w_1 w_2) = \gamma(w_1)\gamma(w_2)$ for any words w_1 and w_2 over A and B. Therefore, γ is a group homomorphism. It is less trivial to check that γ is one-to-one.

PROPOSITION 30 (RCA_0). *If $w_1 \neq w_2$ in $A * B$, then $\gamma(w_1) \neq \gamma(w_2)$ in $Tri_{\mathbb{Q}[C]}$.*

In order to prove this proposition, we need several lemmas. Throughout these lemmas $a \in A$, $b \in B$ and w_1, w_2 are arbitrary words in $A*B$. Our first goal is to derive formulas for $\alpha'(a)$ and by analogy $\beta'(b)$. Let $f = \alpha(a) \cdot X$ and $g = X^{-1}$, so $\alpha'(a) = g \cdot f$. More explicitly, g is given by $g(i,i) = 1$, $g(i,j) = 0$ for $i > j$ and for $i < j$

$$g(i,j) = -x_{ij} + \sum_{i<k_1<j} x_{ik_1}x_{k_1 j} - \sum_{i<k_1<k_2<j} x_{ik_1}x_{k_1k_2}x_{k_2 j} + \cdots + (-1)^{j-i}(x_{i(i+1)} \cdots x_{(j-1)j}).$$

As a matrix, this looks like:

$$g = \begin{pmatrix} 1 & -x_{12} & -x_{13} + x_{12}x_{23} & \cdots \\ 0 & 1 & -x_{23} & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

f can be given explicitly by:

$$f(i,j) = \begin{cases} 1 & i = j \ \wedge \ i \text{ is odd} \\ a & i = j \ \wedge \ i \text{ is even} \\ x_{ij} & i < j \ \wedge \ i \text{ is odd} \\ ax_{ij} & i < j \ \wedge \ i \text{ is even} \\ 0 & i > j \end{cases}$$

$$f = \begin{pmatrix} 1 & x_{12} & x_{13} & \cdots \\ 0 & a & ax_{23} & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

LEMMA 31 (RCA_0).

$$\alpha'(a)(i,i) = \begin{cases} 1 & i \text{ is odd} \\ a & i \text{ is even} \end{cases}$$

Proof. This formula comes directly from the formulas for f and g. ■

The formulas for $\alpha'(a)(i,j)$ when $i < j$ are given below. We will prove Lemma 32 in Section 6. The proofs of Lemmas 33, 34 and 35 are similar and are omitted.

LEMMA 32 (RCA_0). *If $i < j$ and i, j are both even, then*

$$\alpha'(a)(i,j) = (1-a)\sum_{\substack{n=i+1 \\ n\ odd}}^{j-1}\Bigg(-x_{in}x_{nj} + \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) - \\ - \sum_{i<k_1<k_2<n}(x_{ik_1}x_{k_1k_2}x_{k_2n}x_{nj}) + \cdots + (-1)^{n-i}x_{i(i+1)}\cdots x_{(n-1)n}x_{nj}\Bigg)$$

LEMMA 33 (RCA_0). *If $i < j$, i is even, and j is odd then*

$$\alpha'(a)(i,j) = (1-a)(-x_{ij}) + (1-a)\sum_{\substack{n=i+1 \\ n\ even}}^{j-1}\Bigg(x_{in}x_{nj} - \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) + \\ + \sum_{i<k_1<k_2<n}x_{ik_1}x_{k_1k_2}x_{k_nn}x_{nj} - \cdots + (-1)^{n-i}x_{ii+1}\cdots x_{n-1n}x_{nj}\Bigg)$$

LEMMA 34 (RCA_0). *If $i < j$ and i, j are both odd, then*

$$\alpha'(a)(i,j) = (1-a)\sum_{\substack{n=i+1 \\ n\ even}}^{j-1}\Bigg(x_{in}x_{nj} - \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) + \\ + \sum_{i<k_1<k_2<n}(x_{ik_1}x_{k_1k_2}x_{k_2n}x_{nj}) + \cdots + (-1)^{n-i}x_{i(i+1)}\cdots x_{(n-1)n}x_{nj}\Bigg)$$

LEMMA 35 (RCA_0). *If $i < j$, i is odd, and j is even then*

$$\alpha'(a)(i,j) = (1-a)(x_{ij}) + (1-a)\sum_{\substack{n=i+1 \\ n\ odd}}^{j-1}\Bigg(-x_{in}x_{nj} + \sum_{i<k_1<n}(x_{ik_1}x_{k_1n}x_{nj}) - \\ - \sum_{i<k_1<k_2<n}x_{ik_1}x_{k_1k_2}x_{k_nn}x_{nj} + \cdots + (-1)^{n-i}x_{i(i+1)}\cdots x_{(n-1)n}x_{nj}\Bigg)$$

The same results hold for $\beta'(b)$ with b substituted into the formulas for a and y_{ij} substituted for x_{ij}. From these formulas, it is clear that if $a = 1_A$ then $\alpha'(a) = I$ in $\mathrm{Tri}_{\mathbb{Q}[C]}$, and similarly for b. Also, if $a \neq 1_A$, then in particular, the diagonal elements of $\alpha'(a)$ are not all 1, so $\alpha'(a) \neq I$. A closer look at these formulas reveals the following lemma.

LEMMA 36 (RCA_0). *If $a \neq 1_A$ and $b \neq 1_B$ then for any i, j with $i \leq j$, $\alpha'(a)(i,j) \neq 0$ and $\beta'(b)(i,j) \neq 0$.*

We are now ready to prove Proposition 30.

Proof. To show that $w_1 \neq w_2$ in $A * B$ implies that $\gamma(w_1) \neq \gamma(w_2)$ in $\mathrm{Tri}_{\mathbb{Q}[C]}$, it suffices to show that $\gamma(w) \neq I$ for an arbitrary nonidentity element w. Let $w = a_1 b_1 \cdots a_t b_t$ be an arbitrary nonidentity word in $A * B$ that is reduced, except that possibly $a_1 = 1_A$ or $b_t = 1_B$. It suffices to show for $i < j$ that $\gamma(w)(i,j) \neq 0$.

The multiplication formula in $\mathrm{Tri}_{\mathbb{Q}[C]}$ extends to the following formula for the product of m functions $f_1, \ldots, f_m$ in $\mathrm{Tri}_{\mathbb{Q}[C]}$: for $i > j$, $f_1 \cdots f_m(i,j) = 0$ and for $i \leq j$

$$f_1 \cdots f_m(i,j) = \sum_{i \leq k_1 \leq \cdots \leq k_{m-1} \leq j} f_1(i,k_1) f_2(k_1,k_2) \cdots f_m(k_{m-1},j).$$

We consider the case in which $a_1 \neq 1_A$ and $b_t \neq 1_B$. By the multiplication formula, if $c = \alpha''(a_1)\beta''(b_1) \cdots \alpha''(a_t)\beta''(b_t)$, then for $i \leq j$

$$c(i,j) = \sum_{i \leq k_i \leq \cdots \leq k_{2t-1} \leq j} \Big(\alpha''(a_1)(i,k_1)\beta''(b_1)(k_1,k_2) \cdots \\ \cdots \alpha''(a_t)(k_{2t-2},k_{2t-1})\beta''(b_t)(k_{2t-1},j) \Big).$$

Applying the formulas for multiplication and inverses, we have

$$\alpha''(a)(i,j) = \frac{1}{u_i} \alpha'(a)(i,j) u_j$$
$$\beta''(b)(i,j) = \frac{1}{v_i} \beta'(b)(i,j) v_j.$$

As before, the notation $\frac{1}{u_i}$ stands for u_i^{-1} Putting these formulas together gives us:

$$c(i,j) = \sum_{i \leq k_1 \leq \cdots \leq k_{2t-1} \leq j} \Big(\frac{u_{k_1}}{u_i} \frac{v_{k_2}}{v_{k_1}} \frac{u_{k_3}}{u_{k_2}} \cdots \frac{v_j}{v_{k_{2t-1}}} \alpha'(a_1)(i,k_1) \cdot \\ \cdot \; \beta'(b_1)(k_1,k_2) \cdots \alpha'(a_t)(k_{2t-2},k_{2t-1})\beta'(b_t)(k_{2t-1},j) \Big).$$

Viewing $c(i,j)$ as a polynomial in the variables $u_r, v_r, 1/u_r$ and $1/v_r$ for $i \leq r \leq j$, it is clear that none of the terms in the polynomial cancel. Also, since $\alpha'(a_m)(r,s) \neq 0$, $\beta'(b_m)(r,s) \neq 0$ for any $i \leq r \leq s \leq j$, and since any group ring has no zero divisors, none of the terms drop out because they are zero. The remaining cases, $a_1 = 1_A, b_t \neq 1_B$ etc., are similar. Thus $c \neq I$. ■

Recall that comparing arbitrary elements of $\mathrm{Tri}_{\mathbb{Q}[C]}$ involves comparing sequences with order type $\omega \cdot \omega$. The key to proving Theorem 16 in RCA_0 is to show that if $w_1 \neq w_2 \in A * B$ then comparing $\gamma(w_1)$ and $\gamma(w_2)$ requires only comparing sequences of elements of $\mathbb{Q}[C]$ with order type ω.

DEFINITION 37 (RCA_0). If $r \in \mathbb{Q}[C]$ then define r^{+n} to be the element of $\mathbb{Q}[C]$ that looks just like r except the subscripts on x_{ij}, y_{ij}, u_i and v_i are all adjusted by $+n$. That is, $x_{ij} \mapsto x_{(i+n)(j+n)}$, $u_i \mapsto u_{i+n}$, etc.

PROPOSITION 38 (RCA_0). *If $f \in Tri_{\mathbb{Q}[C]}$ is in the image of γ then*

$$f(1,j)^{+2n} = f(1+2n, j+2n)$$
$$f(2,j)^{+2n} = f(2+2n, j+2n).$$

DEFINITION 39 (RCA_0). If the conditions in the conclusion of Proposition 38 hold for f, then we say f possesses the *shift property.*

The proof of Proposition 38 is broken into several lemmas.

LEMMA 40 (RCA_0). *If $f, g \in Tri_{\mathbb{Q}[C]}$ possess the shift property, then so does $f \cdot g$.*

Proof. Consider $(f \cdot g)(1,j)$. If $j = 1$, then we have:

$$\begin{aligned}(f \cdot g)(1+2n, 1+2n) &= f(1+2n, 1+2n)g(1+2n, 1+2n) \\ &= f(1,1)^{+2n} g(1,1)^{+2n} \\ &= \left((f \cdot g)(1,1)\right)^{+2n}.\end{aligned}$$

If $j > 1$ then we have:

$$\begin{aligned}
(f \cdot g)(1+2n, j+2n) &= \sum_{m=1+2n}^{j+2n} f(1+2n, m)g(m, j+2n) \\
&= \sum_{m=1}^{j} f(1+2n, m+2n)g(m+2n, j+2n) \\
&= \sum_{m=1}^{j} f(1,m)^{+2n} g(m,j)^{+2n} \\
&= \sum_{m=1}^{j} \big(f(1,m)g(m,j)\big)^{+2n} = \big((f \cdot g)(1,j)\big)^{+2n}.
\end{aligned}$$

The cases for $(f \cdot g)(2,j)$ are similar. ■

LEMMA 41 (RCA_0). *If $a \in A$ then $\alpha'(a)$ and $\alpha'(a^{-1})$ have the shift property.*

Proof. This proof utilizes the formulas which we derived for $\alpha'(a)$. Along the principal diagonal, we have:

$$\alpha'(a)(i,i) = \begin{cases} 1 & i \text{ is odd} \\ a & i \text{ is even} \end{cases}$$

This satisfies the shift property for the cases $\alpha'(a)(1,1)$ and $\alpha'(a)(2,2)$. If $j > 1$ and odd, then using our formulas:

$$\begin{aligned}
\alpha'(a)(1,j) \;=\; (1-a) \sum_{\substack{m=2 \\ \text{m even}}}^{j-1} \Bigg(& x_{1m}x_{mj} \;-\; \sum_{1<k_1<m} (x_{1k_1}x_{k_1m}x_{mj}) \;+ \\
+ \sum_{1<k_1<k_2<m} & (x_{1k_1}x_{k_1k_2}x_{k_2m}x_{mj}) \;+ \cdots + (-1)^{m-1} x_{12} \cdots x_{m-1m}x_{mj} \Bigg).
\end{aligned}$$

When we write the formula for $\alpha'(a)(1+2n, j+2n)$ instead of letting m range from $2+2n$ to $j-1+2n$, we let it range from 2 to $j-1$ and adjust the subscripts inside the sum.

$$\alpha'(a)(1+2n, j+2n) \;=\; (1-a) \sum_{\substack{m=2 \\ \text{m even}}}^{j-1} \Bigg(x_{(1+2n)(m+2n)} x_{(m+2n)(j+2n)} -$$

$$- \sum_{1<k_1<m} \left(x_{(1+2n)(k_1+2n)} x_{(k_1+2n)(m+2n)} x_{(m+2n)(j+2n)} \right) + \cdots$$

$$+ \cdots (-1)^{m+2n-(1+2n)} \left(x_{(1+2n)(1+2n+1)} \cdots x_{(m+2n)(j+2n)} \right) \Bigg)$$

Once you observe that $m+2n-(1+2n) = m-1$, it is clear that these two sums can be obtained from one another by a shift in the indices of $+2n$. The other cases follow similarly using the formulas for $\alpha'(a)$ and $\alpha'(a^{-1})$. ■

LEMMA 42 (RCA_0). *If $a \in A$ then $\alpha''(a)$ and $\alpha''(a^{-1})$ have the shift property.*

Proof. This follows from the fact that

$$\alpha''(a)(i,j) = \frac{u_j}{u_i} \alpha'(a)(i,j)$$

We have

$$\begin{aligned} \alpha''(a)(i+2n, j+2n) &= \frac{u_{j+2n}}{u_{i+2n}} \alpha'(a)(i+2n, j+2n) \\ &= \frac{u_{j+2n}}{u_{i+2n}} \alpha'(a)(i,j)^{+2n} \\ &= \alpha''(a)(i,j)^{+2n}. \end{aligned}$$

The case for $\alpha''(a^{-1})$ is similar. ■

LEMMA 43 (RCA_0). *If $b \in B$ then $\beta'(b), \beta'(b^{-1}), \beta''(b)$ and $\beta''(b^{-1})$ have the shift property.*

Proof. The proof is the same as for $\alpha'(a)$ and $\alpha''(a)$. ■

We can now prove Proposition 38.

Proof. By assumption $\gamma(w) = f$ for some $w \in A * B$. From the facts that w is a word over A and B, that γ is a homomorphism, that $\gamma(a), \gamma(a^{-1}), \gamma(b)$ and $\gamma(b^{-1})$ have the shift property for all $a \in A$ and $b \in B$, and that the shift property is preserved under multiplication, it follows that f has the shift property. ■

It remains to show how to pull the order on $\mathrm{Tri}_{\mathbb{Q}[C]}$ back to $A * B$. Suppose that $f \in \mathrm{Tri}_{\mathbb{Q}[C]}$, $f \neq I$, and f has the shift property. Since $f \neq I$, there is some pair $\langle i, j \rangle$ such that $f(i,j) \neq I(i,j)$. In order to tell if $f \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$ we need to look down the diagonals until we find the first such pair. However, because f has the shift property, if f and I agree on the first two entries in any diagonal, they will agree on all entries in that diagonal. Comparing f and I is now easy. Thinking of them as matrices, we compare the entries in the following order:

$$\begin{pmatrix} 1 & 3 & 5 & 7 & \dots \\ \cdot & 2 & 4 & 6 & \dots \\ \multicolumn{5}{c}{--\,irrelevant\,--} \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

We only need to search through a sequence of elements with order type ω. If we know that $f \neq I$ then we can find the first place they differ in this sequence. We finally show how to define $P(A*B)$ from $P(\mathrm{Tri}_{\mathbb{Q}[C]})$.

$$P(A*B) = \{1_{A*B}\} \cup \{x \in A*B \mid x \neq 1_{A*B} \wedge \gamma(x) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})\}$$

RCA_0 proves the existence of this set because for any $x \neq 1_{A*B}$, we know that $\gamma(x) \neq I$ and $\gamma(x)$ has the shift property. Therefore, RCA_0 proves there is a first place in the sequence of matrix elements indicated above in which the entry differs from the entry in the identity matrix. We compare this entry with the corresponding entry in the identity matrix to determine if $\gamma(x) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$. It remains to show that this set is in fact the positive cone of a full order on $A * B$.

CLAIM 44. *$P(A * B)$ is normal, pure and closed under multiplication.*

Verifying these conditions is similar, so we restrict ourselves to checking that $P(A * B)$ is closed under multiplication. Assume $x, y \in P(A * B)$. Since $P(\mathrm{Tri}_{\mathbb{Q}[C]})$ is closed under multiplication and $\gamma(x), \gamma(y) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$, we have $\gamma(x)\gamma(y) = \gamma(xy) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$. Also, assuming that at least one of x, y is not 1_{A*B}, then x and y cannot be inverses because $P(\mathrm{Tri}_{\mathbb{Q}[C]})$ is pure. Thus, $\gamma(xy) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$ implies that $xy \in P(A*B)$ and so $P(A*B)$ is closed under multiplication.

CLAIM 45. *$P(A * B)$ is full.*

Assume $\gamma(x) \notin P(\mathrm{Tri}_{\mathbb{Q}[C]})$. We need to show that $\gamma(x)^{-1} = \gamma(x^{-1}) \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$. Notice that $\gamma(x) \neq I$. Before splitting into cases, note that $\gamma(x)(1,1) = 1$ for every $x \in A*B$, and if $x \in A*B$ is the word $a_1 b_1 \cdots a_k b_k$, then $\gamma(x)(2,2) \in \mathbb{Q}[C]$ is the single element sum $1_{\mathbb{Q}} ab$, where $ab \in C$ is the element whose projection onto A is $a = a_1 \cdot_A a_2 \cdots_A a_k$ and whose projection onto B is $b = b_1 \cdot_B b_2 \cdots_B b_k$. The proof splits into two cases.

CASE 46. $\gamma(x)(2,2) \neq 1$.

Since $\gamma(x)(1,1) = 1$ and $\gamma(x) \notin P(\mathrm{Tri}_{\mathbb{Q}[C]})$, we know that $\gamma(x)(2,2) < 1$ in $\mathbb{Q}[C]$. Assume that x is the word $a_1b_1 \cdots a_kb_k$ and $\gamma(x)(2,2) = 1_{\mathbb{Q}}ab$ as above. The inequality $1_{\mathbb{Q}}ab < 1_{\mathbb{Q}}1_C$ in $\mathbb{Q}[C]$ means that $1_{\mathbb{Q}}1_C - 1_{\mathbb{Q}}ab \in P(\mathbb{Q}[C])$. Because membership in $P(\mathbb{Q}[C])$ is determined by looking at the coefficient for the $\leq_C$-least element in this sum, we must have $1_C <_C ab$ in the group C. However, $\gamma(x)^{-1}(2,2) = 1_{\mathbb{Q}}(ab)^{-1}$. From $1_C <_C ab$, it follows that $(ab)^{-1} <_C 1_C$ and hence that $1_{\mathbb{Q}}1_C < 1_{\mathbb{Q}}(ab)^{-1}$. Therefore, $\gamma(x)^{-1}(2,2) > 1$. Since $\gamma(x)^{-1}(1,1) = 1$, we have $\gamma(x)^{-1} \in P(\mathrm{Tri}_{\mathbb{Q}[C]})$ as required.

CASE 47. $\gamma(x)(1,1) = \gamma(x)(2,2) = 1$

Because $\gamma(x)$ has the shift property, there is a least $j > 1$ such that either $\gamma(x)(1,j) \neq 0$ or $\gamma(x)(2,j) \neq 0$ and $\gamma(x)(1,j) = 0$. Assume that $\gamma(x)(1,j) \neq 0$. The other case is similar. Since $\gamma(x) \notin P(\mathrm{Tri}_{\mathbb{Q}[C]})$ it must be that $\gamma(x)(1,j) < 0$. Using the fact that $\gamma(x)(n,n) = 1$ for all n, the formula for $\gamma(x)^{-1}(1,j)$ gives:

$$\gamma(x)^{-1}(i,j) = -\gamma(x)(1,j) \; + \sum_{1<k_1<j} \gamma(x)(1,k_1)\gamma(x)(k_1,j) \; - \cdots$$
$$\cdots + (-1)^{j-1}(\gamma(x)(1,2) \cdots \gamma(x)(j-1,j)).$$

All the terms drop out except for the first one because $\gamma(x)(1,k) = 0$ for any $1 < k < j$. Thus, $\gamma(x)^{-1}(1,j) = -\gamma(x)(1,j) > 0$. The check that $\gamma(x)^{-1}(k,k+s) = 0$ for the appropriate k, s is similar.

We have completed the proof of Theorem 16.

6 Proofs for $\mathrm{Tri}_{\mathbb{Q}[C]}$

In this section, we prove some of the technical formulas about Tri_K and $\mathrm{Tri}_{\mathbb{Q}[C]}$ that we omitted in Sections 4 and 5. Specifically, we prove Lemmas 28, 29 and 32. We have restated these lemmas below. Recall that K is an f.o. ring. If $f \in \mathrm{Tri}_K$, then $f(n,n)$ is invertible for all $n \in \mathbb{N}^+$ and hence we can write it in the denominator of fractions.

LEMMA 48 (RCA_0). *If $f \in Tri_K$, then f has an inverse $g \in Tri_K$, in the* *sense that $f \cdot g = g \cdot f = I$, given by:*

$$g(i,j) = \begin{cases} 0 & j < i \\ f(i,j)^{-1} & i = j \\ -\frac{f(i,j)}{f(i,i)f(j,j)} + \sum_{i<k_1<j} \frac{f(i,k_1)f(k_1,j)}{f(i,i)f(k_1,k_1),f(j,j)} - & \\ \quad - \sum_{i<k_1<k_2<j} \frac{f(i,k_1)f(k_1,k_2)f(k_2,j)}{f(i,i)f(k_1,k_1)f(k_2,k_2)f(j,j)} + \cdots & i < j \\ \quad \cdots + (-1)^{j-i} \frac{f(i,i+1)\cdots f(j-1,j)}{f(i,i)f(i+1,i+1)\cdots f(j,j)} & \end{cases}$$

Proof. We verify that $(f \cdot g)(i,j) = I(i,j)$ for all i and j. If $i > j$ then we have already noted that for $f, g \in \mathrm{Tri}_K$, $(f \cdot g)(i,j) = 0$.

For each j, the case for $i \leq j$ proceeds by induction on $j - i$. For the base case when $j - i = 0$, we have $i = j$. Since $g(i,i) = f(i,i)^{-1}$, we have $(f \cdot g)(i,i) = f(i,i) \cdot f(i,i)^{-1} = 1$ as required. For the induction case, assume that $j - i = l > 0$ and that the formula is correct for $g(j-k,j)$ for all $0 \leq k < l$. We need to show that $(f \cdot g)(j-l,j) = 0$. That is, we need to show that

$$f(j-l,j-l)g(j-l,j) + f(j-l,j-l+1)g(j-l+1,j) + \cdots \\ \cdots + f(j-l,j)g(j,j) = 0.$$

Solving this equation for $g(j-l,j)$, we need to show that

$$g(j-l,j) = \sum_{n=0}^{l-1} - \frac{f(j-l,j-n)}{f(j-l,j-l)} g(j-n,j).$$

To finish the proof, we need to show that this sum is equal to

$$- \frac{f(j-l,j)}{f(j-l,j-l)f(j,j)} + \sum_{k_1=1}^{l-1} \frac{f(j-l,j-k_1)f(j-k_1,j)}{f(j-l,j-l)f(j-k_1,j-k_1)f(j,j)} - \\ \sum_{k_1=1}^{l-2} \sum_{k_2=k_1+1}^{l-1} \frac{f(j-l,j-k_2)f(j-k_2,j-k_1)f(j-k_1,j)}{f(j-l,j-l)f(j-k_1,j-k_1)f(j-k_2,j-k_2)f(j,j)} + \cdots \\ \cdots + (-1)^l \frac{f(j-l,j-l+1)f(j-l+1,j-l+2)\cdots f(j-1,j)}{f(j-l,j-l)f(j-l+1,j-l+1)\cdots f(j,j)}. \quad (1)$$

To prove this equality, we split Equation (1) into a sum with summands of the form

$$- \frac{f(j-l,j-n)}{f(j-l,j-l)} \cdot X$$

and show that $X = g(j-n, j)$. When $n = 0$, $-f(j-l, j)/f(j-l, j-l)$ appears only in the first summand $-f(j-l, j)/(f(j-l, j-l)f(j, j))$ of Equation (1). In this case $X = f(j, j)^{-1} = g(j, j)$ as required.

When $n = 1$, the term $-f(j-l, j-1)/f(j-l, j-l)$ appears only in the second sum of Equation (1) and only when $k_1 = 1$. Thus in this case, we have $X = -f(j-1, j)/(f(j-1, j-1)f(j, j))$ which by the induction hypothesis is $g(j-1, j)$.

In general, for $1 \leq n < l$, the term $-f(j-l, j-n)/f(j-l, j-l)$ does not appear in the first summand of Equation (1), but does appear in each of the other summands up to the $(n+1)^{\text{st}}$ one. If we examine how it appears in each of these summands, we see that the second term contributes

$$- \frac{f(j-n, j)}{f(j-n, j-n)f(j, j)}$$

to X, which is the first term in $g(j-n, j)$. The third term contributes something to X whenever $k_2 = n$ and hence we get a total contribution of

$$\sum_{k_1=1}^{n-1} \frac{f(j-n, j-k_1)f(j-k_1, j)}{f(j-n, j-n)f(j-k_1, j-k_1)f(j, j)}.$$

which equals the second term in $g(j-n, j)$. This process continues until we reach the $(n+1)^{\text{st}}$ term, which contributes to X only when $k_1 = 1, k_2 = 2, \ldots k_n = n$. This give us

$$(-1)^n \; \frac{f(j-n, j-n+1) \cdots f(j-1, j)}{f(j-n, j-n) \cdots f(j, j)}$$

which is the last term of $g(j-n, j)$ and shows that $X = g(j-n, j)$ as required. We have now shown that $f \cdot g = I$. From here, we have that $g \cdot f \cdot g = g$. By a simpler induction, it can be shown that if $h \cdot g = g$ then $h = I$. Hence $g \cdot f = I$ as well. ■

LEMMA 49 (RCA_0).

1. *If $f, g \in P(Tri_K)$ then $f \cdot g \in P(Tri_K)$.*
2. *If $f \in P(Tri_K)$ and $f \neq I$ then $f^{-1} \notin P(Tri_K)$.*
3. *If $f \in P(Tri_K)$ and $g \in Tri_K$ then $gfg^{-1} \in P(Tri_K)$.*

Proof. We prove the first statement of this lemma. (The proofs of the second and third statement are similar case analyses of the entries in the matrices f^{-1} and gfg^{-1}.) To prove the first statement of the lemma, assume $f, g \in P(\mathrm{Tri}_K)$. For notational purposes, let $h = f \cdot g$. We need to show $h \in P(\mathrm{Tri}_K)$. Without loss of generality, assume that $f, g, h \neq I$. There are two cases to consider.

CASE 50. $\exists i(f(i,i) \neq 1 \vee g(i,i) \neq 1)$

Let i be the least such number. Then, $h(i,i) = f(i,i)g(i,i) > 1$ and for all $j < i$, $h(j,j) = 1$. Thus $h \in P(\mathrm{Tri}_K)$.

CASE 51. $\forall i(f(i,i) = 1 \wedge g(i,i) = 1)$

Let the pair $\langle i, j\rangle$ be a witness for $f > I$. Without loss of generality, assume that $g(i,j) \geq 0$ and that $g(k, k+s) = 0$ for all k and $s > 0$ such that $i + s < j$ or $i + s = j$ and $k < i$. That is, assume that the witness to $g > I$ comes later in the order on the diagonals than the witness for f. We are going to show that $h(i,j) > 0$, that $h(k, k+s) = 0$ for k, s as above and that $h(n,n) = 1$ for all n.

Since $f(n,n) = g(n,n) = 1$, it is clear that $h(n,n) = 1$. To show that $h(i,j) > 0$, we examine

$$h(i,j) = \sum_{n=i}^{j} f(i,n)g(n,j).$$

By the assumptions made above on f and g, we have that $f(i,i) = g(j,j) = 1$ and $f(i, i+1)$ through $f(i, j-1)$ are all 0. Thus, this sum reduces to $g(i,j) + f(i,j)$. Since $g(i,j) \geq 0$ and $f(i,j) > 0$, we have that $h(i,j) > 0$ are required.

Suppose $s > 0$, $i + s < j$ or $i + s = j$ and $k < i$. We have the following equalities:

$$\begin{aligned} h(k, k+s) &= \sum_{n=k}^{k+s} f(k,n)g(n, k+s) \\ &= \sum_{n=0}^{s} f(k, k+n)g(k+n, k+s) \\ &= f(k,k)g(k, k+s) + f(k, k+s)g(k+s, k+s) + \\ &\quad + \sum_{n=1}^{s-1} f(k, k+n)g(k+n, k+s). \end{aligned}$$

The first term in the last equation is 0 because $g(k, k+s) = 0$. The second term is 0 because $f(k, k+s) = 0$. For the third term, since $i + s \leq j$ we have that $i + n < j$ for all n in the sum. Thus $f(k, k+n) = 0$ and the third term is 0. This shows that $h(k, k+s) = 0$ and finishes the proof of the first statement of the lemma. ■

Finally, we give a proof of Lemma 32. We refer the reader back to Section 5 for the notation in this lemma, in particular for the formulas for the functions $f = \alpha(a) \cdot X$ and $g = X^{-1}$.

LEMMA 52 (RCA_0). *If $i < j$ and i, j are both even, then*

$$\alpha'(a)(i,j) = (1-a) \sum_{\substack{n=i+1 \\ n\ odd}}^{j-1} \Bigg(-x_{in}x_{nj} + \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) - \\ - \sum_{i<k_1<k_2<n} (x_{ik_1}x_{k_1k_2}x_{k_2n}x_{nj}) + \cdots + (-1)^{n-i} x_{i(i+1)} \cdots x_{(n-1)n}x_{nj} \Bigg)$$

Proof. The proof consists of grinding through the calculations one step at a time, and breaking the sum up into pieces.

$$\alpha'(a)(i,j) = \sum_{n=i}^{j} g(i,n)f(n,j)$$

$$= \underbrace{g(i,i)f(i,j)}_{(I)} + \underbrace{g(i,j)f(j,j)}_{(II)} + \underbrace{\sum_{n=i+1}^{j-1} g(i,n)f(n,j)}_{(III)}$$

Since i is even, (I) is ax_{ij}. Since j is even, $f(j,j) = a$, and so (II) equals

$$a \left(-x_{ij} + \sum_{i<k_1<j} (x_{ik_1}x_{k_1j}) - \cdots + (-1)^{j-i}(x_{i(i+1)} \cdots x_{(j-1)j}) \right)$$

(III) breaks into two cases: when n is even and when n is odd.

$$\underbrace{\sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1} \big(g(i,n)\cdot x_{nj}\big)}_{(IV)} + \underbrace{\sum_{\substack{n=i+1\\ \text{n even}}}^{j-1} \big(g(i,n)\cdot a x_{nj}\big)}_{(V)} =$$

$$\sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1} \left(-x_{in}x_{nj} + \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) - \cdots + (-1)^{n-i}(x_{i(i+1)}\cdots x_{nj})\right) +$$

$$a\cdot \sum_{\substack{n=i+1\\ \text{n even}}}^{j-1} \left(-x_{in}x_{nj} + \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) - \cdots + (-1)^{n-i}(x_{i(i+1)}\cdots x_{nj})\right)$$

There are a couple of important observations. First, (I) cancels with the first term in (II). Second, all of the terms in (V) appear in and cancel with terms in (II). Third, since j is even, it follows that $j-1$ is odd and so the last term in (II) does not cancel. Performing the cancelations, we are left with

$$a\cdot\left(\sum_{\substack{i<k_1<j\\ k_1 \text{ odd}}} (x_{ik_1}x_{k_1j}) - \sum_{\substack{i<k_1<k_2<j\\ k_2 \text{ odd}}} (x_{ik_1}x_{k_1k_2}x_{k_2j}) + \right.$$
$$\left. + \cdots + (-1)^{j-i}(x_{i(i+1)}\cdots x_{(j-1)j})\right) +$$
$$+\sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1} \left(-x_{in}x_{nj} + \sum_{i<k_1<n} (x_{ik_1}x_{k_1n}x_{nj}) - \cdots + (-1)^{n-i}(x_{i(i+1)}\cdots x_{nj})\right).$$

This equation yields the formula in the statement of the lemma once the following general rewriting principles are applied.

$$\sum_{\substack{i<k_1<j\\ k_1 \text{ odd}}} x_{ik_1}x_{k_1j} \;\Rightarrow\; -\sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1} -x_{in}x_{nj}$$

$$-\sum_{\substack{i<k_1<k_2<j\\ k_2 \text{ odd}}} x_{ik_1}x_{k_1k_2}x_{k_2j} \;\Rightarrow\; -\sum_{\substack{n=i+1\\ \text{n odd}}}^{j-1}\left(\sum_{i<k_1<n} x_{ik_1}x_{k_1n}x_{nj}\right)$$

These principles continue for longer linear sequences of subscripted k's. For example, a similar rewriting rule can be applied to the sum over $i < k_1 < k_2 < k_3 < j$ with k_3 odd. ■

BIBLIOGRAPHY

[1] M.A. Dabkowska, M.K. Dabkowski, V.S. Harizanov and A.A. Togha, "Spaces of orders and their Turing degree spectra", to appear in *Annals of Pure and Applied Logic*.

[2] R. Downey and S.A. Kurtz, "Recursion theory and ordered groups", *Annals of Pure and Applied Logic*, vol. 32, 1986, 137-151.

[3] R. Downey, D. Hirschfeldt, S. Lempp and R. Solomon, "Reverse mathematics and the Nielsen-Schreier Theorem", in S.S. Goncharov, ed., *Proceedings of the International Conference in Logic Honoring Ershov on his 60th Birthday and Maltsev on his 90th Birthday*, Novosibirsk, 2002, 59-71.

[4] L. Fuchs, *Partially ordered algebraic systems*, Pergamon Press, Oxford, 1963.

[5] A. Kokorin and V. Kopytov, *Fully ordered groups*, Halsted Press, New York, 1974.

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

[7] G. Revesz, "Full orders on free groups", in S. Wolfenstein, ed., *Algebra and Order: Proceedings of the First International Symposium on Ordered Algebraic Structures Luminy-Marseille 1984*, 1986, 105-111.

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

[9] R. Solomon, "Reverse mathematics and ordered groups", *Notre Dame Journal of Formal Logic*, vol. 39, 1998, 157-189.

[10] R. Solomon, "Ordered groups: a case study in reverse mathematics", *Bulletin of Symbolic Logic*, vol. 5 (1) March 1999, 45-58.