Computer-Assisted Proofs and the $F^{a,b,c}$ Conjecture

Dale C. Sutherland

A Thesis submitted for the degree of Doctor of Philosophy

University of St. Andrews

March 2006

für elise...

Contents

Declarations

I, Dale Christina Sutherland, hereby certify that this thesis, which is approximately 60,000 words in length, has been written by me, that it is the record of work carried out by me and that it has not been submitted in any previous application for a higher degree.

date: 06/03/06 signature of candidate:
name of candidate: Dale C. Sutherland

I was admitted as a research student in September 2002, and as a candidate for the degree of Doctor of Philosophy in September 2003; the higher study for which this is a record was carried out in the University of St Andrews between 2002 and 2005.

date: 06/03/06 signature of candidate:
name of candidate: Dale C. Sutherland

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of Doctor of Philosophy in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree.

date: 6/03/06 signature of supervisor
name of supervisor: Prof. Edmund F. Robertson

In submitting this thesis to the University of St Andrews I understand that I am giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. I also understand that the title and abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker.

date: 06/03/06 signature of candidate:
name of candidate: Dale C. Sutherland

Acknowledgements

With gratitude, I would like to acknowledge those who provided me with help and support during this degree. I wish to first thank my supervisor, Prof. Edmund F. Robertson, who gave me so much time, encouragement, assistance and direction throughout these three years. For all their ideas and collaboration in my research, I must thank both Dr. George Havas and Prof. Robertson.

For providing financial support, I want to express my appreciation to the three funding bodies: the Overseas Research Students Awards Scheme, the University of St Andrews and the School of Mathematics and Statistics at the University of St Andrews. This funding could not have been attained without the help of my supervisor as well as Prof. Nikola Ruškuc and Dr. Colin M. Campbell.

Finally, I would like to acknowledge my family and friends. You were there for me, and I thank you.

Abstract

This thesis studies finitely presented groups and the process known as coset enumeration, which finds the index of a finitely generated subgroup in a finitely presented group, provided this index is finite. The Todd-Coxeter algorithm for coset enumeration is described, as well as its modified version, additionally finding a presentation for the subgroup. Coset enumeration is suitable for computer implementation, and GAP and ACE, two programs containing such functions using different strategies, are outlined.

Proof Extraction After Coset Enumeration (PEACE) is a computer program that allows one to show a group element is in the subgroup. Descriptions are provided of modifications to PEACE, giving this program the extra functionality of creating subgroup presentations with the Modified Todd-Coxeter algorithm. Using different strategies during the enumeration to determine varied subgroup presentations is also discussed. Additionally, a program converting the output of the original PEACE program, showing an element's membership of the subgroup, into a lemma-based step by step proof is implemented and described.

'The $F^{a,b,c}$ conjecture' was proposed by Campbell, Coxeter and Robertson in 1977 to classify the groups

$$F^{a,b,c} = \langle r, s | r^2, rs^a rs^b rs^c \rangle$$

by considering the homomorphic image $H^{a,b,c} = \langle r, s | r^2, rs^a rs^b rs^c, s^{2(a+b+c)} \rangle$. The lemma-based proof generating program is used as an aid in considering the groups $F^{a,b,c}$ and the corresponding conjecture. Lastly, a proof showing this conjecture to be true is provided.

Chapter 1

Introduction

1.1 Definitions and Elementary Theory

As this thesis concentrates largely on groups within the class having finite presentations, we begin by introducing necessary definitions and concepts for this area of group theory.

Definition 1.1 Let X be a set, and let A consist of the alphabet formed from the union of X and $X' = \{x^{-1} | x \in X\}$. A word w over A is said to be *reduced* if neither xx^{-1} nor $x^{-1}x$ appear as a subword of w for any $x \in X$.

To describe the concept of a group of reduced words, we need first to introduce an identity element. This will be the empty word, composed of no letters. It is obviously a reduced word itself, and we denote it by 1. For a word, $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$, where each $x_i \in X$ and $\epsilon_i \in \{-1, 1\}$ for $i \in \{1, 2, .., n\}$, the inverse w^{-1} is $x_n^{-\epsilon_n} \ldots x_2^{-\epsilon_2} x_1^{-\epsilon_1}$. This leaves only to describe the composition of two reduced words. The concatenation of two reduced words may not itself be reduced, but from it, we can produce a reduced word by continually cancelling each xx^{-1} or $x^{-1}x$ that appears until, for every $x \in X$, no such subwords occur.

Definition 1.2 Let X be a set. The *free group generated by* X, $\mathcal{F}(X)$, is the set of all reduced words over $X \cup \{x^{-1} | x \in X\}$ under the binary operation of concatenation with reduction.

Definition 1.3 Let G be a group and $H \leq G$ be a subgroup. For any $a \in G$, the *right coset* of H generated by a is the set $Ha = \{ha|h \in H\}$. Similarly, the *left coset* of H determined by a is the set $\{ah|h \in H\}$, which is denoted by aH.

Some elementary results follow from the concept of cosets.

Theorem 1.4 Let G be a group, and let $H \leq G$.

- For $a \in G$, where H is finite, $|Ha| = |aH| = |H|$. When H is infinite, all of Ha, aH and H have the same cardinality.
- $G = \bigcup_{a \in G} Ha = \bigcup_{a \in G} aH$.
- For $a, b \in G$, either $Ha = Hb$ or $Ha \cap Hb = \emptyset$. Similarly, either $aH = bH$ or $aH \cap bH = \emptyset$.
- For $a, b \in G$, then $Ha = Hb$ if and only if $ab^{-1} \in H$. For left cosets, $aH = bH$ if and only if $a^{-1}b \in H$.

Theorem 1.5 Let G be a group, and let $H \leq G$. If $R = \{Ha|a \in G\}$ and $L = \{aH|a \in G\}$, then $|R| = |L|$ where R or L is a finite set. Where either are infinite, R and L have the same cardinality.

Definition 1.6 Let G be a group and $H \leq G$ be a subgroup. The *index* of H in G, denoted $[G : H]$, is the number of right cosets, or equivalently, left cosets of H in G.

Definition 1.7 Let G be a group. For $h, g \in G$, the *conjugate* of h by g, written h^g, is the group element $g^{-1}hg$.

Definition 1.8 Let G be a group and $N \leq G$. N is said to be a *normal subgroup* of G, denoted $N \trianglelefteq G$, if, for every $g \in G$ and $h \in N$, the conjugate h^g lies in N. Equivalently, for some $h_1 \in N$, we have $h^g = h_1$.

Where $N \trianglelefteq G$, it also holds that $g^{-1}Ng = N$ for any $g \in G$, each right coset of N in G is also a left coset and $Na = aN$ for every $a \in G$. Given this, it follows that the set of cosets of N in G forms a group when $N \trianglelefteq G$.

Definition 1.9 Let G be a group and $N \trianglelefteq G$. The *factor, or quotient, group* of N in G, written G/N, is the group formed from all the left, or right, cosets of N in G with the binary operation

$$(aN)(bN) = (ab)N, \quad a, b \in G.$$

Definition 1.10 Let G be a group and $R \subseteq G$. The *normal closure* of R in G is the intersection of all normal subgroups containing R.

Where G is a group, the normal closure of a subset $R \subseteq G$ is generated by the set of conjugates, $\{g^{-1}hg | g \in G, h \in R\}$, and is the smallest normal subgroup containing R.

Definition 1.11 Let X be a set and $R \subseteq \mathcal{F}(X)$. If we consider the group $G = \mathcal{F}(X)/N$, where N is the normal closure of R in $\mathcal{F}(X)$, then $\langle X|R\rangle$ is said to be a *presentation* of G, and we write $G \cong \langle X|R\rangle$. The elements of X are referred to as *defining generators* and the elements of R as *defining relators.*

Oftentimes, if G has a group presentation, we will simply write $G = \langle X|R\rangle$ rather than $G \cong \langle X|R\rangle$. We may also refer to a relation $r = 1$ where we mean the relator $r \in R$, and G can be presented as $G = \langle X|\{r = 1|r \in R\}\rangle$.

Definition 1.12 G is said to be *finitely presented* if there exists a presentation, $G = \langle X|R\rangle$, such that both X and R are finite sets.

Where $G = \langle X|R\rangle$ is a finitely presented group with $X = \{x_1, \ldots, x_n\}$ and $R = \{r_1, \ldots, r_m\}$, then for simplicity, the presentation can be written as

$$G = \langle x_1, \ldots, x_n | r_1, \ldots, r_m\rangle$$

rather than $G = \langle \{x_1, \dots, x_n\} | \{r_1, \dots, r_m\} \rangle$.

1.2 Coset Enumeration

The main aim of group theory is to gather information on and make classifications of groups, most of whose size render hand calculations impractical. Computing the size and structure of large groups by listing each element is inefficient with regards to both time and memory and impossible for infinite groups. As such, designing algorithms to simplify these computations has become an important problem in computational group theory.

Given a group G and a subgroup $H \leq G$, the problem of determining the index of H in G is called coset enumeration and is one of the most important tools for investigating finitely presented groups. When H is trivial, coset enumeration determines the size of G, and where the size and structure of H are already known, it may reveal information on the same characteristics for the whole group, without considering all the elements.

Although it was probably first used by E. H. Moore [25] to find abstract definitions of groups, the method for the enumeration of cosets, given a finitely generated subgroup of finite index in a finitely presented group, was first described by J.A. Todd and H.S.M. Coxeter in 1936 [29]. Several modifications of this algorithm have also been outlined, which have the added benefit of constructing a presentation for the subgroup in terms of the subgroup generators as well as determining the index. As many of our results were obtained from programs based on this procedure, we will give an outline of both the Todd-Coxeter coset enumeration algorithm and the Modified Todd-Coxeter coset enumeration algorithm.

1.2.1 The Todd-Coxeter Coset Enumeration Algorithm

Let G be a finitely presented group such that

$$G \cong \langle X | R \rangle,$$

with $X = \{x_1, x_2, \dots, x_n\}$ and $R = \{r_1, r_2, \dots, r_m\}$, and let $H \leq G$ be a subgroup generated by a finite set of group elements, $\{h_1, h_2, \dots, h_l\}$. Provided $[G : H]$ is finite and the elements of both the relator set R and the generating set of H are written as products of the defining generators of G and their inverses, the Todd-Coxeter coset enumeration algorithm gives a method for computing the index of H in G.

The method refers to cosets as numbers, usually determined by the order in which they are introduced into the process. As H is itself a coset, it is indicated by the number 1 and at the start of the algorithm, is the only coset defined. Three types of tables, relator, subgroup generator and coset, are created in the first step, and coset enumeration proceeds by continually adding information to the tables until all the rows are complete, or closed, when the process terminates. The number of rows in the coset table, each representing a coset, is the index.

Let us consider a subgroup generator h_i of H. H is a subgroup, and so, for any $h \in H$, we must have $hh_i \in H$, thus $Hh_i = H$ or $1h_i = 1$. For each subgroup generator $h_i = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \dots x_{i_s}^{\epsilon_{i_s}}$ of H, where $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \dots, s\}$, the associated one-row table is:

	$x_{i_1}^{\epsilon_{i_1}}$	$x_{i_2}^{\epsilon_{i_2}}$	$\dots$	$x_{i_s}^{\epsilon_{i_s}}$	
1					1

.

The relator tables are formed based on the fact that, in the group G, each relator $r_j \in R$ is equivalent to the identity, and as such, given any coset a, we have $ar_j = a$. Thus, for each $r_j = x_{j_1}^{\epsilon_{j_1}} x_{j_2}^{\epsilon_{j_2}} \dots x_{j_t}^{\epsilon_{j_t}} \in R$, where $x_{j_k} \in X$ and $\epsilon_{j_k} \in \{-1, 1\}$ for $k \in \{1, 2, \dots, t\}$, we form the table:

	$x_{j_1}^{\epsilon_{j_1}}$	$x_{j_2}^{\epsilon_{j_2}}$	$\dots$	$x_{j_t}^{\epsilon_{j_t}}$	
1					1

The relationship holds for each coset, and so, unlike the one-row subgroup tables, for every new coset defined during the enumeration, an additional row, containing the new coset number in the first and last columns, is added to the relator tables.

Information regarding the relationships amongst cosets when acted upon by group generators is indicated in these two types of tables in the same way. If, in one row of the table corresponding to the word $w = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \ldots x_{i_s}^{\epsilon_{i_s}}$, where $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \ldots, s\}$, the j-th and $j+1$-th column entries are the cosets a and b, respectively, then we know $ax_{i_j}^{\epsilon_{i_j}} = b$ and $bx_{i_j}^{-\epsilon_{i_j}} = a$.

The coset table contains a column for each of the group generators $x \in X$ as well as its inverse and grows during the enumeration to contain a row for each coset. This table is used to store the relationships amongst cosets through the multiplication by a generator. If we have determined that $ax_k^{\epsilon_k} = b$, for cosets a and b and $\epsilon_k \in \{-1, 1\}$, then the entry in the column headed by $x_k^{\epsilon_k}$ and in the a-th row is b.

Information is added to the tables in any of three different ways: definitions, deductions or coincidences. A definition is the simplest form of new information and involves introducing a new coset into the process to fill an empty entry in a table. Definitions are immediately added to the coset table and used to help complete rows in the other tables. Numerous cosets may need to be defined before new information of another type is found.

When the last empty entry in a row in either a relation or a subgroup table is filled, we may obtain new information called a deduction. If the relationship $ax_r^{\epsilon_r} = b$ had been used to complete the row in the table:

$$\begin{array}{c|c|c} & x_r^{\epsilon_r} & x_s^{\epsilon_s} \\ \hline a & \underline{b} & \underline{c} \end{array}$$

then we obtain new information, $bx_s^{\epsilon_s} = c$, indicated by the underline. This deduction can then be added to the other tables, possibly resulting in further deductions.

A coincidence occurs when a deduction has been obtained, but the coset table already contains a different value for the corresponding entry. Here, two cosets, a and b, have been revealed to be the same, and b is removed from the tables by replacing every occurrence of b by a and by deleting the b-th rows from the coset and relator tables. Processing coincident cosets can result in the discovery of further deductions and coincidences.

The process is guaranteed to terminate in a finite number of steps if the index of the subgroup H in G is finite, although the time required and number of cosets defined can vary dramatically, even if G is trivial. Obviously, if the index of the subgroup is infinite, the ever-growing coset table can never be completed, and the process will continue forever. During coset enumeration, we cannot know whether the process will ever actually terminate. At any stage of a long enumeration, it may be that the number of cosets is, in fact, infinite or that the index is finite, but the process requires a very large, but finite, number of steps. Thus, coset enumeration provides us with information only when it terminates, and it cannot determine that the index of a particular group over one of its subgroups is infinite.

As process termination depends only on the index being finite, not on the order of the coset definition sequence, coset enumeration allows for a great variation of approaches. There have been numerous strategies, such as Felsch-type, Hasselgrove-Leech-Trotter-type (HLT-style) and Lookahead-type definition styles, suggested for the order in which cosets should be defined to minimise the required time and number of defined cosets during the process.

1.2.2 The Modified Todd-Coxeter Algorithm

The Modified Todd-Coxeter algorithm for coset enumeration proceeds in a fashion much the same as that of the original coset enumeration method, using a similar set up of relator, subgroup and coset tables. In this modification, however, we have an augmented coset table, and as well as keeping track of each coset, the process also involves choosing an element of each coset, known as its coset representative. The set of coset representatives is used to find a presentation for the subgroup H.

With the original Todd-Coxeter coset enumeration algorithm, a number indicated an entire coset, and in the initial step of the process, the number 1 was set to indicate the entire coset H. The table entries now, however, refer to the coset representative τ_a of a coset a, and in the augmented coset table, the coset representative of H is given to be the identity element and is indicated by 1.

Previously, both the first and last columns of a row in the relator and subgroup tables contained the coset number that the row represented. Because the numbers indicated entire cosets, this resulted from the fact that for any coset a, any relator r and any subgroup generator h, then $ar = a$ and $1h = 1$. Using the idea of coset representatives, the triviality of the relators allows us to write $\tau_a r = \tau_a$ for any relator r and any coset a with representative τ_a, and our new relator tables can be set up as before. We require some changes, however, with the formation of the subgroup tables. Here, 1 represents the identity rather than the entire subgroup H, and for any subgroup generator h, we no longer have $1h = 1$, but $1h = h1$. Thus, while the first column entry is 1, the last column now contains $h1$.

During this modified version, if we deduce that $\tau_a x_k^{\epsilon_k} \in b$ for cosets a and b, $x_k \in X$, $\epsilon_k \in \{-1, 1\}$ and τ_a and τ_b the coset representatives of a and b, respectively, it cannot be assumed that $\tau_a x_k^{\epsilon_k} = \tau_b$. Both $\tau_a x_k^{\epsilon_k} \in b$ and $\tau_b \in b$, and since $H\tau_b = b$, then $\tau_a x_k^{\epsilon_k} \in H\tau_b$. Thus, there must exist a subgroup element $h \in H$ such that $\tau_a x_k^{\epsilon_k} = h\tau_b$, and as the coset table deals in coset representatives rather than cosets, we need to find this element h in terms of the subgroup generators. In the τ_a-th row and in the column headed by $x_k^{\epsilon_k}$, the augmented table would contain the entry $h\tau_b$.

The idea of computing corrective subgroup elements to allow relationships amongst cosets to be expressed in terms of their coset representatives can be extended to products of group generators. Finding the subgroup element, using the concept of coset representatives, is a matter of successively replacing each coset representative-generator pair by its corresponding augmented coset table entry. If τ_a, τ_b and τ_c are the coset representatives of the cosets a, b and c, respectively, and $h_k, h_l \in H$ have been found such that $\tau_a x_i^{\epsilon_i} = h_k \tau_b$ and $\tau_b x_j^{\epsilon_j} = h_l \tau_c$, then both $ax_i^{\epsilon_i} = b$ and $bx_j^{\epsilon_j} = c$. Let us consider $\tau_a(x_i^{\epsilon_i} x_j^{\epsilon_j})$. Obviously, it lies within the coset c, but we want to find $h \in H$ so that

$\tau_a(x_i^{\epsilon_i} x_j^{\epsilon_j}) = h\tau_c$. Here,

$$\begin{aligned} h\tau_c &= \tau_a(x_i^{\epsilon_i} x_j^{\epsilon_j}) \\ &= \underline{\tau_a x_i^{\epsilon_i}} x_j^{\epsilon_j} \\ &= h_k \tau_b x_j^{\epsilon_j} \\ &= h_k \underline{\tau_b x_j^{\epsilon_j}} \\ &= h_k h_l \tau_c, \end{aligned}$$

and $h = h_k h_l$.

We do not need to worry about determining this subgroup element when making new definitions. If, during the process, we define $\tau_a x_k^{\epsilon_k} = \tau$ for some coset a with representative τ_a, $x_k \in X$ and $\epsilon_k \in \{-1, 1\}$, then where $b = a x_k^{\epsilon_k}$, we take the coset representative of b to be exactly the element τ. Thus, the corresponding coset table entry for $\tau_a x_k^{\epsilon_k}$ is simply τ.

The augmented coset table begins to contain these corrective subgroup elements after a deduction is made in a subgroup table. For each subgroup generator $h_i = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \dots x_{i_s}^{\epsilon_{i_s}} \in H$, with $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \dots, s\}$, we have $Hh_i = h_i H$ and $1h_i = h_i 1$. If the table for h_i closes giving a deduction implying $a x_{i_k}^{\epsilon_{i_k}} = b$ for cosets a and b, then

$$1 x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \dots x_{i_s}^{\epsilon_{i_s}} = h_i 1$$

and

$$1 x_{i_1}^{\epsilon_{i_1}} \dots x_{i_k}^{\epsilon_{i_k}} = h_i 1 x_{i_s}^{-\epsilon_{i_s}} \dots x_{i_{k+1}}^{-\epsilon_{i_{k+1}}},$$

with $1 x_{i_1}^{\epsilon_{i_1}} \dots x_{i_{k-1}}^{\epsilon_{i_{k-1}}} \in a$ and $1 x_{i_s}^{-\epsilon_{i_s}} \dots x_{i_{k+1}}^{-\epsilon_{i_{k+1}}} \in b$. Since the subgroup table is closed, there must be an entry in the augmented coset table corresponding to each entry in the row, excepting that of the deduction. From these, we can form the words w_1 and w_2 so that

$$1 x_{i_1}^{\epsilon_{i_1}} \dots x_{i_{k-1}}^{\epsilon_{i_{k-1}}} = w_1 \tau_a \quad \text{and} \quad 1 x_{i_s}^{-\epsilon_{i_s}} \dots x_{i_{k+1}}^{-\epsilon_{i_{k+1}}} = w_2 \tau_b.$$

Both w_1 and w_2 are products of subgroup generators, and we have

$$\begin{aligned} 1x_{i_1}^{\epsilon_{i_1}}x_{i_2}^{\epsilon_{i_2}}\dots x_{i_s}^{\epsilon_{i_s}} &= h_i 1 \\ 1x_{i_1}^{\epsilon_{i_1}}\dots x_{i_k}^{\epsilon_{i_k}} &= h_i 1 x_{i_s}^{-\epsilon_{i_s}}\dots x_{i_{k+1}}^{-\epsilon_{i_{k+1}}} \\ w_1\tau_a x_{i_k}^{\epsilon_{i_k}} &= h_i w_2 \tau_b. \end{aligned}$$

Hence, our augmented coset table entry for $\tau_a x_{i_k}^{\epsilon_{i_k}}$ is

$$w_1^{-1}h_i w_2\tau_b.$$

As any relator $r_j = x_{j_1}^{\epsilon_{j_1}}x_{j_2}^{\epsilon_{j_2}}\dots x_{j_t}^{\epsilon_{j_t}}$, with $x_{j_k}\in X$ and $\epsilon_{j_k}\in\{-1,1\}$ for $k\in\{1,2,\dots,t\}$, is trivial, then given any coset a with representative τ_a, we have $ar_j = a$ and $\tau_a r_j = \tau_a$. If the deduction implying $ax_{j_k}^{\epsilon_{j_k}} = b$ occurs from the completion of the τ_c-th row of the relator table, where all a, b and c are cosets with representatives τ_a, τ_b and τ_c, then

$$\tau_c x_{j_1}^{\epsilon_{j_1}}x_{j_2}^{\epsilon_{j_2}}\dots x_{j_t}^{\epsilon_{j_t}} = \tau_c$$

and

$$\tau_c x_{j_1}^{\epsilon_{j_1}}x_{j_2}^{\epsilon_{j_2}}\dots x_{j_k}^{\epsilon_{j_k}} = \tau_c x_{j_t}^{-\epsilon_{j_t}}\dots x_{j_{k+1}}^{-\epsilon_{j_{k+1}}}.$$

Using the augmented coset table, we can then find the two words, w_1 and w_2, over the subgroup generators so that

$$\tau_c x_{j_1}^{\epsilon_{j_1}}\dots x_{j_{k-1}}^{\epsilon_{j_{k-1}}} = w_1\tau_a \quad \text{and} \quad \tau_c x_{j_t}^{-\epsilon_{j_t}}\dots x_{j_{k+1}}^{-\epsilon_{j_{k+1}}} = w_2\tau_b.$$

Thus,

$$w_1\tau_a x_{j_k}^{\epsilon_{j_k}} = w_2\tau_b,$$

and the augmented coset table entry for $\tau_a x_{j_k}^{\epsilon_{j_k}}$ is

$$w_1^{-1}w_2\tau_b.$$

Coincidences may also occur in this modified version of the Todd-Coxeter algorithm. When two cosets, a and b, are found to be the same, however, we cannot remove τ_b, the representative of b, from the tables in the same fashion as the original method, by merely replacing each occurrence with τ_a, the representative of a. While a and b are identical, it is not necessarily the case that the representatives were chosen to be the same coset element and so, they cannot be used interchangably. If a and b are found to be coincident from a deduction implying $cx_k^{\epsilon_k} = a$, where $cx_k^{\epsilon_k} = b$ had previously been determined, then we must have words w_1 and w_2, both products of subgroup generators, such that

$$\tau_c x_k^{\epsilon_k} = w_1\tau_a \quad \text{and} \quad \tau_c x_k^{\epsilon_k} = w_2\tau_b.$$

Thus, $w_1\tau_a = w_2\tau_b$, and we can remove τ_b from the tables by replacing each occurrence of τ_b with $w_2^{-1}w_1\tau_a$.

Once all the tables have closed, then the index has been determined and the set of coset representatives, along with the augmented coset table, can be used to find a presentation for the subgroup. One of the benefits of using the modified Todd-Coxeter algorithm is that the resulting presentation for the subgroup is given in terms of the original subgroup generators, rather than a new generating set as is seen in other methods, such as the Reidemeister-Schreier method.

For any trivial word $w = x_{j_1}^{\epsilon_{j_1}} x_{j_2}^{\epsilon_{j_2}} \dots x_{j_t}^{\epsilon_{j_t}} = 1$, with $x_{j_k} \in X$ and $\epsilon_{j_k} \in \{-1, 1\}$ for $k \in \{1, 2, \dots, t\}$, then it must be the case that $w\tau_a = \tau_a w = \tau_a$ for any coset a with representative τ_a. Applying our augmented coset table, we obtain:

$$\begin{aligned}
\tau_a &= \tau_a w \\
&= \tau_a x_{j_1}^{\epsilon_{j_1}} x_{j_2}^{\epsilon_{j_2}} \dots x_{j_t}^{\epsilon_{j_t}} \\
&= w_1\tau_b x_{j_2}^{\epsilon_{j_2}} \dots x_{j_t}^{\epsilon_{j_t}} \\
&= \dots \\
&= w_1 w_2 \dots w_s \tau_a,
\end{aligned}$$

where the table contains $\tau_a x_{j_1}^{\epsilon_{j_1}} = w_1\tau_b$, $\tau_b x_{j_2}^{\epsilon_{j_2}} = w_2\tau_c$ and so on. Thus, $w = w_1 w_2 \dots . w_s = 1$. As, for $i \in \{1, 2, \dots, s\}$, each w_i is obtained from the augmented coset table, it must be a product of the subgroup generators $\{h_1, \ldots, h_l\}$, so $w = 1$ has been rewritten in terms of these generators. Any relator of the group G is also a relator of the subgroup H, and from our augmented coset table, can be rewritten for the subgroup presentation. The method employs this rewriting step when a deduction is found in a relator table, and therefore, new information for the subgroup presentation is found only in lines of relator tables where a deduction has not occurred.

The method also used the step $1h_i = h_i 1$ where deductions were found in the subgroup table for $h_i \in \{h_1, \ldots, h_l\}$. After the tables have been completed, in any subgroup table where a deduction did not occur, we obtain new information. Using our rewriting process, where $h_i = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \ldots x_{i_s}^{\epsilon_{i_s}} \in H$, with $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \ldots, s\}$, then we can find a word w over the subgroup generators so that

$$1h_i = 1x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \ldots x_{i_s}^{\epsilon_{i_s}} = w1.$$

Thus, $h_i 1 = w1$, and we have a new relator $w^{-1}h_i$, a product of subgroup generators, for our presentation.

Where G is a group with finite presentation $\langle X | R \rangle$, $|X| = n$ and $|R| = m$, it has been shown [26] that a presentation for a subgroup $H = \langle h_1, \ldots, h_l \rangle$ of G with finite index $[G : H] = a$, where the cosets are numbered contiguously, can be given as

$$\begin{aligned} \langle h_1, \ldots, h_l \quad | \quad & 1h_i = h_i 1 \text{ for } i \in \{1, 2, \ldots, l\}, \\ & jrj^{-1} = 1 \text{ for } j \in \{1, 2, \ldots, a\} \text{ and } r \in R \rangle. \end{aligned}$$

Thus, using the augmented coset table and the rows of the relator and subgroup tables without deductions, we are able to determine all the relators necessary to form the presentation of our subgroup H.

1.3 Coset Enumeration, Strategies and Computer Implementation

Both forms of the Todd-Coxeter coset enumeration method allow for computer implementation, and it is thought that the first such occurrence was a partial implementation of the original Todd-Coxeter method by Haselgrove in 1953 on the EDSAC I at Cambridge, described by Leech [24]. Even in the modern group theory programming language and computer system, GAP [16], most methods for finitely presented groups rely on coset enumeration.

The main issue in the implementation of coset enumeration is determining the best rule for introducing new cosets. When the index of the subgroup in the group is finite, the algorithm is guaranteed to terminate. The tables will eventually close for any sequence of coset definitions, as long as for each defined coset a that does not become coincident, then each of the cosets $ax_i^{\epsilon_i}$ for $x_i \in X$ and $\epsilon_i \in \{-1, 1\}$ will be introduced in a finite number of steps. This simple condition is known as Mendelsohn's condition, and a theorem proving this is given by Neubüser in [26]. The length of sequences with this property, however, can vary dramatically as a result of the definition strategy.

As computer programs are judged according to their time and space efficiency, and the total number of defined cosets determines the memory required as well as greatly influences the running time, an implementation that defines the fewer number of redundant cosets is generally regarded as the better one. Even the strategies in the earliest coset enumeration implementations by Felsch [12], Leech [24], Haselgrove and Trotter [30] were proposed to reduce total cosets, and since then, extensive experimental studies on various strategies have been performed, such as in [8] and [18].

In the Todd-Coxeter algorithm for coset enumeration, there are three types of tables, and relator and subgroup tables are used to determine deductions once a row is completed. This is equivalent, however, to performing scans of the relators and subgroup generators both from the left and right using the coset table and so, the storage of relator and subgroup tables is very inefficient with regard to space. Rarely do implementations include tables other than the coset table.

There are two classical strategies of coset enumeration. The first, known as the Felsch-method after the first description of a program using this method was given by Felsch in 1961 [12], concentrates primarily on the coset table, making definitions so that table entries are filled line by line. After each definition $ax = b$ for cosets a and b, scans are made from coset a of all cyclic permutations of the relators beginning with x and then, from coset b, ones beginning with x^{-1}, so that resultant deductions and coincidences can be found and processed. This Felsch-type definition strategy tends to find fewer redundant cosets as deductions and coincidences are found and handled before any new definitions are made. The scans required after each definition, however, can lead to longer running times.

The Haselgrove-Leech-Trotter (HLT) method, the other of the earliest described strategies and the basis of the implementation by Haselgrove, makes definitions in an attempt to close a line in one of the relator or subgroup tables. The method proceeds by completing a scan from every coset for each relator, at each stage making definitions enough to fill the row in the corresponding table. Additionally, for the subgroup, scans are made of the subgroup generators as well. Only after the scan of a row is complete and this new deduction formed are the new definitions processed to find the resulting deductions and coincidences. The many scans involved in the Felsch method are avoided using the HLT method, although leaving all deductions and coincidences until a row has been filled tends to cause more redundant cosets to be introduced.

It can be a faster method, but the HLT style does not attempt to make use of any new information resulting from definitions made while tracing relators until much later. In a strategy based mostly on the HLT method, described in [8] and called the Lookahead method, enumeration alternates between two phases. In the first, definitions are made in the HLT style, considering rows in relator and subgroup tables without processing definitions to find deductions and coincidences until a certain number of cosets have been defined in the phase. The process then switches from this defining phase to the lookahead phase, using the definitions to find impending deductions and coincidences to add to the tables. According to their comparisons with the Felsch method, and the pure HLT method, Cannon, Dimino, et al. [8], formed the conclusion that the Lookahead method was, in general, better than the other two.

1.3.1 GAP: Groups, Algorithms, Programming

The GAP computational discrete algebra system [16] provides a programming language as well as libraries of algorithms and algebraic objects. Although many of the functions in GAP are implemented in the GAP programming language itself, the kernel of GAP is written in the C programming language. GAP was developed mainly to facilitate computational research in group theory, although it includes many packages providing links to other systems and is used in research and teaching of various areas of algebra.

As the GAP system and programming language provide an extensive set of functions for finitely presented groups, most of which employ some form of the coset enumeration method in their implementation, GAP is used as a tool in much of this thesis. Both the Todd-Coxeter coset enumeration algorithm and its modified version are included in the GAP functions for finitely presented groups, so we shall briefly describe their implementations.

Coset enumeration is performed in GAP using the Felsch-type definition strategy and thus, the rule for determining the next definition is to search the table, row by row, for the next empty entry. After making a definition to fill this entry and expanding the table if necessary, scans of all applicable subgroup generators and cyclic permutations of the relators are made. Here, storage is needed for the coset table, the subgroup generators and all cyclic permutations of the relators. Any GAP function requiring coset enumeration uses the function *CosetTableFromGensAndRels*, which requires three lists, the group generators, the group relators and the subgroup generators, as input. The user is also able to set a maximum value for the number of cosets defined in the process. As long as the number of live cosets at any point does not exceed the maximum or the available memory, this function, written in the GAP language, outputs a data structure representing the coset table, whose length is the index.

In the GAP system, the faster language, C, is used to implement time critical operations, and as the time necessary to perform the numerous relator and subgroup generator scans is one of the disadvantages of using the Felsch strategy, *CosetTableFromGensAndRels* does not perform these required scans itself. To reduce the running time, this GAP function passes the scanning task to a C function, *FuncMakeConsequences*, which also determines and processes any deductions and passes control, in turn, to the C function *HandleCoinc* when a coincidence occurs.

GAP also has the capability of finding subgroup presentations of finitely presented groups and contains functions implementing the Modified Todd-Coxeter algorithm as well as those using a modification of the Reidemeister-Schreier method. The Reidemeister-Schreier method builds a subgroup presentation using Tietze tranformations and a completed coset table, although it does not necessarily produce a presentation in the original subgroup generators. Recall that the Modified Todd-Coxeter method of coset enumeration has the advantage of producing a presentation in the original subgroup generators, but the entries in the augmented coset table can become very large and the method can produce quite lengthy relators.

The subgroup elements of the augmented coset table can be expressed as words in the given generators of H, but in general, these words tend to become unmanageable because of their enormous lengths. The GAP implementation of the Modified Todd-Coxeter methods is based on an algorithm outlined by Arrell and Robertson [2] using a tree structure and Tietze transformations to cut down the length of the presentation and reduce the size requirements of the augmented coset table.

In Arrell and Robertson's algorithm, products in the augmented coset table of length greater than one are not allowed to be carried through the enumeration. A highly redundant list of subgroup generators is built up starting from the original generators of H and adding additional generators, which are defined as abbreviations of products of length two in the preceding generators. Thus, each of the subgroup elements in the augmented coset table can be expressed as a word of length at most one in the resulting subgroup generators.

If $H = \langle X_H | R_H \rangle$ and the product $h_i^{\epsilon_1} h_j^{\epsilon_2}$ is encountered, where $h_i, h_j \in$

X_H and $\epsilon_1, \epsilon_2 \in \{-1, 1\}$, then a new subgroup generator $h = h_i^{\epsilon_1} h_j^{\epsilon_2}$ is introduced. Adding h to the set of subgroup generators and $h = h_i^{\epsilon_1} h_j^{\epsilon_2}$ to the set of relators of H produces

$$\langle X_H \cup \{h\} | R_H \cup \{h^{-1} h_i^{\epsilon_1} h_j^{\epsilon_2}\} \rangle,$$

an equivalent presentation to that of $H = \langle X_H | R_H \rangle$, as it has merely undergone a Tietze transformation.

The additional products in the coset table will now only be in the form of single subgroup generators, or their inverses. Thus, only the index of the element in the set of generators, with a negative sign to indicate an inverse, needs to be stored in the augmented coset table. Although a tree structure is required to keep track of the definitions of new subgroup generators, this is still better space-wise than forming an augmented coset table in the usual way.

Similarly to the original Todd-Coxeter method functions in GAP, the modified version, *AugmentedCosetTableMtc*, also uses the Felsch definition strategy, passing control to the C functions, *FuncMakeConsequences2* and *HandleCoinc2*, to perform necessary scans and to find and handle deductions and coincidences. *AugmentedCosetTableMtc* returns a data structure representing the augmented coset table as well as the tree to decode the secondary generators. This function is usually called from within another GAP function, and the returned augmented table can be used to form the subgroup relators in the new subgroup generator set. The decoding tree is then used to convert the resultant presentation to one over the original subgroup generator set, and rather than simply performing back substitution, attempts are made to reduce the number and length of relators and eliminate generators by performing Tietze transformations.

1.3.2 ACE: Advanced Coset Enumerator

The Advanced Coset Enumerator (ACE) exists both as a stand-alone program written in C [17] as well as a package for the GAP system [15] and provides a very powerful tool for research with finitely presented groups.

ACE allows for experimentation in coset definition strategy and enumeration style through user controlled options, and the biggest advantage of the ACE coset enumerator is the huge number of options available with regard to strategy, style, and manipulation of the presentation. There also exist options allowing the user to interact with ACE during an enumeration as well as those for running an enumeration on equivalent presentations of the group, using different combinations of relator orderings, permutations and inversions.

While the built-in GAP coset enumerator allows only for the use of the Felsch coset definition strategy, in ACE, one can choose from various predefined strategies or can tailor strategies using a combination of styles. Here, when a new coset number has to be defined, there are basically three possible types. A definition using the Felsch strategy, scanning the coset table and filling the first empty entry, is known as a C-style definition, and based on the HLT strategy, an R-style definition refers to one in which a coset is defined to fill the first empty entry during a relator scan. ACE also creates a stack of coset definition possibilities that will complete the scan of a relator from a coset, and one may choose to make definitions from this Preferred Definition Stack. Using preferred definitions follows a strategy known as the minimal gaps strategy, where the idea is that by closing a row in a relator table, a deduction is immediately obtained.

The enumeration styles are mainly determined by different combinations of the C style and R style definitions, which are controlled through alterations of the values of the *ct factor* and *rt factor* options. There are eight styles: C style, Cr style, CR style, R style, R* style, Rc style, R/C style and defaulted R/C style, and by assigning values to *ct factor* and *rt factor*, one of the styles can be selected. Other options influencing the enumeration strategy are *asis, fill factor, lookahead, mendolsohn, no relators in subgroup, pd mode, pd size* and *row filling*. Thus, the user can control the enumeration by choosing an appropriate set of options for a specific presentation, which is beneficial for experimentation with enumeration strategies to find the best definition style, producing the fewest redundant cosets.

Alternatively, ACE contains various commands for predefined enumeration strategies formed from the eight styles and other options. If no strategy option is passed to ACE, *default* is used, which presumes that the enumeration will be easy, although switches to a strategy designed for more difficult enumerations if this is found to be untrue. Two other straightforward options are *easy* and *hard*. *Easy* will quickly succeed or fail, *default* may succeed quickly or will try the *hard* strategy, and *hard* will run more slowly, from the beginning.

The remaining predefined strategies are *felsch, hlt, pure ct, pure rt* and *sims*, where *felsch* can have either of the values 0 or 1 and *sims* can be assigned any of the values 1, 3, 5, 7 or 9. The ACE definition styles and strategies are outlined in detail in the manuals of both the ACE GAP package and the ACE stand-alone.

The coset enumeration is invoked by either of the commands, *begin* or *start*, and ACE will return the index if there is sufficient memory for the maximum number of defined cosets in the table at every point in the process. If an enumeration is attempted and insufficient memory is available for this maximum number of cosets required to find the index, one can make changes in style, strategy or in the group presentation and subgroup generator list themselves and start a new enumeration.

However, ACE also allows the user to change some parameters and continue with the enumeration, retaining any information in the coset table and building upon it. There are two modes in which this can be done. The mode with command *continue* resumes the subgroup generator and relator scans from where the enumeration left off, while the *redo* or *check* mode keeps all the current table information but begins scanning from coset 1 again. If the enumeration stopped during the relator scans for coset number α and if the changes to the enumeration would invalidate the current coset table, such as if the *add relators* or *add generators* commands had been used to add elements to the set of group relators or subgroup generators, then it is not guaranteed that the scans of the relators and generators for the cosets with numbers less than α would still be completely determined by the table. Thus, only the ACE mode *redo*, rather than *continue*, can be used to resume an enumeration in this case.

As the purpose of ACE is to find the index of a finitely presented group over a finitely generated subgroup, where, in many cases, an extremely large number of cosets are required, space saving is critical, and once a coincidence has been determined, there is no longer any need to keep a record of the inactive coset. Thus, ACE provides two commands which control the recovery of memory allocated to redundant cosets from the coset table, leaving a compacted table where all active cosets are numbered contiguously. The *compaction* option defines the percentage of rows of the table that must be redundant before ACE will automatically begin to reallocate table rows during an enumeration. The *recover* command allows the user to explicitly invoke a table compaction.

The ACE commands, *aep* and *rep*, allow the user to run the enumeration for different combinations of relator orderings, rotations and inversions. The *aep* option, for all equivalent presentations, takes in an integer value from 1 to 7, which, written in binary, represents the active flags for the three types of relator manipulations. An enumeration is then performed for each combination of the orderings, rotations, and inversions that are active according to this set of flags. The option *rep* stands for random equivalent presentations and takes in two integer arguments, where the first is the same flag representing integer as that of *aep* and the second is the number of presentations to be generated and tested.

The ACE package provides both an interactive and non-interactive GAP interface with the Todd-Coxeter coset enumeration functions of the ACE stand-alone C program. Using input and output streams, the ACE package controls the commands written to these streams according to the GAP function call and translates the C program output read from these streams into appropriate GAP output. The user may still control enumeration style and definition strategy in this interface as the package allows options to either be specified during a function call or pushed onto a stack before the function is invoked.

As well as functions for each of the facilities available in the ACE stand-alone, the GAP interface also provides the function *ACECosetTableFromGensAndRels*, accepting the same inputs as the built-in GAP enumerator

CosetTableFromGensAndRels, but using the ACE enumerator to find the coset table. As such, one can employ the powerful ACE enumerator with any of the ACE options and strategies to generate different coset tables in GAP than would be produced by the built-in function.

Many of the GAP functions for finitely presented groups require coset enumeration, and although *CosetTableFromGensAndRels* is the main driver in GAP for coset enumeration, it is regarded as an internal function, often being called from within another function for groups of this type. GAP allows, however, for the usual coset enumerator to be supplanted by the ACE coset enumerator so that the function, *ACECosetTableFromGensAndRels*, becomes the main driver and ACE is used for coset enumeration. This is easily obtained by assigning

$$TCENUM := ACETCENUM;$$

so that a call to *CosetTableFromGensAndRels*, either directly by the user or indirectly from within a function, actually calls the ACE equivalent. When coset enumeration is called internally, any options passed to the calling function are in turn passed to *ACECosetTableFromGensAndRels* and so, the strategies and style options of ACE can still be employed. The GAP enumerator can be reset to the original GAP coset enumerator by the command

$$TCENUM := GAPTCENUM;$$

With this, using the ACE package in GAP can be very helpful in experimentation and programming with finitely presented groups, as it allows the user access to the various GAP functions for groups of this type as well as provides the user with the ability to control the enumeration, normally unavailable in GAP.

Although many strategies and style options are available for coset enumeration, ACE does not contain functionality for the Modified Todd-Coxeter version or any other method of finding presentations for subgroups. As the main driver for the GAP functions using the Modified Todd-Coxeter algorithm is *CosetTableFromGensAndRelsMtc* rather than *CosetTableFromGensAndRels* and only the latter is reassigned by the command

$$TCENUM := ACETCENUM;,$$

replacing the default GAP enumerator with that of ACE does not influence the Modified Todd-Coxeter functions within GAP.

Considering methods for generating presentations for subgroups of finitely presented groups and attempting to find 'better' such presentations is where our research began. Although ACE allows one to experiment with coset enumeration, no such tool existed for the Modified Todd-Coxeter method of generating subgroup presentations. The C program, Proof Extraction After Coset Enumeration (PEACE), uses an ACE-based enumerator, and our work of modifying this program for the Modified Todd-Coxeter algorithm and developing a GAP package is covered in the next chapter.

Chapter 2

PEACE: Proof Extraction after Coset Enumeration

2.1 Introduction

Once coset enumeration has been employed to find the index of a finitely presented group G over a finitely generated subgroup $H \leq G$ and a complete coset table has been formed, one can use this to prove that a group element $h \in G$ is also a member of the subgroup. If

$$G \cong \langle X | R \rangle$$

with $X = \{x_1, x_2, \ldots, x_n\}$ and $R = \{r_1, r_2, \ldots, r_m\}$, then expressing h in terms of the group generators and their inverses, we can write

$$h = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \ldots x_{i_s}^{\epsilon_{i_s}},$$

where $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \ldots, s\}$. As the index $[G : H]$ has been found and the coset table is closed, we are able to then determine the set of cosets $\{1, \alpha_1, \alpha_2, \ldots, \alpha_s\}$ such that

$$\begin{aligned}\alpha_1 &= 1x_{i_1}^{\epsilon_{i_1}}, \\ \alpha_2 &= \alpha_1 x_{i_2}^{\epsilon_{i_2}}, \\ &\ldots \\ \alpha_s &= \alpha_{s-1} x_{i_s}^{\epsilon_{i_s}}.\end{aligned}$$

Thus, $1h = 1x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \ldots x_{i_s}^{\epsilon_{i_s}} = \alpha_s$. As H is a subgroup and the coset table does not contain any redundant cosets, then h is actually a subgroup element only if $\alpha_s = 1$. Otherwise, $h \notin H$ where $\alpha_s \neq 1$.

The ability to show the membership of a group element in the subgroup relies on the validity of the coset table, and for a specific enumeration performed using the Todd-Coxeter algorithm, this cannot be easily checked. Thus, although proofs have been given for the correctness of enumerations using some coset definition strategies, we would require such a proof for the strategy of our specific enumeration before we could assume the coset table is valid. However, using the definition sequence of a completed enumeration, the C program, Proof Extraction After Coset Enumeration (PEACE) [19], written by George Havas and Colin Ramsay, allows one to extract an easily verified proof of the subgroup membership for a group element.

In its output, PEACE produces a string expressing a reduced group element $h \in G$ as a product of subgroup generators and, possibly conjugated, group relators. As it freely reduces to the original word and, when the relators are removed, reduces to a product of subgroup generators, it is easily shown that this proof word represents h in both its original form as well as written as a product of the subgroup generators. Thus, it forms a proof that $h \in H$, and the proof word as well as the presentation of G, the generators of H and the original group element h make up the proof certificate.

Example 2.1 As an example of a PEACE proof word and certificate, consider the presentation for A_5,

$$A_5 \cong \langle a, b | a^2, b^3, (ab)^5 \rangle,$$

with the subgroup generated by $\{a^b, b^a\}$ and isomorphic to A_4. For the group element $w = a^{-1}b^4ab^3$, PEACE produces the proof word

$$[Aba][Aba][Aba][Aba](bbb),$$

where A represents the inverse of the generator a, square brackets enclose subgroup generators and round brackets, group relators. Removing the brackets, it is easily seen that the proof word reduces to Ab^4ab^3, which is exactly the original word w, and as the relator (b^3) is trivial, then

$$\begin{aligned} w &= Ab^4ab^3 \\ &= [Aba][Aba][Aba][Aba](bbb) \\ &= [Aba][Aba][Aba][Aba] \\ &= (b^a)^4. \end{aligned}$$

We have thus obtained a proof of $w \in \langle a^b, b^a \rangle$. This simple example can also be easily shown by hand since $(b^3) = 1$ and $a^{-1}b^4ab^3 = a^{-1}ba = b^a \in \langle a^b, b^a \rangle$.

As already indicated, the main inputs of PEACE include the group presentation, the subgroup generators and the group element whose membership in the subgroup is to be proved. PEACE allows for presentations with a generating set of size of up to 26, and each generator must be input as a lower case letter. PEACE then refers to the inverse of a generator as its corresponding upper case letter, and the inverse of the generator x can be input as either $x-1$ or X. In this chapter, we will keep to our notation of referring to the generator inverse as x^{-1}. To input the group G and subgroup $H \leq G$ defined by

$$G \cong \langle x_1, x_2, \ldots, x_n | r_1, r_2, \ldots, r_m \rangle \text{ and } H = \langle h_1, h_2, \ldots, h_l \rangle,$$

where $m, n \in \mathbb{Z}^+$, $l \in \mathbb{Z}^*$, $n \leq 26$, the group generators are all lower case letters and elements of the set of relators as well as those of the set of subgroup generators are words over the defining generators and generator inverses, we require the initial PEACE commands:

group generators: $x_1, x_2, \ldots, x_n$;
group relators: $r_1, r_2, \ldots, r_m$;
subgroup generators: $h_1, h_2, \ldots, h_l$;

Typically, a PEACE run involves 3 steps:

1. generation of a definition sequence by coset enumeration,
2. manipulation of the definition sequence,
3. production of a proof table and resulting proof words.

The outputs of PEACE are whether or not the group element, which is input after the proof table has been generated, is also a subgroup element, and if it is found to be so, the associated proof certificate.

We will complete our introduction of PEACE by describing the three steps of a run for the original C program. The rest of this chapter will be devoted to outlining our modifications of PEACE to perform the Modified Todd-Coxeter algorithm for coset enumeration as well as our development of a PEACE package for GAP. We designed such tools with the aim of using them to experiment with forming subgroup presentations, to try and find 'better' such presentations than formulated by the built-in GAP functions.

2.1.1 Coset Enumeration and Definition Sequences

The objective of a PEACE run is to find a proof showing the presence of a group element in the subgroup, and as the produced proofs vary with different definition sequences, an ACE-based enumerator is used, allowing for experimentation to obtain different sequences and thus, different proofs.

Similarly to ACE, all of the predefined strategy commands, *default, easy, felsch, hard, hlt, pure c, pure r* and *sims*, are included in the PEACE enumerator. PEACE also allows the strategy to be defined by the user with the options, *asis, ct factor, fill factor, lookahead, mendolsohn, no relators in subgroup, pd mode, pd size, rt factor* and *row filling*. An additional option, *col* *ordering*, controls the order in which the group generators and their inverses are laid out in columns of the coset table. This option can be useful for strategies such as *felsch*, where definitions are made according to the coset table, filling the left most empty column entry in the first incomplete row.

The enumeration is queued using the *begin* or *start* commands, and if the enumeration is able to complete, the resultant table can be printed with the *print table* input. An incomplete enumeration may be resumed in PEACE with different parameters using the *continue* command, and similarly to ACE, this mode retains all the information of the coset table and the relator and subgroup generator scans are resumed from where they left off before the enumeration halted. However, as no options exist that modify the presentation and would require the command *redo* rather than *continue* in ACE, there is no PEACE command equivalent to *redo*, which began the scanning of all relators and subgroup generators again from coset 1. Each of the other two steps of a PEACE run are invoked only by user commands, and thus, the enumeration step can be performed multiple times with different combinations of options and styles to produce a definition sequence of a desired type before the proof table is formulated.

In addition to a column for each generator and generator inverse, the PEACE coset table also contains four auxiliary columns. Unlike ACE, where redundant cosets have no further use and the coset table can be compacted to remove these redundant cosets, in PEACE, the entire definition sequence must be retained as it is necessary to build the proof table. Thus, for each row, the entries in the first two auxiliary columns contain information on whether the coset is redundant and with which other coset it is coincident as well as linking to the next pending coincidences in the queue. The last two auxiliary columns contain the coset α and the generator or generator inverse a defining the coset β represented by the row of the table, such that $\alpha a = \beta$.

Although the second step of a PEACE run is not actually required once a complete definition sequence has been produced, there are some options, such as *ds op, enumds* and *prune*, which allow for the output or manipulation of the sequence. The *ds op* command prompts PEACE to output the definition sequence of the last enumeration, either to a file or to the standard output stream.

The *enumds* command takes in an integer argument specifying the number of definitions to be tried, which must be smaller than the current definition sequence legnth, and PEACE attempts enumerations with all definition sequences of this specified length.

The option, *prune*, based on the short-cut method of the Interactive Todd-Coxeter (ITC) GAP package [13], tries to reduce the length of a complete definition sequence. If this length is l, then tracing backward from the last processed coset number α_l, the coset numbers $\{\alpha_{l_k}, \ldots, \alpha_{l_2}, \alpha_{l_1}\}$ can be found such that the definition sequence contains

$$\alpha_{l_1} = 1x_{l_1}^{\epsilon_{l_1}} \quad \text{and} \quad \alpha_{l_i} = \alpha_{l_{i-1}} x_{l_i}^{\epsilon_{l_i}},$$

where $x_{l_i}^{\epsilon_{l_i}}$ is a generator or generator inverse for each $i \in \{2, 3, \ldots, k\}$ and $\alpha_l = \alpha_{l_k}$. Thus, they are the cosets involved in the definitions that were actually used to reach coset number α_l. These coset numbers are marked as 'indispensable', and the definition of each coset in this set is moved to the beginning of the definition sequence. The definitions of the remaining cosets in the original sequence are placed at the end, and the enumeration is then begun again using this re-arranged sequence. Although it must complete the enumeration, as the original definition sequence was enough to lead to a full table closure, the enumeration may finish before all of the definitions have been processed. The subset of definitions of the re-arranged sequence closing the tables then becomes the new definition sequence, and this procedure is repeated, creating shorter definition sequences, until all cosets are marked 'indispensable' and the final, pruned definition sequence has been produced.

2.1.2 The Proof Table

Setting up the Table

Given that a complete definition sequence has been formulated, the final step of a PEACE run is to build a table from which a proof word can be produced. The proof table is set up similarly to that of the coset table in an enumeration and, in a sense, an entry retains the reason or the event in the enumeration resulting in this entry. As we will be referring to two different tables, let us adopt the notation $CT(row, col)$ to mean the entry in the coset table for the coset number row and generator or generator inverse col. We will use $PT(row, col)$ for the corresponding entry in the proof table.

Once PEACE has a completed coset table, the generation of the proof table is performed on the PEACE command *pt*. The command loop parses this command and calls the function *puce_pt()*, which clears the coset table by setting each entry to 0, excepting the last two auxiliary columns containing the definition sequence. These definitions were enough to close the tables, so the current coset table size is sufficient and the proof table is allocated memory enough for the same number of rows and columns. Unlike the coset table, however, each entry consists of a pointer accessing a linked-list detailing the history of all the events that obtained new information for this entry. Initially, the state of each of these proof table entries is NULL and modified to be that of a list once the entry is filled or altered by a definition, deduction or coincidence. The proof table also contains one auxiliary column, which, similarly to the first auxiliary column of the coset table, records the coincidences as well as their proof words.

Each element of the linked list is a structure with three main attributes in addition to the *next* pointer for the proceeding element in the list. The attributes are *seq*, the number indicating where in the sequence of events this new information was determined, *result*, the resulting coset for the coset-generator pair corresponding to the proof table entry containing the linked list, and *data*, a pointer to the data or the determined proof word for this deduction or coincidence. Thus, where α is a coset number and $x_i^{\epsilon_i}$ is either a group generator or its inverse, the entry $PT(\alpha, x_i^{\epsilon_i})$ is a list, not only indicating the coset numbers β_j such that we have found $\alpha x_i^{\epsilon_i} = \beta_j$ by definition or deduction, but also the proof word showing the deductions and coincidences involved in determining each of these relationships. Each entry in the auxiliary column of the proof table is a single element of this structure type, containing the proof word formed from the relator or subgroup generator scan resulting in the coincidence.

After the coset table has been cleared and the shell of the proof table built, each definition in the sequence saved in the third and fourth auxiliary columns of the coset table is processed in order, entered into the tables and placed on the deduction stack. Here, with the definition $\alpha x_i^{\epsilon_i} = \beta$ for coset numbers α and β, group generator x_i and $\epsilon_i \in \{-1, 1\}$, the entry $CT(\alpha, x_i^{\epsilon_i})$ is reset to β. Memory is allocated for the data structure representing this definition where the member attribute *seq*, for the sequence number, is given a value accordingly and *result* is assigned the value β. For definitions, the *data* field pointer and *next* pointer are both NULL, and as no deductions will have yet been found or processed, the pointer $PT(\alpha, x_i^{\epsilon_i})$ is set from NULL to the single element list containing this definition.

Using the Tables: Scans, Deductions and Coincidences

The process for building the proof table proceeds similarly to coset enumeration, using information in the table to perform relator and subgroup generator scans to deduce new information. Before continuing with the method generating a proof table, descriptions are required of some functions used within *puce_pt()*, namely *al0_apply*, *al0_coinc* and *al0_dedn*. From within these functions, there are also calls to the function, *ptbld1*, for generating proof words, and functions dealing with secondary coincidences, *al0_cols12*, *ptbld2* and *ptbld3*.

Relator and Subgroup Generator Scans

The *al0_apply* function takes in a coset number and subgroup generator or cyclic permutation of a relator and applies the coset to this group element using the coset table in an attempt at finding a new deduction or coincidence. If the application is on the coset α by the word

$$x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \dots x_{i_j}^{\epsilon_{i_j}},$$

with $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \dots, j\}$, then firstly, a forward scan is initiated, stopping when all of the cosets α_s for $s \in \{1, 2, \dots, a\}$ have been found such that

$$\alpha x_{i_1}^{\epsilon_{i_1}} = \alpha_1, \quad \alpha_1 x_{i_2}^{\epsilon_{i_2}} = \alpha_2, \quad \ldots \quad \alpha_{a-1} x_{i_a}^{\epsilon_{i_a}} = \alpha_a$$

and either there is no coset table entry for $\alpha_a x_{i_{a+1}}^{\epsilon_{i_{a+1}}}$ or the forward scan completes and $j = a$. In the latter case, then there may be a coincidence and it needs to be checked that, for coset numbers, $\alpha_a = \alpha$. If $a < j$, however, a backward scan is then performed, finding cosets β_t for $t \in \{1, 2, \ldots, b\}$ so that

$$\alpha x_{i_j}^{-\epsilon_{i_j}} = \beta_1, \quad \beta_1 x_{i_{j-1}}^{-\epsilon_{i_{j-1}}} = \beta_2, \quad \ldots \quad \beta_{b-1} x_{i_{j-(b-1)}}^{-\epsilon_{i_{j-(b-1)}}} = \beta_b.$$

It stops where either there is no coset table entry for $\beta_b x_{i_{j-b}}^{-\epsilon_{i_{j-b}}}$ or the backward scan has reached the same point as that of the forward scan and $a = j - b$. Here, the equivalent row in the relator or subgroup generator table would be

$$\begin{array}{c|c c c c|c|c c c c|c}
\multicolumn{2}{c}{x_{i_1}^{\epsilon_{i_1}}} & \cdots & \multicolumn{2}{c}{x_{i_a}^{\epsilon_{i_a}}} & \multicolumn{2}{c}{x_{i_{j-b+1}}^{\epsilon_{i_{j-b+1}}}} & \cdots & \multicolumn{2}{c}{x_{i_j}^{\epsilon_{i_j}}} \\
\hline
\alpha & \alpha_1 & & \alpha_{a-1} & & \alpha_a, \beta_b & \beta_{b-1} & & \beta_1 & & \alpha
\end{array}$$

and both α_a and β_b have been determined for one entry. Thus, a check for a coincidence must be done and when, for coset numbers, $\alpha_a \neq \beta_b$, *al0_apply* passes control to the function *al0_coinc*.

If the backward scan stopped with $a < j - b - 1$ then there is insufficient information in the coset table to close the row of this table. However, where $a = j - b - 1$, then

$$\begin{array}{c|c c c|c|c|c c c|c}
\multicolumn{2}{c}{x_{i_1}^{\epsilon_{i_1}}} & \cdots & x_{i_a}^{\epsilon_{i_a}} & x_{i_{a+1}}^{\epsilon_{i_{a+1}}} & x_{i_{j-b+1}}^{\epsilon_{i_{j-b+1}}} & \cdots & \multicolumn{2}{c}{x_{i_j}^{\epsilon_{i_j}}} \\
\hline
\alpha & \alpha_1 & & & \alpha_a & \beta_b & & \beta_1 & & \alpha
\end{array}$$

The coset numbers α_a and β_b appear as adjacent entries, and the deduction $\alpha_a x_{i_{a+1}}^{\epsilon_{i_{a+1}}} = \beta_b$ has been found. This new information is pushed onto the deduction stack to be processed later, and *ptbld1* is then called.

Proof Words from Deductions

When a deduction has occurred, this new information needs to be added to the linked list of events that have modified the result of the appropriate proof table entry. The function *ptbld1* determines the proof word for the *data* pointer attribute of the new element to be added to the list. In PEACE, if a deduction $\beta x_{i_j}^{\epsilon_{i_j}} = \gamma$ is found whilst scanning the relator

$$r_i = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \ldots x_{i_s}^{\epsilon_{i_s}}$$

for the coset α with $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \ldots, s\}$, then this deduction resulted from the use of the coset table to find the cosets

$$\alpha_1 = \alpha_{s+1} = \alpha \quad \text{and} \quad \alpha_t = \alpha_{t-1} x_{i_{t-1}}^{\epsilon_{i_{t-1}}} \text{ for } t \in \{2, 3, \ldots, s+1\}.$$

Thus, $\beta = \alpha_j$, $\gamma = \alpha_{j+1}$ and

$$\begin{aligned}
\beta x_{i_j}^{\epsilon_{i_j}} &= \beta x_{i_{j-1}}^{-\epsilon_{i_{j-1}}} \ldots x_{i_1}^{-\epsilon_{i_1}} (r_i) x_{i_s}^{-\epsilon_{i_s}} \ldots x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \alpha_j x_{i_{j-1}}^{-\epsilon_{i_{j-1}}} \ldots x_{i_1}^{-\epsilon_{i_1}} (r_i) x_{i_s}^{-\epsilon_{i_s}} \ldots x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \alpha_{j-1} x_{i_{j-2}}^{-\epsilon_{i_{j-2}}} \ldots x_{i_1}^{-\epsilon_{i_1}} (r_i) x_{i_s}^{-\epsilon_{i_s}} \ldots x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \ldots \\
&= \alpha_2 x_{i_1}^{-\epsilon_{i_1}} (r_i) x_{i_s}^{-\epsilon_{i_s}} \ldots x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \alpha (r_i) x_{i_s}^{-\epsilon_{i_s}} \ldots x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \alpha x_{i_s}^{-\epsilon_{i_s}} \ldots x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \alpha_s x_{i_{s-1}}^{-\epsilon_{i_{s-1}}} \ldots x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \ldots \\
&= \alpha_{j+2} x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \\
&= \alpha_{j+1} \\
&= \gamma.
\end{aligned}$$

The new element of the linked list for the proof table entry $PT(\beta, x_{i_j}^{\epsilon_{i_j}})$ has *result* set to γ, while the member attribute *data* points to the proof word of the form

$$\beta\ x_{i_{j-1}}^{-\epsilon_{i_{j-1}}}\ \alpha_{j-1}\ \ldots x_{i_2}^{-\epsilon_{i_2}}\ \alpha_2\ x_{i_1}^{-\epsilon_{i_1}}\ \alpha\ (r_i)\ \alpha\ x_{i_s}^{-\epsilon_{i_s}}\ \alpha_s\ x_{i_{s-1}}^{-\epsilon_{i_{s-1}}} \ldots\ \alpha_{j+2}\ x_{i_{j+1}}^{-\epsilon_{i_{j+1}}}\ \gamma$$

Subgroup generators involved in deductions are indicated by square brackets, and similarly, for the same deduction obtained from a scan of a subgroup generator s_i with $\alpha = 1$, the proof word *data* attribute accesses the string

$$\beta \; x_{i_{j-1}}^{-\epsilon_{i_{j-1}}} \; \alpha_{j-1} \; \ldots x_{i_2}^{-\epsilon_{i_2}} \; \alpha_2 \; x_{i_1}^{-\epsilon_{i_1}} \; 1 \; [s_i] \; 1 \; x_{i_s}^{-\epsilon_{i_s}} \; \alpha_s \; x_{i_{s-1}}^{-\epsilon_{i_{s-1}}} \cdots \; \alpha_{j+2} \; x_{i_{j+1}}^{-\epsilon_{i_{j+1}}} \; \gamma$$

Involving the coset numbers in the proof word is important. A proof word contains the reasoning behind and events resulting in new information in the coset table. For example, consider the proof table entry $PT(\alpha, x_i^{\epsilon_i})$ where one of the elements of this linked list has the simple proof word

$$\alpha \; x_j^{-\epsilon_j} \; \beta \; x_k^{-\epsilon_k} \; \gamma \; (r) \; \gamma$$

and *result* γ. Obviously, the proof word indicates that this entry was obtained scanning relator $r = x_k^{\epsilon_k} x_j^{\epsilon_j} x_i^{\epsilon_i}$ from coset γ, but to show the entire sequence of events resulting in this deduction, we need to include the reasoning and events behind each of $\alpha x_j^{\epsilon_j} = \beta$ and $\beta x_j^{\epsilon_j} = \gamma$. Thus, where $\alpha \; w_1 \; \beta$ and $\beta \; w_2 \; \gamma$ are the respective proof words, then we can make the expansion

$$\begin{aligned} & \alpha \; x_j^{-\epsilon_j} \; \beta \; x_k^{-\epsilon_k} \; \gamma \; (r) \; \gamma \\ \Rightarrow \quad & \alpha \; w_1 \; \beta \; w_2 \; \gamma \; (r) \; \gamma. \end{aligned}$$

Through continual expansion, the justification for $\alpha x_i^{\epsilon_i} = \gamma$ then includes all the events leading to this deduction.

Coincidences

Once a proof word is found and entered into the proof table, however, later deduction processing may yield a coincidence making one of the coset numbers in the proof word redundant. A coincidence of coset numbers β and γ, found so γ becomes redundant, means that some proof table entry $PT(\alpha, x_i^{\epsilon_i})$ contains a list of least two elements, namely, one with *result* β and one with *result* γ, each possessing different proof words. Although γ is now redundant, it may have been involved in a previous deduction and appear in a proof word of another proof table entry. If the string $\alpha \; x_i^{\epsilon_i} \; \gamma \; x_j^{\epsilon_j} \; \delta$ is a substring of a proof word, then the events and reasoning behind this proof word includes that of the deduction $\alpha x_i^{\epsilon_i} = \gamma$, not $\alpha x_i^{\epsilon_i} = \beta$. Therefore, the expansion requires the proof word for the entry with result γ. However, as γ had become redundant, no further deductions would be made for γ and there may be no entry for $\gamma x_j^{\epsilon_j} = \delta$. Thus, the expanded proof word becomes $\alpha \; x_i^{\epsilon_i} \; {}_{\gamma=\beta} \; x_j^{\epsilon_j} \; {}_{\delta}$ and incorporates the proof words for $\alpha x_i^{\epsilon_i} = \gamma$ and $\beta x_j^{\epsilon_j} = \delta$, as well as that of the coincidence $\gamma = \beta$.

Coincidences are handled by the function *al0_coinc*, making the coset with highest index redundant. In the coset table, cosets can be indicated as redundant using the first two auxiliary columns, and it is simply a matter of replacing each occurrence of the now inactive coset with the other and clearing the entries in the redundant row. Handling coincidences in the proof table cannot be done in the same way. As mentioned above, coset numbers are a necessary part of proof words and can appear in the proof words of various proof table entries if they are part of the scan which resulted in the deduction. Since redundant coset numbers are needed even after a coincidence has been found, the coincidence is indicated in the auxiliary column of the proof table and the event resulting in this new information is recorded in the form of a proof word. Thus, whenever the redundant coset is encountered in a proof word expansion, there is a proof word outlining the reason for the coincidence, which must be included in the proof word so that processing can continue from the non-redundant equivalent of the coset.

If a coincidence is found during a relator or subgroup generator scan, then this is a primary coincidence and the proof word for the auxiliary column of the proof table in the redundant row is determined by the function *ptbld2*. The proof word is found in a similar manner to that of a deduction, and where the scan involved the word

$$w_i = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \dots x_{i_j}^{\epsilon_{i_j}}$$

for coset α with $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \dots, j\}$, then the equivalent row in the relator or subgroup generator table would be

$$\begin{array}{cc|c c c|c|c c c|c|c}
\multicolumn{3}{c}{x_{i_1}^{\epsilon_{i_1}}} & \cdots & \multicolumn{3}{c}{x_{i_a}^{\epsilon_{i_a}} \qquad\qquad x_{i_{a+1}}^{\epsilon_{i_{a+1}}}} & & \cdots & \multicolumn{2}{c}{x_{i_j}^{\epsilon_{i_j}}} \\
\hline
\alpha & & \alpha_1 & & \alpha_{a-1} & \alpha_a, \beta_{j-a} & \beta_{b-1} & & \beta_1 & & \alpha
\end{array}$$

for some $a \in \{1, 2, \ldots, j\}$ given that the forward scan produced the coset numbers α_s for $s \in \{1, 2, \ldots, a\}$ and the backward scan produced the coset numbers β_t for $t \in \{1, 2, \ldots, j - a\}$. Thus, α_a and β_{j-a} are found to be coincident and the coset with highest coset number is redundant. Using

$$1 = x_a^{-\epsilon_a} \ldots x_{i_2}^{-\epsilon_{i_2}} x_{i_1}^{-\epsilon_{i_1}} (w_i) x_{i_j}^{-\epsilon_{i_j}} x_{i_{j-1}}^{-\epsilon_{i_{j-1}}} \ldots x_{i_{a+1}}^{-\epsilon_{i_{a+1}}},$$

then where the coset numbers $\alpha_a > \beta_{j-a}$, the auxiliary column entry in row α_a of the proof table would contain the proof word for $\alpha_a = \beta_{j-a}$ as

$$\alpha_a \ x_{i_a}^{-\epsilon_{i_a}} \cdots \ \alpha_1 \ x_{i_1}^{-\epsilon_{i_1}} \ \alpha \ (w_i) \ \alpha \ x_{i_j}^{-\epsilon_{i_j}} \ \beta_1 \ \cdots x_{i_{a+1}}^{-\epsilon_{i_{a+1}}} \ \beta_{j-a}.$$

Alternatively, when $\alpha_a < \beta_{j-a}$, then the proof word of $\beta_{j-a} = \alpha_a$ in the auxiliary column entry of row β_{j-a} would be

$$\beta_{j-a} \ x_{i_{a+1}}^{\epsilon_{i_{a+1}}} \cdots \ \beta_1 \ x_{i_j}^{\epsilon_{i_j}} \ \alpha \ (w_i)^{-1} \ \alpha \ x_{i_1}^{\epsilon_{i_1}} \ \alpha_1 \ \cdots x_{i_a}^{\epsilon_{i_a}} \ \alpha_a.$$

Given a coincidence of coset numbers α and β, the function *al0_coinc* also handles the transfer of information from β, the redundant coset number, to α. For each generator or generator inverse $x_i^{\epsilon_i}$, the entries $CT(\alpha, x_i^{\epsilon_i})$ and $CT(\beta, x_i^{\epsilon_i})$ must be compared to use the information in the β-th row to fill empty entries and modify current entries in that of the α-th row of the tables and to find secondary coincidences. The inverse entries are also updated accordingly.

Various cases exist and require different proof words to show both the coincidence and any secondary coincidences. The PEACE manual [19] outlines the formation of the proof words for each case, although we will describe this formation for a few of the most general cases. Obviously, if $CT(\beta, x_i^{\epsilon_i}) = 0$, then nothing needs to be done.

Where $CT(\alpha, x_i^{\epsilon_i}) = 0$ and $CT(\beta, x_i^{\epsilon_i}) = \beta$, then there are two cases. If $CT(\alpha, x_i^{-\epsilon_i}) = 0$, then $PT(\alpha, x_i^{\epsilon_i})$ becomes the list composed of the single element with *result* α and proof word

$$\alpha{=}\beta \ x_i^{\epsilon_i} \ \beta{=}\alpha,$$

while a single element is assigned to the empty list $PT(\alpha, x_i^{-\epsilon_i})$, having *result* α and proof word

$$\alpha{=}\beta\ x_i^{-\epsilon_i}\ \beta{=}\alpha.$$

If $CT(\alpha, x_i^{-\epsilon_i}) = \gamma \neq 0$, however, then a secondary coincidence has been found involving the cosets α and γ, which is added to the coincidence queue.

For $CT(\alpha, x_i^{\epsilon_i}) = 0$ and $CT(\beta, x_i^{\epsilon_i}) = \gamma \neq \beta$, the entry $PT(\alpha, x_i^{\epsilon_i})$, which had previously been NULL, is given a list element with *result* γ and the proof word attribute *data* of

$$\alpha{=}\beta\ x_i^{\epsilon_i}\ \gamma.$$

The list at entry $PT(\gamma, x_i^{-\epsilon_i})$ must contain an element with *result* β and is given a new head element with *result* α and *data*

$$\gamma\ x_i^{-\epsilon_i}\ \beta{=}\alpha.$$

Lastly, the coset table is adjusted so that $CT(\alpha, x_i^{\epsilon_i}) = \gamma$ and $CT(\beta, x_i^{\epsilon_i}) = 0$, and the coincidence is added to the first two auxiliary column entries of row β.

During the formation of the rest of the proof table, if $\alpha x_i^{\epsilon_i}$ or $\gamma x_i^{-\epsilon_i}$ occurs during a scan, then the resulting cosets will be given as γ or α, respectively. Any new proof word using one of these new relationships will contain the substring $\alpha\ x_i^{\epsilon_i}\ \gamma$ or $\gamma\ x_i^{-\epsilon_i}\ \alpha$. Proof words formed before the coincidence was discovered, however, are left unchanged and may still contain $\beta\ x_i^{\epsilon_i}\ \gamma$ or $\gamma\ x_i^{-\epsilon_i}\ \beta$. The entries of the proof table are not cleared after a coincidence, and so there is still an element of the list $PT(\beta, x_i^{\epsilon_i})$ with result γ and proof word $\beta\ w_1\ \gamma$ for some string w_1 of generators, generator inverses, coset numbers and either '=' symbols or a relator or subgroup generator, which can be used for the expansion. The same is true of the list $PT(\gamma, x_i^{-\epsilon_i})$ for an element with result β, whose proof word is $\gamma\ w_1^{-1}\ \beta$. Using the proof table, where the coincidence of cosets α and β is given in the auxiliary column of the β-th row with proof word $\beta\ w_2\ \alpha$ for some string w_2, the expansions of

$\alpha\ x_i^{\epsilon_i}\ \gamma$ and $\gamma\ x_i^{-\epsilon_i}\ \alpha$ are then

$$\begin{aligned}
\alpha\ x_i^{\epsilon_i}\ \gamma\ &\Rightarrow\ \alpha{=}\beta\ x_i^{\epsilon_i}\ \gamma \\
&\Rightarrow\ \alpha\ w_2^{-1}\ \beta\ x_i^{\epsilon_i}\ \gamma \\
&\Rightarrow\ \alpha\ w_2^{-1}\ \beta\ w_1\ \gamma
\end{aligned}$$

and

$$\begin{aligned}
\gamma\ x_i^{-\epsilon_i}\ \alpha\ &\Rightarrow\ \gamma\ x_i^{-\epsilon_i}\ \beta{=}\alpha \\
&\Rightarrow\ \gamma\ w_1^{-1}\ \beta{=}\alpha \\
&\Rightarrow\ \gamma\ w_1^{-1}\ \beta\ w_2\ \alpha.
\end{aligned}$$

Thus, the justifications include the fact that the new deductions had been obtained from old deductions plus a coincidence.

Where $CT(\beta, x_i^{\epsilon_i}) = \lambda \neq 0$ and $CT(\alpha, x_i^{\epsilon_i}) = \delta \neq 0$, there is a possible secondary coincidence of cosets λ and δ, and several special cases arrise where $\{\alpha, \beta\} \cap \{\lambda, \delta\} \neq \emptyset$. Secondary coincidences can trigger a sequence of coincidences, which must be reflected in the proof word. Each of these is added to the coincidence queue handled by the function *al0_cols12* and, athough coincidences are processed in the order in which they are determined, secondary coincidences must be immediately marked in the first auxiliary columns of the coset and proof tables and their proof words determined as they affect the resulting proof table entries. If $\{\alpha, \beta\} \cap \{\lambda, \delta\} = \emptyset$, then the proof word for the new element of $PT(\alpha, x_i^{\epsilon_i})$ cannot be formed until the representatives of cosets λ and δ are determined, assuming α is not found redundant. A previously determined coincidence involving either λ or δ may still be unprocessed and in the coincidence queue and thus, either λ or δ may be marked as redundant and represented by a different coset. However, once all secondary coincidences are found for this case and where λ and δ are found to be represented by the cosets λ' and δ', respectively, then the proof word of this final secondary coincidence will take the form

$$\lambda'{=}\ \cdots\ {=}\lambda\ x_i^{-\epsilon_i}\ \beta{=}\alpha\ x_i^{\epsilon_i}\ \delta{=}\ \cdots\ {=}\delta',$$

if, for coset numbers, $\lambda' > \delta'$. Otherwise, the form is

$$\delta' = \cdots = \delta \; x_i^{-\epsilon_i} \; \alpha = \beta \; x_i^{\epsilon_i} \; \lambda = \cdots = \lambda'.$$

Filling the Proof Table

Having processed the definition sequence and saved all of these definitions in the coset and proof tables, *puce_pt* performs an initial scan of the subgroup generators for coset 1 as well as of cyclic permutations of the relators for all cosets before the deduction stack is processed. This scan, using *al0_apply*, occurs to determine any deductions and push them onto the deduction stack, all the while entering the appropriate data in the coset and proof tables. It also occurs solely in case the definition sequence, and thus the deduction stack, had been empty.

A call to *al0_dedn* is then made by *puce_pt* to process the deduction stack. Popping off the top most deduction $\alpha x_i^{\epsilon_i} = \beta$, all the cyclic permutations of the relators beginning with $x_i^{\epsilon_i}$ are applied to coset α, and all cyclic permutations of the relators ending with $x_i^{\epsilon_i}$ are scanned from coset β using calls to *al0_apply*. Any new deduction is added to the deduction stack, the proof word of the new proof table entry element is determined by *ptbld1* and coincidences handled by *al0_coinc*. This process continues until the deduction stack is empty and all deductions have been processed. However, since *al0_dedn* only applies the deductions to relators, another loop is required to scan the subgroup generators. This, of course, may result in further deductions and the deduction stack will need to be processed again. Thus, *puce_pt* alternates between calls to *al0_dedn* and a loop scanning each subgroup generator using *al0_apply* until the subgroup generator scans produce no deductions or coincidences and the deduction stack is empty.

If the definition sequence is valid, these definitions will have been enough to close the tables and complete the enumeration. At this point in the construction of the proof table, the coset table should be complete and the scans of all subgroup generator and all cyclic permutations of the relators should contain no holes. For safety, *puce_pt* calls the function *chkct*, which checks the coset table by performing these scans.

To help illustrate the process of forming a proof table, we shall work through a small case.

Example 2.2 The quaternian group Q_8 can be given by the presentation

$$\langle a, b | a^4, b^4, a^2b^{-2}, aba^{-1}b \rangle$$

and the subgroup $\langle a \rangle$ over Q_8 has index 2. Using the definition sequence $2 = 1b^{-1}, 3 = 2b^{-1}, 4 = 3b^{-1}$, these definitions are first added to the coset table to obtain:

coset	a	a^{-1}	b	b^{-1}	coinc	chain	defn
1	0	0	0	2	n/a	n/a	n/a
2	0	0	1	3	0	0	$1b^{-1}$
3	0	0	2	4	0	0	$2b^{-1}$
4	0	0	3	0	0	0	$3b^{-1}$

Before these deductions are processed, we must perform the subgroup generator and relator scans. Firstly, the subgroup generator a is applied to coset 1. The forward and backward scans result in the deduction $1a = 1$, and as this was from a subgroup generator scan, then $PT(1, a)$ is given the element with *result* 1 and proof word $_1\ [a]\ _1$. Similarly, an element is added to $PT(1, a^{-1})$ with *result* 1 and proof word $_1\ [a^{-1}]\ _1$. The coset table is updated so that both $CT(1, a) = 1$ and $CT(1, a^{-1}) = 1$.

Moving to the relator scans and beginning with coset 1, no new deductions are obtained for the relator a^4. For b^4, there is no information in the table for the forward scan. The backward scan, however, gives $_1\ b^{-1}\ _2\ b^{-1}\ _3\ b^{-1}\ _4$, so we obtain $_1\ b\ _4\ b\ _3\ b\ _2\ b\ _1$ and the deduction $1b = 4$. An element with *result* 4 and proof word

$$_1\ (b^4)\ _1\ b^{-1}\ _2\ b^{-1}\ _3\ b^{-1}\ _4$$

is added to the proof table entry $PT(1, b)$. The inverse entry $PT(4, b^{-1})$ is given an element with *result* 1 and proof word $_4\ b\ _3\ b\ _2\ b\ _1\ (b^{-4})_1$, and the coset table is modified as well.

At this point, the partial coset and proof tables are:

coset	a	a^{-1}	b	b^{-1}	coinc	chain	defn
1	1	1	4	2	n/a	n/a	n/a
2	0	0	1	3	0	0	$1b^{-1}$
3	0	0	2	4	0	0	$2b^{-1}$
4	0	0	3	1	0	0	$3b^{-1}$

coset #1

a	1	$1[a]1$
a^{-1}	1	$1[a^{-1}]1$
b	4	$1(b^4)1b^{-1}2b^{-1}3b^{-1}4$
b^{-1}	2	$defn$
coinc		n/a

coset #2

a	NULL	
a^{-1}	NULL	
b	1	$defn$
b^{-1}	3	$defn$
coinc		$null$

coset #3

a	NULL	
a^{-1}	NULL	
b	2	$defn$
b^{-1}	4	$defn$
coinc		$null$

coset #4

a	NULL	
a^{-1}	NULL	
b	3	$defn$
b^{-1}	1	$4b3b2b1(b^{-4})1$
coinc		$null$

Considering the next relator a^2b^{-2} with coset 1, the forward scan completes and results in ${}_1\, a\, {}_1\, a\, {}_1\, b^{-1}\, {}_2\, b^{-1}\, {}_3$. Since the scan should finish on 1, we have obtained a primary coincidence of cosets 1 and 3. Thus, the associated proof word is

$$_3\, b\, {}_2\, b\, {}_1\, a^{-1}\, {}_1\, a^{-1}\, {}_1\, (a^2b^{-2})\, {}_1.$$

We now need to transfer any relevant information from the redundant coset 3 to coset 1. For both a and a^{-1}, nothing needs to be done as $CT(3, a) = 0$ and $CT(3, a^{-1}) = 0$. For the group generator b, however, we have $CT(1, b) = 4$ and $CT(3, b) = 2$ and, thus, have encountered the secondary coincidence of the cosets 2 and 4. Since no previous and unprocessed coincidences involving either 2 or 4 had been found, then the representatives of these cosets are just themselves and the proof word is

$$4 \; b^{-1} \; 1 = 3 \; b \; 2.$$

This coincidence is added to the chain of pending coincidences, and coset 4 is marked as redundant and represented by 2. The proof table entry $PT(1, b)$ involves the coincidence of cosets 2 and 4 and is left until this coincidence is processed, when it will be handled along with its inverse, $PT(2, b^{-1})$. $CT(3, b)$ is then reset to 0 and, as $CT(2, b^{-1})$ will be handled when the coincidence of 2 and 4 is processed, this entry is also reset to from 3 to 0.

The last step of processing the coincidence of cosets 1 and 3 is to consider $CT(1, b^{-1})$ and $CT(3, b^{-1})$. Since the former contains 2 and the latter 4, we have the secondary coincidence of cosets 2 and 4. As this coincidence has already been determined, although not yet completely processed, the coset table indicates that the representative coset of 4 is actually 2. As the entry of $CT(1, b^{-1})$ is already 2, then nothing needs to be done except to reset both $CT(3, b^{-1})$ and $CT(4, b)$ to 0. The tables at this stage are:

coset	a	a^{-1}	b	b^{-1}	coinc	chain	defn
1	1	1	4	2	n/a	n/a	n/a
2	0	0	1	0	0	0	$1b^{-1}$
3	0	0	0	0	1	4	$2b^{-1}$
4	0	0	0	1	2	0	$3b^{-1}$

coset #1

a	1	$1[a]1$
a^{-1}	1	$1[a^{-1}]1$
b	4	$1(b^4)1b^{-1}2b^{-1}3b^{-1}4$
b^{-1}	2	$defn$
coinc		n/a

coset #2

a	NULL	
a^{-1}	NULL	
b	1	$defn$
b^{-1}	3	$defn$
coinc		*null*

coset #3

a	NULL	
a^{-1}	NULL	
b	2	$defn$
b^{-1}	4	$defn$
coinc	1	$3b2b1a^{-1}1a^{-1}1(a^2b^{-2})1$

coset #4

a	NULL	
a^{-1}	NULL	
b	3	$defn$
b^{-1}	1	$4b3b2b1(b^{-4})1$
coinc	2	$4b^{-1}1 = 3b2$

Before we can return to the relator scans, we still need to process the coincidence of cosets 2 and 4, which is sitting in the chain of pending coincidences. As the coset table entries for row 4 are all 0 for the group generators a, a^{-1} and b, nothing needs to be done for these cases. For b^{-1}, then since $CT(2, b^{-1}) = 0$ and $CT(4, b^{-1}) = 1$, we add a new element to $PT(2, b^{-1})$ with *result* 1 and proof word $_{2=4}\, b^{-1}\, _1$. The coset table is updated so $CT(4, b^{-1}) = 0$ and $CT(2, b^{-1}) = 1$. Additionally, for $PT(1, b)$, a new list element is added with *result* 2 and proof word $_1\, b\, _{4=2}$, and $CT(1, b)$ is changed to 2.

coset	a	a^{-1}	b	b^{-1}	coinc	chain	defn
1	1	1	2	2	n/a	n/a	n/a
2	0	0	1	1	0	0	$1b^{-1}$
3	0	0	0	0	1	0	$2b^{-1}$
4	0	0	0	0	2	0	$3b^{-1}$

coset #1

a	1	$1[a]1$
a^{-1}	1	$1[a^{-1}]1$
b	2	$1b4 = 2$
	4	$1(b^4)1b^{-1}2b^{-1}3b^{-1}4$
b^{-1}	2	$defn$
coinc		n/a

coset #2

a	NULL	
a^{-1}	NULL	
b	1	$defn$
b^{-1}	1	$2 = 4b^{-1}1$
	3	$defn$
coinc		$null$

coset #3

a	NULL	
a^{-1}	NULL	
b	2	$defn$
b^{-1}	4	$defn$
coinc	1	$3b2b1a^{-1}1a^{-1}1(a^2b^{-2})1$

coset #4

a	NULL	
a^{-1}	NULL	
b	3	$defn$
b^{-1}	1	$4b3b2b1(b^{-4})1$
coinc	2	$4b^{-1}1 = 3b2$

There are no more pending coincidences and we can return to the relator scans, with coset 1 and relator $aba^{-1}b$. Using the current coset table, the forward scan gives $_1\ a\ _1\ b\ _2$, while the backward scan yields $_1\ b^{-1}\ _2$. Together, we have $_1\ a\ _1\ b\ _2\ a^{-1}{}_2\ b\ _1$ and the deduction $2a^{-1} = 2$. Thus, since $CT(2, a^{-1}) = 0$, this coset table entry is set to 2 and a new list element is given to $PT(2, a^{-1})$ with *result* 2 and proof word

$$_2\ b^{-1}\ _1\ a^{-1}\ _1\ (aba^{-1}b)\ _1\ b^{-1}\ _2.$$

Similary, we set $CT(2, a) = 2$ and a new list element is added to $PT(2, a)$ with *result* 2 and proof word

$$_2\ b\ _1\ (b^{-1}ab^{-1}a^{-1})\ _1\ a\ _1\ b\ _2.$$

Here, the tables are:

coset	a	a^{-1}	b	b^{-1}	coinc	chain	defn
1	1	1	2	2	n/a	n/a	n/a
2	2	2	1	1	0	0	$1b^{-1}$
3	0	0	0	0	1	0	$2b^{-1}$
4	0	0	0	0	2	0	$3b^{-1}$

coset #1

a	1	$1[a]1$
a^{-1}	1	$1[a^{-1}]1$
b	2	$1b4 = 2$
	4	$1(b^4)1b^{-1}2b^{-1}3b^{-1}4$
b^{-1}	2	$defn$
coinc		n/a

coset #2

a	2	$2b1(b^{-1}ab^{-1}a^{-1})1a1b2$
a^{-1}	2	$2b^{-1}1a^{-1}1(aba^{-1}b)1b^{-1}2$
b	1	$defn$
b^{-1}	1	$2 = 4b^{-1}1$
	3	$defn$
coinc		$null$

coset #3

a	NULL	
a^{-1}	NULL	
b	2	$defn$
b^{-1}	4	$defn$
coinc	1	$3b2b1a^{-1}1a^{-1}1(a^2b^{-2})1$

coset #4

a	NULL	
a^{-1}	NULL	
b	3	$defn$
b^{-1}	1	$4b3b2b1(b^{-4})1$
coinc	2	$4b^{-1}1 = 3b2$

As neither scanning each relator for coset 2 nor processing each of the previously determined deductions yields any further coincidences or deductions, the proof table is complete.

Using a complete proof table, a group element h can be shown to also be a subgroup element by extracting its proof word from the proof table. The peace command, *prove: h*, extracts the proof word if it is a subgroup element, and either *cert* or *acert* prints out the proof certificate. While *cert* allows cyclic permutations of the relators to appear in the proof word, *acert* produces the proof word with the original relators. Where

$$h = x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \ldots x_{i_s}^{\epsilon_{i_s}},$$

with $x_{i_k} \in X$ and $\epsilon_{i_k} \in \{-1, 1\}$ for $k \in \{1, 2, \ldots, s\}$, then, using the coset table, the non-redundant coset numbers α_t for $t \in \{0, 1, \ldots, s\}$ can be found so that

$$\alpha_0 = 1 \quad \text{and} \quad \alpha_k = \alpha_{k-1} x_{i_k}^{\epsilon_{i_k}} \text{ for } k \in \{1, 2, \ldots, s\}.$$

As long as the coset number $\alpha_s = 1$, then h is a subgroup element, and from

$$1 \; x_{i_1}^{\epsilon_{i_1}} \; \alpha_1 \; x_{i_2}^{\epsilon_{i_2}} \cdots \; \alpha_{s-1} \; x_{i_s}^{\epsilon_{i_s}} \; 1,$$

the proof word can be formulated by continually expanding it through the substitution of proof table entries. For h, the first expansion would involve the element with *result* α_k in the list at entry $PT(\alpha_{k-1}, x_{i_k}^{\epsilon_{i_k}})$ for each $k \in \{1, 2, \ldots, s\}$. Where the associated proof word is $\alpha_{k-1} \; w_k \; \alpha_k$ for strings w_k, then

$$\begin{aligned} & 1 \; x_{i_1}^{\epsilon_{i_1}} \; \alpha_1 \; x_{i_2}^{\epsilon_{i_2}} \cdots \; \alpha_{s-1} \; x_{i_s}^{\epsilon_{i_s}} \; 1 \\ \Rightarrow \; & 1 \; w_1 \; \alpha_1 \; w_2 \cdots \; \alpha_{s-1} \; w_s \; 1. \end{aligned}$$

If the list element with *result* α_k is a definition, then no substitution occurs and $\alpha_{k-1} \; x_{i_k}^{\epsilon_{i_k}} \; \alpha_k$ remains. The expansion proceeds by continually scanning left to right, replacing each coset number-generator pair, or coset number-= pair indicating a coincidence, with its corresponding proof word according to the resulting coset number until each such pair is a definition.

After every scan, the intermediate proof word is reduced, so that any substring of the form $w_1 \; \alpha \; w_2 \; \beta \; w_2^{-1} \; \alpha \; w_3$ for strings w_1, w_2 and w_3 becomes $w_1 \; \alpha \; w_3$. This reduces the size of the proof word in PEACE and requires fewer substitutions to complete the expansion. The proof table contains only one element of the list $PT(\alpha, x)$ with *result* β for generator or generator inverse x, and the entry $PT(\beta, x^{-1})$ has only one element of *result* α. The associated proof word of the latter is the inverse of that of the former, so reducing at each stage does not affect the resulting proof word.

Example 2.3 As a simple example, consider

$$\langle p | p^3, p^2 \rangle,$$

a presentation of the trivial group. Using the trivial subgroup, coset enumeration is performed and the proof table is built and output with the PEACE input commands,

```
gr: p;
rel: p3, p2;
start;
pt;
pr pt;
```

The PEACE output of the proof table is given below, where the column entries indicate *result*, *seq* or the number indicating where in the sequence of events this deduction was made and *data*. The bottom row represents the auxiliary column of the proof table, outlining whether the coset is redundant, if it is a primary (P) or secondary (S) coincidence and the associated data proof word. We will use the table to show how PEACE forms the proof word of p^4 to prove it is also a subgroup element.

coset #1			
p	1	6	$1 = 2p1$
	2	4	$1(pp)1P2$
P	1	7	$1P2 = 1$
	2	1	$defn$
coinc			n/a

coset #2			
p	1	2	$defn$
P	1	3	$2p1(PP)1$
coinc	P	5	$2P1P2P1(ppp)1$

Consider the group element p^4, which is obviously in the trivial subgroup as the group is $\{1\}$. From the coset table, p^4 becomes

$$1 \,{}^{p}\, 1 \,{}^{p}\, 1 \,{}^{p}\, 1 \,{}^{p}\, 1,$$

and using the proof table, $_1\,p\,_1$ expands to

$$\begin{aligned}
& 1\ {}^{p}\ 1 \\
\Rightarrow\ & 1{=}2\ {}^{p}\ 1 \\
\Rightarrow\ & {}_1\ {}^{(P^3)}\ {}_1\ {}^{p}\ {}_2\ {}^{p}\ {}_1\ {}^{p}\ {}_2\ {}^{p}\ {}_1 \\
\Rightarrow\ & {}_1\ {}^{(P^3)}\ {}_1\ {}^{(p^2)}\ {}_1\ {}^{P}\ {}_2\ {}^{p}\ {}_1\ {}^{(p^2)}\ {}_1\ {}^{P}\ {}_2\ {}^{p}\ {}_1 \\
\Rightarrow\ & {}_1\ {}^{(P^3)}\ {}_1\ {}^{(p^2)}\ {}_1\ {}^{(p^2)}\ {}_1,
\end{aligned}$$

and

$$1\ {}^{p}\ 1\ {}^{p}\ 1\ {}^{p}\ 1\ {}^{p}\ 1\ \Rightarrow \underbrace{{}_1\ {}^{(P^3)}\ {}_1\ {}^{(p^2)}\ {}_1\ {}^{(p^2)}}_{\times 4}\ 1.$$

Thus, the proof word for p^4 is

$$(P^3)(p^2)(p^2)(P^3)(p^2)(p^2)(P^3)(p^2)(p^2)(P^3)(p^2)(p^2),$$

which freely reduces to p^4. Removing the relators, it reduces to 1.

Example 2.4 For an example containing subgroup generators, consider the element $w = ab^3a$ of the group $G \cong \langle a, b | a^4, b^3, a^{-1}b^{-1}ab\rangle$ with subgroup $\langle a^2 \rangle$, which has index 6 in G. This is input into PEACE by

```
gr:ab;
rel:a4,b3,ABab;
gen:a2;
start;
pt;
pr pt;
```

The formulated proof table is then

coset #1

a	2	16	$1[aa]1A2$
A	2	1	$defn$
b	4	18	$1(bbb)1B3B4$
B	3	3	$defn$
coinc			n/a

coset #2

a	1	2	$defn$
A	1	15	$2a1[AA]1$
b	6	22	$2(bbb)2B5B6$
B	5	20	$2a1(ABab)1B3A5$
coinc			$null$

coset #3

a	5	24	$3b1a2(ABab)2B5$
A	5	7	$defn$
b	1	4	$defn$
B	4	5	$defn$
coinc			$null$

coset #4

a	6	31	$4 = 7a6$
	8	28	$4(aaaa)4A6A7A8$
A	6	25	$4b3(BAba)3A5B6$
b	3	6	$defn$
B	1	17	$4b3b1(BBB)1$
coinc			$null$

coset #5

a	3	8	$defn$
A	3	23	$5b2(BAba)2A1B3$
b	2	19	$5a3b1(BAba)1A2$
B	6	9	$defn$
coinc			$null$

coset #6

a	4	26	$6b5a3(ABab)3B4$
A	4	32	$6A7 = 4$
	7	11	$defn$
b	5	10	$defn$
B	2	21	$6b5b2(BBB)2$
coinc			$null$

coset #7

a	6	12	$defn$
A	8	13	$defn$
b			$null$
B			$null$
coinc	S	30	$7A8 = 6a4$

coset #8

a	7	14	$defn$
A	4	27	$8a7a6a4(AAAA)4$
b			$null$
B			$null$
coinc	P	29	$8A4b3a5(ABab)5B6$

From the coset table, ab^3a becomes

$$1 \; ^a \; 2 \; ^b \; 6 \; ^b \; 5 \; ^b \; 2 \; ^a \; 1,$$

and using the proof table, it expands with reduction to

$$
\begin{aligned}
& {}_1\, a\, {}_2\, b\, {}_6\, b\, {}_5\, b\, {}_2\, a\, {}_1 \\
\Rightarrow\ & {}_1\, [a^2]_1\, A\, {}_2\, (b^3)\, {}_2\, B\, {}_5\, B\, {}_6\, b\, {}_5\, a\, {}_3\, b\, {}_1\, (BAba)\, {}_1\, A\, {}_2\, a\, {}_1 \\
\Rightarrow\ & {}_1\, [a^2]_1\, A\, {}_2\, (b^3)\, {}_2\, B\, {}_5\, a\, {}_3\, b\, {}_1\, (BAba)\, {}_1 \\
\Rightarrow\ & {}_1\, [a^2]_1\, A\, {}_2\, (b^3)\, {}_2\, a\, {}_1\, (ABab)\, {}_1\, B\, {}_3\, A\, {}_5\, a\, {}_3\, b\, {}_1\, (BAba)\, {}_1 \\
\Rightarrow\ & {}_1\, [a^2]_1\, A\, {}_2\, (b^3)\, {}_2\, a\, {}_1\, (ABab)\, {}_1\, (BAba)\, {}_1 \\
\Rightarrow\ & {}_1\, [a^2]_1\, A\, {}_2\, (b^3)\, {}_2\, a\, {}_1.
\end{aligned}
$$

Thus, the proof word for ab^3a is $[a^2]A(b^3)a$. With the commands,

```
prove:ab3a;
cert;
```

the proof certificate is output.

```
#– PEACE 1.100 proof certificate ———-
* Group Generators
  ab
* Group Relators
  bbb
  aaaa
  ABab
* Subgroup Generators
  aa
* Word
  abbba
* Proof Word
  [aa]A(bbb)a
#————————————————-
```

2.2 PEACE and the Modified Todd-Coxeter Algorithm

Once PEACE has been described, it is easy to see the similarities of the Modified Todd-Coxeter coset enumeration algorithm with the methods to produce a proof table and extract a proof word. A subgroup presentation is formed in the Modified Todd-Coxeter algorithm by rewriting each subgroup generator and group relator in terms of the subgroup generators to determine the subgroup relators. The proof table provides a way to rewrite a subgroup element in terms of the subgroup generators, so, as they must be subgroup elements, each of the subgroup generators and group relators can be rewritten from this table.

Recall that in the Modified Todd-Coxeter algorithm, when the first deduction is determined in the table of a subgroup generator h, we use the fact that $1h = h1$ to find the augmented coset table element. For example, where $h = abc$ and this initial subgroup generator deduction resulted from the information $1a = \alpha$ and $1c^{-1} = \beta$ obtained from the augmented table, then we write

$$\begin{aligned} 1abc &= h1 \\ \alpha b &= h1c^{-1} \\ \alpha b &= h\beta. \end{aligned}$$

Thus, the table entry for row α and column corresponding to b is $h\beta$. This new entry is carried through the enumeration so that whenever αb is encountered in a relator or subgroup generator table scan, it is replaced by $h\beta$.

Consider the same deduction in the construction of the PEACE proof table. Here, writing

$$b = a^{-1}[abc]c^{-1},$$

then the determined proof word for the element of the list $PT(\alpha, b)$ with result β would be

$$\alpha \; A \; 1 \; [abc] \; 1 \; C \; \beta,$$

where, in PEACE, A and C represent a^{-1} and c^{-1}, respectively. Only the result of this deduction, however, is carried through the formation of the proof table. For the group element $w = w_1 b w_2$, with w_1 and w_2 also group elements, scanning from coset number γ where we have found either $\gamma w_1 = \alpha$ from the forward scan or, from the backward scan, $\gamma w_2^{-1} = \beta$, then only $\beta \; B \; \alpha$ will appear in the proof word for this deduction assuming neither α nor β have been found redundant. However, a word g that is either a subgroup generator or a group relator must be in the subgroup, and once the proof table has been completed, we are able to continually expand g to find a proof word. Rewriting g as its corresponding string of coset numbers and generators and, again, assuming neither α nor β are redundant coset numbers, if there is a substring $\alpha \; b \; \beta$, then the substitution $\alpha \; A \; 1 \; [abc] \; 1 \; C \; \beta$ would be made in the expansion. Therefore, expanding any such proof word in the proof table results in a proof word that has a form alike that of the augmented coset table entry, although it also contains group generators and generator inverses. These extra elements are those coset number-generator pairs that resulted from definitions, could not be further expanded and were necessary only to show the resultant proof word freely reduces to the original word.

Deductions involving relators found during the construction of the proof table are handled similarly to those involving subgroup generators, and the relator is enclosed with parentheses, rather than square brackets. In the Modified Todd-Coxeter algorithm, however, these types of deductions use $\gamma r = \gamma$ rather than $\gamma r = r\gamma$ for a relator r and coset number γ, and thus, r does not appear in the deduced augmented coset table entry. However, if a proof word in a proof table entry had all relator substrings removed and was then reduced, the resulting proof word could be expanded to form a proof word similar to that of the corresponding augmented coset table entry of the Modified Todd-Coxeter algorithm.

It is easy to see that the method of determining proof table entries for a deduction could be changed to simulate that for determining the augmented coset table entries. In fact, the complete proof table could be itself used to obtain the subgroup presentation for the Modified Todd-Coxeter algorithm. This coset enumeration algorithm employs the fact that, if G is a group with finite presentation $\langle X|R\rangle$, $|X| = n$ and $|R| = m$, then a presentation for a subgroup $H = \langle h_1, \ldots, h_l\rangle$ of G with finite index $[G : H] = a$ can be given as

$$\begin{aligned}\langle h_1, \ldots, h_l \quad | \quad & 1h_i = h_i 1 \text{ for } i \in \{1, 2, \ldots, l\}, \\ & jrj^{-1} = 1 \text{ for } j \in \{1, 2, \ldots, a\} \text{ and } r \in R\rangle.\end{aligned}$$

Consider the constructed proof table. Each entry can be expanded and slightly altered, removing relators and reducing, to resemble the corresponding augmented coset table entry. If, for a subgroup generator h_i, we extract its proof word from the table, then we obtain a string which, when all the brackets are removed, reduces to h_i. When the relators are removed and the resulting string reduced, we are left with a product of subgroup generators equivalent to h_i and a new relation of the subgroup. This corresponds to the relator $1h_i = h_i 1$ of the subgroup presentation.

The same can be done for a relator $r \in R$ and coset number 1. The extraction from the proof table of the proof word for r rewrites $r = 1$ in terms of the subgroup generators and corresponds to the relator $1r1 = 1$ of the subgroup presentation.

It remains to determine the subgroup relators jrj^{-1} for $r \in R$ and $j \in \{2, 3, \ldots, a\}$. The *prove* command in PEACE only allows a scan from coset 1, but, using the proof table and the same method for extracting a proof, we can obtain a string of subgroup generators and conjugates of relators by expanding from $\alpha_j \; r \; \alpha_j$. Reducing freely, we are left with r and, after removing any relators, we obtain a conjugated product of subgroup generators. The latter is either trivial or has the form $g^{-1}hg$ for a group element g and product of subgroup generators h. Because this is equivalent to r and we know $r = 1$, we have $g^{-1}hg = 1$ and $h = 1$, a new subgroup relator. The group element g^{-1} is such that it belongs to coset j and $j = Hg^{-1}$. From Example 2.4 with relator a^4 and coset number 2, then $2 \; a^4 \; 2$ is rewritten as $_2\,a\,_1\,a\,_2\,a\,_1\,a\,_2$, and

$$
\begin{aligned}
& {}_2\,a\,_1\,a\,_2\,a\,_1\,a\,_2 \\
\Rightarrow\ & {}_2\,a\,_1\,[aa]\,_1\,A\,_2\,a\,_1\,[aa]\,_1\,A\,_2 \\
\Rightarrow\ & {}_2\,a\,_1\,[aa]\,_1\,[aa]\,_1\,A\,_2.
\end{aligned}
$$

Removing coset numbers leaves ah^2a^{-1} where h is the subgroup generator aa. This still freely reduces to $r = a^4$ and so, is also trivial. As such, $ah^2a^{-1} = 1$ and $h^2 = 1$, which is the subgroup relator corresponding to $2a^42 = 1$.

Hence, from our proof table, we can extract each of the necessary relators for the subgroup presentation.

Example 2.5 Consider again the group presented by

$$\langle a, b | a^4, b^3, a^{-1}b^{-1}ab \rangle$$

with subgroup $\langle a^2 \rangle$ from Example 2.4. Using the same proof table, then the proof words extracted for each relator and non-redundant coset are

Coset	Group Relator	Proof Word	Subgroup Relator
1	a^4	$[aa][aa]$	$[aa]^2 = 1$
	b^3	(bbb)	$1 = 1$
	$ABab$	$(ABab)$	$1 = 1$
2	a^4	$a[aa][aa]A$	$[aa]^2 = 1$
	b^3	(bbb)	$1 = 1$
	$ABab$	$(ABab)$	$1 = 1$

Coset	Group Relator	Proof Word	Subgroup Relator
3	a^4	$b[aa]A(ABab)a(ABab)[aa]$ $A(ABab)a(ABab)B$	$[aa]^2 = 1$
	b^3	$b(bbb)B$	$1 = 1$
	$ABab$	$(ABab)$	$1 = 1$
4	a^4	$b(BAba)A(BAba)ab(BAba)$ $A(BAba)a[AA]BB(aaaa)$ $b(BAba)A(BAba)ab(BAba)$ $A(BAba)a[AA]BB(aaaa)$	$[AA]^2 = 1$
	b^3	$bb(bbb)BB$	$1 = 1$
	$ABab$	$b(BAba)b(BAba)A(BBB)$ $a(bbb)BB$	$1 = 1$
5	a^4	$ab[aa]A(ABab)a(ABab)[aa]A$ $(ABab)a(ABab)BA$	$[aa]^2 = 1$
	b^3	$ab(BAba)A(bbb)a(ABab)BA$	$1 = 1$
	$ABab$	$ab(BAba)A(BAba)a[AA]B$ $(BAba)A(BAba)ab(BAba)$ $A(BAba)a[AA]BB(aaaa)b$ $(BAba)A$	$1 = 1$
6	a^4	$b(BAba)ab(BAba)A(BAba)a$ $[AA]BB(aaaa)b(BAba)A$ $(BAba)ab(BAba)A(BAba)a$ $[AA]BB(aaaa)b(BAba)AB$	$[AA]^2 = 1$
	b^3	$bab(BAba)A(bbb)a(ABab)BAB$	$1 = 1$
	$ABab$	$ba(ABab)B(AAAA)bb[aa]A$ $(ABab)a(ABab)BA(ABab)$ $a(ABab)b(BBB)[aa]A(bbb)$ $a(ABab)BAB$	$[aa]^2 = 1$

Therefore, using $h = a^2$, the subgroup presentation is $\langle h | h^2 \rangle$.

Having thus realised that the Modified Todd-Coxeter method for determining subgroup presentations in terms of the original subgroup generators could be simulated using PEACE, we set about to make additions to the program to give PEACE this functionality. Presentations can be judged in terms of length, efficiency, ease of computability or any other desirable trait. The built-in Modified Todd-Coxeter method in GAP uses the Felsch strategy for coset definitions and so does not allow for experimentation in determining 'better' subgroup presentations. Different proof tables are obtained from different definition sequences, and as PEACE uses an ACE-based enumerator, which controls the resulting definition sequence, adding this new functionality to the PEACE program would allow for such experimentation in the hopes of producing various presentations of a subgroup.

2.3 Additions to PEACE

The version of PEACE for which we made our modifications and additions, to allow for the formation of subgroup presentations using the Modified Todd-Coxeter algorithm, was version 1.1. Our idea was that, by experimenting with different enumerations and definition sequences, we might be able to form different and, potentially, better such presentations.

PEACE was designed with the intention of having the ability to work alongside the GAP package, Interactive Todd Coxeter (ITC) [13], a program that allows the user to interact with an enumeration of a subgroup of a finitely presented group, executing single steps using a graphics surface, and thus, letting the user see exactly what is happening. Definition sequences can be input to and output from ITC, and the PEACE commands *ds ip* and *ds op* were added to allow for these sequences to be created or modified in either PEACE or ITC and passed back and forth between the two programs.

In this version of PEACE, however, while the option *ds op* had been added to allow for a definition sequence to be output in various formats to a file or to the screen, the implementation of the option *ds ip* had not been completed, and the use of this command in PEACE resulted solely in the production of the message, "** The ds ip feature has not been (fully) implemented yet". Therefore, our first addition to PEACE was the completion of the functions needed for this option.

The *ds ip* option invokes a call to *al2_readds*, which parses in a comma separated definition sequence either from a file or from standard user input. This definition sequence is stored in two arrays, where, if the coset number i is defined as $i = jx$, then the entry at index $i - 1$ of one contains the coset number j and that of the other, the generator letter x. The coset table is then set up and initialised as for an enumeration, except the definition sequence is entered into the last two auxiliary tables. Each definition is saved in the coset table and pushed onto the deduction stack. The subgroup generators are then scanned from coset 1 and the cosets in the table are processed against the relators by a call to *procdefn* for each coset. This function determines and processes further deductions and coincidences to fill the table. The validity of the coset table is then checked with *chkct*, testing for any holes in the subgroup generator and relator scans.

Only complete definition sequences are accepted with the PEACE command *ds ip*. If the coset table formed using *ds ip* is not valid and there are holes found in the scans of *chkct*, then the PEACE run is aborted. Thus, another user command was added to PEACE to allow for partial definition sequences. *ds ipp* behaves similarly to *ds ip* except, rather than checking the table after processing the definitions, the table is completed using the function *al1_start*, which resumes the enumeration using the current definition strategy, similarly to the *continue* PEACE command.

To modify PEACE for the Modified Todd-Coxeter algorithm of determining subgroup presentations, the keywords, *mt, pr mt, rewrite* and *presentation*, were added. It would have been possible to form the subgroup presentation from a proof table, removing any relators from the resultant proof words of the subgroup generators and relators to find the equivalent product of subgroup generators for a new subgroup relator. Additional functionality would then only have been needed to extract the proof words of the relators for coset numbers other than 1. However, from Example 2.5, we can see that the extracted proof words of even a very simple case can grow quite long. It was desired to be able to use the modified PEACE program to find subgroup presentations for much larger and more complicated groups and subgroups and so, the command *mt* was added to form a new modified table.

The function *puce_mt* produces the modified table, which has the exact same structure as that of a proof table. This function is based on the proof table version, *puce_pt*, making calls to *al0_apply* and *al0_dedn* to use the saved definition sequence and build the table. The first step of *puce_mt*, however, is to set the new global variable *mtbuild* to true. The words in each element of the lists of a table entry are identical to those that would be in the proof table, except without any relators, so rather than introducing new functions for each of the functions, *al0_apply* and *al0_dedn*, as well as the proof word and coincidence building functions, *ptbld1, ptbld2* and *al0_cols12*, these functions were modified slightly so relators are omitted from the produced words when the *mtbuild* flag is true. Also, when the flag is true and h_i is the i-th subgroup generator as ordered by PEACE, then where $[h_i]$ or $[h_i^{-1}]$ would appear in a word in the proof table, the modified table uses the notation $[\_x\_i]$ and $[\_X\_i]$, respectively, in the corresponding word. After the modified table is completed, *mtbuild* is reset to false. The command *pr mt* outputs the formulated modified table.

For any coset other than the subgroup, if the usual method was employed for extracting the proof word of a relator from the table, however, a conjugated product of subgroup generators would be produced, rather than the desired unconjugated product. The new reduction function *mtcred* was then implemented, based on the reduction function for the extraction of a proof word *pwred*, but changed so that, as well as removing any strings $x^{-1}x$ from the modified proof words, a word with the form xyx^{-1} was reduced to y for strings x and y.

The command *rewrite* was added as a modified table equivalent to the *prove* and *acert/cert* input commands for the proof table. This command takes in a word h, and if the initial trace finds that it is, in fact, a subgroup element, extracts the modified proof word from the modified table. This word is equivalent to h and written as a product of subgroup generators, using the new notation of $[\_x\_i]$ for the i-th subgroup generator.

The last new command implemented for PEACE was *presentation*. Our aim for this enhanced PEACE program was to incorporate it into a GAP package based on the one formed for ACE. This package acts as an interface to the C program, interacting with ACE through input and output streams. Thus, the *presentation* command does not produce the actual subgroup presentation, but extracts the modified proof word from the table for each subgroup generator and relator for coset 1 and for each relator for all other non-redundant cosets. Thus, it lists all the necessary subgroup relators for the presentation, which could easily be read in by the GAP interface and turned into a formal presentation.

Example 2.6 The Fibonacci group $F(2,5)$ [9], defined by the presentation

$$\langle a, b, c, d, e | abc^{-1}, bcd^{-1}, cde^{-1}, dea^{-1}, eab^{-1} \rangle,$$

has been shown to be isomorphic to C_{11}, the cyclic group of order 11 [10]. Of course, as $[F(2,5) : \langle a \rangle] = 1$, then a must generate the entire group and have order 11.

```
PEACE 1.100
==============================
gr:abcde;
rel:abC,bcD,cdE,deA,eaB;
gen:a;
start;
INDEX = 1 (a=1 r=1 h=5 n=5; l=4 c=0.00; m=4 t=4)
mt;
#- Modified Todd-Coxeter Table build ——
Initialising the CT/MT ...
Filling the CT/MT ...
Checking the CT/MT ...
CPU=0.00
#-----------------------------
pres;
From subgroup generators:
a = [_x_1]
```

From relators:
Coset #:1
abC = [_x_1][_x_1][_x_1][_x_1][_x_1][_x_1][_x_1][_x_1][_x_1][_x_1][_x_1]
bcD =
cdE = [_X_1][_X_1][_X_1][_X_1][_X_1][_X_1][_X_1][_X_1][_X_1][_X_1][_X_1]
deA =
eaB =
#——————————————-

Thus, we have the subgroup presentation $\langle x_1 | x_1^{11} \rangle$.

Example 2.7 For a larger example, the group $A_6 = PSL(2,9)$ can be presented as

$$\langle a, b | a^2, b^4, (ab)^5, (ab^2)^5 \rangle.$$

Here, $\langle a, a^b \rangle$ is a Sylow 2-subgroup, and using the modified PEACE program, we obtain:

PEACE 1.100
==============================
gr:ab;
rel:a2,b4,(ab)5,(ab2)5;
gen:a,Bab;
hard;
start;
INDEX = 45 (a=45 r=1 h=50 n=50; l=4 c=0.00; m=45 t=49)
mt;
#– Modified Todd-Coxeter Table build ——
Initialising the CT/MT ...
Filling the CT/MT ...
Checking the CT/MT ...
CPU=0.00
#——————————————-
pres;

PEACE then outputs the resulting subgroup relators. Where $a =$ [_x_1] and $Bab =$ [_x_2], the non-trivial subgroup relators given by PEACE are:

Coset #	Relator	Subgroup Relator
1	a^2	[_x_1][_x_1]
2	a^2	[_x_2][_x_2]
11	b^4	[_X_1][_X_1]
12	b^4	[_X_1][_X_1]
21	b^4	[_X_2][_X_2]
22	b^4	[_X_2][_X_2]
26	$(ab)^5$	[_x_1][_x_2][_x_1][_x_2][_x_1][_x_2][_X_1][_X_2]
33	$(ab)^5$	[_x_1][_x_2][_x_1][_x_2][_x_1][_x_2][_X_1][_X_2]
39	a^2	[_x_1][_x_2][_x_1][_x_2][_X_1][_X_2][_X_1][_x_2]
		[_x_1][_X_2][_X_1][_x_2][_x_1][_X_2][_X_1][_X_2]
42	a^2	[_x_2][_x_2]
43	$(ab)^5$	[_x_1][_x_2][_x_1][_x_2][_x_1][_x_2][_X_1][_X_2]
44	a^2	[_x_1][_x_1]
45	a^2	[_x_1][_x_2][_x_1][_x_2][_X_1][_X_2][_X_1][_x_2]
		[_x_1][_X_2][_X_1][_x_2][_x_1][_X_2][_X_1][_X_2]
47	$(ab)^5$	[_x_1][_x_2][_x_1][_x_2][_X_1][_X_2][_x_1][_x_2]
48	a^2	[_x_2][_x_1][_x_2][_X_1][_X_2][_x_1][_x_2][_X_1]
		[_X_2][_x_1][_x_2][_x_1][_x_2][_x_1][_x_2][_X_1]
		[_X_2][_x_1][_x_2][_X_1][_X_2][_x_1][_x_2][_x_1]
	$(ab)^5$	[_x_2][_x_1][_x_2][_X_1][_X_2][_x_1][_x_2][_x_1]
49	b^4	[_X_1][_X_2][_X_1][_X_2][_X_1][_X_2][_X_1][_X_2]

As $x_1 = x_1^{-1}$ and $x_2 = x_2^{-1}$, the set of relators is then $\{x_1^2, x_2^2, (x_1x_2)^4\}$ and the subgroup presentation is

$$\langle x_1, x_2 | x_1^2, x_2^2, (x_1x_2)^4 \rangle.$$

2.4 The PEACE GAP package

From our modified version of PEACE, a GAP package was created, based on the ACE GAP package. The GAP code acted as an interface to the C program through input and output streams, providing functions to perform tasks by writing commands and options to the C program and reading and interpreting the resultant output. As well as the PEACE equivalents for most of the functions of ACE, the package was augmented for the various procedures of the PEACE C program to contain interactive and non-interactive functions, such as *PEACEGenerateProofTable*, *PEACEGenerateModifiedTable*, *PEACEProve*, *PEACEProofCertificate*, *PEACEProof*, *PEACEProofNoStart*, *PEACEGeneratePresentation*, *PEACESubgroupPresentation* and *PEACESubgroupPresentationNoStart*.

The main driver of the Modified Todd-Coxeter algorithm in GAP is *AugmentedCosetTableMtc*, which outputs a data structure for the augmented coset table containing secondary generators and a tree from which these can be converted back into products of primary generators. Implementing a PEACE equivalent would involve creating a new table in GAP from the modified table by expanding each $_\alpha x _\beta$, where for non-redundant coset numbers α and β and generator or generator inverse x, the entry of the coset table at row α and column corresponding to x is β. Then, a set of secondary generators would need to be introduced to produce a table of the correct structure. Our main goal, however, was to use PEACE to produce the subgroup presentations, rather than GAP, which builds subgroup presentations using the Modified Todd-Coxeter method by producing this augmented table and then employing a rewriting process to generate the new subgroup relators. We thus decided it was more beneficial to first implement a PEACE equivalent of the GAP function *PresentationSubgroupMtc*, so that PEACE was used entirely to produce the subgroup presentation.

PEACEPresentationSubgroupMtc takes in, as input, a finitely presented group G, a subgroup $H \leq G$ and, optionally, the string to be given as the subgroup generator name in the produced presentation. PEACE strategy options and styles can also specified for use during and after the enumeration by being either passed as options in the function call or pushed onto the option stack before *PEACEPresentationSubgroupMtc* is invoked. The function *PEACESubgroupPresentation* is then called to create a new PEACE session, from which *PEACEStart*, *PEACEGenerateModifiedTable* and *PEACE-GeneratePresentation* are employed to perform the enumeration, generate the modified table and prompt PEACE to output the subgroup relators. *PEACEGeneratePresentation* then reads the subgroup relators into GAP, creating the set of elements to be used as the relators of the presentation, which is returned to *PEACESubgroupPresentation*.

As shown in Example 2.7, the relators may appear numerous times in the output and one relator may also appear as a substring of another. To reduce the number of unnecessary relators and the length of some relators in the new subgroup presentation, *PEACEGeneratePresentation* calls the GAP function *SimplifyPresentation*, which searches for relator subwords in each relator of the presentation and reduces the number and length of the relators. Thus, *PEACEPresentationSubgroupMtc* outputs the presentation produced by PEACE, where the relators have been reduced by Tietze transformations.

The GAP enumerator is supplanted by the ACE enumerator when the assignment

$$TCENUM := ACETCENUM;$$

is made. Using the PEACE package, the similar assignment

$$TCENUM := PEACETCENUM;$$

causes *PEACECosetTableFromGensAndRels* to be employed whenever a call is made to *CosetTableFromGensAndRels*. This results because $TCENUM$ is a data record with member attribute *CosetTableFromGensAndRels*, and both $ACETCENUM$ and $PEACETCENUM$ are similar records with the attribute *CosetTableFromGensAndRels* assigned to be *ACECosetTableFrom-GensAndRels* and *PEACECosetTableFromGensAndRels*, respectively. Supplanting the GAP function *PresentationSubgroupMtc*, therefore, would require $PEACETCENUM$ to contain a new member attribute *Presentation-SubgroupMtc:=PEACEPresentationSubgroupMtc*. The addition of the record element *PresentationSubgroupMtc* would also be required in the internal data record $TCENUM$ of GAP to allow this function to be overwritten.

2.5 Results

In order to test our modified version of PEACE against GAP, a script was written to run our new function *PEACEPresentationSubgroupMtc* 100 times on a specific group and subgroup with different, randomly generated style option values. A presentation for each of the five shortest resulting total relator lengths was then logged to a file. The script also called the GAP version of this function, so the PEACE outputs could be compared.

The group presentations and subgroup generating sets used in our initial trials of PEACE were obtained from the Ph.D. thesis of Ali-Reza Jamali [23]. Where PEACE produced a presentation with different total relator length than that of GAP, to check the results were accurate and defined the same group, the function *IsomorphismGroups* was used to show that the two groups defined by the differing presentations were isomorphic.

Example 2.8

$$A_5 \cong PSL(2,5) \cong PSL(2,4) \cong \langle a, b | a^2, b^3, (ab)^5 \rangle$$

- Taking the subgroup $\langle a, [b,a]^2 b^{-1} \rangle$, which is a Sylow 2-subgroup, GAP produced a presentation with 2 generators and 3 relators of total length 8. In each of 100 runs of PEACE using randomly generated style options, a presentation of the same length and generator and relator set sizes was produced.

- GAP returned a presentation for the Sylow 3-subgroup $\langle b \rangle$ having 1 generator and 1 relator of length 3. PEACE produced a presentation with the same characteristics for each of its 100 runs.

- For the Sylow 5-subgroup $\langle ab \rangle$, both GAP and PEACE output presentations with 1 generator and 1 relator of length 5.

- For the three maximal subgroups, $A_4 \cong \langle a^b, b^a \rangle$, $D_{10} \cong \langle a^{ba}, bab \rangle$ and $S_3 \cong \langle a, bab^{-1}(ab)^2 \rangle$, both GAP and PEACE produced similar presentations, one with 2 generators and 3 relators of total length 11 for A_4 and D_{10} and one with 2 generators and 3 relators of total length 9 for S_3.

Example 2.9

$$PSL(2,7) \cong PSL(3,2) \cong \langle a, b | a^2, b^3, (ab)^7, [a,b]^4 \rangle$$

- For the Sylow 2-subgroup $\langle a, a^b \rangle$, each of the 100 runs of PEACE produced a presentation with 2 generators and 3 relators of length 12, similarly to GAP.
- The Sylow 3-subgroup $\langle b \rangle$ produced the same result, as both PEACE and GAP returned presentations with 1 generator and 1 relator of length 3.
- Likewise for the Sylow 7-subgroup $\langle ab \rangle$, the PEACE output was comparable to that of GAP, with presentations made up of a single generator and relator with length 7.
- Both generating sets for the maximal subgroup S_4, namely $\{a, b^{ab}\}$ and $\{a, b^{ab^{-1}}\}$, resulted in comparable presentations from PEACE and GAP, creating presentations with 2 generators and 3 relators of total length 13.
- Finally, for the maximal subgroup $7:3$ given by $\langle b^a, b^{ab} \rangle$, GAP produced a presentation with 2 generators and 3 relators of total length 12. For the 100 PEACE runs, two different presentations were created. A presentation with total length 12 appeared 57 times, while the remaining 43 runs resulted in a presentation with total length 18.

The 2 previous examples involved quite small groups and subgroups and were used as a test that the output of PEACE was accurate. In these cases, *PEACEPresentationMtc* produced comparable results to that of the GAP version of this function. When we moved on to larger groups, such as A_6, $PSL(2,8)$ and then $PSL(2,11)$, we began to see more variable results.

Example 2.10

$$A_6 \cong PSL(2,9) \cong \langle a, b | a^2, b^4, (ab)^5, (ab^2)^5 \rangle$$

- Both PEACE and GAP produced a presentation with 2 generators and 3 relators of total length 12 for the Sylow 2-subgroup $\langle a, a^b \rangle$.

- Using the Sylow 3-subgroup $\langle ab^{-1}abab^2, bab^{-1}(ab)^2 \rangle$, GAP produced a presentation with 2 generators and 3 relators of total length 10. Likewise, each of the 100 PEACE runs output the same presentation for the subgroup.

- A 1-generator, 1-relator presentation with relator length 5 was produced with both the PEACE and GAP functions for the Sylow 5-subgroup $\langle ab \rangle$.

- While, for the maximal subgroup $A_5 \cong \langle a, ab^2ab^{-1}ab \rangle$, GAP produced a presentation with 2 generators and 3 relators of total length 15, the simplified presentations output from PEACE for the 100 runs included 43 with total relator length 15, 17 of length 41, 28 of length 61 and 12 of length 93.

- A_5 can also be generated by the set $\{a, abab^{-1}ab^2\}$, and the presentation formed by GAP for this subgroup had 2 generators and 4 relators of total length 45, which simplified to a presentation with 2 generators and 3 relators of total length 15. The presentations for A_5 given by PEACE included 24 of length 15, 42 of length 41, 26 of length 61 and 8 of total relator length 93.

- For the maximal subgroup $3^2 : 4 \cong \langle a^b, b^a \rangle$, the GAP function gave a subgroup presentation with 2 generators and 3 relators of total length

17. Of the 100 PEACE runs, 5 of the resultant subgroup presentations had length 17 and 95 had length 23.

- PEACE was able to produce a subgroup presentation with relator length smaller than the simplified presentation given by GAP for the maximal subgroup, $S_4 \cong \langle a, bab(ab^2)^2 \rangle$. The presentation returned by GAP has 2 generators and 4 relators of total length 33, simplifying to a presentation with 2 generators and 4 relators of total length 21. While PEACE produced a presentation with length 21 for 21 of the 100 runs, it also constructed a presentation with length 13 for 79 runs. For one such instance, the presentation was $\langle h_1, h_2 | h_1^2, h_2^3, h_1h_2^{-1}h_1h_2^{-1}h_1h_2^{-1}h_1h_2^{-1} \rangle$, and, using the GAP function *IsomorphismGroups*, we were assured that the group formed from this presentation was the same as that of the presentation given by GAP. Alternatively, one could rewrite this presentation as $\langle h_1, h_3 | h_1^2, h_3^3, (h_1h_3)^4 \rangle$, where $h_3 = h_2^{-1}$, which is a standard presentation for S_4.

- S_4 can also be generated by the set $\{a, (b^2a)^2bab\}$, and for this subgroup, the presentation given by GAP was one with 2 generators and 3 relators of total length 13. 83 runs of PEACE produced a presentation with the same relator length. There were also 15 occurrences of a presentation with length 21 and 2 with length 33.

Example 2.11

$$PSL(2,8) \cong SL(2,8) \cong \langle a, b | a^2, b^3, (ab)^9, ((ab)^3(ab^{-1})^4)^2 \rangle$$

- For the maximal subgroup $2^3 : 7 \cong \langle a, bab^{-1}(ab)^2 \rangle$, GAP output a presentation with 2 generators and 4 relators of total length 26, which could not be simplified further by the function *SimplifyPresentation*. Of the 100 PEACE runs, however, 19 produced a presentation with length 18, 1 of length 21 and 80 of length 26. One of the presentations of length 18 was $\langle h_1, h_2 | h_1^2, h_2^7, h_2^{-1}h_1h_2^{-2}h_1h_2^3h_1 \rangle$ and was shown to define the same group as that produced by GAP through the use of the function *IsomorphismGroups*.

- For the maximal subgroup $D_{18} \cong \langle a, a^{bab} \rangle$, both GAP and PEACE produced presentations with 2 generators and 3 relators of total length 22.

Example 2.12

$$PSL(2,11) \cong \langle a, b | a^2, b^3, (ab)^{11}, ((ab)^3(ab^{-1})^3)^2 \rangle$$

$PSL(2,11)$ has order 660 and, even using the Sylow 2-subgroup $\langle a, a^{(ba)^2b} \rangle$, 100 runs of PEACE could not be completed for this case. The process was extremely slow and after eight runs, the C program halted in the middle of extracting a proof for a relator, leaving GAP waiting for output that would never arrive. However, in the eight completed PEACE runs, each produced a presentation with total length 8, similarly to the GAP function, *PresentationSubgroupMtc*.

As indicated, the PEACE package produced comparable results to the GAP function for formulating subgroup presentations with the Modified Todd-Coxeter algorithm. In many cases, by experimenting with the coset definition style, PEACE returned various different presentations for a subgroup, and in a few instances, produced presentations with shorter total relator length than GAP. Thus, it was shown that PEACE could be used for experimentation with coset definition styles and strategies with the Modified Todd-Coxeter algorithm for finding presentations of subgroups. However, even for relatively small cases, such as the group $PSL(2,11)$ with order 660, the extractions of proof words for each relator produced intermediate proof words that were extremely long, too long for the C program to manage. Larger groups caused slower proceedings and more occurrences of failed runs due to insufficient memory. Thus, as we wanted to be able to experiment with much larger groups, where the subgroup presentations were more complex, PEACE was deemed an impractical tool.

Chapter 3

From Proofwords to Proofs

3.1 Proof Trees

As we have seen, once PEACE produces a proof word for an element h of the group, it has proved that h is also an element of the subgroup. This can be easily verified as the proof word is a product of subgroup generators and conjugated relators and, removing all brackets, freely reduces to h. While the proof word is itself a proof, it does not show any step by step reasoning usually provided in a mathematical proof. Oftentimes, similar steps and reasonings to those of an established proof can be used in the proofs of other cases or changed to make generalisations for objects with similar characteristics. We wondered whether, given a proof word, we could use it to prove similar cases for other group and subgroup pairs, and we, thus, attempted to implement a procedure converting a proof word into such a step by step logical proof to aid in this process.

We found that producing a step by step proof from a PEACE proof certificate is a matter of recursively dividing the proof word into disjoint products. If p is the proof word and q is obtained from p by removing the relators and reducing, then clearly, p and q represent the same element and $pq^{-1} = 1$. Here, q is merely h written as a product of the subgroup generators.

Let us consider the word w that is obtained from pq^{-1} where we have removed the square brackets indicating subgroup generators and then reduced the resulting word to obtain a product of group generators and relators.

Lemma 3.1 Proving $w = 1$ is equivalent to providing a proof of $p = q$.

Proof. For each subgroup generator that had appeared in p, the inverse is found in q^{-1}. Consider the first such generator of q^{-1}. By the construction of q^{-1}, it is the inverse of the last subgroup generator of p. Thus, the subword of pq^{-1} between the generator and its inverse is a product of conjugated relators and must be trivial. Therefore, the generator acts as a conjugator of this trivial subword, and this conjugated subword is also trivial. Continuing inductively, each subgroup generator of q^{-1} acts as a conjugator for the subword of pq^{-1} found between itself and its inverse, producing yet another trivial subword.

We need now to check that w, too, has this form. As it has been reduced after removing the square brackets surrounding the subgroup generators, it may be the case that all or part of a subgroup generator has disappeared in the process. In this instance, however, consider the subword between and including this partial subgroup generator a and its inverse a^{-1} in the unreduced word. The part of this word that disappears with the subgroup generator must have the form a^{-1} and also be part of a conjugate of a relator. Thus, similarly to the a^{-1} that had been the inverse of the original partial subgroup generator a, it must be such that a lies within this subword on the other side of the relator. After having reduced, either a and a^{-1} are adjacent and also disappear in the reduction, or both a and a^{-1} are in the reduced word, conjugating the subword between them. Thus, removing the relators in w, we would then be left with the identity, and, removing the square brackets, w is a valid proof word itself: a proof word for the identity. Proving $w = 1$ is equivalent to providing a proof of $p = q$. □

Example 3.2 The group

$$F(2,5) = \langle a, b, c, d, e | abc^{-1}, bcd^{-1}, cde^{-1}, dea^{-1}, eab^{-1} \rangle$$

is isomorphic to C_{11}. The subgroup $\langle a \rangle$ is the entire group and so, $b \in \langle a \rangle$.

For the element b, PEACE produces the proof certificate

#– PEACE 1.100 proof certificate ———-

* Group Generators

$abcde$

* Group Relators

abC

bcD

cdE

deA

eaB

* Subgroup Generators

a

* Word

b

* Proof Word

$d(aED)(dCB)(bAE)D(deA)[a][a]c(eDC)C(cBA)[a](bcD)d$
$(dCB)(bAE)D(deA)[a][a](cBA)[a](bAE)(eDC)[A][A](aED)$
$d(eaB)(bcD)D(dCB)[A](abC)c(cdE)(eaB)(bcD)C(cdE)$
$(eaB)[A](abC)[A][A](aED)d(eaB)(bcD)D(dCB)[A](abC)$
$c(cdE)C[A][A](aED)d(eaB)(bcD)(deA)D(dCB)[A](abC)$
$[A][A](aED)d(eaB)(bcD)D(dCB)[A](abC)c(cdE)C[A][A]$
$(aED)d(eaB)(bcD)(deA)(bAE)D(deA)[a][a]$

#——————————————-

Where p is the proof word, then removing relators and reducing, q becomes

$$[A][A][A][A][A][A][A],$$

and the adjusted proof word w, obtained from pq^{-1} by removing any square brackets, is then

$$
\begin{aligned}
w \quad = \quad & d(aED)(dCB)(bAE)D(deA)aac(eDC)C(cBA)a(bcD)d \\
& (dCB)(bAE)D(deA)aa(cBA)a(bAE)(eDC)AA(aED) \\
& d(eaB)(bcD)D(dCB)A(abC)c(cdE)(eaB)(bcD)C \\
& (cdE)(eaB)A(abC)AA(aED)d(eaB)(bcD)D(dCB)A \\
& (abC)c(cdE)CAA(aED)d(eaB)(bcD)(deA)D(dCB)A \\
& (abC)AA(aED)d(eaB)(bcD)D(dCB)A(abC)c(cdE)CA \\
& A(aED)d(eaB)(bcD)(deA)(bAE)D(deA)aaaaaaaaa
\end{aligned}
$$

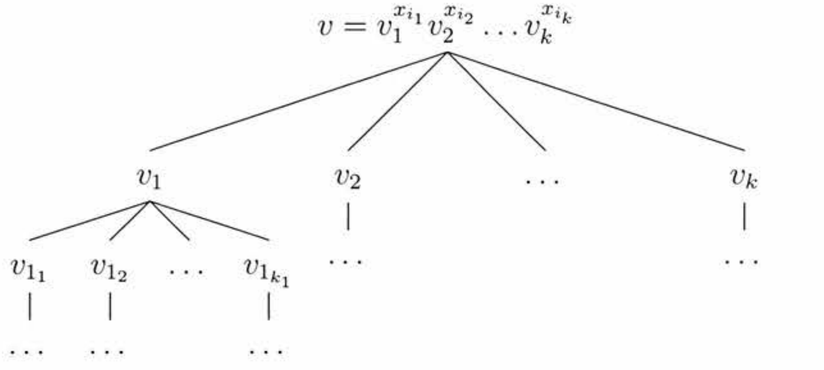
Freely reducing, w becomes ba^7, while removing the relators, w reduces to 1.

Given that w is formed from products of conjugates of trivial elements, which can be further decomposed into products of conjugates of trivial elements, then w can be broken up into disjoint products, such that

$$w = w_1^{x_1} w_2^{x_2} \dots w_n^{x_n},$$

where x_i is a word over the group generators and conjugates w_i. Each w_i is either a relator, an inverse relator or, like w, can be broken down further into disjoint conjugated products. Thus, the proof word w can be recursively broken down until all such products are relators.

A rooted tree can then be created with w as the root and each vertex, a subword of w. For a vertex, v, where we would write $v = v_1^{x_{i_1}} v_2^{x_{i_2}} \dots v_k^{x_{i_k}}$ with each x_{i_j} being a word over the group generators, then the children of v are the words $v_1, v_2, \dots, v_k$ such that v_1 is the left-most child of v.



The leaves of the tree are then relators or their inverses and each vertex in the tree is equivalent to the group identity. We are now in a position to build up our step-by-step proof.

A subtree can be viewed as a proof for the word r at the root, where the last line of this proof is $1 = r$. Beginning with one branch in the tree, consider the leaf vertex v_j and its parent, $v = v_1^{x_{i_1}} \dots v_{j-1}^{x_{i_{j-1}}} v_j^{x_{i_j}} v_{j+1}^{x_{i_{j+1}}} \dots v_k^{x_{i_k}}$. As v_j is a leaf, it must be a relator and so, is trivial. Our proof begins with the lines

$$\begin{aligned} 1 &= v_j \\ &= x_{i_j}^{-1} v_j x_{i_j} \end{aligned}$$

where each line has been reduced.

Using the subtrees rooted at every v_n for $n \in \{1, \dots, j-1\} \cup \{j+1, \dots k\}$, we can form the proofs for each of $1 = v_n$ and extend them to obtain $1 = x_{i_n}^{-1} v_n x_{i_n}$. Now, to obtain $1 = v$ in our proof, we need sucessively apply each of the proofs of $1 = v_n^{x_{i_n}}$ for integers n from $j - 1$ down to 1 and then for integers n from $j + 1$ to k.

When considering the word $v_n^{x_{i_n}}$ for $n < j$, from the proof $1 = x_{i_n}^{-1} v_n x_{i_n}$, we form the lemma $a = b$ where b^{-1} is the subword of $v_n^{x_{i_n}}$ of maximal length such that

$$x_{i_n}^{-1} v_n x_{i_n} = ab^{-1},$$

and the last line of our main proof is $1 = bw'$. Thus, by substituting a for b, the next line of our proof would be

$$1 = aw'.$$

For $n > j$, from the proof $1 = x_{i_n}^{-1} v_n x_{i_n}$, we form the lemma $c = d$ where c^{-1} is the subword of maximal length such that

$$x_{i_n}^{-1} v_n x_{i_n} = c^{-1} d,$$

and the last line of our main proof is $1 = w'c$. Thus, by substituting d for c, the next line of our proof is

$$1 = w'd.$$

Each substitution is equivalent to multiplying either on the right or left by $x_{i_n}^{-1} v_n x_{i_n}$, thus, iteratively applying the substitutions obtained from these lemmas for n from $j-1$ down to 1 and then for n from $j+1$ to k, we end up with a proof for

$$1 = v_1^{x_{i_1}} \dots v_{j-1}^{x_{i_{j-1}}} v_j^{x_{i_j}} v_{j+1}^{x_{i_{j+1}}} \dots v_k^{x_{i_k}} = v.$$

Example 3.3 For a simple example, consider the group $F^{-1,1,3}$, presented by

$$F^{-1,1,3} = \langle r, s | r^2, rs^{-1}rs^1rs^3 \rangle,$$

over the subgroup $\langle rsr \rangle$. For the element s^6, PEACE produces the proofword

$$[RSR](R^2)[rsr](R^2)(rSrsrs^3)S^3(R^2)(rSrsrs^3)s^3,$$

which shows $s^6 = 1$, and of course, $s^6 \in \langle rsr \rangle$. Thus, our adjusted proof word is simply the original proof word having removed any square brackets:

$$r^{-1}s^{-1}r^{-1}(r^{-2})rsr(r^{-2})(rs^{-1}rsrs^3)s^{-3}(r^{-2})(rs^{-1}rsrs^3)s^3.$$

We can now divide the proofword up into disjoint products.

$$\begin{aligned} a &= r^{-1}s^{-1}r^{-1}(r^{-2})rsr \\ b &= (r^{-2})(rs^{-1}rsrs^3) \\ c &= s^{-3}(r^{-2})(rs^{-1}rsrs^3)s^3. \end{aligned}$$

Reducing further gives

$$\begin{aligned} a_1 &= r^{-2} \\ b_1 &= r^{-2} \\ b_2 &= rs^{-1}rsrs^3 \\ c_1 &= r^{-2} \\ c_2 &= rs^{-1}rsrs^3. \end{aligned}$$

Then, the proofword can be written as $(a_1)^{rsr}(b_1b_2)(c_1c_2)^{s^3}$, and our resulting tree structure is

$$r^{-1}s^{-1}r^{-1}(r^{-2})rsr(r^{-2})(rs^{-1}rsrs^3)s^{-3}(r^{-2})(rs^{-1}rsrs^3)s^3$$
$$= (\mathbf{a_1})^{\mathbf{rsr}}(\mathbf{b_1b_2})(\mathbf{c_1c_2})^{\mathbf{s^3}}$$

$$\begin{array}{ccc} r^{-2} & (r^{-2})(rs^{-1}rsrs^3) & (r^{-2})(rs^{-1}rsrs^3) \\ = \mathbf{a_1} & = (\mathbf{b_1})(\mathbf{b_2}) & = (\mathbf{c_1})(\mathbf{c_2}) \end{array}$$

$$\begin{array}{cccc} r^{-2} & rs^{-1}rsrs^3 & r^{-2} & rs^{-1}rsrs^3 \\ = \mathbf{b_1} & = \mathbf{b_2} & = \mathbf{c_1} & = \mathbf{c_2} \end{array}$$

If, in this example, we always use the leftmost child as the main branch of a subtree, then the first line of our proof is $a_1 = 1$, which we obtain because a_1 is a relator. We then need to find the lemmas corresponding to $(b_1)(b_2)$ and $(c_1)(c_2)$, which are obtained from the proofs constructed by the subtrees rooted at these elements, to apply them to $a_1 = 1$. Now, in these subtrees, the main branches are b_1 and c_1, respectively, and we require the lemmas corresponding to b_2 and c_2. These nodes are both leaves and so, are relators. Thus, we obtain $b_2 = 1$ and $c_2 = 1$ in the first line of the proofs of these lemmas. We need to find a subword w of b_1 so that $b_1 = w_1w$, $b_2 = w^{-1}w_2$ and b_1b_2 reduces to w_1w_2. Here as $b_1 = r^{-2}$ and $b_2 = rs^{-1}rsrs^3$, then $w = r^{-1}$, and the required lemma corresponding to b_2 is $r^{-1} = s^{-1}rsrs^3$. Similarly, the required lemma for c_2 is $r^{-1} = s^{-1}rsrs^3$. Thus, using this lemma and the relator $b_1 = c_1 = r^{-2}$, we can find the proofs of $b_1b_2 = c_1c_2 = r^{-1}s^{-1}rsrs^3 = 1$.

Again, as neither b_1b_2 nor c_1c_2 are the main branches of the tree, we need to convert the proofs, $b_1b_2 =$ and $c_1c_2 = 1$, into useful lemmas to apply in the main proof. The current line in our proof is $a_1 = 1$, but before we can use each of $b_1b_2 =$ and $c_1c_2 = 1$, we need to conjugate a_1 by rsr and reduce, thus resulting in the next line in our proof, $r^{-1}s^{-1}r^{-2}sr = 1$. Now, multiplying a_1^{rsr} by $b_1b_2 = r^{-1}s^{-1}rsrs^3$ on the right would result in $r^{-1}s^{-1}r^{-1}srs^3$ and so, the proof $b_1b_2 = 1$ needs to be converted to the lemma $r^{-1}sr = srs^3$. Using this, the next line in our proof is then $r^{-1}s^{-1}r^{-1}srs^3 = 1$. We need now to apply $(c_1c_2)^{s^3} = s^{-3}r^{-1}s^{-1}rsrs^6$ on the right, resulting in s^6. Here, our proof of $c_1c_2 = 1$ is converted to the necessary lemma by first conjugating by s^3 and then re-arranging the new relation to obtain $r^{-1}s^{-1}r^{-1}srs^3 = s^6$. Thus, the final line of our proof, corresponding to the proof of the root of the entire tree and obtained from this new lemma, would be $s^6 = 1$, as required.

The proof as well as the necessary and sometimes, very simple, lemmas formed from the tree are as follows:

Lemma 3.3.1 $r^{-1} = s^{-1}rsrs^3$

Proof

$$\begin{aligned} 1 &= rs^{-1}rsrs^3 && \text{from } b_2 \text{ or } c_2 \\ r^{-1} &= s^{-1}rsrs^3 \end{aligned}$$

Lemma 3.3.2 $r^{-1}sr = srs^3$

Proof

$$\begin{aligned} 1 &= r^{-1}.r^{-1} && \text{from } b_1 \\ &= r^{-1}s^{-1}rsrs^3 && \text{from Lemma 3.3.1} \\ r^{-1}sr &= srs^3 \end{aligned}$$

Lemma 3.3.3 $r^{-1}s^{-1}r^{-1}srs^3 = s^6$

Proof

$$\begin{aligned} 1 &= r^{-1}.r^{-1} && \text{from } c_1 \\ &= r^{-1}s^{-1}rsrs^3 && \text{from Lemma 3.3.1} \\ &= s^{-3}(r^{-1}s^{-1}rsrs^3)s^3 \\ &= s^{-3}r^{-1}s^{-1}rsrs^6 \\ s^6 &= r^{-1}s^{-1}r^{-1}srs^3 \end{aligned}$$

Lemma 3.3.1 corresponds to the leaves, b_2 and c_2, Lemma 3.3.2 corresponds to the subtree rooted at b_1b_2 and Lemma 3.3.3, to that of c_1c_2, extended for $(c_1c_2)^{s^3}$. Our proof is then

$$
\begin{aligned}
1 &= (r^{-2}) && \text{from } a_1 \\
&= r^{-1}s^{-1}r^{-1}(r^{-2})rsr \\
&= r^{-1}s^{-1}r^{-1}.r^{-1}sr \\
&= r^{-1}s^{-1}r^{-1}srs^{3} && \text{from Lemma 3.3.2} \\
&= s^{6} && \text{from Lemma 3.3.3}
\end{aligned}
$$

3.2 Lemma-based Proof Generating Program

From our method of obtaining these lemma-based proofs from PEACE proof words, we implemented code to automate this procedure. The main wrapper function for this procedure is *findProof*, which takes in both a proof word string and a filename to which the lemmas and step by step proof are output. As any necessary relators and subgroup generators will appear in the proof word and are indicated by their respective types of brackets, the function does not require any of the group generator, group relator or subgroup generator sets.

findDisjConj is employed to first break the proof word up into disjoint conjugates and place these words as vertices in a tree structure, beginning at the root and continually subdividing, considering one level of the tree at a time. The tree is then a list representing the successive levels in the tree, where each element is also a list, corresponding to the nodes in order from left to right. The tree is structured so that every branch has the same length. Thus, if a relator is obtained in an early step, then the corresponding branch is extended by a path of vertices, each with the relator as the corresponding word, until the branch is the same length as the others and the final list in the tree contains all of the leaves, or relators. Since extra brackets are added to surround each disjoint product of the word in a node, it is easy to determine the number of children required for each vertex when using this tree to construct the required lemmas and proofs.

Once *findDisjConj* has returned the tree containing the subdivided proof word, *findProofTree* builds up the required lemmas and the step by step proof. Each node is given a proof structure, containing a list of strings involved in the proof, a lemma number, a height number to indicate in which level of the tree it sits, as well as a list containing the numbers of the lemmas involved in the proof. Beginning at the bottom of the tree, the proof for each leaf node is created, with lemma number 0, height 0, an empty list of involved lemmas and a single element string list containing *"r_i=1"*, where r_i is the relator corresponding to this leaf. Working up towards the root of the tree, each level of the tree is processed in turn, generating the proofs of the nodes in that level. As the tree has been extended in parts so that each branch has the same length and the leaves all appear in this bottom level, then working upwards, not each node in the same level of the tree will be given the same height number. If the node contains only one relator, the proof of this node is simply the proof of its child, with the same height number, string elements, list of involved lemmas and lemma number.

The proof for each node is created from the proofs of its children. In an attempt to require fewer lemmas in our final proof, the child with the proof having the maximum height number is chosen as the main branch, and our new proof is given a height one greater than this. The lists of strings of the proofs for each of the children nodes are also given either one or two new string elements. These convert the proofs into the required lemmas, showing the re-arrangement of the trivial word $ab = 1$ into $a^{-1} = b$ to be used in the main proof. The extra string element is added if the trivial word needs to be conjugated before being re-arranged. Each of the lemma numbers of the children used in this proof is then added to the list of involved lemmas for the proof, where the number of the main branch is the first element, followed by those multiplied on the left and then those multiplied on the right. The lemma number for this node is then given a value accordingly. When the proof for the tree root has been determined, the process terminates.

Ignoring very trivial lemmas, such as those relators with lemma number 0 that have not been re-arranged, *findProof* writes the proofs in order of lemma number to the specified file. As such, the output is not very user friendly; the main proof is given in segments amongst the required lemmas, but one can determine this main proof by working backwards, using the list of involved lemmas at each step to determine the number of the main branch. Although the program contains recursive functions, a type which can be very expensive in terms of running time and algorithm complexity, this was not thought to be an issue as the internal processing of PEACE can produce long internal proof words and so, insufficient memory prevents extremely long proof words from being produced.

Example 3.4 The Klein group $K = \langle a, b | a^2, b^2, (ab)^2 \rangle$ has order 4. For the proof that K is abelian, we require $a^{-1}b^{-1}ab = 1$ and so, over the trivial subgroup, we can use PEACE to generate the proof word of $a^{-1}b^{-1}ab \in \langle 1 \rangle$. PEACE produces the word $A(B^2)a(A^2)(abab)$, freely reducing to $ABab$ and, having removed relators, to 1.

Original/Adjusted Proofword:

$A(B^2)a(A^2)(abab)$

Original/Adjusted Equation:

$ABab = 1$

Lemma #:

0 $abab = 1$

$A = bab$

1 $B^2 = 1$

$A(B^2)a = 1$

$AB^2a = 1$

2 $A.A = 1$

$Abab = 1$

$Ba = ab$

resulting from:[0]

3 $AB.Ba = 1$

$ABab = 1$

resulting from:[1, 2]

Example 3.5 For a more complicated example, the group E_1 is defined by the presentation

$$E_1 = \langle a, b, c | c^{-1}aca^{-2}, a^{-1}bab^{-2}, b^{-1}cbc^{-2} \rangle.$$

This group is actually trivial, although it is not obviously so, and E_1 is interesting because it also a possible counter-example to the Andrews-Curtis conjecture [1]. Higman [22] proved E_1 to be trivial by showing that one generator could be expressed in terms of the others and by then using a result involving derived groups. He manually proved $c = ba^{-4}b^{-1}a^2b$ to show this. Using PEACE, Havas and Ramsay [20] provided a proof word of the same, containing only eight relators and showing $c \in \langle a, b \rangle$. Here, we use this proof word to give a step by step proof of $c = ba^{-4}b^{-1}a^2b$, through $cb^{-1}a^{-2}ba^4b^{-1} = 1$. The output from our program, interpreted into lemmas and a main proof, is as follows.

Havas and Ramsay's Original Proofword:

$$(Cbc^2B)[b][A][A](a^2CAc)[A][A](a^2CAc)[B](bC^2Bc)$$
$$Cb(ca^2CA)(aB^2Ab)Bc(CacA^2)[a][a](Cbc^2B)[b]$$

Original Equation:

$$c = bA^4Ba^2b$$

Adjusted Equation:

$$cBA^2ba^4B = 1$$

Adjusted ProofWord:

$$(Cbc^2B)bA^2(a^2CAc)A^2(a^2CAc)B(bC^2Bc)Cb(ca^2CA)$$
$$(aB^2Ab)Bc(CacA^2)a^2(Cbc^2B)bBA^2ba^4B$$

Lemma 3.5.1 $a^{-1} = b^{-2}a^{-1}b$

Proof

$$\begin{array}{rcll} 1 & = & ab^{-2}a^{-1}b & \text{from } 2^{nd} \text{ relator} \\ a^{-1} & = & b^{-2}a^{-1}b & \end{array}$$

Lemma 3.5.2 $bc^{-1} = c^{-1}bc$

Proof

$$\begin{array}{rcll} 1 & = & bc^{-2}b^{-1}c & \text{from } 3^{rd} \text{ relator} \\ bc^{-1} & = & c^{-1}bc & \end{array}$$

Lemma 3.5.3 a) $a^{-1}c = ca^{-2}$ and b) $c^{-1}a = a^2c^{-1}$

Proof

$$\begin{aligned} 1 &= c^{-1}aca^{-2} \quad \text{from } 1^{st} \text{ relator} \\ a^{-1}c &= ca^{-2} \end{aligned}$$

Lemma 3.5.4 $b^{-1}ca^{-2} = c^2b^{-1}a^{-2}$

Proof

$$\begin{aligned} 1 &= c^{-1}bc^2b^{-1} && \text{from } 3^{rd} \text{ relator} \\ &= a^2(c^{-1}bc^2b^{-1})a^{-2} \\ &= a^2c^{-1}bc^2b^{-1}a^{-2} \\ b^{-1}ca^{-2} &= c^2b^{-1}a^{-2} \end{aligned}$$

Lemma 3.5.5 $bc^{-2}b^{-1}c = 1$

Proof

$$\begin{aligned} 1 &= c^{-1}bc^2b^{-1} && \text{from } 3^{rd} \text{ relator} \\ &= bc^{-2}b^{-1}c \end{aligned}$$

The proof is then

$$\begin{aligned} 1 &= ca^2c^{-1}a^{-1} && \text{from } 1^{st} \text{ relator} \\ &= ca^2c^{-1}.a^{-1} \\ &= ca^2c^{-1}b^{-2}a^{-1}b && \text{from Lemma 3.5.1} \\ &= c^{-1}b(ca^2c^{-1}b^{-2}a^{-1}b)b^{-1}c \\ &= c^{-1}bca^2c^{-1}b^{-2}a^{-1}c \\ &= c^{-1}bca^2c^{-1}b^{-2}.a^{-1}c \\ &= c^{-1}bca^2c^{-1}b^{-2}ca^{-2} && \text{from Lemma 3.5.3a} \\ &= c^{-1}bca^2c^{-1}b^{-1}.b^{-1}ca^{-2} \\ &= c^{-1}bca^2c^{-1}b^{-1}c^2b^{-1}a^{-2} && \text{from Lemma 3.5.4} \end{aligned}$$

$$
\begin{aligned}
&= c^{-1}bc.a^2c^{-1}b^{-1}c^2b^{-1}a^{-2} && \\
&= bc^{-1}a^2c^{-1}b^{-1}c^2b^{-1}a^{-2} && \text{from Lemma 3.5.2} \\
&= b^{-1}(bc^{-1}a^2c^{-1}b^{-1}c^2b^{-1}a^{-2})b && \\
&= c^{-1}a^2c^{-1}b^{-1}c^2b^{-1}a^{-2}b && \\
&= c^{-1}a.ac^{-1}b^{-1}c^2b^{-1}a^{-2}b && \\
&= a^2c^{-1}ac^{-1}b^{-1}c^2b^{-1}a^{-2}b && \text{from Lemma 3.5.3b} \\
&= a^{-2}(a^2c^{-1}ac^{-1}b^{-1}c^2b^{-1}a^{-2}b)a^2 && \\
&= c^{-1}ac^{-1}b^{-1}c^2b^{-1}a^{-2}ba^2 && \\
&= c^{-1}a.c^{-1}b^{-1}c^2b^{-1}a^{-2}ba^2 && \\
&= a^2c^{-2}b^{-1}c^2b^{-1}a^{-2}ba^2 && \text{from Lemma 3.5.3b} \\
&= ba^{-2}(a^2c^{-2}b^{-1}c^2b^{-1}a^{-2}ba^2)a^2b^{-1} && \\
&= bc^{-2}b^{-1}c^2b^{-1}a^{-2}ba^4b^{-1} && \\
&= bc^{-2}b^{-1}c.cb^{-1}a^{-2}ba^4b^{-1} && \text{from Lemma 3.5.5} \\
&= cb^{-1}a^{-2}ba^4b^{-1} &&
\end{aligned}
$$

The results we obtained from using PEACE along with our lemma-based proofs generated from proof words by our new program are contained in the following chapter.

Chapter 4

The $F^{a,b,c}$ Conjecture

4.1 Introduction

In 1966, at a conference held in Waterloo, Ontario, R. M. Foster, an electrical engineer, presented a census of symmetric trivalent graphs with up to 400 vertices. His work in this area had started in the 1920s, due to his interest in electrical networks and the use of symmetric graphs. The census was compiled largely by hand, with only one omission of order up to 402, and is now known as the Foster Census [14].

H. S. M. Coxeter had one of the few copies of this document and he, too, became interested in the subject. During Coxeter's research, while considering groups with Cayley graphs that are $0-$symmetric [11], he defined the finitely presented groups, $F^{a,b,c}$.

Where $a, b, c \in \mathbb{Z}$, the finitely presented group $F^{a,b,c}$ is defined as

$$F^{a,b,c} = \langle r, s | r^2, rs^a rs^b rs^c \rangle.$$

The $F^{a,b,c}$ groups fall in the class having a two-generator, two-relator presentation, and as known finite groups of this class were few, Campbell, Coxeter and Robertson began an investigation which led to 'the $F^{a,b,c}$ conjecture', published in 1977 [3]. In the work leading to the conjecture, the structure of $F^{a,b,c}$ was examined by considering the homomorphic image,

$$H^{a,b,c} = \langle r, s | r^2, s^{2n}, rs^a rs^b rs^c \rangle \quad \text{where } n = a + b + c.$$

Where $\theta : F^{a,b,c} \to H^{a,b,c}$ is the natural homomorphism, then θ is also an epimorphism. Thus, by the first isomorphism theorem, we have

$$F^{a,b,c}/ker\theta \cong H^{a,b,c}.$$

Campbell, Coxeter and Robertson were able to completely determine the structure of the groups $H^{a,b,c}$, and where $d = (a - b, b - c)$, they found that when $(a, b, c) = 1$, unless $n = 0$ or $(d, 6) = 6$, $H^{a,b,c}$ is a finite metabelian group. Also when $(a, b, c) = 1$, if $d \geq 6$ or $n = 0$, the groups $F^{a,b,c}$ are infinite. When $(a, b, c) = t \neq 1$, the groups $F^{a,b,c}$ and $H^{a,b,c}$ are infinite unless $H^{a/t,b/t,c/t}$ was abelian, in which case, $F^{a,b,c} \cong H^{a,b,c} \cong C_{2n}$. It was then left to determine the structure of the kernel of θ with $F^{a,b,c}$ for $d \leq 5$ and $(a, b, c) = 1$.

While all of the results used in [3] to determine the structure of $H^{a,b,c}$ are true, the proof of Lemma 3.3, stating that the derived group of $H^{a,b,c}$ is abelian when $(a, b, c) = 1$, is flawed. As the $F^{a,b,c}$ conjecture only completely determines groups of this type if the structure of $H^{a,b,c}$ is known, it is imperative that the required lemma holds. We thus give a revised proof for Lemma 3.3 of [3] in Appendix A.

In the following chapters, we will use the notation $x \sim y$ to refer to x commutes with y for two elements x and y.

The $F^{a,b,c}$ conjecture is as follows.

The $F^{a,b,c}$ Conjecture: (Campbell, Coxeter and Robertson [3, §12]) Suppose $(a, b, c) = 1$ with $n = a + b + c \neq 0$ and let

$$\theta : F^{a,b,c} \to H^{a,b,c}$$

be the natural homomorphism. Setting $N = ker\theta$, then

- $N = 1$ if $d = 1$,

- $N = 1$ if $d = 2$,
- $N \cong C_2$ if $d = 3$,
- $N \cong Q_8$ if $d = 4$, and
- $N \cong SL(2, 5)$ if $d = 5$.

The conjecture was proved true when $d = 1$ in [5], and an alternative proof can be found in Corollary 3.4 of [6]. Many special cases supporting the conjecture have been proved, as in [3], [6], [7], [27] and [28], and quite recently, a proof for $d = 5$ was given by Havas and Robertson [21], which also appears in Appendix B. The proof of the conjecture in the cases $d \in \{2, 3, 4\}$ is quite different in nature from $d = 5$, due to the fact that in the former cases, $(d, 6) \neq 1$. In this chapter, we shall outline the process from which we obtained proofs for these last three cases.

4.2 Using Lemma based PEACE proofs

Since its formulation in 1977, other than for some special cases, attempts at proving the $F^{a,b,c}$ conjecture had been unsuccessful by conventional means, and the cases $d \in \{2, 3, 4\}$ remained open. We began our research with groups of this type after testing our program for generating lemma based proofs from PEACE proofwords using a few small groups of the form, $F^{a,b,c}$, and found it to be a very useful tool.

A group, $F^{a,b,c}$ for $a, b, c \in \mathbb{Z}$ where $d = 2$, can be shown to be a supporting instance of the conjecture if it can be proved that $F^{a,b,c} \cong H^{a,b,c}$ or, equivalently, $s^{2n} = 1$. Thus, this would be done by finding the PEACE proofword of s^{2n} for the group $F^{a,b,c}$ over the trivial subgroup and, with our program, generating its corresponding step by step proof.

Our first attempts using PEACE and our proof generating program were for the element s^{2k+8} in the subgroup $\langle rsr \rangle$ of the group $F^{1,3,k}$, for $k = 3, 5, 7, 9$. All of these groups fall into the case $d = 2$, and, using our script, PEACE was run 1000 times with randomly generated variables and strategies. Our aim was to find the shortest proofwords, where length was measured by the number of relators appearing in the proofword. We used the subgroup $\langle rsr \rangle$ in an attempt to reduce the size of the proofwords, and therefore, the length and complexity of the resultant proofs. By running coset enumeration, it was easy to see that $s^{2k+8} = 1$ for these small examples, as including the relator s^{2k+8} did not change the index over the trivial subgroup, and so, $s^{2k+8} \in \langle rsr \rangle$. Thus, $s^{2k+8} \sim s$, and since $s^{2k+8} = rs^t r$ for some integer t, then $s^{2k+8} \sim rsr$ and s^{2k+8} is central. Here, $s^{2k+8} = s^t$ and $s^{2k+8} = 1$, so $t = 0$, and a proof of $s^{2k+8} \in \langle rsr \rangle$ is actually a proof of $s^{2k+8} = 1$ as our proofword would reduce to the identity after removing all relators.

For the instances involving $k = 7$ and $k = 9$, the proofwords generated were extremely long and so, to shorten the definition sequence and reduce the size of the resultant proofword, runs using the PEACE *prune* option were also initiated.

For each group, the five best proofwords were considered and we used our program to produce proofs from these proofwords. As even short proofwords result in proofs with many steps using our method, those obtained from our PEACE runs for the groups $F^{1,3,k}$ with $k = 3, 5, 7, 9$ were very long. The shortest proofword of s^{18} in the subgroup $\langle rsr \rangle$ of the group $F^{1,3,5}$ had a relator length of 17, yet produced a 44 step proof, while the shortest proofword of s^{26} for $F^{1,3,9}$ had length of 37 and yielded a 250 step proof.

Although we could not hope to find patterns and make generalisations from such proofs, we did try to observe common characteristics and seek significant ideas within the proofs. After comparing and studying each of our PEACE-generated proofs, we were able to make the following observations:

- The difficulty did not seem to increase with increasing values of k.
- Expressions longer than 4 syllables rarely appeared in the proofs of $s^{2k+8} = 1$, so after $r^2 = 1$, all words in the proof were essentially of the form $rs^\alpha rs^\beta rs^\gamma rs^\delta = 1$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$.
- The proofs seemed to use the fact that, in this particular case, $b - a = 2a$.

From these observations, we were able to formulate a proof that $s^{2k+8} = 1$ in the groups $F^{1,3,k}$ for $k \in \mathbb{Z}$. The resulting theorem, along with its proof, is given below.

Theorem 4.1 For the groups

$$F^{1,3,k} = \langle r, s | r^2, rsrs^3rs^k \rangle$$

where $k \in \mathbb{Z}$, then $s^{2k+8} = 1$ and

$$F^{1,3,k} \cong H^{1,3,k} = \langle r, s | r^2, rsrs^3rs^k, s^{2k+8} \rangle.$$

Proof. For $F^{1,3,k}$ with $k \in \mathbb{Z}$, we have

$$\begin{aligned}
rsr &= s^{-k}rs^{-3} && (4.1)\\
rs^3r &= s^{-1}rs^{-k} && (4.2)\\
rs^kr &= s^{-3}rs^{-1} &&\\
rs^{k-3}r &= (rs^{-3}r)(rs^kr) &&\\
&= s^krs^{-2}rs^{-1} && (4.3)\\
rs^{k+3}r &= (rs^3r)(rs^kr) &&\\
&= s^{-1}rs^{-(k+3)}rs^{-1} && (4.4)\\
rs^2r &= (rsr)(rsr) &&\\
&= s^{-k}rs^{-(k+3)}rs^{-3} && (4.5)
\end{aligned}$$

We now show that $s^{2k+8} = 1$ in $F^{1,3,k}$.

$$
\begin{aligned}
1 &= rsrs^3rs^k \\
&= s^3rsrs^3rs^{k-3} \\
&= s^3rs^k.s^{-k+1}rs^3rs^{k-3} \\
&= rs^{-1}rs^{-k+1}rs^3rs^{k-3} && \text{by 4.1} \\
&= s^{-1}rs^{-k+1}rs^3.rs^{k-3}r \\
&= s^{-1}rs^{-k+1}rs^{k+3}rs^{-2}rs^{-1} && \text{by 4.3} \\
&= rs^{-k+1}rs^{k+3}.rs^{-2}r.s^{-2} \\
&= rs^{-k+1}rs^{k+3}.s^3rs^{k+3}rs^k.s^{-2} && \text{by 4.5} \\
&= rs^{-k+1}rs^{k+6}rs^{k+3}rs^{k-2} \\
&= rs^{-k+1}rs^{k+6}.rs^{k+3}r.s^{k-2} \\
&= rs^{-k+1}rs^{k+6}.s^{-1}rs^{-(k+3)}rs^{-1}.s^{k-2} && \text{by 4.4} \\
&= s^{-k+1}rs^{k+5}rs^{-(k+3)}.rs^{k-3}r \\
&= s^{-k+1}rs^{k+5}rs^{-(k+3)}.s^krs^{-2}rs^{-1} && \text{by 4.3} \\
&= s^{-k+1}rs^{k+5}rs^{-3}rs^{-2}rs^{-1} \\
&= s^{-k}rs^{k+5}.rs^{-3}r.s^{-2}r \\
&= s^{-k}rs^{k+5}.s^krs.s^{-2}r && \text{by 4.2} \\
&= s^{-k}rs^{2k+5}.rs^{-1}r \\
&= s^{-k}rs^{2k+5}.s^3rs^k && \text{by 4.1} \\
&= s^{-k}rs^{2k+8}rs^k \\
&= s^{2k+8}
\end{aligned}
$$

□

Encouraged by our success with the computer generated proofs for $F^{1,3,k}$, we then tried to find proofs for the groups $F^{3,5,k}$ with $k \in \mathbb{Z}$, where k is odd to ensure $d = 2$. However, the same characteristics of the $F^{1,3,k}$ proofs did not appear in those for $F^{3,5,k}$, as the proofs found by PEACE increased in difficulty with the size of k and more than 4 syllables were involved in the relations at many stages of the proofs. Also, in this case, we did not have $b - a = 2a$, so our proof for $F^{1,3,k}$ could not easily be generalised for $F^{3,5,k}$.

We did, however, make the observation that relations of a certain type continually appeared in the resulting PEACE proofs as well as in our attempted manipulations of the relators. For $F^{3,5,7}$, we used PEACE and our proof generating program to verify the truth of relations

$$(rs^{10}rs^{5})^2 = 1, (rs^{12}rs^{3})^2 = 1 \text{ and } (rs^{14}rs)^2 = 1$$

in the group. It was recognised that proving the validity of all relations of this form in such a sequence is sufficient since $(rs^0rs^{15})^2 = 1$ is a member of this sequence and

$$1 = (rs^0rs^{15})^2 = s^{30},$$

as required.

Examining different proofs for $F^{3,5,k}$ with small k, we found that the relations

$$(rs^{2m+3}rs^{k-2m+5})^2 = 1 \quad \text{for } m \in \mathbb{Z}$$

held, and having discovered what we should try to prove, we used induction to obtain a proof of this result. As k must be an odd integer to force $d = 2$, then $k + 5$ must be even. Thus, substituting $m = (k + 5)/2$ into our new relation sequence gives $(rs^{k+8}rs^0)^2 = rs^{2k+16}r = 1$ and $s^{2k+16} = 1$, proving $F^{3,5,k} \cong H^{3,5,k}$ for an odd integer k.

We had noticed in the case of $F^{1,3,k}$ that our proof required the fact that there existed a relation amongst the three powers, $a = 1$, $b = 3$ and $c = k$, namely $b - a = 2a$. This did not hold in the groups $F^{3,5,k}$ and was the reason the proof could not be modified for groups of this type. Thus, we chose to next consider groups of the type $F^{a-2,a,a+2}$ for an odd integer a, as, for such a group, there can be found some symmetry in its form. Here, if a is an odd integer, then $d = 2$, $(a - 2, a, a + 2) = 1$ and the relations $(a + 2) - a = a - (a - 2) = 2$ exist. We hoped these relationships amongst $a - 2$, a and $a + 2$ could be used to help find a proof.

Studying the resultant PEACE proofs for groups of this type, we were able to see occurrences of members of the sequence

$$(rs^{2m}rs^{3a-2m})^2 = 1 \quad \text{for } m \in \mathbb{Z}.$$

It would be enough if we could show that all relations of this type held, as substituting $m = 0$ would give $s^{2n} = s^{6a} = 1$ and the kernel of the natural homomorphism $\theta : F^{a-2,a,a+2} \rightarrow H^{a-2,a,a+2}$ would be trivial, as required.

However, using the special relationships amongst the powers of s in the relator $rs^{a-2}rs^{a}rs^{a+2}$, we were able to determine that both $s^{2a} \sim rs^{2}r$ and $r \sim s^{-2}rs^{4}$ and found that it was sufficient to show that every element of the sequence

$$(rs^{2m}rs^{3a-2m})^{2} = 1 \quad \text{for } m \in \mathbb{Z}$$

was a relation in the group. An induction proof was thus employed, and our proof for the case $F^{a-2,a,a+2}$ is as follows.

Theorem 4.2 For the groups

$$F^{a-2,a,a+2} = \langle r, s | r^{2}, rs^{a-2}rs^{a}rs^{a+2} \rangle$$

where $a \in \mathbb{Z}$ and a odd, then $s^{6a} = 1$ and

$$F^{a-2,a,a+2} \cong H^{a-2,a,a+2} = \langle r, s | r^{2}, rs^{a-2}rs^{a}rs^{a+2}, s^{6a} \rangle.$$

Proof. For $F^{a-2,a,a+2}$ where a is odd, we have

$$\begin{aligned} n &= a-2+a+a+2 \\ &= 3a, \\ 1 &= (a-2, a, a+2) \quad \text{and} \\ d &= ((a-2)-a, a-(a+2)) \\ &= 2. \end{aligned}$$

Also,

$$\begin{aligned} rs^{a-2}r &= s^{-a-2}rs^{-a}, \\ rs^{a}r &= s^{2-a}rs^{-a-2} \quad \text{and} \\ rs^{a+2}r &= s^{-a}rs^{2-a}. \end{aligned}$$

As it is easily seen that $F^{a,b,c} = F^{-c,-b,-a}$, then $F^{a-2,a,a+2} = F^{-a-2,-a,-a+2}$ and we need only prove cases where a is an odd natural number.

Outline of proof:

1. $s^{2a} \sim rs^2r$ and $r \sim s^{-2}rs^4$.
2. $(rs^{2a}rs^a)^2 = 1$.
3. $(rs^{2m}rs^{a-2m})^2 = s^{2a}$ for all positive integers m.
4. $s^{6a} = 1$.

Proof of 1: $s^{2a} \sim rs^2r$ and $r \sim s^{-2}rs^4$

Since $rs^{a-2}rs^ars^{a+2} = 1$ and $r^2 = 1$, then

$$\begin{aligned} rs^{2a}r &= (rs^ar)(rs^ar) \\ &= s^{2-a}rs^{-a-2}.s^{2-a}rs^{-a-2} \\ &= s^{2-a}rs^{-2a}rs^{-a-2}, \end{aligned}$$

$$\begin{aligned} rs^{2a}r &= (rs^{a+2}r)(rs^{a-2}r) \\ &= s^{-a}rs^{2-a}.s^{-2-a}rs^{-a} \\ &= s^{-a}rs^{-2a}rs^{-a} \end{aligned}$$

and so,

$$\begin{aligned} rs^{2a}r &= s^{2-a}(s^ars^{2a}rs^a)s^{-a-2} \\ &= s^2rs^{2a}rs^{-2}. \end{aligned}$$

Hence, $s^{2a} \sim rs^2r$.

Also,

$$\begin{aligned} rs^2r &= (rs^{2-a}r)(rs^ar) \\ &= s^ars^{a+2}.s^{2-a}rs^{-a-2} \\ &= s^ars^4rs^{-a-2} \\ &= s^a(s^ars^4rs^{-2}rs^4rs^{-a-2})s^{-a-2}. \end{aligned}$$

So, as $s^{2a} \sim rs^2r$, then $rs^2r = rs^4rs^{-2}rs^4rs^{-4}$ and $rs^2rs^{-2}rs^4rs^{-4} = 1$. Thus, $rs^{-2}rs^4r = s^{-2}rs^4$ and $r \sim s^{-2}rs^4$.

Proof of 2: $(rs^{2a}rs^a)^2 = 1$

$$\begin{aligned} rs^{2a}rs^ars^{2a}rs^a &= rs^{2a}(s^{2-a}rs^{-a-2})s^{2a}rs^a \\ &= rs^{a+2}rs^{a-2}rs^a \\ &= 1 \end{aligned}$$

Proof of 3: $(rs^krs^{a-k})^2 = s^{2a}$ for k an even positive integer

Proof by induction:

Base step

$k = 2$

$$\begin{aligned} rs^2rs^{a-2}rs^2rs^{a-2} &= rs^2(s^{-a-2}rs^{-a})s^2rs^{a-2} \\ &= rs^{-a}rs^{2-a}rs^{a-2} \\ &= s^{a+2}s^{a-2} \\ &= s^{2a} \end{aligned}$$

$k = 4$

$$\begin{aligned} rs^4rs^{a-4}rs^2rs^{a-4} &= rs^4rs^{a-2}.s^{-2}rs^4.rs^{a-4} \\ &= rs^4rs^{a-2}rs^{-2}rs^a \quad \text{as } r \sim s^{-2}rs^4 \\ &= rs^4(s^{2-a}rs^{-a})s^{-2}rs^a \\ &= rs^{2-a}rs^{-a-2}rs^a \\ &= rs^{2-a}(s^{a-2}rs^a)s^a \\ &= s^{2a} \end{aligned}$$

Inductive step

Assume for all $k \leq i+2$, i and k even and $2 \leq i$,

$$(rs^krs^{a-k})^2 = s^{2a},$$

and so, $rs^k rs^{a-k} = s^{a+k} rs^{-k} r$ as well. Thus, for all $k \leq i+2$, i and k even and $2 \leq i$,

$$(s^{a+k} rs^{-k} r)^2 = s^{2a}.$$

Also, $rs^k rs^{a-k} rs^k rs^{a-k} = s^{2a}$, giving $rs^{a-k} rs^k r = s^{-k} rs^{a+k}$. Now, choose $k = i+4$. Using $r \sim s^{-2} rs^4$,

$$\begin{aligned}
& (s^{a+i} rs^{-i} r)^2 (rs^{i+4} rs^{a-i-4})^2 (s^{i-a} rs^{-i} r)^2 \\
= \; & s^{a+i} rs^{-i} rs^{a+i} rs^4 rs^{a-i-4} rs^{i+4} rs^{-4} rs^{-i} rs^{i-a} rs^{-i} r \\
= \; & s^{a+i} rs^{-i} rs^{a+i+2} rs^{-2} rs^{a-i} rs^i rs^2 rs^{-i-2} rs^{i-a} rs^{-i} r \\
= \; & s^{a+i} rs^{-i} rs^{a+i+2} rs^{-2} . rs^{a-i} rs^i r . s^2 rs^{-i-2} rs^{i-a} rs^{-i} r \\
= \; & s^{a+i} rs^{-i} rs^{a+i+2} rs^{-2} (s^{-i} rs^{a+i}) s^2 rs^{-i-2} rs^{i-a} rs^{-i} r \\
= \; & s^{a+i} rs^{-i} rs^{a+i+2} rs^{-i-2} rs^{a+i+2} rs^{-i-2} rs^{i-a} rs^{-i} r \\
= \; & s^{a+i} rs^{-i} r . s^{a+i+2} rs^{-i-2} rs^{a+i+2} rs^{-i-2} r . s^{i-a} rs^{-i} r \\
= \; & s^{a+i} rs^{-i} r (s^{2a}) s^{i-a} rs^{-i} r \\
= \; & s^{a+i} rs^{-i} rs^{a+i} rs^{-i} r \\
= \; & (s^{a+i} rs^{-i} r)^2 \\
= \; & s^{2a}.
\end{aligned}$$

However, since $(s^{a+i} rs^{-i} r)^2 = s^{2a}$ and $(s^{i-a} rs^{-i} r)^2 = s^{-2a}$, then

$$(rs^{i+4} rs^{a-i-4})^2 = s^{2a}.$$

Therefore, for all even integers k, where $k \geq 2$,

$$(rs^k rs^{a-k})^2 = s^{2a}.$$

Proof of 4: $s^{6a} = 1$

We can assume that a is an odd natural number, so $2a$ is even and positive. Substituting $k = 2a$ in our relations $(rs^k rs^{a-k})^2 = s^{2a}$ gives

$$(rs^{2a}rs^{-a})^2 = s^{2a},$$

and so,

$$\begin{aligned}
s^{6a} &= s^{2a}s^{2a}s^{2a} \\
&= s^{2a}(rs^{2a}rs^{-a}rs^{2a}rs^{-a})s^{2a} \\
&= rs^{2a}rs^{a}rs^{2a}rs^{a} \quad \text{by 1} \\
&= (rs^{2a}rs^{a})^2 \\
&= 1.
\end{aligned}$$

Thus, as $s^{6a} = 1$, then we have $F^{a-2,a,a+2} \cong H^{a-2,a,a+2}$ for a an odd integer, as required. □

The relationships amongst the powers of s in the relator $rs^{a-2}rs^{a}rs^{a+2}$ were able to help us prove the conjecture for groups of the type $F^{a-2,a,a+2}$ with a an odd integer. The next step, therefore, was to study the groups $F^{a-3,a,a+3}$ for $a \in \mathbb{Z}$ where $(a, 3) = 1$, and see if our proof of $F^{a-2,a,a+2}$ could be modified for this case. We found that we could easily prove steps corresponding to steps 1, 2 and 3 from Theorem 4.2 for $F^{a-3,a,a+3}$. Similar steps could also easily be shown for the groups $F^{a-4,a,a+4}$ with $(a, 4) = 1$. Using different substitutions for k in the resultant sequences $(rs^{ck}rs^{a-ck})^2 = s^{2a}$ in $F^{a-c,a,a+c}$ for $c = 3$ or $c = 4$ where $(a, c) = 1$, we found we were able to prove the conjecture for groups of this type. The proof follows in the next section.

The use of PEACE and our program to generate step by step proofs from proofwords had thus provided us with sufficient results to take a very large first step in our work with the $F^{a,b,c}$ conjecture. From our proof of $F^{a-c,a,a+c}$ for $c \in \{2, 3, 4\}$ with $(a, c) = 1$, we made continual generalisations and modifications, with an increasingly difficult induction proof at each stage, to form the proofs for the cases,

$$F^{a-c,a,a+2c} \quad \text{with } (a,c)=1,$$
$$F^{a-c,a,a+kc} \quad \text{with } (a,c)=1,$$
$$F^{a-2c,a,a+kc} \quad \text{with } (a,c)=1 \text{ and } k \text{ odd}$$

and finally,

$$F^{a-jc,a,a+kc} \quad \text{with } (a,c)=1 \text{ and } (j,k)=1,$$

for $a, j, k \in \mathbb{Z}$ with $c \in \{2,3,4\}$. These proofs will be given in the remaining sections of this chapter. Once we had found the proof for groups of type, $F^{a-c,a,a+c}$ for $c \in \{2,3,4\}$ with $(a,c)=1$, we no longer relied on PEACE and the technique of converting proofwords to proofs. However, each subsequent proof was based on the information we had originally obtained through its use. By studying and comparing examples of PEACE proofs for small cases, one can find try to find patterns and make observations in the aim of generalising to a broader class of groups, and this technique was found to be a very useful tool in solving the $F^{a,b,c}$ conjecture.

4.3 $F^{a-c,a,a+c}$ for $a, c \in \mathbb{Z}$

The $F^{a,b,c}$ conjecture relies on the condition that $(a,b,c)=1$. For the groups, $F^{a-c,a,a+c}$ with $a, c \in \mathbb{Z}$, this means we require $(a,c)=1$. Additionally, previous results have shown the $F^{a,b,c}$ conjecture to be true for $d=1$ and $d=5$, where d is defined to be $(a-b, b-c)$. For $d \geq 6$ with $(a,b,c)=1$, the groups $F^{a,b,c}$ are infinite. Thus, we need only consider $c \in \{2,3,4\}$ to show the conjecture holds for all groups of the type $F^{a-c,a,a+c}$ for $a, c \in \mathbb{Z}$ where $(a,c)=1$.

Modifying our proof of $F^{a-2,a,a+2}$ for $F^{a-3,a,a+3}$ was relatively simple. The first three steps of the proof were updated merely by the substitutions of $a-3$ for any occurrence of $a-2$ and of $a+3$ for any $a+2$ in the first few lines, altering any resultant calculations. Once these steps had been determined, it was actually found that in this case, the first two are sufficient to show

$s^{12a} = 1$. Using a result from [6], this is enough to show the cyclic group of order 2 is the kernel of the natural homomorphism from $F^{a-3,a,a+3}$ to $H^{a-3,a,a+3}$.

Formulating the proof for the case $c = 4$, however, required a bit more effort. The kernel of the previous two cases is either trivial or C_2, whereas for $F^{a-4,a,a+4}$, it adopts a more complicated form as the quaternion group Q_8. A presentation for Q_8 is $\langle x, y | x^4, x^2 = y^2, y^{-1}xy = x^{-1}\rangle$. Thus, taking $x = s^{6a}$ and $y = rs^{6a}r$, we needed to show that s^{24a} is trivial, s^{12a} is central and $rs^{-6a}rs^{6a}rs^{6a}r = s^{-6a}$ as well as that the kernel is generated by s^{6a} and $rs^{6a}r$ to prove $F^{a-4,a,a+4}/Q_8 \cong H^{a-4,a,a+4}$. While the modifications of the three steps of Theorem 4.2 followed similarly to the alterations made for $c = 3$, additional steps were required to show the kernel had the correct form.

According to the $F^{a,b,c}$ conjecture, we must have $(a, b, c) = 1$ to ensure proper results. Consider $F^{a-c,a,a+c}$. Here, $s^{2n} = s^{6a}$ and $d = c$. For $c \in \{2, 3, 4\}$, if $(a - c, a, a + c) \neq 1$, then a must either be a multiple of c or, where $c = 4$, a could alternatively be a multiple of 2. Thus, the conjecture holds only when $(a, c) = 1$ for $c \in \{2, 3, 4\}$. However, we noticed that the first three steps of Theorem 4.2, altered for the correct value of c, held regardless of whether $(a, c) = 1$ or otherwise. Using these facts, we were able to find an additional result when $(a, c) \neq 1$, and we include it in our proof of the groups $F^{a-c,a,a+c}$ for $a, c \in \mathbb{Z}$.

Theorem 4.3 For the groups

$$F^{a-c,a,a+c} = \langle r, s | r^2, rs^{a-c}rs^a rs^{a+c}\rangle$$

with $a \in \mathbb{Z}$ and $c \in \{2, 3, 4\}$, let

$$H^{a-c,a,a+c} = \langle r, s | r^2, rs^{a-c}rs^a rs^{a+c}, s^{6a}\rangle.$$

If,

- $c = 2$ and $(a, 2) = 1$, then $s^{6a} = 1$ and

$$F^{a-2,a,a+2} \cong H^{a-2,a,a+2},$$

- $c = 3$ and $(a, 3) = 1$, then $s^{12a} = 1$ and

$$F^{a-3,a,a+3}/C_2 \cong H^{a-3,a,a+3},$$

- $c = 4$ and $(a, 4) = 1$, then $s^{24a} = 1$, $s^{12a} \sim r$ and

$$F^{a-4,a,a+4}/Q_8 \cong H^{a-4,a,a+4},$$

- $(a, c) \neq 1$ then $(a - c, a, a + c) \neq 1$, $s^{6a} = 1$ and

$$F^{a-c,a,a+c} \cong H^{a-c,a,a+c}.$$

Proof. For $F^{a-c,a,a+c}$, we have

$$\begin{aligned} n &= a - c + a + a + c \\ &= 3a, \\ s^{2n} &= s^{6a}, \\ 1 &= (a - c, a, a + c) \text{ when } (a, c) = 1 \quad \text{and} \\ d &= ((a - c) - a, a - (a + c)) \\ &= c. \end{aligned}$$

Also,

$$\begin{aligned} rs^{a-c}r &= s^{-a-c}rs^{-a}, \\ rs^{a}r &= s^{c-a}rs^{-a-c} \quad \text{and} \\ rs^{a+c}r &= s^{-a}rs^{c-a}. \end{aligned}$$

From Lemma 2.1 in [3], we have $F^{a,b,c} = F^{-c,-b,-a}$, so

$$F^{a-c,a,a+c} = F^{-a-c,-a,-a+c}$$

and we need only prove the case where a is positive.

Our proof begins with the three necessary steps (I - III) to prove each of the cases $c = 2$, $c = 3$ and $c = 4$.

I. $s^{2a} \sim rs^c r$ and $r \sim s^{-c} r s^{2c}$

Since $rs^{a-c}rs^a rs^{a+c} = 1$ and $r^2 = 1$, then

$$\begin{aligned} rs^{2a}r &= (rs^a r)(rs^a r) \\ &= (s^{c-a} r s^{-a-c})(s^{c-a} r s^{-a-c}) \\ &= s^{c-a} r s^{-2a} r s^{-a-c} \end{aligned}$$

and

$$\begin{aligned} rs^{2a}r &= (rs^{a+c} r)(rs^{a-c} r) \\ &= (s^{-a} r s^{c-a})(s^{-c-a} r s^{-a}) \\ &= s^{-a} r s^{-2a} r s^{-a}, \end{aligned}$$

so,

$$\begin{aligned} rs^{2a}r &= s^{c-a}(s^a r s^{2a} r s^a) s^{-a-c} \\ &= s^c r s^{2a} r s^{-c}. \end{aligned}$$

Hence, $s^{2a} \sim rs^c r$.

Also,

$$\begin{aligned} rs^c r &= (rs^{c-a} r)(rs^a r) \\ &= (s^a r s^{a+c})(s^{c-a} r s^{-a-c}) \\ &= s^a r s^{2c} r s^{-a-c} \\ &= s^a (s^a r s^{2c} r s^{-a-c})(s^a r s^{2c} r s^{-a-c}) s^{-a-c} \\ &= s^{2a} r s^{2c} r s^{-c} r s^{2c} r s^{-2a-2c}. \end{aligned}$$

So, as $s^{2a} \sim rs^c r$,

$$\begin{aligned} rs^c r &= rs^{2c} r s^{-c} r s^{2c} r s^{-2c} \\ 1 &= rs^c r s^{-c} r s^{2c} r s^{-2c}. \end{aligned}$$

Thus, $rs^{-c}rs^{2c}r = s^{-c}rs^{2c}$ and $r \sim s^{-c}rs^{2c}$.

II. $(rs^{2a}rs^{a})^2 = 1$

$$\begin{aligned} rs^{2a}rs^{a}rs^{2a}rs^{a} &= rs^{2a}(s^{c-a}rs^{-a-c})s^{2a}rs^{a} \\ &= rs^{a+c}rs^{a-c}rs^{a} \\ &= 1 \end{aligned}$$

III. $(rs^{ck}rs^{a-ck})^2 = s^{2a}$ in $F^{a-c,a,a+c}$, $\forall k \in \mathbb{N}$, $c \in \{2,3,4\}$

Proof by induction:

Base step

$k = 1$

$$\begin{aligned} rs^{c}rs^{a-c}rs^{c}rs^{a-c} &= rs^{c}(s^{-a-c}rs^{-a})s^{c}rs^{a-c} \\ &= rs^{-a}rs^{c-a}rs^{a-c} \\ &= s^{a+c}s^{a-c} \\ &= s^{2a} \end{aligned}$$

$k = 2$

$$\begin{aligned} rs^{2c}rs^{a-2c}rs^{2c}rs^{a-2c} &= rs^{2c}rs^{a-c}s^{-c}rs^{2c}rs^{a-2c} \\ &= rs^{2c}rs^{a-c}rs^{-c}rs^{a} \\ &= rs^{2c}(s^{-a-c}rs^{-a})s^{-c}rs^{a} \\ &= rs^{c-a}rs^{-a-c}rs^{a} \\ &= s^{a}s^{a} \\ &= s^{2a} \end{aligned}$$

Inductive step

Assume $(rs^{ck}rs^{a-ck})^2 = s^{2a}$ for all integers k, with $k \leq i$.

Then, using $k = i$, we know

$$\begin{aligned}
(rs^{ci}rs^{a-ci})^2 &= s^{2a} \\
rs^{ci}rs^{a-ci} &= s^{a+ci}rs^{-ci}r \\
(s^{a+ci}rs^{-ci}r)^2 &= s^{2a}
\end{aligned}$$

and, using $k = i-1$,

$$\begin{aligned}
(rs^{ci-c}rs^{a-ci+c})^2 &= s^{2a} \\
rs^{a-ci+c}rs^{ci-c}r &= s^{c-ci}rs^{a+ci-c} \\
(s^{-a+ci-c}rs^{c-ci}r)^2 &= s^{-2a} \\
(s^{a+ci-c}rs^{c-ci}r)^2 &= s^{2a}.
\end{aligned}$$

Now, consider $k = i+1$, or $(rs^{ci+c}rs^{a-ci-c})^2$.

$$\begin{aligned}
& (s^{a+ci-c}rs^{c-ci}r)^2(rs^{ci+c}rs^{a-ci-c})^2(s^{-a+ci-c}rs^{c-ci}r)^2 \\
= \;& s^{a+ci-c}rs^{c-ci}rs^{a+ci-c}rs^{2c}rs^{a-ci-c}rs^{ci+c}rs^{-2c}rs^{c-ci}rs^{-a+ci-c}rs^{c-ci}r \\
= \;& s^{a+ci-c}rs^{c-ci}rs^{a+ci}rs^{-c}rs^{a-ci+c}rs^{ci-c}rs^{c}rs^{-ci}rs^{-a+ci-c}rs^{c-ci}r \\
= \;& s^{a+ci-c}rs^{c-ci}rs^{a+ci}rs^{-c}.rs^{a-ci+c}rs^{ci-c}r.s^{c}rs^{-ci}rs^{-a+ci-c}rs^{c-ci}r \\
= \;& s^{a+ci-c}rs^{c-ci}rs^{a+ci}rs^{-c}s^{c-ci}rs^{a+ci-c}s^{c}rs^{-ci}rs^{-a+ci-c}rs^{c-ci}r \\
= \;& s^{a+ci-c}rs^{c-ci}rs^{a+ci}rs^{-ci}rs^{a+ci}rs^{-ci}rs^{-a+ci-c}rs^{c-ci}r \\
= \;& s^{a+ci-c}rs^{c-ci}r.s^{a+ci}rs^{-ci}rs^{a+ci}rs^{-ci}r.s^{-a+ci-c}rs^{c-ci}r \\
= \;& s^{a+ci-c}rs^{c-ci}rs^{a+ci-c}rs^{c-ci}r \\
= \;& s^{2a}
\end{aligned}$$

Since $(s^{a+ci-c}rs^{c-ci}r)^2 = s^{2a}$ and $(s^{-a+ci-c}rs^{c-ci}r)^2 = s^{-2a}$, then $(rs^{ci+c}rs^{a-ci-c})^2 = s^{2a}$.

Thus, by induction, $(rs^{ck}rs^{a-ck})^2 = s^{2a}$ in $F^{a-c,a,a+c}$ for $k \in \mathbb{N}$ and $c \in \{2, 3, 4\}$.

1. Proof of the Case $c = 2$

   Given in Theorem 4.2.

2. Proof of the Case $c = 3$

$$F^{a-3,a,a+3} = \langle r, s | r^2, rs^{a-3}rs^a rs^{a+3} \rangle$$

For $F^{a-3,a,a+3}$, if we can show that $s^{2n} = s^{6a} = s^{-6a}$, or $s^{12a} = 1$, then we have shown that

$$F^{a-3,a,a+3}/C_2 \cong H^{a-3,a,a+3} = \langle r, s | r^2, s^{6a}, rs^{a-3}rs^a rs^{a+3} \rangle.$$

- $s^{2a} \sim rs^3 r$ and $r \sim s^{-3}rs^6$ from I
- $(rs^{2a}rs^a)^2 = 1$ from II
- $rs^{6a}r = s^{-6a}$

$$\begin{aligned}
1 &= rs^{2a}rs^a rs^{2a}rs^a \\
&= rs^{2a}rs^a(s^{a-3}rs^a rs^{a+3})s^{2a}rs^a \\
&= rs^{2a}rs^{2a-3}rs^a rs^{3a+3}rs^a \\
&= s^{3a-3}rs^{2a}rs^{-a}rs^a rs^{3a+3}rs^a \\
&= s^{3a-3}rs^{2a}(s^{a+3}rs^{a-3})s^a rs^{3a+3}rs^a \\
&= s^{3a-3}rs^{3a+3}rs^{2a-3}rs^{3a+3}rs^a \\
&= s^{3a-3}rs^{3a+3}rs^{-3}rs^{3a+3}rs^{3a} \\
&= s^{3a-3}rs^{-a+3}rs^{-3}rs^{7a+3}rs^{3a} \\
&= s^{3a-3}rs^{-a}rs^6 rs^{7a-3}rs^{3a} \\
&= s^{4a}rs^{a+3}rs^{7a-3}rs^{3a} \\
&= s^{3a}rs^{6a}rs^{3a} \\
&= s^{6a}rs^{6a}r
\end{aligned}$$

Thus, $s^{-6a} = rs^{6a}r$.

- $s^{12a} = 1$ and $s^{6a} \sim r$

Since $s^{-6a} = rs^{6a}r$, then we have

$$\begin{aligned} rs^{-6a} &= s^{6a}r \quad \text{and} \\ rs^{6a} &= s^{-6a}r. \end{aligned}$$

Hence,

$$\begin{aligned} s^{6a} &= rs^{a-3}rs^{a}rs^{a+3}s^{6a} \\ &= rs^{a-3}rs^{a}.rs^{6a}.s^{a+3} \\ &= rs^{a-3}rs^{-5a}rs^{a+3} \\ &= rs^{a-3}.rs^{-6a}.s^{a}rs^{a+3} \\ &= rs^{7a-3}rs^{a}rs^{a+3} \\ &= rs^{6a}.s^{a-3}rs^{a}rs^{a+3} \\ &= s^{-6a}rs^{a-3}rs^{a}rs^{a+3} \\ &= s^{-6a}. \end{aligned}$$

Thus, $s^{12a} = 1$ and $s^{6a} \sim r$.

- $F^{a-3,a,a+3}/C_2 \cong H^{a-3,a,a+3}$ when $(a,3) = 1$.

  Consider $\langle x \rangle$ where $x = s^{6a}$. Obviously it is a subgroup of the kernel of the homomorphism from F to H, and since

$$rxr = rs^{6a}r = s^{6a} = x$$

$$\text{and} \quad s^{-1}xs = x,$$

  then $\langle x \rangle$ is the kernel.

  We have shown that $s^{4n} = s^{12a} = 1$ and s^{6a} generates the kernel of the homomorphism. Thus, either $F^{a-3,a,a+3} \cong H^{a-3,a,a+3}$ or $F^{a-3,a,a+3}/C_2 \cong H^{a-3,a,a+3}$. It cannot be that $a-3 \equiv a \equiv a+3 \pmod 6$ and we also have

$$(a-3-a, a-(a+3), 3) = (-3, 3, 3) = 3,$$

so, by Theorem 3.3 of [6], $H^{a-3,a,a+3}$ is finite and has Schur multiplicator C_2.

We now know $F^{a-3,a,a+3}$ is finite and as it has a 2-generator, 2-relator presentation, it has deficiency 0 and, by Corollory 1.2 of [31], a trivial multiplicator. Thus, $F^{a-3,a,a+3} \ncong H^{a-3,a,a+3}$, and it must be such that, when a is not a multiple of 3,

$$F^{a-3,a,a+3}/C_2 \cong H^{a-3,a,a+3}.$$

3. Proof of the Case $c = 4$

$$F^{a-4,a,a+4} = \langle r, s | r^2, rs^{a-4}rs^a rs^{a+4} \rangle$$

For $F^{a-4,a,a+4}$, we want to prove that $s^{24a} = 1$, s^{12a} is central and $rs^{-6a}rs^{6a}rs^{6a}r = s^{-6a}$. Thus, the kernel of the natural homomorphism from F to H could be shown to be generated by $x = s^{6a}$ and $y = rs^{6a}r$ and would be

$$\langle x, y | x^4, x^2 = y^2, y^{-1}xy = x^{-1} \rangle,$$

which is a presentation for Q_8.

- $s^{2a} \sim rs^4r$ and $r \sim s^{-4}rs^8$ from I
- $s^{4a} \sim rs^2r$

  From $s^{2a} \sim rs^4r$, we have $s^{4a} \sim rs^4r$. Also, as a is odd, we know $2a + 2 \equiv 0 \pmod 4$ and

$$rs^{4a}r = s^{-2a-2}rs^{4a}rs^{2a+2}.$$

  So,

$$\begin{aligned} rs^2rs^{4a}rs^{-2}r &= rs^2s^{-2a-2}rs^{4a}rs^{2a+2}s^{-2}r \\ &= rs^{-2a}rs^{4a}rs^{2a}r \\ &= rs^{-2a}rrs^{2a}rs^{4a} \\ &= s^{4a} \end{aligned}$$

and $s^{4a} \sim rs^2r$.

- $(rs^{2a}rs^a)^2 = 1$ from II
- $rs^{7a-4}rs^{7a}rs^{7a+4} = 1$

$$\begin{aligned}
1 &= rs^{2a}rs^ars^{2a}rs^a \\
&= rs^{2a}rs^a(s^{a-4}rs^ars^{a+4})s^{2a}rs^a \\
&= rs^{2a}rs^{2a-4}rs^ars^{3a+4}rs^a \\
&= s^{4a-4}rs^{2a}rs^{-2a}rs^ars^{3a+4}rs^a \\
&= s^{5a-4}rs^{2a}(s^ars^{2a}rs^a)s^ars^{3a+4}r \\
&= s^{5a-4}rs^{3a}rs^{2a}rs^{2a}rs^{3a+4}r \\
&= s^{9a-4}rs^{3a}rs^{2a}rs^{2a}rs^{3a+4}rs^{-4a} \\
&= s^{9a-4}rs^{3a}rs^{2a}rs^{2a}rs^{4-a}rs^{-4a}rs^{4a}r \\
&= s^{9a-4}rs^{3a}rs^{2a}rs^{2a}(s^ars^{a+4})s^{-4a}rs^{4a}r \\
&= s^{9a-4}rs^{3a}rs^{2a}rs^{3a}rs^{-3a+4}rs^{4a}r \\
&= s^{9a-4}rs^{3a}rs^{2a}rs^{3a}rs^{4-a}rs^{4a}rs^{-2a} \\
&= s^{7a-4}rs^{3a}rs^{2a}rs^{3a}rs^{4-a}rs^{4a}r \\
&= s^{7a-4}rs^{3a}rs^{2a}rs^{3a}(s^ars^{a+4})s^{4a}r \\
&= s^{7a-4}rs^{3a}rs^{2a}rs^{4a}rs^{5a+4}r \\
&= s^{7a-4}rs^{7a}rs^{7a+4}r.
\end{aligned}$$

So, $rs^{7a-4}rs^{7a}rs^{7a+4} = 1$.

- $(rs^{4k}rs^{a-4k})^2 = s^{2a}$, $\forall k \in \mathbb{N}$ from III
- We know we can assume a is a natural number, so setting $k = a$ in the previous equation, we have

$$rs^{4a}rs^{-3a}rs^{4a}rs^{-3a} = s^{2a}$$

and

$$\begin{aligned}
s^{5a} &= rs^{4a}rs^{-3a}rs^{4a}r \\
&= s^{-4a}rs^{4a}rs^{a}rs^{4a}r \quad \text{as } rs^{4a}r \sim s^2 \\
s^{9a} &= rs^{4a}.rs^{a}r.s^{4a}r \\
&= rs^{2a}rs^{-a}.rs^{2a}r. \quad \text{as } (s^{2a}rs^{a})^2 = 1 \\
&= rs^{2a}rs^{-2a}rs^{-2a}rs^{-a} \quad \text{again, as } (s^{2a}rs^{a})^2 = 1 \\
s^{6a} &= rs^{2a}rs^{-2a}rs^{-2a}rs^{-4a} \\
&= rs^{2a}rs^{-6a}rs^{-2a}r \quad \text{as } rs^{2a}r \sim s^4.
\end{aligned}$$

Thus, as $rs^{2a}r \sim s^4$, then

$$s^{6a} = rs^{6a}rs^{-6a}rs^{-6a}r. \tag{4.6}$$

- Substituting $k = 2a$, we have

$$rs^{8a}rs^{-7a}rs^{8a}rs^{-7a} = s^{2a}.$$

So,

$$\begin{aligned}
s^{4a} &= s^{2a}rs^{8a}rs^{-7a}rs^{8a}rs^{-7a} \\
&= rs^{8a}rs^{2a}s^{-7a}rs^{8a}rs^{-7a} \\
&= rs^{8a}rs^{-5a}rs^{8a}rs^{-7a} \\
&= rs^{8a}rs^{-13a}rs^{8a}rs^{a} \\
&= rs^{8a}rs^{-13a}rs^{7a+4}.s^{a-4}rs^{a} \\
&= rs^{8a}rs^{-13a}rs^{7a+4}rs^{-a-4}r \\
&= rs^{8a}rs^{-13a}(s^{-7a}rs^{-7a+4})s^{-a-4}r \\
&= rs^{8a}rs^{-20a}rs^{-8a}r \\
&= s^{-20a}.
\end{aligned}$$

Thus, $s^{24a} = 1$.

- Using $k = 3a$ and $s^{12a} = s^{-12a}$ gives

$$rs^{-12a}rs^{-11a}rs^{-12a}rs^{-11a} = s^{2a}.$$

So,

$$\begin{aligned} rs^{-12a}rs^{-11a}rs^{-12a}r &= s^{13a} \\ rs^{-12a}rs^{-7a}rs^{-12a}r &= s^{17a} \\ rs^{-12a}(s^{7a+4}rs^{7a-4})s^{-12a}r &= s^{-7a} \\ rs^{-5a+4}rs^{-5a-4}r &= s^{-7a}. \end{aligned}$$

Now,

$$\begin{aligned} 1 &= rs^{7a-4}rs^{7a}rs^{7a+4} \\ &= rs^{7a-4}(s^{5a+4}rs^{5a-4})s^{7a+4} \\ &= rs^{12a}rs^{12a} \\ &= rs^{12a}rs^{-12a}. \end{aligned}$$

Thus, $s^{12a} \sim r$ and s^{12a} is central.

- Let $x = s^{6a}$ and $y = rs^{6a}r$, and consider $\langle x, y \rangle$. Obviously, $\langle x, y \rangle$ is a subgroup of the kernel of the homomorphism from F to H.

  It is also easily seen that $rxr = y$, $ryr = x$ and $s^{-1}xs = x$, and we only need to test $s^{-1}ys$ to show that $\langle x, y \rangle$ is the kernel.

  Since $rs^{a-4}rs^{a}rs^{a+4} = rs^{7a-4}rs^{7a}rs^{7a+4}$,

$$\begin{aligned} 1 &= rs^{-a}rs^{6a}rs^{7a}rs^{6a} \quad \text{and} \\ rs^{6a}r &= s^{a}rs^{-6a}rs^{-7a}. \end{aligned}$$

  We know a is an odd number, so we have two cases.

  (a) $a \equiv 1 \pmod 4$
  Here, $a + 1 \equiv 2 \pmod 4$ and $6a \equiv 2 \pmod 4$, so $7a + 1 \equiv 0 \pmod 4$.

Thus,

$$\begin{aligned} rs^{6a}r &= s^{7a+1}rs^{6a}rs^{-7a-1} \quad \text{and} \\ s^{-1}rs^{6a}rs &= s^{7a}rs^{6a}rs^{-7a}, \end{aligned}$$

and we have

$$\begin{aligned} s^{-1}rs^{6a}rs &= s^{7a}rs^{6a}rs^{-7a} \\ &= s^{8a}rs^{-6a}rs^{-14a} \\ &= rs^{-6a}rs^{-6a} \\ &= y^{-1}x^{-1}. \end{aligned}$$

(b) $a \equiv 3 \pmod 4$
Now, $a + 1 \equiv 0 \pmod 4$.
Thus,

$$\begin{aligned} rs^{6a}r &= s^{a+1}rs^{6a}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a}rs &= s^{a}rs^{6a}rs^{-a}, \end{aligned}$$

and so,

$$\begin{aligned} s^{-1}rs^{6a}rs &= s^{a}rs^{6a}rs^{-a} \\ &= s^{2a}rs^{-6a}rs^{-8a} \\ &= s^{-6a}rs^{-6a}r \\ &= x^{-1}y^{-1}. \end{aligned}$$

Hence, $\{x, y\}$ generates the kernel. Also, x and y both have order dividing 4, and $x^2 = y^2$ as s^{12a} is central. We have also shown $y^{-1}xy = x^{-1}$ from 4.6, so therefore, $\langle x, y\rangle$ is a homomorphic image of Q_8, which has derived length 2. It is left to prove $\langle x, y\rangle \cong Q_8$. Consider the group

$$G^{a,b,c} = \langle r, s | r^2, s^8, rs^a rs^b rs^c\rangle,$$

which is obviously a homomorphic image of $F^{a,b,c}$. Here, $G^{a,b,c} \cong G^{a',b',c'}$, where a', b' and c' are a, b and c modulo 8. Using $F^{a-4,a,a+4}$ for the case $d = 4$, then a is odd and $a' \in \{1, 3, 5, 7\}$. Thus, we are left with only four cases for $G^{a-4,a,a+4}$, namely $G^{5,1,5}$, $G^{7,3,7}$, $G^{1,5,1}$ and $G^{3,7,3}$. Using GAP, we obtain that each of these four groups has derived length 4. Thus, as $G^{a-4,a,a+4}$ is a homomorphic image of $F^{a-4,a,a+4}$, the latter must have derived length of at least 4.

From Theorem 3.5 of [3], we know that all groups $H^{a,b,c}$ are finite metabelian groups when $(a, b, c) = 1$, $n \neq 0$ and $(d, 6) \neq 6$. As a is odd and $d = 4$, then $H^{a-4,a,a+4}$ is finite metabelian and, therefore, has derived length 2. This implies that $\langle x, y\rangle$, the kernel of the natural homomorphism from $F^{a-4,a,a+4}$ to $H^{a-4,a,a+4}$, must have derived length at least 2. Thus, $\langle x, y\rangle \cong Q_8$.

4. Proof of the Case $(a, c) \neq 1$

When $(a, c) \neq 1$ for $c \in \{2, 3, 4\}$, then we have $(a - c, a, a + c) \neq 1$ and either of two cases

(a) a is a multiple of c or

(b) $c = 4$ and a is a multiple of 2.

If a is a multiple of c, then all of $a - c$, a and $a + c$ are divisible by c and, as such, are not co-prime. If we consider $F^{a-c,a,a+c}$ where $a = ck$ for some integer k, then it is the case that $rs^{2a}r \sim s^a$ since $rs^{2a}r \sim s^c$. Therefore,

$$\begin{aligned} 1 &= rs^{a-c}rs^{a}rs^{a+c} \\ &= rs^{3a-c}rs^{a}rs^{c-a} \\ &= rs^{3a-c}(s^{c-a}rs^{-a-c})s^{c-a} \\ &= rs^{2a}rs^{-2a}, \end{aligned}$$

and so, $s^{2a} \sim r$.

The relation $rs^{2a}rs^{a}rs^{2a}rs^{a} = 1$ from II, then reduces to $s^{6a} = 1$, and we find that where a is a multiple of c, $F^{a-c,a,a+c} \cong H^{a-c,a,a+c}$.

We just need to look at the case where $c = 4$ and $a = 2m$ for some odd integer m. Using $(rs^{4k}rs^{a-4k})^2 = s^{2a}$ with $k = m$ gives

$$\begin{aligned} s^{2a} &= (rs^{4k}rs^{a-4k})^2 \\ &= (rs^{4m}rs^{a-4m})^2 \\ &= (rs^{2a}rs^{a-2a})^2 \\ &= (rs^{2a}rs^{-a})^2 \end{aligned}$$

and $rs^{2a}rs^{-a}rs^{2a}r = s^{3a}$.

Since we have $rs^{2a}r \sim s^4$, then $rs^{2a}r \sim s^{2a}$, and

$$\begin{aligned} s^{3a} &= rs^{2a}rs^{-a}rs^{2a}r \\ s^{5a} &= s^{2a}(rs^{2a}rs^{-a}rs^{2a}r) \\ &= rs^{2a}rs^{a}rs^{2a}r. \end{aligned}$$

We also know $rs^{2a}rs^{a}rs^{2a}rs^{a} = 1$, so $s^{5a} = s^{-a}$ and $s^{6a} = 1$. Thus, $F^{a-4,a,a+4} \cong H^{a-4,a,a+4}$ where $a = 2m$ for m odd.

□

4.4 $F^{a-c,a,a+2c}$ for $a, c \in \mathbb{Z}$

It was the symmetry of the relator $rs^{a-c}rs^{a}rs^{a+c}$ in the groups $F^{a-c,a,a+c}$ with $c \in \{2, 3, 4\}$ that played a large role in our proof of the $F^{a,b,c}$ conjecture for groups of this type. Thus, for our next step, it seemed the natural progression to study groups of a similar form, namely $F^{a-c,a,a+2c}$, as there still exists simple relationships amongst the powers of s in the relator $rs^{a-c}rs^{a}rs^{a+2c}$.

For the groups

$$F^{a-c,a,a+2c} = \langle r, s | r^2, rs^{a-c}rs^{a}rs^{a+2c} \rangle,$$

we have $n = a - c + a + a + 2c = 3a + c$, $d = ((a - c) - a, a - (a + 2c)) = c$ and $s^{2n} = s^{6a+2c}$.

After having proved the case of $F^{a-c,a,a+c}$ for $c \in \{2, 3, 4\}$, we looked to see if this proof could be modified for the groups $F^{a-c,a,a+2c}$. Several problems arose, however. In our original proof, we required the two facts, $s^{2a} \sim rs^c r$ and $r \sim s^{-c} rs^{2c}$, in both the induction proof of the relation sequence $(rs^{ck} rs^{a-ck})^2 = s^{2a}$ for $k \in \mathbb{N}$ and the reasoning linking our relation sequence to the final results. The same arguments for these two facts could not be used with the groups $F^{a-c,a,a+2c}$ as, we had $|(a-c)-a| = |a-(a+c)|$ for $F^{a-c,a,a+c}$, but here, the equivalent relationship $|(a-c)-a| = |a-(a+2c)|$ did not hold.

Using a similar idea and further manipulations of the relators, however, we did find that we could prove $rs^{6a+2c} r \sim s^c$. We also returned to our earlier work in $F^{a-2,a,a+2}$, when we had noticed

$$(rs^{2k} rs^{3a-2k})^2 = 1 \quad \text{for } k \in \mathbb{Z}.$$

In our study of the groups $F^{a-c,a,a+2c}$, relations of a similar type appeared. These relations had the form

$$(rs^{a+ck+c} rs^{2a-ck})^2 = 1 \quad \text{for } k \in \mathbb{Z},$$

and we recognised that if we could prove such a sequence of relations existed in $F^{a-c,a,a+2c}$, we would have enough to prove at least the case where $c = 2$.

Thus, we set out to find an inductive proof for this new sequence of relations. We found, however, that it was easier to prove if we considered the two elements, $(rs^{a+ck+c} rs^{2a-ck})^2 = 1$ and $(rs^{2a+ck+c} rs^{a-ck})^2 = 1$, together and, similarly to the case $F^{a-c,a,a+c}$, we were able to prove the conjecture for groups of the type $F^{a-c,a,a+2c}$ for $c \in \{2, 3, 4\}$ using our sequence and $rs^{6a+2c} r \sim s^c$.

One of the conditions of the $F^{a,b,c}$ conjecture is that a, b and c must be co-prime. As well as showing the conjecture is correct for groups of the type, $F^{a-c,a,a+2c}$ with $c \in \{2, 3, 4\}$ and $(a, c) = 1$, our proof method also allowed us to extend our research to the cases where $(a,c) \neq 1$, and we include it in the proof for groups of the type $F^{a-c,a,a+2c}$ for $c \in \{2,3,4\}$.

Theorem 4.4 For the groups

$$F^{a-c,a,a+2c} = \langle r, s | r^2, rs^{a-c}rs^a rs^{a+2c} \rangle$$

with $a \in \mathbb{Z}$ and $c \in \{2,3,4\}$, let

$$H^{a-c,a,a+2c} = \langle r, s | r^2, rs^{a-c}rs^a rs^{a+2c}, s^{6a+2c} \rangle.$$

If,

- $c = 2$ and $(a,2) = 1$, then $s^{6a+4} = 1$ and

$$F^{a-2,a,a+4} \cong H^{a-2,a,a+4},$$

- $c = 3$ and $(a,3) = 1$, then $s^{12a+12} = 1$ and

$$F^{a-3,a,a+6}/C_2 \cong H^{a-3,a,a+6},$$

- $c = 4$ and $(a,4) = 1$, then $s^{24a+32} = 1$, $s^{12a+16} \sim r$ and

$$F^{a-4,a,a+8}/Q_8 \cong H^{a-4,a,a+8},$$

- $(a,c) \neq 1$ then $(a-c,a,a+2c) \neq 1$, $s^{6a+2c} = 1$ and

$$F^{a-c,a,a+2c} \cong H^{a-c,a,a+2c}.$$

Proof. In $F^{a-c,a,a+2c}$, we have

$$\begin{aligned} n &= a-c+a+a+2c \\ &= 3a+c, \\ s^{2n} &= s^{6a+2c}, \\ 1 &= (a-c,a,a+2c) \text{ when } (a,c)=1 \quad \text{and} \\ d &= ((a-c)-a, a-(a+2c)) \\ &= c. \end{aligned}$$

Also,

$$\begin{aligned} rs^{a-c}r &= s^{-a-2c}rs^{-a}, \\ rs^{a}r &= s^{c-a}rs^{-a-2c} \quad \text{and} \\ rs^{a+2c}r &= s^{-a}rs^{c-a}. \end{aligned}$$

Hence,

$$\begin{aligned} rs^{2a-2c}r &= (rs^{a-c}r)^2 \\ &= s^{-a-2c}rs^{-2a-2c}rs^{-a}, \qquad (4.7) \end{aligned}$$

$$\begin{aligned} rs^{2a-c}r &= (rs^{a-c}r)(rs^{a}r) \\ &= s^{-a-2c}rs^{c-2a}rs^{-a-2c} \quad \text{and} \qquad (4.8) \\ &= (rs^{a}r)(rs^{a-c}r) \\ &= s^{c-a}rs^{-2a-4c}rs^{-a}, \qquad (4.9) \end{aligned}$$

$$\begin{aligned} rs^{2a}r &= (rs^{a}r)^2 \\ &= s^{c-a}rs^{-2a-c}rs^{-2c-a}, \qquad (4.10) \end{aligned}$$

$$
\begin{aligned}
rs^{2a+c}r &= (rs^{a-c}r)(rs^{a+2c}r) \\
&= s^{-a-2c}rs^{-2a}rs^{c-a} \quad \text{and} \qquad (4.11) \\
&= (rs^{a+2c}r)(rs^{a-c}r) \\
&= s^{-a}rs^{-2a-c}rs^{-a}, \qquad (4.12)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a+2c}r &= (rs^{a}r)(rs^{a+2c}r) \\
&= s^{c-a}rs^{-2a-2c}rs^{c-a} \quad \text{and} \qquad (4.13) \\
&= (rs^{a+2c}r)(rs^{a}r) \\
&= s^{-a}rs^{2c-2a}rs^{-a-2c}, \qquad (4.14)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a+4c}r &= (rs^{a+2c})^2 \\
&= s^{-a}rs^{c-2a}rs^{c-a}, \qquad (4.15)
\end{aligned}
$$

$$
\begin{aligned}
rs^{c}r &= (rs^{a}r)(rs^{c-a}r) \\
&= s^{c-a}rs^{-2c}rs^{a+2c} \quad \text{and} \qquad (4.16) \\
&= (rs^{c-a}r)(rs^{a}r) \\
&= s^{a}rs^{3c}rs^{-a-2c}. \qquad (4.17)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2c}r &= (rs^{a+2c}r)(rs^{-a}r) \\
&= s^{-a}rs^{3c}rs^{a-c} \quad \text{and} \qquad (4.18) \\
&= (rs^{-a}r)(rs^{a+2c}r) \\
&= s^{a+2c}rs^{-c}rs^{c-a}, \qquad (4.19)
\end{aligned}
$$

$$
\begin{aligned}
rs^{3c}r &= (rs^{a+2c}r)(rs^{c-a}r) \\
&= s^{-a}rs^{c}rs^{a+2c} \quad \text{and} \qquad (4.20) \\
&= (rs^{c-a}r)(rs^{a+2c}r) \\
&= s^{a}rs^{2c}rs^{c-a}. \qquad (4.21)
\end{aligned}
$$

So,

$$\begin{aligned}
rs^{2a-c}r &= s^{-a-2c}rs^{c-2a}rs^{-a-2c} \\
&= s^{-a-2c}(s^a rs^{2a+4c}rs^{a-c})s^{-a-2c} \quad \text{from 4.8 and 4.9} \\
&= s^{-2c}rs^{2a+4c}rs^{-3c}, \qquad (4.22)
\end{aligned}$$

$$\begin{aligned}
rs^{2a+c}r &= s^{-a}rs^{-c-2a}rs^{-a} \\
&= s^{-a}(s^{a-c}rs^{2a}rs^{a+2c})s^{-a} \quad \text{from 4.12 and 4.11} \\
&= s^{-c}rs^{2a}rs^{2c}, \qquad (4.23)
\end{aligned}$$

$$\begin{aligned}
rs^{2a+2c}r &= s^{c-a}rs^{-2c-2a}rs^{c-a} \\
&= s^{c-a}(s^{a+2c}rs^{2a-2c}rs^{a})s^{c-a} \quad \text{from 4.13 and 4.14} \\
&= s^{3c}rs^{2a-2c}rs^{c}. \qquad (4.24)
\end{aligned}$$

We begin by proving the two steps (I and II) necessary to prove each of the cases, $c = 2$, $c = 3$ and $c = 4$.

I. $rs^{6a+2c}r \sim s^c$

Using equations 4.23, 4.22 and 4.24 gives

$$\begin{aligned}
rs^{6a+2c}r &= (rs^{2a+c}r)(rs^{2a-c}r)(rs^{2a+2c}r) \\
&= s^{-c}rs^{6a+2c}rs^{c}.
\end{aligned}$$

II. In $F^{a-c,a,a+2c}$ for all integers k,

$$\begin{aligned}
(rs^{2a+ck+c}rs^{a-ck})^2 &= 1 \quad \text{and} \\
(rs^{2a-ck}rs^{a+ck+c})^2 &= 1.
\end{aligned}$$

Proof by induction for $k \geq -1$:

Base step

$k = -1$

$$\begin{aligned} rs^{2a}rs^{a+c}rs^{2a}rs^{a+c} &= rs^{2a}rs^{a+c}(s^c rs^{2a+c}rs^{-2c})s^{a+c} \\ &= rs^{2a}rs^{a+2c}rs^{2a+c}rs^{a-c} \\ &= rs^{2a}(s^{-a}rs^{c-a})s^{2a+c}rs^{a-c} \\ &= rs^a rs^{a+2c}rs^{a-c} \\ &= 1 \end{aligned}$$

$$\begin{aligned} rs^{2a+c}rs^a rs^{2a+c}rs^a &= rs^{2a+c}(s^{c-a}rs^{-a-2c})s^{2a+c}rs^a \\ &= rs^{a+2c}rs^{a-c}rs^a \\ &= 1 \end{aligned}$$

$k = 0$

$$rs^{2a+c}rs^a rs^{2a+c}rs^a = 1 \quad \text{from base case, } k = -1$$

$$rs^{2a}rs^{a+c}rs^{2a}rs^{a+c} = 1 \quad \text{from base case, } k = -1$$

$k = 1$

$$\begin{aligned} rs^{2a+2c}rs^{a-c}rs^{2a+2c}rs^{a-c} &= rs^{2a+2c}(s^{-a-2c}rs^{-a})s^{2a+2c}rs^{a-c} \\ &= rs^a rs^{a+2c}rs^{a-c} \\ &= 1 \end{aligned}$$

$$\begin{aligned} rs^{2a-c}rs^{a+2c}rs^{2a-c}rs^{a+2c} &= rs^{2a-c}(s^{-a}rs^{c-a})s^{2a-c}rs^{a+2c} \\ &= rs^{a-c}rs^a rs^{a+2c} \\ &= 1 \end{aligned}$$

Inductive step

Assume for all integers i, with $-1 \leq i < k$,

$$\begin{aligned}(rs^{2a+ci+c}rs^{a-ci})^2 &= 1 \quad \text{and} \\ (rs^{2a-ci}rs^{a+ci+c})^2 &= 1.\end{aligned}$$

So,

$$\begin{aligned}rs^{a+ci+c}r &= s^{ci-2a}rs^{-a-ci-c}rs^{ci-2a} \quad \text{and} \\ rs^{a-ci}r &= s^{-2a-ci-c}rs^{ci-a}rs^{-2a-ci-c}.\end{aligned}$$

Since we have shown it to be true for $k \in \{-1, 0, 1\}$, we can assume $k \geq 2$.

Consider $i = k$ with $2 \leq k$. We know that because $-1 \leq k-3 < k$, we have

$$\begin{aligned}rs^{a+ck-2c}r &= s^{-2a+ck-3c}rs^{-a-ck+2c}rs^{-2a+ck-3c} \quad \text{and} \\ rs^{a-ck+3c}r &= s^{-2a-ck+2c}rs^{-a+ck-3c}rs^{-2a-ck+2c}.\end{aligned}$$

Also, $0 < k-1 < k$ gives us

$$rs^{a-ck+c}r = s^{-2a-ck}rs^{-a+ck-c}rs^{-2a-ck}.$$

Thus, using

$$\begin{aligned}rs^{a+ck-2c}r &= s^{-2a+ck-3c}rs^{-a-ck+2c}rs^{-2a+ck-3c}, \\ rs^{3c}r &= s^{a}rs^{2c}rs^{c-a}, \\ rs^{-a+ck-3c}r &= s^{2a+ck-2c}rs^{a-ck+3c}rs^{2a+ck-2c} \\ &\text{and} \\ rs^{2a+ck}r &= s^{-a+ck-c}rs^{-2a-ck}rs^{-a+ck-c},\end{aligned}$$

we find

$$
\begin{aligned}
& rs^{a+ck+c}r \\
= \ & (rs^{a+ck-2c}r)(rs^{3c}r) \\
= \ & (s^{-2a+ck-3c}rs^{-a-ck+2c}rs^{-2a+ck-3c})(s^{a}rs^{2c}rs^{c-a}) \\
= \ & s^{-2a+ck-3c}rs^{-a-ck+2c}.rs^{-a+ck-3c}r.s^{2c}rs^{c-a} \\
= \ & s^{-2a+ck-3c}.rs^{a}r.s^{a-ck+3c}rs^{2a+ck}rs^{c-a} \\
= \ & s^{-2a+ck-3c}(s^{c-a}rs^{-a-2c})s^{a-ck+3c}rs^{2a+ck}rs^{c-a} \\
= \ & s^{-3a+ck-2c}rs^{-ck+c}.rs^{2a+ck}r.s^{c-a} \\
= \ & s^{-3a+ck-2c}.rs^{-a}r.s^{-2a-ck}rs^{-2a+ck} \\
= \ & s^{-3a+ck-2c}(s^{a+2c}rs^{a-c})s^{-2a-ck}rs^{-2a+ck} \\
= \ & s^{-2a+ck}rs^{-a-ck-c}rs^{-2a+ck}.
\end{aligned}
$$

Given,

$$
\begin{aligned}
rs^{a-ck+c}r &= s^{-2a-ck}rs^{-a+ck-c}rs^{-2a-ck}, \\
rs^{-c}r &= s^{a+2c}rs^{-3c}rs^{-a}, \\
rs^{-a-ck+2c}r &= s^{2a-ck+3c}rs^{a+ck-2c}rs^{2a-ck+3c} \\
&\text{and} \\
rs^{2a-ck}r &= s^{-a-ck-c}rs^{-2a+ck}rs^{-a-ck-c},
\end{aligned}
$$

we obtain

$$
\begin{aligned}
& rs^{a-ck}r \\
= \; & (rs^{a-ck+c}r)(rs^{-c}r) \\
= \; & (s^{-2a-ck}rs^{-a+ck-c}rs^{-2a-ck})(s^{a+2c}rs^{-3c}rs^{-a}) \\
= \; & s^{-2a-ck}rs^{-a+ck-c}.rs^{-a-ck+2c}r.s^{-3c}rs^{-a} \\
= \; & s^{-2a-ck}.rs^{a+2c}r.s^{a+ck-2c}rs^{2a-ck}rs^{-a} \\
= \; & s^{-2a-ck}(s^{-a}rs^{c-a})s^{a+ck-2c}rs^{2a-ck}rs^{-a} \\
= \; & s^{-3a-ck}rs^{ck-c}.rs^{2a-ck}r.s^{-a} \\
= \; & s^{-3a-ck}.rs^{-a-2c}r.s^{-2a+ck}rs^{-2a-ck-c} \\
= \; & s^{-3a-ck}(s^{a-c}rs^{a})s^{-2a+ck}rs^{-2a-ck-c} \\
= \; & s^{-2a-ck-c}rs^{-a+ck}rs^{-2a-ck-c}.
\end{aligned}
$$

By induction, for all integers $k \geq -1$,

$$
\begin{aligned}
(rs^{2a+ck+c}rs^{a-ck})^2 &= 1 \quad \text{and} \\
(rs^{2a-ck}rs^{a+ck+c})^2 &= 1.
\end{aligned}
$$

Now we need to consider the integers $k < -1$. Let $i > 0$. Here, using $k = -i$, then

$$
\begin{aligned}
(rs^{2a+ck+c}rs^{a-ck})^2 &= (rs^{2a-ci+c}rs^{a+ci})^2 \\
&= (rs^{2a-c(i-1)}rs^{a+c(i-1)+c})^2 \quad \text{and} \\
(rs^{2a-ck}rs^{a+ck+c})^2 &= (rs^{2a+ci}rs^{a-ci+c})^2 \\
&= (rs^{2a+c(i-1)+c}rs^{a-c(i-1)})^2.
\end{aligned}
$$

Thus, the case $k = -i$ is equivalent to that of $i - 1$ for $i > 0$. Since $i > 0$, then $i - 1 \geq -1$, and so,

$$
\begin{aligned}
(rs^{2a+ck+c}rs^{a-ck})^2 &= 1 \quad \text{and} \\
(rs^{2a-ck}rs^{a+ck+c})^2 &= 1 \quad \text{for } k < -1.
\end{aligned}
$$

Therefore, for all integers k,

$$\begin{aligned}(rs^{2a+ck+c}rs^{a-ck})^2 &= 1 \quad \text{and} \\ (rs^{2a-ck}rs^{a+ck+c})^2 &= 1.\end{aligned}$$

1. Proof of the Case $c = 2$

$$F^{a-2,a,a+4} = \langle r, s | r^2, rs^{a-2}rs^a rs^{a+4}\rangle$$

For $F^{a-2,a,a+4}$, if we can prove $s^{2n} = s^{6a+4} = 1$, then we have shown that $F^{a-2,a,a+4} \cong H^{a-2,a,a+4} = \langle r, s | r^2, s^{6a+4}, rs^{a-2}rs^a rs^{a+4}\rangle$.

- For all integers k,

$$\begin{aligned}(rs^{2a+2k+2}rs^{a-2k})^2 &= 1 \text{ and} \\ (rs^{2a-2k}rs^{a+2k+2})^2 &= 1 \quad \text{by II.}\end{aligned}$$

- Using $k = a$ in the above equations, we have

$$\begin{aligned}1 &= (rs^{2a-2a}rs^{a+2a+2})^2 \\ &= (rs^0 rs^{3a+2})^2 \\ &= (s^{3a+2})^2 \\ &= s^{6a+4}.\end{aligned}$$

2. Proof of the Case $c = 3$

$$F^{a-3,a,a+6} = \langle r, s | r^2, rs^{a-3}rs^a rs^{a+6}\rangle$$

For $F^{a-3,a,a+6}$, $n = a - 3 + a + a + 6 = 3a + 3$. If we prove $s^{2n} = s^{6a+6} = s^{-6a-6}$, or $s^{12a+12} = 1$, in $F^{a-3,a,a+6}$, then we can show that $F^{a-3,a,a+6}/C_2 \cong H^{a-3,a,a+6} = \langle r, s | r^2, s^{6a+6}, rs^{a-3}rs^a rs^{a+6}\rangle$.

- For all integers k,

$$\begin{aligned} (rs^{2a+3k+3}rs^{a-3k})^2 &= 1 \text{ and} \\ (rs^{2a-3k}rs^{a+3k+3})^2 &= 1 \quad \text{by II.} \end{aligned}$$

- Substituting $k = a$ in the above equations gives

$$\begin{aligned} 1 &= (rs^{a+3a+3}rs^{2a-3a})^2 \\ &= s^{4a+3}rs^{-a}rs^{4a+3}rs^{-a}r \\ &= s^{4a+3}(s^{a+6}rs^{a-3})s^{4a+3}(s^{a+6}rs^{a-3}) \\ &= s^{5a+9}rs^{6a+6}rs^{a-3} \\ &= s^{5a+9}rs^{6a+6}rs^{a-3} \\ &= s^{6a+6}rs^{6a+6}r. \end{aligned}$$

Thus, $rs^{6a+6}r = s^{-6a-6}$ and $s^{6a+6} = rs^{-6a-6}r$.

- We know $rs^{a-3}rs^ars^{a+6} = 1$ and $rs^{6a+6}r = s^{-6a-6}$ so,

$$\begin{aligned} s^{-6a-6} &= (rs^{a-3}rs^ars^{a+6})(s^{-6a-6}) \\ &= rs^{a-3}rs^a.rs^{-6a-6}.s^{a+6} \\ &= rs^{a-3}rs^{7a+6}rs^{a+6} \\ &= rs^{a-3}.rs^{6a+6}.s^ars^{a+6} \\ &= rs^{-5a-9}rs^ars^{a+6} \\ &= rs^{-6a-6}.s^{a-3}rs^ars^{a+6} \\ &= s^{6a+6}rs^{a-3}rs^ars^{a+6} \\ &= s^{6a+6}. \end{aligned}$$

Thus, $s^{-6a-6} = s^{6a+6}$, s^{6a+6} is central and $s^{12a+12} = 1$.

- $F^{a-3,a,a+6}/C_2 \cong H^{a-3,a,a+6}$ where $(a, 3) = 1$.

Consider $\langle x \rangle$, where $x = s^{6a+6}$. Obviously it is a subgroup of the kernel of the homomorphism from F to H, and since

$$rxr = rs^{6a+6}r = s^{6a+6} = x$$

$$\text{and} \quad s^{-1}xs = x,$$

then $\langle x \rangle$ is the kernel.

We have shown that $s^{4n} = s^{12a+12} = 1$ and s^{6a+6} generates the kernel of the homomorphism. Thus, either $F^{a-3,a,a+6} \cong H^{a-3,a,a+6}$ or $F^{a-3,a,a+6}/C_2 \cong H^{a-3,a,a+6}$. It cannot be that $a-3 \equiv a \equiv a+6 \pmod 6$ and we also have

$$(a-3-a, a-(a+6), 3) = (-3, -6, 3) = 3,$$

so, by Theorem 3.3 of [6], $H^{a-3,a,a+6}$ is finite and has Schur multiplicator C_2.

We now know $F^{a-3,a,a+6}$ is finite and as it has a 2-generator, 2-relator presentation, it has deficiency 0 and, by Corollory 1.2 of [31], a trivial multiplicator. Thus, $F^{a-3,a,a+6} \ncong H^{a-3,a,a+6}$, and it must be such that, when a is not a multiple of 3,

$$F^{a-3,a,a+6}/C_2 \cong H^{a-3,a,a+6}.$$

3. Proof of the Case $c = 4$

$$F^{a-4,a,a+8} = \langle r, s | r^2, rs^{a-4}rs^a rs^{a+8} \rangle$$

For $F^{a-4,a,a+8}$, we need to prove that $rs^{-6a-8}rs^{6a+8}rs^{6a+8}r = s^{-6a-8}$, $s^{24a+32} = 1$ and s^{12a+16} is central in $F^{a-4,a,a+8}$. A presentation for Q_8 is $\langle x, y | x^4, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$. Thus, taking $x = s^{6a+8}$ and $y = rs^{6a+8}r$ and proving that the kernel is generated by s^{6a+8} and $rs^{6a+8}r$, we would then be able to show $F^{a-4,a,a+8}/Q_8 \cong H^{a-4,a,a+8}$.

- $rs^{6a+8}r \sim s^4$ by I.

- For all integers k,

$$\begin{aligned}
(rs^{2a+4k+4}rs^{a-4k})^2 &= 1 \text{ and} \\
(rs^{2a-4k}rs^{a+4k+4})^2 &= 1 \qquad \text{by II.}
\end{aligned}$$

- Setting $k = a$ and $k = 0$ in the previous equations, we obtain

$$\begin{aligned}
rs^{-2a}rs^{5a+4}rs^{-2a}rs^{5a+4} &= 1 \quad \text{and} \\
rs^{2a+4}rs^{a}rs^{2a+4}rs^{a} &= 1.
\end{aligned}$$

So, as $rs^{2a}r = s^4rs^{2a+4}rs^{-8}$, then

$$\begin{aligned}
1 &= rs^{-2a}rs^{5a+4}rs^{-2a}rs^{5a+4} \\
&= (s^8rs^{-2a-4}rs^{-4})s^{5a+4}(s^8rs^{-2a-4}rs^{-4})s^{5a+4} \\
&= s^8rs^{-2a-4}rs^{5a+8}rs^{-2a-4}rs^{5a} \\
&= rs^{-2a-4}rs^{5a+8}rs^{-2a-4}rs^{5a+8} \\
&= rs^{-2a-4}rs^{5a+8}(s^{a}rs^{2a+4}rs^{a})s^{5a+8} \\
&= rs^{-2a-4}rs^{6a+8}rs^{2a+4}rs^{6a+8}.
\end{aligned}$$

We also know that $rs^{6a+8}r \sim s^4$ and, as a must be odd to ensure $(a-4, a, a+8) = 1$, then $rs^{6a+8}r \sim s^{2a+2}$. Thus,

$$\begin{aligned}
1 &= rs^{-2a-4}rs^{6a+8}rs^{2a+4}rs^{6a+8} \\
&= rs^{-2}rs^{6a+8}rs^{2}rs^{6a+8}
\end{aligned}$$

and $s^{-2}rs^{6a+8}rs^2 = rs^{-6a-8}r$.

- We know a must be odd, so s^{6a+6} is a multiple of 4. Therefore, from $s^{-2}rs^{6a+8}rs^2 = rs^{-6a-8}r$ and $rs^{6a+8}r \sim s^4$, we obtain

$$\begin{aligned}
rs^{-6a-8}rs^{6a+8}rs^{6a+8}r &= s^{-6a-8} \quad \text{and} \\
rs^{6a+8}rs^{6a+8}rs^{-6a-8}r &= s^{-6a-8}. \qquad (4.25)
\end{aligned}$$

- We have

$$\begin{aligned} s^{-6a-8}rs^{6a+8}rs^{6a+8} &= rs^{-6a-8}r \quad \text{so,} \\ s^{6a+8}rs^{6a+8} &= rs^{6a+8}rs^{-6a-8}r. \end{aligned}$$

  Alternatively,

$$\begin{aligned} s^{6a+8}rs^{6a+8}rs^{-6a-8} &= rs^{-6a-8}r \quad \text{so,} \\ s^{6a+8}rs^{6a+8} &= rs^{-6a-8}rs^{6a+8}r. \end{aligned}$$

  Hence,

$$\begin{aligned} rs^{6a+8}rs^{-6a-8}r &= rs^{-6a-8}rs^{6a+8}r \\ s^{12a+16} &= rs^{12a+16}r, \end{aligned}$$

  and s^{12a+16} is central.

  Also,

$$\begin{aligned} rs^{6a+8}rs^{-6a-8}r &= (rs^{6a+8}rs^{-6a-8}r)^{-1} \\ s^{6a+8}rs^{6a+8} &= s^{-6a-8}rs^{-6a-8} \\ s^{12a+16} &= rs^{-12a-16}r. \end{aligned}$$

  Thus, $s^{12a+16} = s^{-12a-16}$ and $s^{24a+32} = 1$.

- Since we have that $rs^{-6a-8}rs^{6a+8}rs^{6a+8}r = s^{-6a-8}$, $s^{24a+32} = 1$ and s^{12a+16} is central, we need only check that $\{s^{6a+8}, rs^{6a+8}r\}$ generates the kernel of the homomorphism from F to H. Let $x = s^{6a+8}$ and $y = rs^{6a+8}r$, and consider $\langle x, y\rangle$. Obviously, $\langle x, y\rangle$ is a subgroup of the kernel, and we have $rxr = y$, $ryr = x$ and $s^{-1}xs = x$. We now need to test $s^{-1}ys \in \langle x, y\rangle$ to show that $\langle x, y\rangle$ is the kernel.

Using $k = a+1$ in $(rs^{2a+4k+4}rs^{a-4k})^2 = 1$, we have

$$\begin{aligned} 1 &= rs^{6a+8}rs^{-3a-4}rs^{6a+8}rs^{-3a-4} \quad \text{and} \\ s^a rs^{6a+8}rs^{-a} &= s^{4a+4}rs^{-6a-8}rs^{2a+4}. \end{aligned}$$

We also know $rs^{6a+8}r \sim s^4$, so

$$\begin{aligned} s^a rs^{6a+8}rs^{-a} &= s^{4a+4}rs^{-6a-8}rs^{2a+4} \\ &= rs^{-6a-8}rs^{6a+8}. \end{aligned}$$

As it must be such that a is an odd number, we have two cases.

(a) $a \equiv 1 \pmod 4$
Here, $a+1 \equiv 2 \pmod 4$.
Thus,

$$\begin{aligned} rs^{6a+8}r &= s^{a+1}rs^{-6a-8}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a+8}rs &= s^a rs^{-6a-8}rs^{-a}, \end{aligned}$$

and we have

$$\begin{aligned} s^{-1}rs^{6a+8}rs &= s^a rs^{-6a-8}rs^{-a} \\ &= rs^{-6a-8}rs^{6a+8} \\ &= y^{-1}x. \end{aligned}$$

(b) $a \equiv 3 \pmod 4$
Now, $a+1 \equiv 0 \pmod 4$.
Thus,

$$\begin{aligned} rs^{6a+8}r &= s^{a+1}rs^{6a+8}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a+8}rs &= s^a rs^{6a+8}rs^{-a}, \end{aligned}$$

and hence,

$$\begin{aligned} s^{-1}rs^{6a+8}rs &= s^a rs^{6a+8}rs^{-a} \\ &= s^{-6a-8}rs^{6a+8}r \\ &= x^{-1}y. \end{aligned}$$

Therefore, $\{x, y\}$ generates the kernel. Also, x and y both have order dividing 4, we know $y^{-1}xy = x^{-1}$ from 4.25 and, since s^{12a+16} is central, $x^2 = y^2$. Given this, we know $\langle x, y\rangle$ is a homomorphic image of Q_8, which has derived length 2. It is left to show $\langle x, y\rangle \cong Q_8$.

Consider the group

$$G^{a,b,c} = \langle r, s | r^2, s^8, rs^a rs^b rs^c\rangle,$$

a homomorphic image of $F^{a,b,c}$. Here, $G^{a,b,c} \cong G^{a',b',c'}$, where a', b' and c' are a, b and c modulo 8. Using $F^{a-4,a,a+8}$ for the case $d = 4$, then we know a is odd and so, $a' \in \{1, 3, 5, 7\}$. Thus, we are left with only four cases for $G^{a-4,a,a+8}$: $G^{5,1,1}$, $G^{7,3,3}$, $G^{1,5,5}$ and $G^{3,7,7}$. Using GAP, we obtain that each of these four groups has derived length 4, and $F^{a-4,a,a+8}$ must have derived length of at least 4.

From Theorem 3.5 of [3], the groups $H^{a,b,c}$ are finite metabelian groups when $(a, b, c) = 1$, $n \neq 0$ and $(d, 6) \neq 6$. As a is odd and $d = 4$, then $H^{a-4,a,a+8}$ is finite metabelian and, therefore, has derived length 2. This implies that $\langle x, y\rangle$, the kernel of the natural homomorphism from $F^{a-4,a,a+8}$ to $H^{a-4,a,a+8}$, must have derived length at least 2 and $\langle x, y\rangle \cong Q_8$.

4. Proof of the Case $(a, c) \neq 1$

When $(a, c) \neq 1$ for $c \in \{2, 3, 4\}$, then we have $(a - c, a, a + 2c) \neq 1$ and either of two cases

(a) a is a multiple of c or

(b) $c = 4$ and a is a multiple of 2.

If a is a multiple of c, then all of $a - c$, a and $a + 2c$ are divisible by c and, as such, are not co-prime. For $F^{a-c,a,a+2c}$ where $a = cm$ for some integer m, then using $(rs^{2a+ck+c}rs^{a-ck})^2 = 1$ and substituting $k = m$, we have

$$\begin{aligned} 1 &= (rs^{2a+ck+c}rs^{a-ck})^2 \\ &= (rs^{2a+cm+c}rs^{a-cm})^2 \\ &= (rs^{2a+a+c}rs^{a-a})^2 \\ &= (rs^{3a+c}rs^{0})^2 \\ &= rs^{6a+2c}r, \end{aligned}$$

and so, $s^{6a+2c} = 1$.

We find that where a is a multiple of c, $F^{a-c,a,a+2c} \cong H^{a-c,a,a+2c}$.

We just need to look at the case where $c = 4$ and $a = 2m$ for some odd integer m. Using $k = m$ in $(rs^{2a-4k}rs^{a+4k+4})^2 = 1$ gives

$$\begin{aligned} 1 &= (rs^{2a-4k}rs^{a+4k+4})^2 \\ &= (rs^{2a-4m}rs^{a+4m+4})^2 \\ &= (rs^{2a-2a}rs^{a+2a+4})^2 \\ &= (s^{3a+4})^2 \\ &= s^{6a+8}, \end{aligned}$$

and $s^{2n} = s^{6a+8} = 1$. Hence, $F^{a-4,a,a+8} \cong H^{a-4,a,a+8}$ where $a = 2m$ for m odd.

Thus, if $c \in \{2, 3, 4\}$ and $(a - c, a, a + 2c) \neq 1$, we find that

$$F^{a-c,a,a+2c} \cong H^{a-c,a,a+2c}.$$

$\square$

4.5 $F^{a-c,a,a+kc}$ for $a, c, k \in \mathbb{Z}$

Having formulated proofs of the conjecture for two similar types of groups, $F^{a-c,a,a+c}$ and $F^{a-c,a,a+2c}$ for $c \in \{2,3,4\}$, we hoped we could use them to make a generalisation for a larger set of groups, and our next step was, therefore, to try groups of the type $F^{a-c,a,a+kc}$ for an integer k.

At first glance, it seemed the transition from our proof of $F^{a-c,a,a+2c}$ to a proof of $F^{a-c,a,a+kc}$ would be relatively easy. In $F^{a-c,a,a+kc}$, we have $s^{2n} = s^{6a+2kc-2c}$, and it was easy to obtain $rs^{6a+2kc-2c} \sim s^c$ using the same arguments as in the former proof. It was also noted that if we could prove equivalent relation sequences in $F^{a-c,a,a+kc}$ to those in $F^{a-c,a,a+2c}$, the desired results for each of the cases, $c = 2$, $c = 3$ and $c = 4$, would follow similarly to the proof of $F^{a-c,a,a+2c}$.

Thus, we concentrated on trying to prove the relation sequences,

$$\begin{aligned} (rs^{2a+cm+kc-c}rs^{a-cm})^2 &= 1 \quad \text{and} \\ (rs^{2a-cm}rs^{a+cm+kc-c})^2 &= 1 \end{aligned}$$

for an integer m, and set out to first find an inductive proof over m for $m \geq -1$. Although we could prove the base cases, $m = 0$ and $m = 1$, the first problem occurred with the base case $m = -1$, which we realised was no longer obvious.

A much larger difficulty was found in the inductive step. In the proof of

$$\begin{aligned} (rs^{2a+cm+c}rs^{a-cm})^2 &= 1 \quad \text{and} \\ (rs^{2a-cm}rs^{a+cm+c})^2 &= 1 \end{aligned}$$

for $F^{a-c,a,a+2c}$, the first line of this step involved rewriting $rs^{a+cm+c}r$ as $(rs^{a+cm-2c}r)(rs^{3c}r)$. We could continue because $rs^{a+cm-2c}r$ is determined in the case $m-3$ and, given that we had three base cases beginning with -1, then $2 \leq m$ and $-1 \leq m-3 < m$. Hence, we could assume the relation $(rs^{2a-cm+3c}rs^{a+cm-2c}r)^2 = 1$ from our inductive hypothesis.

If we were to use the same proof for our relation sequence, the first line, modified slightly to fit the new type of groups, would be

$$rs^{a+cm+kc-c}r = (rs^{a+cm-2c}r)(rs^{kc+c}r).$$

However, to continue, we would need to be able to assume the relation $(rs^{2a-cm+kc+c}rs^{a+cm-2c}r)^2 = 1$, which falls in the case $m - k - 1$ of the relation sequences. Thus, to use our inductive hypothesis, we would need $0 \leq m-k-1 < m$ and $k+1 \leq m$. Even being able to prove all the three base cases $m \in \{-1, 0, 1\}$ would not be enough if $k > 2$.

However, we noticed that if, instead of having $k+1$ base cases, we were able to prove both relations for the case $m-k-1$, then the induction proof from $F^{a-c,a,a+2c}$ could be easily modified and used for the groups $F^{a-c,a,a+kc}$. It required some work, and once we had found a proof for the relations of this case, our proof only required the two base cases, $m = 0$ and $m = 1$. As these had already been determined, we were able to formulate a proof of the conjecture for the groups $F^{a-c,a,a+kc}$ with $a, k \in \mathbb{Z}$ and $c \in \{2, 3, 4\}$, which we now state in the form of a theorem.

Theorem 4.5 For the groups

$$F^{a-c,a,a+kc} = \langle r, s | r^2, rs^{a-c}rs^a rs^{a+kc} \rangle$$

with $a \in \mathbb{Z}$ and $c \in \{2, 3, 4\}$, let

$$H^{a-c,a,a+kc} = \langle r, s | r^2, rs^{a-c}rs^a rs^{a+kc}, s^{6a+2kc-2c} \rangle.$$

If,

- $c = 2$ and $(a, 2) = 1$, then $s^{6a+4k-4} = 1$ and

$$F^{a-2,a,a+2k} \cong H^{a-2,a,a+2k},$$

- $c = 3$ and $(a, 3) = 1$, then $s^{12a+12k-12} = 1$ and

$$F^{a-3,a,a+3k}/C_2 \cong H^{a-3,a,a+3k},$$

- $c = 4$ and $(a, 4) = 1$, then $s^{24a+32k-32} = 1$, $s^{12a+16k-16} \sim r$ and

$$F^{a-4,a,a+4k}/Q_8 \cong H^{a-4,a,a+4k},$$

- $(a, c) \neq 1$ then $(a-c, a, a+kc) \neq 1$, $s^{6a+2kc-2c} = 1$ and

$$F^{a-c,a,a+kc} \cong H^{a-c,a,a+kc}.$$

Proof. In $F^{a-c,a,a+kc}$, we have

$$\begin{aligned} n &= a - c + a + a + kc \\ &= 3a + kc - c, \\ s^{2n} &= s^{6a+2kc-2c}, \\ 1 &= (a-c, a, a+kc) \text{ when } (a,c) = 1 \quad \text{and} \\ d &= ((a-c) - a, a - (a+kc)) \\ &= c. \end{aligned}$$

Also,

$$\begin{aligned} rs^{a-c}r &= s^{-a-kc}rs^{-a}, \\ rs^{a}r &= s^{c-a}rs^{-a-kc} \quad \text{and} \\ rs^{a+kc}r &= s^{-a}rs^{c-a}. \end{aligned}$$

Hence,

$$\begin{aligned} rs^{2a-2c}r &= (rs^{a-c}r)^2 \\ &= s^{-a-kc}rs^{-2a-kc}rs^{-a}, \end{aligned} \tag{4.26}$$

$$\begin{aligned} rs^{2a-c}r &= (rs^{a-c}r)(rs^{a}r) \\ &= s^{-a-kc}rs^{c-2a}rs^{-a-kc} \quad \text{and} \qquad (4.27)\\ &= (rs^{a}r)(rs^{a-c}r) \\ &= s^{c-a}rs^{-2a-2kc}rs^{-a}, \qquad (4.28) \end{aligned}$$

$$\begin{aligned} rs^{2a}r &= (rs^{a}r)^2 \\ &= s^{c-a}rs^{-2a-kc+c}rs^{-a-kc}, \qquad (4.29) \end{aligned}$$

$$\begin{aligned} rs^{2a+kc-c}r &= (rs^{a-c}r)(rs^{a+kc}r) \\ &= s^{-a-kc}rs^{-2a}rs^{c-a} \quad \text{and} \qquad (4.30)\\ &= (rs^{a+kc}r)(rs^{a-c}r) \\ &= s^{-a}rs^{-2a-kc+c}rs^{-a}, \qquad (4.31) \end{aligned}$$

$$\begin{aligned} rs^{2a+kc}r &= (rs^{a}r)(rs^{a+kc}r) \\ &= s^{c-a}rs^{-2a-kc}rs^{c-a} \quad \text{and} \qquad (4.32)\\ &= (rs^{a+kc}r)(rs^{a}r) \\ &= s^{-a}rs^{2c-2a}rs^{-a-kc}, \qquad (4.33) \end{aligned}$$

$$\begin{aligned} rs^{2a+2kc}r &= (rs^{a+kc})^2 \\ &= s^{-a}rs^{c-2a}rs^{c-a}, \qquad (4.34) \end{aligned}$$

$$\begin{aligned} rs^{c}r &= (rs^{a}r)(rs^{c-a}r) \\ &= s^{c-a}rs^{-kc}rs^{a+kc} \quad \text{and} \qquad (4.35)\\ &= (rs^{c-a}r)(rs^{a}r) \\ &= s^{a}rs^{kc+c}rs^{-a-kc}, \qquad (4.36) \end{aligned}$$

$$\begin{aligned} rs^{kc}r &= (rs^{a+kc}r)(rs^{-a}r) \\ &= s^{-a}rs^{kc+c}rs^{a-c} \quad \text{and} \qquad (4.37) \\ &= (rs^{-a}r)(rs^{a+kc}r) \\ &= s^{a+kc}rs^{-c}rs^{c-a}, \qquad (4.38) \end{aligned}$$

$$\begin{aligned} rs^{kc+c}r &= (rs^{a+kc}r)(rs^{c-a}r) \\ &= s^{-a}rs^{c}rs^{a+kc} \quad \text{and} \qquad (4.39) \\ &= (rs^{c-a}r)(rs^{a+kc}r) \\ &= s^{a}rs^{kc}rs^{c-a}. \qquad (4.40) \end{aligned}$$

So,

$$\begin{aligned} rs^{2a-c}r &= s^{-a-kc}rs^{c-2a}rs^{-a-kc} \\ &= s^{-a-kc}(s^{a}rs^{2a+2kc}rs^{a-c})s^{-a-kc} \quad \text{from 4.27 and 4.28} \\ &= s^{-kc}rs^{2a+2kc}rs^{-kc-c}, \qquad (4.41) \end{aligned}$$

$$\begin{aligned} rs^{2a+kc-c}r &= s^{-a}rs^{-2a-kc+c}rs^{-a} \\ &= s^{-a}(s^{a-c}rs^{2a}rs^{a+kc})s^{-a} \quad \text{from 4.31 and 4.30} \\ &= s^{-c}rs^{2a}rs^{kc}, \qquad (4.42) \end{aligned}$$

$$\begin{aligned} rs^{2a+kc}r &= s^{c-a}rs^{-2a-kc}rs^{c-a} \\ &= s^{c-a}(s^{a+kc}rs^{2a-2c}rs^{a})s^{c-a} \quad \text{from 4.32 and 4.33} \\ &= s^{kc+c}rs^{2a-2c}rs^{c}. \qquad (4.43) \end{aligned}$$

I. $rs^{6a+2kc-2c}r \sim s^{c}$

Using equations 4.42, 4.41 and 4.43 gives

$$\begin{aligned} rs^{6a+2kc-2c}r &= (rs^{2a+kc-c}r)(rs^{2a-c}r)(rs^{2a+kc}r) \\ &= s^{-c}rs^{6a+2kc-2c}rs^{c}. \end{aligned}$$

II. In $F^{a-c,a,a+kc}$, for all integers $m \geq 0$,

$$\begin{aligned}(rs^{2a+cm+kc-c}rs^{a-cm})^2 &= 1 \quad \text{and} \\ (rs^{2a-cm}rs^{a+cm+kc-c})^2 &= 1.\end{aligned}$$

Proof by induction:

Base step

$m = 0$

$$\begin{aligned}& rs^{2a+kc-c}rs^{a}rs^{2a+kc-c}rs^{a} \\ = \;& rs^{2a+kc-c}(s^{c-a}rs^{-a-kc})s^{2a+kc-c}rs^{a} \\ = \;& rs^{a+kc}rs^{a-c}rs^{a} \\ = \;& 1\end{aligned}$$

$$\begin{aligned}& rs^{2a}rs^{a+kc-c}rs^{2a}rs^{a+kc-c} \\ = \;& rs^{2a}rs^{a+kc-c}(s^{c}rs^{2a+kc-c}rs^{-kc})s^{a+kc-c} \\ = \;& rs^{2a}rs^{a+kc}rs^{2a+kc-c}rs^{a-c} \\ = \;& rs^{2a}(s^{-a}rs^{c-a})s^{2a+kc-c}rs^{a-c} \\ = \;& rs^{a}rs^{a+kc}rs^{a-c} \\ = \;& 1\end{aligned}$$

$m = 1$

$$\begin{aligned}& rs^{2a+kc}rs^{a-c}rs^{2a+kc}rs^{a-c} \\ = \;& rs^{2a+kc}(s^{-a-kc}rs^{-a})s^{2a+kc}rs^{a-c} \\ = \;& rs^{a}rs^{a+kc}rs^{a-c} \\ = \;& 1\end{aligned}$$

$$\begin{aligned}
& rs^{2a-c}rs^{a+kc}rs^{2a-c}rs^{a+kc} \\
= \; & rs^{2a-c}(s^{-a}rs^{c-a})s^{2a-c}rs^{a+kc} \\
= \; & rs^{a-c}rs^{a}rs^{a+kc} \\
= \; & 1
\end{aligned}$$

Inductive step

Assume for $0 \leq i < m$,

$$\begin{aligned}
(rs^{2a+ci+kc-c}rs^{a-ci})^2 &= 1 \quad \text{and} \\
(rs^{2a-ci}rs^{a+ci+kc-c})^2 &= 1.
\end{aligned}$$

Since we have shown it to be true for $m \in \{0, 1\}$, we can assume $m \geq 2$.

Consider $i = m$, with $2 \leq m$. We know $0 \leq m - 2 < m$, so

$$\begin{aligned}
(rs^{2a+cm+kc-3c}rs^{a-cm+2c})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm+2c}rs^{a+cm+kc-3c})^2 &= 1.
\end{aligned}$$

Also, $0 < m - 1 < m$, so

$$\begin{aligned}
(rs^{2a+cm+kc-2c}rs^{a-cm+c})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm+c}rs^{a+cm+kc-2c})^2 &= 1.
\end{aligned}$$

We need some additional equations for our proof. Consider $m - k - 1$. Where $m \leq k$, then $m - k - 1 < 0$ and we cannot assume that either

$$\begin{aligned}
(rs^{2a-c(m-k-1)}rs^{a+c(m-k-1)+kc-c})^2 &= (rs^{2a-cm+kc+c}rs^{a+cm-2c})^2 \\
&= 1 \quad \text{or} \\
(rs^{2a+c(m-k-1)+kc-c}rs^{a-c(m-k-1)})^2 &= (rs^{2a+cm-2c}rs^{a-cm+kc+c})^2 \\
&= 1.
\end{aligned}$$

Using our inductive hypothesis, however, we can form the proofs for these necessary equations. We have

$$
\begin{aligned}
r &= s^{kc} r s^{a-c} r s^{c} r s^{-a-kc}, \quad \text{from 4.38}\\
1 &= (r s^{a+cm+kc-2c} r s^{2a-cm+c})^2,\\
1 &= (r s^{-a+cm-2c} r s^{-2a-cm-kc+3c})^2
\end{aligned}
$$

and

$$
1 = (r s^{2a+cm+kc-2c} r s^{a-cm+c})^2,
$$

which gives

$$
\begin{aligned}
& r s^{2a-cm+kc+c} r s^{a+cm-2c} r\\
=\ & r s^{2a-cm+kc+c} r s^{a+cm-2c} . r.\\
=\ & r s^{2a-cm+kc+c} . r s^{a+cm+kc-2c} r . s^{a-c} r s^{c} r s^{-a-kc}\\
=\ & r s^{kc} r s^{-a-cm-kc+2c} . r s^{-a+cm-2c} r . s^{c} r s^{-a-kc}\\
=\ & r s^{kc} r s^{a-c} r s^{a-cm+2c} . r s^{2a+cm+kc-2c} r . s^{-a-kc}\\
=\ & r s^{kc} . r s^{a-c} r . s^{c} r s^{-2a-cm-kc+2c} r s^{-2a+cm-kc-c}\\
=\ & r s^{kc} (s^{-a-kc} r s^{-a}) s^{c} r s^{-2a-cm-kc+2c} r s^{-2a+cm-kc-c}\\
=\ & r s^{-a} . r s^{c-a} r . s^{-2a-cm-kc+2c} r s^{-2a+cm-kc-c}\\
=\ & r s^{-a} (s^{a} r s^{a+kc}) s^{-2a-cm-kc+2c} r s^{-2a+cm-kc-c}\\
=\ & s^{-a-cm+2c} r s^{-2a+cm-kc-c}.
\end{aligned}
$$

From

$$
\begin{aligned}
r &= s^{a+kc} r s^{a-c} r s^{a},\\
r &= s^{c-a} r s^{-a-kc} r s^{-a},\\
1 &= (r s^{2a+cm+kc-2c} r s^{a-cm+c})^2,\\
1 &= (r s^{-2a+cm-kc-c} r s^{-a-cm+2c})^2
\end{aligned}
$$

and

$$
1 = (r s^{2a-cm+kc+c} r s^{a+cm-2c})^2,
$$

we obtain

$$\begin{aligned}
& rs^{a-cm+kc+c}rs^{2a+cm-2c}r \\
= \ & rs^{a-cm+kc+c}rs^{2a+cm-2c}.r. \\
= \ & rs^{a-cm+kc+c}rs^{3a+cm+kc-2c}rs^{a-c}rs^{a} \\
= \ & rs^{a-cm+kc+c}.r.s^{3a+cm+kc-2c}rs^{a-c}rs^{a} \\
= \ & rs^{-cm+kc+2c}rs^{-a-kc}.rs^{2a+cm+kc-2c}r.s^{a-c}rs^{a} \\
= \ & rs^{-cm+kc+2c}.rs^{-2a+cm-kc-c}r.s^{-2a-cm-kc+2c}rs^{cm-2c}rs^{a} \\
= \ & rs^{a+kc}rs^{2a-cm+kc+c}.rs^{-a-kc}r.s^{cm-2c}rs^{a} \\
= \ & rs^{a+kc}rs^{2a-cm+kc+c}(s^{a-c}rs^{a})s^{cm-2c}rs^{a} \\
= \ & .rs^{a+kc}r.s^{3a-cm+kc}rs^{a+cm-2c}rs^{a} \\
= \ & (s^{-a}rs^{c-a})s^{3a-cm+kc}rs^{a+cm-2c}rs^{a} \\
= \ & s^{-a}.rs^{2a-cm+kc+c}rs^{a+cm-2c}r.s^{a} \\
= \ & s^{-2a-cm+2c}rs^{-a+cm-kc-c}.
\end{aligned}$$

Thus,

$$\begin{aligned}
(rs^{2a-cm+kc+c}rs^{a+cm-2c})^2 &= 1 \quad \text{and} \\
(rs^{2a+cm-2c}rs^{a-cm+kc+c})^2 &= 1.
\end{aligned}$$

Now, let $i = m$.

From

$$\begin{aligned}
rs^{a+cm-2c}r &= s^{-2a+cm-kc-c}rs^{-a-cm+2c}rs^{-2a+cm-kc-c}, \\
rs^{kc+c}r &= s^{a}rs^{kc}rs^{c-a}, \\
rs^{-a+cm-kc-c}r &= s^{2a+cm-2c}rs^{a-cm+kc+c}rs^{2a+cm-2c} \\
&\text{and} \\
rs^{2a+cm+kc-2c}r &= s^{-a+cm-c}rs^{-2a-cm-kc+2c}rs^{-a+cm-c},
\end{aligned}$$

we find

$$
\begin{aligned}
& rs^{a+cm+kc-c}r \\
= \;& (rs^{a+cm-2c}r)(rs^{kc+c}r) \\
= \;& s^{-2a+cm-kc-c}rs^{-a-cm+2c}.rs^{-a+cm-kc-c}r.s^{kc}rs^{c-a} \\
= \;& s^{-2a+cm-kc-c}.rs^{a}r.s^{a-cm+kc+c}rs^{2a+cm+kc-2c}rs^{c-a} \\
= \;& s^{-2a+cm-kc-c}(s^{c-a}rs^{-a-kc})s^{a-cm+kc+c}rs^{2a+cm+kc-2c}rs^{c-a} \\
= \;& s^{-3a+cm-kc}rs^{-cm+c}.rs^{2a+cm+kc-2c}r.s^{c-a} \\
= \;& s^{-3a+cm-kc}.rs^{-a}r.s^{-2a-cm-kc+2c}rs^{-2a+cm} \\
= \;& s^{-3a+cm-kc}(s^{a+kc}rs^{a-c})s^{-2a-cm-kc+2c}rs^{-2a+cm} \\
= \;& s^{-2a+cm}rs^{-a-cm-kc+c}rs^{-2a+cm},
\end{aligned}
$$

and, using

$$
\begin{aligned}
rs^{a-cm+c}r &= s^{-2a-cm-kc+2c}rs^{-a+cm-c}rs^{-2a-cm-kc+2c}, \\
rs^{-c}r &= s^{a+kc}rs^{-kc-c}rs^{-a}, \\
rs^{-a-cm+2c}r &= s^{2a-cm+kc+c}rs^{a+cm-2c}rs^{2a-cm+kc+c} \\
&\text{and} \\
rs^{2a-cm}r &= s^{-a-cm-kc+c}rs^{-2a+cm}rs^{-a-cm-kc+c},
\end{aligned}
$$

we have

$$\begin{aligned}
& rs^{a-cm}r \\
= \ & (rs^{a-cm+c}r)(rs^{-c}r) \\
= \ & s^{-2a-cm-kc+2c}rs^{-a+cm-c}.rs^{-a-cm+2c}r.s^{-kc-c}rs^{-a} \\
= \ & s^{-2a-cm-kc+2c}.rs^{a+kc}r.s^{a+cm-2c}rs^{2a-cm}rs^{-a} \\
= \ & s^{-2a-cm-kc+2c}(s^{-a}rs^{c-a})s^{a+cm-2c}rs^{2a-cm}rs^{-a} \\
= \ & s^{-3a-cm-kc+2c}rs^{cm-c}.rs^{2a-cm}r.s^{-a} \\
= \ & s^{-3a-cm-kc+2c}.rs^{-a-kc}r.s^{-2a+cm}rs^{-2a-cm-kc+c} \\
= \ & s^{-3a-cm-kc+2c}(s^{a-c}rs^{a})s^{-2a+cm}rs^{-2a-cm-kc+c} \\
= \ & s^{-2a-cm-kc+c}rs^{-a+cm}rs^{-2a-cm-kc+c}.
\end{aligned}$$

Thus, by induction, for all integers $m \geq 0$,

$$\begin{aligned}
(rs^{2a+cm+kc-c}rs^{a-cm})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm}rs^{a+cm+kc-c})^2 &= 1.
\end{aligned}$$

Let us now choose $m < 0$. Using $m = -i$ for an integer $i > 0$, we have

$$\begin{aligned}
(rs^{2a+cm+kc-c}rs^{a-cm})^2 &= (rs^{2a-ci+kc-c}rs^{a+ci})^2 \\
&= (rs^{2a-c(i-k+1)}rs^{a+c(i-k+1)+kc-c})^2 \quad \text{and}
\end{aligned}$$

$$\begin{aligned}
(rs^{2a-cm}rs^{a+cm+kc-c})^2 &= (rs^{2a+ci}rs^{a-ci+kc-c})^2 \\
&= (rs^{2a+c(i-k+1)+kc-c}rs^{a-c(i-k+1)})^2.
\end{aligned}$$

Thus, this is equivalent to the case $m = i - k + 1$. Obviously, as $i > 0$, then $i + 2 > 0$, and we have

$$\begin{aligned}
(rs^{2a+c(i+2)+kc-c}rs^{a-c(i+2)})^2 &= 1 \quad \text{and} \\
(rs^{2a-c(i+2)}rs^{a+c(i+2)+kc-c})^2 &= 1.
\end{aligned}$$

During the proof of m, however, we found that the two expressions were also trivial for $m-k-1$. Hence, for $m=i+2$, we have the equations true for $(i+2)-k-1=i-k+1$, and so, we have a proof for all negative integers as well.

Hence, for all integers m,

$$\begin{aligned}(rs^{2a+cm+kc-c}rs^{a-cm})^2 &= 1 \quad \text{and}\\ (rs^{2a-cm}rs^{a+cm+kc-c})^2 &= 1.\end{aligned}$$

1. Proof of the Case $c=2$

$$F^{a-2,a,a+2k} = \langle r,s|r^2, rs^{a-2}rs^a rs^{a+2k}\rangle$$

For $F^{a-2,a,a+2k}$, $n=3a+2k-2$ and, if we can show that $s^{2n}=s^{6a+4k-4}=1$, then we have proved that $F^{a-2,a,a+2k}\cong H^{a-2,a,a+2k}=\langle r,s|r^2,s^{6a+4k-4},rs^{a-2}rs^a rs^{a+2k}\rangle$.

- For all integers m,

$$\begin{aligned}(rs^{2a+2m+2k-2}rs^{a-2m})^2 &= 1 \text{ and}\\ (rs^{2a-2m}rs^{a+2m+2k-2})^2 &= 1 \quad \text{by II.}\end{aligned}$$

- Using $m=a$ in the above equations, we have

$$\begin{aligned}1 &= (rs^{2a-2a}rs^{a+2a+2k-2})^2\\ &= (rs^0rs^{3a+2k-2})^2\\ &= (s^{3a+2k-2})^2\\ &= s^{6a+4k-4}.\end{aligned}$$

2. Proof of the Case $c=3$

$$F^{a-3,a,a+3k} = \langle r,s|r^2, rs^{a-3}rs^a rs^{a+3k}\rangle$$

For $F^{a-3,a,a+3k}$, then $n = 3a+3k-3$. If we can prove $s^{2n} = s^{6a+6k-6} = s^{-6a-6k+6}$, or $s^{12a+12k-12} = 1$, then we have enough to show

$$F^{a-3,a,a+3k}/C_2 \cong H^{a-3,a,a+3k} = \langle r, s | r^2, s^{6a+6k-6}, rs^{a-3}rs^{a}rs^{a+3k}\rangle.$$

- For all integers m,

$$\begin{aligned} (rs^{2a+3m+3k-3}rs^{a-3m})^2 &= 1 \text{ and} \\ (rs^{2a-3m}rs^{a+3m+3k-3})^2 &= 1 \quad \text{by II.} \end{aligned}$$

- Substituting $m = a$ in the above equation gives

$$\begin{aligned} 1 &= (rs^{a+3a+3k-3}rs^{2a-3a})^2 \\ &= s^{4a+3k-3}rs^{-a}rs^{4a+3k-3}rs^{-a}r \\ &= s^{4a+3k-3}(s^{a+3k}rs^{a-3})s^{4a+3k-3}(s^{a+3k}rs^{a-3}) \\ &= s^{5a+6k-3}rs^{6a+6k-6}rs^{a-3} \\ &= s^{6a+6k-6}rs^{6a+6k-6}r. \end{aligned}$$

Thus, $rs^{6a+6k-6}r = s^{-6a-6k+6}$ and $s^{6a+6k-6} = rs^{-6a-6k+6}r$.

- We know $rs^{a-3}rs^{a}rs^{a+3k} = 1$ and $rs^{6a+6k-6}r = s^{-6a-6k+6}$. So,

$$\begin{aligned} s^{-6a-6k+6} &= (rs^{a-3}rs^{a}rs^{a+3k})(s^{-6a-6k+6}) \\ &= rs^{a-3}rs^{a}.rs^{-6a-6k+6}.s^{a+3k} \\ &= rs^{a-3}rs^{7a+6k-6}rs^{a+3k} \\ &= rs^{a-3}.rs^{6a+6k-6}.s^{a}rs^{a+3k} \\ &= rs^{-5a-6k+3}rs^{a}rs^{a+3k} \\ &= rs^{-6a-6k+6}.s^{a-3}rs^{a}rs^{a+3k} \\ &= s^{6a+6k-6}rs^{a-3}rs^{a}rs^{a+3k} \\ &= s^{6a+6k-6}. \end{aligned}$$

Thus, $s^{6a+6k-6}$ is central and $s^{12a+12k-12} = 1$.

- $F^{a-3,a,a+3k}/C_2 \cong H^{a-3,a,a+3k}$ where $(a,3) = 1$.

Consider $\langle x \rangle$ where $x = s^{6a+6k-6}$. Obviously it is a subgroup of the kernel of the homomorphism from F to H and, since

$$rxr = rs^{6a+6k-6}r = s^{6a+6k-6} = x$$

$$\text{and} \quad s^{-1}xs = x,$$

then $\langle x \rangle$ is the kernel.

We have shown that $s^{4n} = s^{12a+12k-12} = 1$ and $s^{6a+6k-6}$ generates the kernel of the homomorphism. Thus, either $F^{a-3,a,a+3k} \cong H^{a-3,a,a+3k}$ or $F^{a-3,a,a+3k}/C_2 \cong H^{a-3,a,a+3k}$. It cannot be that $a - 3 \equiv a \equiv a + 3k \pmod 6$ and we also have

$$(a - 3 - a, a - (a + 3k), 3) = (-3, -3k, 3) = 3,$$

so, by Theorem 3.3 of [6], $H^{a-3,a,a+3k}$ is finite and has Schur multiplicator C_2.

We now know $F^{a-3,a,a+3k}$ is finite and as it has a 2-generator, 2-relator presentation, it has deficiency 0 and, by Corollory 1.2 of [31], a trivial multiplicator. Thus, $F^{a-3,a,a+3k} \not\cong H^{a-3,a,a+3k}$, and it must be such that, when a is not a multiple of 3,

$$F^{a-3,a,a+3k}/C_2 \cong H^{a-3,a,a+3k}.$$

3. Proof of the Case $c = 4$

$$F^{a-4,a,a+4k} = \langle r, s | r^2, rs^{a-4}rs^{a}rs^{a+4k} \rangle$$

For $F^{a-4,a,a+4k}$, we need to prove that $rs^{-6a-8k+8}rs^{6a+8k-8}rs^{6a+8k-8}r = s^{-6a-8k+8}$, $s^{24a+32k-32} = 1$ and $s^{12a+16k-16}$ is central. A presentation for Q_8 is $\langle x, y | x^4, x^2 = y^2, y^{-1}xy = x^{-1} \rangle$. Thus, taking $x = s^{6a+8k-8}$ and $y = rs^{6a+8k-8}r$ and also proving that $\langle s^{6a+8k-8}, rs^{6a+8k-8}r \rangle$ is the kernel of the natural homomorphism from F to H, we can show the kernel is isomorphic to Q_8.

- $rs^{6a+8k-8}r \sim s^4$ by I.
- For all integers m,

$$\begin{aligned}(rs^{2a+4m+4k-4}rs^{a-4m})^2 &= 1 \text{ and}\\ (rs^{2a-4m}rs^{a+4m+4k-4})^2 &= 1 \quad \text{by II.}\end{aligned}$$

- Setting $m = a$ and $m = 0$ in the previous equations, we obtain

$$\begin{aligned}rs^{-2a}rs^{5a+4k-4}rs^{-2a}rs^{5a+4k-4} &= 1 \quad \text{and}\\ rs^{2a+4k-4}rs^{a}rs^{2a+4k-4}rs^{a} &= 1.\end{aligned}$$

So, as $rs^{2a}r = s^4rs^{2a+4k-4}rs^{-4k}$, then

$$\begin{aligned}1 &= rs^{-2a}rs^{5a+4k-4}rs^{-2a}rs^{5a+4k-4}\\ &= (s^{4k}rs^{-2a-4k+4}rs^{-4})s^{5a+4k-4}(s^{4k}rs^{-2a-4k+4}rs^{-4})s^{5a+4k-4}\\ &= s^{4k}rs^{-2a-4k+4}rs^{5a+8k-8}rs^{-2a-4k+4}rs^{5a+4k-8}\\ &= rs^{-2a-4k+4}rs^{5a+8k-8}rs^{-2a-4k+4}rs^{5a+8k-8}\\ &= rs^{-2a-4k+4}rs^{5a+8k-8}(s^{a}rs^{2a+4k-4}rs^{a})s^{5a+8k-8}\\ &= rs^{-2a-4k+4}rs^{6a+8k-8}rs^{2a+4k-4}rs^{6a+8k-8}.\end{aligned}$$

We also know that $rs^{6a+8k-8}r \sim s^4$ and, because a must be odd if $(a-4, a, a+4k) = 1$, then $rs^{6a+8k-8}r \sim s^{2a+4k+2}$. Thus,

$$\begin{aligned}1 &= rs^{-2a-4k+4}rs^{6a+8k-8}rs^{2a+4k-4}rs^{6a+8k-8}\\ &= rs^{2}rs^{6a+8k-8}rs^{-2}rs^{6a+8k-8}\end{aligned}$$

and $s^{-2}rs^{6a+8k-8}rs^2 = rs^{-6a-8k+8}r$.

- We know a must be odd, so $s^{6a+8k-6}$ is a multiple of 4. Therefore, from $s^{-2}rs^{6a+8k-8}rs^2 = rs^{-6a-8k+8}r$ and $rs^{6a+8k-8}r \sim s^4$, we obtain

$$\begin{aligned} rs^{-6a-8k+8}rs^{6a+8k-8}rs^{6a+8k-8}r &= s^{-6a-8k+8} \quad \text{and} \\ rs^{6a+8k-8}rs^{6a+8k-8}rs^{-6a-8k+8}r &= s^{-6a-8k+8}. \end{aligned} \tag{4.44}$$

- We have

$$\begin{aligned} s^{-6a-8k+8}rs^{6a+8k-8}rs^{6a+8k-8} &= rs^{-6a-8k+8}r \quad \text{and} \\ s^{6a+8k-8}rs^{6a+8k-8} &= rs^{6a+8k-8}rs^{-6a-8k+8}r. \end{aligned}$$

Alternatively,

$$\begin{aligned} s^{6a+8k-8}rs^{6a+8k-8}rs^{-6a-8k+8} &= rs^{-6a-8k+8}r \quad \text{so,} \\ s^{6a+8k-8}rs^{6a+8k-8} &= rs^{-6a-8k+8}rs^{6a+8k-8}r. \end{aligned}$$

Hence,

$$\begin{aligned} rs^{6a+8k-8}rs^{-6a-8k+8}r &= rs^{-6a-8k+8}rs^{6a+8k-8}r \\ s^{12a+16k-16} &= rs^{12a+16k-16}r, \end{aligned}$$

and $s^{12a+16k-16}$ is central.

Also,

$$\begin{aligned} rs^{6a+8k-8}rs^{-6a-8k+8}r &= \left(rs^{6a+8k-8}rs^{-6a-8k+8}r\right)^{-1} \\ s^{6a+8k-8}rs^{6a+8k-8} &= s^{-6a-8k+8}rs^{-6a-8k+8} \\ s^{12a+16k-16} &= rs^{-12a-16k+16}r. \end{aligned}$$

Thus, $s^{12a+16k-16} = s^{-12a-16k+16}$ and $s^{24a+32k-32} = 1$.

- Since we have that $rs^{-6a-8k+8}rs^{6a+8k-8}rs^{6a+8k-8}r = s^{-6a-8k+8}$, $s^{24a+32k-32} = 1$ and $s^{12a+16k-16}$ is central, we need only check that $\{s^{6a+8k-8}, rs^{6a+8k-8}r\}$ generates the kernel of the homomorphism from F to H. Let $x = s^{6a+8k-8}$ and $y = rs^{6a+8k-8}r$, and consider $\langle x, y\rangle$. Obviously, $\langle x, y\rangle$ is a subgroup of the kernel and we have

$rxr = y$, $ryr = x$ and $s^{-1}xs = x$. This leaves only to test $s^{-1}ys$. Using $m = a + k - 1$ in $(rs^{2a+4m+4k-4}rs^{a-4m})^2 = 1$, we have

$$rs^{6a+8k-8}rs^{-3a-4k+4}rs^{6a+8k-8}rs^{-3a-4k+4} = 1$$

and

$$s^a rs^{6a+8k-8}rs^{-a} = s^{4a+4k-4}rs^{-6a-8k+8}rs^{2a+4k-4}.$$

We also know $rs^{6a+8k-8}r \sim s^4$, so

$$\begin{aligned} s^a rs^{6a+8k-8}rs^{-a} &= s^{4a+4k-4}rs^{-6a-8k+8}rs^{2a+4k-4} \\ &= rs^{-6a-8k+8}rs^{6a+8k-8}. \end{aligned}$$

As a is an odd number, we have two cases.

(a) $a \equiv 1 \pmod 4$
Here, $a + 1 \equiv 2 \pmod 4$.
Thus,

$$\begin{aligned} rs^{6a+8k-8}r &= s^{a+1}rs^{-6a-8k+8}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a+8k-8}rs &= s^a rs^{-6a-8k+8}rs^{-a}. \end{aligned}$$

Given this, we find

$$\begin{aligned} s^{-1}rs^{6a+8k-8}rs &= s^a rs^{-6a-8k+8}rs^{-a} \\ &= rs^{-6a-8k+8}rs^{6a+8k-8} \\ &= y^{-1}x. \end{aligned}$$

(b) $a \equiv 3 \pmod 4$
Now, $a + 1 \equiv 0 \pmod 4$.
Thus,

$$\begin{aligned} rs^{6a+8k-8}r &= s^{a+1}rs^{6a+8k-8}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a+8k-8}rs &= s^a rs^{6a+8k-8}rs^{-a}, \end{aligned}$$

and so,

$$\begin{aligned} s^{-1}rs^{6a+8k-8}rs &= s^a rs^{6a+8k-8}rs^{-a} \\ &= s^{-6a-8k+8}rs^{6a+8k-8}r \\ &= x^{-1}y. \end{aligned}$$

Hence, $\{x, y\}$ generates the kernel. Also, x and y both have order dividing 4, $y^{-1}xy = x^{-1}$ from 4.44 and $x^2 = y^2$ since $s^{12a+16k-16}$ is central. Given this, we know $\langle x, y\rangle$ is a homomorphic image of Q_8, which has derived length 2. It is left to show $\langle x, y\rangle \cong Q_8$. Consider the group

$$G^{a,b,c} = \langle r, s | r^2, s^8, rs^a rs^b rs^c \rangle,$$

a homomorphic image of $F^{a,b,c}$. Here, $G^{a,b,c} \cong G^{a',b',c'}$, where a', b' and c' are a, b and c modulo 8. Using $F^{a-4,a,a+4k}$ for the case $d = 4$, then a is odd and $a' \in \{1, 3, 5, 7\}$. Thus, we are left with only eight cases for $G^{a-4,a,a+4k}$. When k is odd, we have $G^{5,1,5}$, $G^{7,3,7}$, $G^{1,5,1}$ and $G^{3,7,3}$, and when k is even, $G^{5,1,1}$, $G^{7,3,3}$, $G^{1,5,5}$ and $G^{3,7,7}$. Using GAP, we obtain that each of these groups has derived length 4 and so, $F^{a-4,a,a+4k}$ must have derived length of at least 4.

From Theorem 3.5 of [3], the groups $H^{a,b,c}$ are finite metabelian groups when $(a, b, c) = 1$, $n \neq 0$ and $(d, 6) \neq 6$. As a is odd and $d = 4$, then $H^{a-4,a,a+4k}$ is finite metabelian and, therefore, has derived length 2. This implies that $\langle x, y\rangle$, the kernel of the natural homomorphism from $F^{a-4,a,a+4k}$ to $H^{a-4,a,a+4k}$, must have derived length at least 2. Thus, $\langle x, y\rangle \cong Q_8$.

4. When $(a, c) \neq 1$

According to the $F^{a,b,c}$ conjecture, we must have $(a, b, c) = 1$ to ensure proper results. Consider $F^{a-c,a,a+kc}$. Here, $s^{2n} = s^{6a+2kc-2c}$ and $d = c$. When $(a, c) \neq 1$ for $c \in \{2, 3, 4\}$, then we have $(a - c, a, a + kc) \neq 1$

and either of two cases

(a) a is a multiple of c or

(b) $c = 4$ and a is a multiple of 2.

If a is a multiple of c, then all of $a - c$, a and $a + kc$ are divisible by c and, as such, are not co-prime. If we consider $F^{a-c,a,a+kc}$ where $a = ci$ for some integer i, then using $m = i$ in $(rs^{2a+cm+kc-c}rs^{a-cm})^2 = 1$ gives

$$\begin{aligned} 1 &= (rs^{2a+ci+kc-c}rs^{a-ci})^2 \\ &= (rs^{2a+a+kc-c}rs^{a-a})^2 \\ &= (rs^{3a+kc-c}r)^2 \\ &= rs^{6a+2kc-2c}r, \end{aligned}$$

and so, $s^{2n} = s^{6a+2kc-2c} = 1$.

We find that where a is a multiple of c, $F^{a-c,a,a+kc} \cong H^{a-c,a,a+kc}$.

We just need to look at the case where $c = 4$ and $a = 2i$ for some odd integer i. Using $m = i$ in $(rs^{2a-4m}rs^{a+4m+4k-4})^2 = 1$ gives

$$\begin{aligned} 1 &= (rs^{2a-4i}rs^{a+4i+4k-4})^2 \\ &= (rs^{2a-2a}rs^{a+2a+4k-4})^2 \\ &= (s^{3a+4k-4})^2 \\ &= s^{6a+8k-8}, \end{aligned}$$

and $s^{2n} = s^{6a+8k-8} = 1$. Hence, $F^{a-4,a,a+4k} \cong H^{a-4,a,a+4k}$ where $a = 2i$ for i odd.

Thus, where $c \in \{2, 3, 4\}$ and $(a - c, a, a + kc) \neq 1$, we find that $F^{a-c,a,a+kc} \cong H^{a-c,a,a+kc}$.

$\square$

4.6 $F^{a-2c,a,a+kc}$ for $a, c, k \in \mathbb{Z}$ with $(2,k) = 1$

With our proof of the groups $F^{a-c,a,a+kc}$ for $a, k \in \mathbb{Z}$ and $d = c \in \{2, 3, 4\}$, we had thus finished the proof of the $F^{a,b,c}$ conjecture for all groups where $d = (a-b, b-c)$ for some $d \in \mathbb{Z}$ and the difference between two of the powers of s in the relator $rs^a rs^b rs^c$ is exactly d.

Our final aim was to show the $F^{a,b,c}$ conjecture true for all groups of the form, $F^{a-jc,a,a+kc}$ for $a, j, k \in \mathbb{Z}$, $(j,k) = 1$ and $d = c \in \{2, 3, 4\}$. However, for the groups $F^{a-c,a,a+kc}$, it had been much easier to generalise our proof of $F^{a-c,a,a+2c}$ than to use that of $F^{a-c,a,a+c}$, and so, before finally considering the groups $F^{a-jc,a,a+kc}$ with $(j,k) = 1$, we decided to take a smaller step and study the groups $F^{a-2c,a,a+kc}$ for $a, k \in \mathbb{Z}$, $(2,k) = 1$ and $d = c \in \{2, 3, 4\}$.

In order to use the same arguments for $F^{a-2c,a,a+kc}$ as in the proof of the groups $F^{a-c,a,a+kc}$, we would need $rs^{6a+2kc-4c}r \sim s^c$ as well as the fact that, for all integers m,

$$\begin{aligned}
(rs^{2a+cm+kc-2c}rs^{a-cm})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm}rs^{a+cm+kc-2c})^2 &= 1.
\end{aligned}$$

Employing a similar proof technique to our former proof and using $(2,k) = 1$, we could easily show $rs^{6a+2kc-4c}r \sim s^c$. It was again our induction proof on $m \geq 0$ for the second required step that caused the most difficulty.

We found that while we could prove the base case $m = 0$, the second base case $m = 1$ was no longer obvious. A proof for $m = 2$, however, required little effort. Also, performing a straightforward conversion of the inductive step using the appropriate changes for the new groups, we found that when considering the case for m, we needed only to assume that the relations were true for $m - 4$ and $m - 2$ in our hypothesis. Both $m - 4$ and $m - 2$ are even whenever m is, and thus, as we had the base cases, $m = 0$ and $m = 2$, we had an inductive proof for the relation sequences for all integers $m \geq 0$ where m is even.

This would not do, however, as even in our following arguments for the most simple case $c = 2$, or the groups $F^{a-4,a,a+2k}$ with $(2,k) = 1$, we required a substitution of $m = a$ into the relation sequences. Since we needed $(a, 2) = 1$ to ensure $(a-4, a, a+2k) = 1$, then we could not make this substitution as a is not even, and it was not enough to have the relations hold for just even integers.

Studying our inductive proof further, however, we realised that when considering the two relations for m, we had been required to prove those for $m-k-2$. As k must be odd and both m and 2 are even, then $m-k-2$ is itself odd, but yet the two relations hold. Thus, for any odd integer l, the two relations hold for $l+k+2$. Additionally, with the proof of $l+k+2$, we have a proof of the relations for $(l+k+2)-k-2 = l$, and hence, the relation sequences hold for all integers m.

Having acquired all the tools that we needed for this case, we formulated the proof of the conjecture for the groups $F^{a-2c,a,a+kc}$ with $a, k \in \mathbb{Z}$, $(2, k) = 1$ and $d = c \in \{2, 3, 4\}$, and we state it now in the form of a theorem.

Theorem 4.6 For the groups

$$F^{a-2c,a,a+kc} = \langle r, s | r^2, rs^{a-2c}rs^a rs^{a+kc} \rangle$$

with $a \in \mathbb{Z}$, $c \in \{2, 3, 4\}$ and $(2, k) = 1$ let

$$H^{a-2c,a,a+kc} = \langle r, s | r^2, rs^{a-2c}rs^a rs^{a+kc}, s^{6a+2kc-4c} \rangle.$$

If,

- $c = 2$ and $(a, 2) = 1$, then $s^{6a+4k-8} = 1$ and

$$F^{a-4,a,a+2k} \cong H^{a-4,a,a+2k},$$

- $c = 3$ and $(a, 3) = 1$, then $s^{12a+12k-24} = 1$ and

$$F^{a-6,a,a+3k}/C_2 \cong H^{a-6,a,a+3k},$$

- $c = 4$ and $(a, 4) = 1$, then $s^{24a+32k-64} = 1$, $s^{12a+16k-32} \sim r$ and

$$F^{a-8,a,a+4k}/Q_8 \cong H^{a-8,a,a+4k},$$

- $(a, c) \neq 1$ then $(a - 2c, a, a + kc) \neq 1$, $s^{6a+2kc-4c} = 1$ and

$$F^{a-2c,a,a+kc} \cong H^{a-2c,a,a+kc}.$$

Proof. In $F^{a-2c,a,a+kc}$, we have

$$\begin{aligned}
n &= a - 2c + a + a + kc \\
&= 3a + kc - 2c, \\
s^{2n} &= s^{6a+2kc-4c}, \\
1 &= (a - 2c, a, a + kc) \text{ when } (a, c) = 1 \quad \text{and} \\
d &= ((a - 2c) - a, a - (a + kc)) \\
&= c \quad \text{when } (2, k) = 1.
\end{aligned}$$

Also,

$$\begin{aligned}
rs^{a-2c}r &= s^{-a-kc}rs^{-a}, \\
rs^{a}r &= s^{2c-a}rs^{-a-kc} \quad \text{and} \\
rs^{a+kc}r &= s^{-a}rs^{2c-a}.
\end{aligned}$$

Hence,

$$\begin{aligned}
rs^{2a-4c}r &= (rs^{a-2c}r)^2 \\
&= s^{-a-kc}rs^{-2a-kc}rs^{-a}, \qquad (4.45)
\end{aligned}$$

$$
\begin{aligned}
rs^{2a-2c}r &= (rs^{a-2c}r)(rs^{a}r) \\
&= s^{-a-kc}rs^{2c-2a}rs^{-a-kc} \quad \text{and} && (4.46)\\
&= (rs^{a}r)(rs^{a-2c}r) \\
&= s^{2c-a}rs^{-2a-2kc}rs^{-a}, && (4.47)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a}r &= (rs^{a}r)^2 \\
&= s^{2c-a}rs^{-2a-kc+2c}rs^{-a-kc}, && (4.48)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a+kc-2c}r &= (rs^{a-2c}r)(rs^{a+kc}r) \\
&= s^{-a-kc}rs^{-2a}rs^{2c-a} \quad \text{and} && (4.49)\\
&= (rs^{a+kc}r)(rs^{a-2c}r) \\
&= s^{-a}rs^{-2a-kc+2c}rs^{-a}, && (4.50)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a+kc}r &= (rs^{a}r)(rs^{a+kc}r) \\
&= s^{2c-a}rs^{-2a-kc}rs^{2c-a} \quad \text{and} && (4.51)\\
&= (rs^{a+kc}r)(rs^{a}r) \\
&= s^{-a}rs^{4c-2a}rs^{-a-kc}, && (4.52)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a+2kc}r &= (rs^{a+kc})^2 \\
&= s^{-a}rs^{2c-2a}rs^{2c-a}, && (4.53)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2c}r &= (rs^{a}r)(rs^{2c-a}r) \\
&= s^{2c-a}rs^{-kc}rs^{a+kc} \quad \text{and} && (4.54)\\
&= (rs^{2c-a}r)(rs^{a}r) \\
&= s^{a}rs^{kc+2c}rs^{-a-kc}, && (4.55)
\end{aligned}
$$

$$\begin{aligned} rs^{kc}r &= (rs^{a+kc}r)(rs^{-a}r) \\ &= s^{-a}rs^{kc+2c}rs^{a-2c} \quad \text{and} && (4.56) \\ &= (rs^{-a}r)(rs^{a+kc}r) \\ &= s^{a+kc}rs^{-2c}rs^{2c-a}, && (4.57) \end{aligned}$$

$$\begin{aligned} rs^{kc+2c}r &= (rs^{a+kc}r)(rs^{2c-a}r) \\ &= s^{-a}rs^{2c}rs^{a+kc} \quad \text{and} && (4.58) \\ &= (rs^{2c-a}r)(rs^{a+kc}r) \\ &= s^{a}rs^{kc}rs^{2c-a}. && (4.59) \end{aligned}$$

So,

$$\begin{aligned} rs^{2a-2c}r &= s^{-a-kc}rs^{2c-2a}rs^{-a-kc} \\ &= s^{-a-kc}(s^{a}rs^{2a+2kc}rs^{a-2c})s^{-a-kc} \quad \text{from 4.46 and 4.47} \\ &= s^{-kc}rs^{2a+2kc}rs^{-kc-2c}, && (4.60) \end{aligned}$$

$$\begin{aligned} rs^{2a+kc-2c}r &= s^{-a}rs^{-2a-kc+2c}rs^{-a} \\ &= s^{-a}(s^{a-2c}rs^{2a}rs^{a+kc})s^{-a} \quad \text{from 4.50 and 4.49} \\ &= s^{-2c}rs^{2a}rs^{kc}, && (4.61) \end{aligned}$$

$$\begin{aligned} rs^{2a+kc}r &= s^{2c-a}rs^{-2a-kc}rs^{2c-a} \\ &= s^{2c-a}(s^{a+kc}rs^{2a-4c}rs^{a})s^{2c-a} \quad \text{from 4.51 and 4.52} \\ &= s^{kc+2c}rs^{2a-4c}rs^{2c}. && (4.62) \end{aligned}$$

We start by proving the necessary steps (I-III) to prove each of the cases, $c = 2$, $c = 3$ and $c = 4$.

I. $rs^{6a+2kc-4c}r \sim s^{c}$

From the equations 4.60, 4.61 and 4.62, we have both

$$\begin{aligned} rs^{6a+2kc-4c}r &= (rs^{2a+kc-2c}r)(rs^{2a-2c}r)(rs^{2a+kc}r) \\ &= s^{-2c}rs^{6a+2kc-4c}rs^{2c} \end{aligned}$$

and

$$\begin{aligned} rs^{6a+2kc-4c}r &= (rs^{2a-2c}r)(rs^{2a+kc}r)(rs^{2a+kc-2c}r) \\ &= s^{-kc}rs^{6a+2kc-4c}rs^{kc}. \end{aligned}$$

Since $(2,k)=1$, then $k-1$ must be a multiple of 2 and

$$\begin{aligned} s^{-c}rs^{6a+2kc-4c}rs^{c} &= s^{kc-c}.s^{-kc}rs^{6a+2kc-4c}rs^{kc}.s^{-kc+c} \\ &= s^{(k-1)c}rs^{6a+2kc-4c}rs^{-(k-1)c} \\ &= rs^{6a+2kc-4c}r. \end{aligned}$$

II. In $F^{a-2c,a,a+kc}$, for all even integers $m \geq 0$,

$$\begin{aligned} (rs^{2a+cm+kc-2c}rs^{a-cm})^2 &= 1 \quad \text{and} \\ (rs^{2a-cm}rs^{a+cm+kc-2c})^2 &= 1. \end{aligned}$$

Proof by induction:

Base step

$m=0$

$$\begin{aligned} & rs^{2a+kc-2c}rs^{a}rs^{2a+kc-2c}rs^{a} \\ = \; & rs^{2a+kc-2c}(s^{2c-a}rs^{-a-kc})s^{2a+kc-2c}rs^{a} \\ = \; & rs^{a+kc}rs^{a-2c}rs^{a} \\ = \; & 1 \end{aligned}$$

$$\begin{aligned}
& rs^{2a}rs^{a+kc-2c}rs^{2a}rs^{a+kc-2c} \\
= \ & rs^{2a}rs^{a+kc-2c}(s^{2c}rs^{2a+kc-2c}rs^{-kc})s^{a+kc-2c} \\
= \ & rs^{2a}rs^{a+kc}rs^{2a+kc-2c}rs^{a-2c} \\
= \ & rs^{2a}(s^{-a}rs^{2c-a})s^{2a+kc-2c}rs^{a-2c} \\
= \ & rs^{a}rs^{a+kc}rs^{a-2c} \\
= \ & 1
\end{aligned}$$

$m = 2$

$$\begin{aligned}
& rs^{2a+kc}rs^{a-2c}rs^{2a+kc}rs^{a-2c} \\
= \ & rs^{2a+kc}(s^{-a-kc}rs^{-a})s^{2a+kc}rs^{a-2c} \\
= \ & rs^{a}rs^{a+kc}rs^{a-2c} \\
= \ & 1
\end{aligned}$$

$$\begin{aligned}
& rs^{2a-2c}rs^{a+kc}rs^{2a-2c}rs^{a+kc} \\
= \ & rs^{2a-2c}(s^{-a}rs^{2c-a})s^{2a-2c}rs^{a+kc} \\
= \ & rs^{a-2c}rs^{a}rs^{a+kc} \\
= \ & 1
\end{aligned}$$

Inductive step

Assume for $0 \le i < m$ and i and m even,

$$\begin{aligned}
(rs^{2a+ci+kc-2c}rs^{a-ci})^2 &= 1 \quad \text{and} \\
(rs^{2a-ci}rs^{a+ci+kc-2c})^2 &= 1.
\end{aligned}$$

Since we have shown it to be true for $m \in \{0, 2\}$, we can assume $m \ge 4$.

Consider $i = m$, with $4 \le m$ and m even. This means $0 \le m - 4 <$

m, so

$$\begin{aligned}
(rs^{2a+cm+kc-6c}rs^{a-cm+4c})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm+4c}rs^{a+cm+kc-6c})^2 &= 1.
\end{aligned}$$

We also have $0 < m-2 < m$, so

$$\begin{aligned}
(rs^{2a+cm+kc-4c}rs^{a-cm+2c})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm+2c}rs^{a+cm+kc-4c})^2 &= 1.
\end{aligned}$$

We need some additional equations for our proof. Consider $m-k-2$. As m is even, but k is odd, then $m-k-2$ is not even and, where $m < k+2$, then $m-k-2 < 0$ and we cannot assume that either

$$\begin{aligned}
(rs^{2a-c(m-k-2)}rs^{a+c(m-k-2)+kc-2c})^2 &= (rs^{2a-cm+kc+2c}rs^{a+cm-4c})^2 \\
&= 1 \quad \text{or} \\
(rs^{2a+c(m-k-2)+kc-2c}rs^{a-c(m-k-2)})^2 &= (rs^{2a+cm-4c}rs^{a-cm+kc+2c})^2 \\
&= 1.
\end{aligned}$$

Using our inductive hypothesis, however, we can form the proofs for these necessary equations. We have

$$\begin{aligned}
r &= s^{kc}rs^{a-2c}rs^{2c}rs^{-a-kc}, \quad \text{from 4.57} \\
1 &= (rs^{a+cm+kc-4c}rs^{2a-cm+2c})^2, \\
1 &= (rs^{-a+cm-4c}rs^{-2a-cm-kc+6c})^2
\end{aligned}$$

and

$$1 = (rs^{2a+cm+kc-4c}rs^{a-cm+2c})^2,$$

which gives

$$\begin{aligned}
& rs^{2a-cm+kc+2c}rs^{a+cm-4c}r \\
= \;& rs^{2a-cm+kc+2c}rs^{a+cm-4c}.r. \\
= \;& rs^{2a-cm+kc+2c}.rs^{a+cm+kc-4c}r.s^{a-2c}rs^{2c}rs^{-a-kc} \\
= \;& rs^{kc}rs^{-a-cm-kc+4c}.rs^{-a+cm-4c}r.s^{2c}rs^{-a-kc} \\
= \;& rs^{kc}rs^{a-2c}rs^{a-cm+4c}.rs^{2a+cm+kc-4c}r.s^{-a-kc} \\
= \;& rs^{kc}.rs^{a-2c}r.s^{2c}rs^{-2a-cm-kc+4c}rs^{-2a+cm-kc-2c} \\
= \;& rs^{kc}(s^{-a-kc}rs^{-a})s^{2c}rs^{-2a-cm-kc+4c}rs^{-2a+cm-kc-2c} \\
= \;& rs^{-a}.rs^{2c-a}r.s^{-2a-cm-kc+4c}rs^{-2a+cm-kc-2c} \\
= \;& rs^{-a}(s^{a}rs^{a+kc})s^{-2a-cm-kc+4c}rs^{-2a+cm-kc-2c} \\
= \;& s^{-a-cm+4c}rs^{-2a+cm-kc-2c}.
\end{aligned}$$

From

$$\begin{aligned}
r &= s^{a+kc}rs^{a-2c}rs^{a}, \\
r &= s^{2c-a}rs^{-a-kc}rs^{-a}, \\
1 &= (rs^{2a+cm+kc-4c}rs^{a-cm+2c})^2, \\
1 &= (rs^{-2a+cm-kc-2c}rs^{-a-cm+4c})^2
\end{aligned}$$

and

$$1 = (rs^{2a-cm+kc+2c}rs^{a+cm-4c})^2,$$

we obtain

$$\begin{aligned}
& rs^{a-cm+kc+2c}rs^{2a+cm-4c}r \\
= \;& rs^{a-cm+kc+2c}rs^{2a+cm-4c}.r. \\
= \;& rs^{a-cm+kc+2c}rs^{3a+cm+kc-4c}rs^{a-2c}rs^{a} \\
= \;& rs^{a-cm+kc+2c}.r.s^{3a+cm+kc-4c}rs^{a-2c}rs^{a} \\
= \;& rs^{-cm+kc+4c}rs^{-a-kc}.rs^{2a+cm+kc-4c}r.s^{a-2c}rs^{a} \\
= \;& rs^{-cm+kc+4c}.rs^{-2a+cm-kc-2c}r.s^{-2a-cm-kc+4c}rs^{cm-4c}rs^{a} \\
= \;& rs^{a+kc}rs^{2a-cm+kc+2c}.rs^{-a-kc}r.s^{cm-4c}rs^{a} \\
= \;& .rs^{a+kc}r.s^{3a-cm+kc}rs^{a+cm-4c}rs^{a} \\
= \;& (s^{-a}rs^{2c-a})s^{3a-cm+kc}rs^{a+cm-4c}rs^{a} \\
= \;& s^{-a}.rs^{2a-cm+kc+2c}rs^{a+cm-4c}r.s^{a} \\
= \;& s^{-2a-cm+4c}rs^{-a+cm-kc-2c}.
\end{aligned}$$

Thus,

$$\begin{aligned}
(rs^{2a-cm+kc+2c}rs^{a+cm-4c})^2 &= 1 \quad \text{and} \\
(rs^{2a+cm-4c}rs^{a-cm+kc+2c})^2 &= 1.
\end{aligned}$$

Now, let $i = m$.

From

$$\begin{aligned}
rs^{a+cm-4c}r &= s^{-2a+cm-kc-2c}rs^{-a-cm+4c}rs^{-2a+cm-kc-2c}, \\
rs^{kc+2c}r &= s^{a}rs^{kc}rs^{2c-a}, \\
rs^{-a+cm-kc-2c}r &= s^{2a+cm-4c}rs^{a-cm+kc+2c}rs^{2a+cm-4c} \\
&\text{and} \\
rs^{2a+cm+kc-4c}r &= s^{-a+cm-2c}rs^{-2a-cm-kc+4c}rs^{-a+cm-2c},
\end{aligned}$$

we find

$$
\begin{aligned}
& rs^{a+cm+kc-2c}r \\
= \;& (rs^{a+cm-4c}r)(rs^{kc+2c}r) \\
= \;& s^{-2a+cm-kc-2c}rs^{-a-cm+4c}.rs^{-a+cm-kc-2c}r.s^{kc}rs^{2c-a} \\
= \;& s^{-2a+cm-kc-2c}.rs^{a}r.s^{a-cm+kc+2c}rs^{2a+cm+kc-4c}rs^{2c-a} \\
= \;& s^{-2a+cm-kc-2c}(s^{2c-a}rs^{-a-kc})s^{a-cm+kc+2c}rs^{2a+cm+kc-4c}rs^{2c-a} \\
= \;& s^{-3a+cm-kc}rs^{-cm+2c}.rs^{2a+cm+kc-4c}r.s^{2c-a} \\
= \;& s^{-3a+cm-kc}.rs^{-a}r.s^{-2a-cm-kc+4c}rs^{-2a+cm} \\
= \;& s^{-3a+cm-kc}(s^{a+kc}rs^{a-2c})s^{-2a-cm-kc+4c}rs^{-2a+cm} \\
= \;& s^{-2a+cm}rs^{-a-cm-kc+2c}rs^{-2a+cm},
\end{aligned}
$$

and given,

$$
\begin{aligned}
rs^{a-cm+2c}r &= s^{-2a-cm-kc+4c}rs^{-a+cm-2c}rs^{-2a-cm-kc+4c}, \\
rs^{-2c}r &= s^{a+kc}rs^{-kc-2c}rs^{-a}, \\
rs^{-a-cm+4c}r &= s^{2a-cm+kc+2c}rs^{a+cm-4c}rs^{2a-cm+kc+2c} \\
&\text{and} \\
rs^{2a-cm}r &= s^{-a-cm-kc+2c}rs^{-2a+cm}rs^{-a-cm-kc+2c},
\end{aligned}
$$

we have

$$\begin{aligned}
& rs^{a-cm}r \\
= \;& (rs^{a-cm+2c}r)(rs^{-2c}r) \\
= \;& s^{-2a-cm-kc+4c}rs^{-a+cm-2c}.rs^{-a-cm+4c}r.s^{-kc-2c}rs^{-a} \\
= \;& s^{-2a-cm-kc+4c}.rs^{a+kc}r.s^{a+cm-4c}rs^{2a-cm}rs^{-a} \\
= \;& s^{-2a-cm-kc+4c}(s^{-a}rs^{2c-a})s^{a+cm-4c}rs^{2a-cm}rs^{-a} \\
= \;& s^{-3a-cm-kc+4c}rs^{cm-2c}.rs^{2a-cm}r.s^{-a} \\
= \;& s^{-3a-cm-kc+4c}.rs^{-a-kc}r.s^{-2a+cm}rs^{-2a-cm-kc+2c} \\
= \;& s^{-3a-cm-kc+4c}(s^{a-2c}rs^{a})s^{-2a+cm}rs^{-2a-cm-kc+2c} \\
= \;& s^{-2a-cm-kc+2c}rs^{-a+cm}rs^{-2a-cm-kc+2c}.
\end{aligned}$$

Thus, by induction, for all even integers $m \geq 0$,

$$\begin{aligned}
(rs^{2a+cm+kc-2c}rs^{a-cm})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm}rs^{a+cm+kc-2c})^2 &= 1.
\end{aligned}$$

III. In $F^{a-2c,a,a+kc}$, for all integers m,

$$\begin{aligned}
(rs^{2a+cm+kc-2c}rs^{a-cm})^2 &= 1 \quad \text{and} \\
(rs^{2a-cm}rs^{a+cm+kc-2c})^2 &= 1.
\end{aligned}$$

Let us now choose an even integer $m < 0$. Using $m = -i$ for an even integer $i > 0$, we have

$$\begin{aligned}
(rs^{2a+cm+kc-2c}rs^{a-cm})^2 &= (rs^{2a-ci+kc-2c}rs^{a+ci})^2 \\
&= (rs^{2a-c(i-k+2)}rs^{a+c(i-k+2)+kc-2c})^2 \quad \text{and}
\end{aligned}$$

$$\begin{aligned}
(rs^{2a-cm}rs^{a+cm+kc-2c})^2 &= (rs^{2a+ci}rs^{a-ci+kc-2c})^2 \\
&= (rs^{2a+c(i-k+2)+kc-2c}rs^{a-c(i-k+2)})^2.
\end{aligned}$$

Thus, this is equivalent to the case $m = i - k + 2$. Obviously, as $i > 0$ and i is even, then $i + 4 > 0$, $i + 4$ is even and the two expressions equal the identity for $m = i + 4$. During the proof of m, however, we found that the two expressions were also trivial for $m - k - 2$. Thus, for $m = i + 4$, we have the equations true for $(i + 4) - k - 2 = i - k + 2$, and the proof holds for all negative even integers as well.

In the proof for m, an even integer, we were able to show the two equations held for $m - k - 2$, which is an odd number as $(2, k) = 1$. Consider $m = i+1$, where i is even. Obviously, $i+k+3$ is even and thus, the two equations hold for $m = i+k+3$. Using the proof for $m = i+k+3$, we can show that the two equations hold for $(i + k + 3) - k - 2 = i + 1$. Thus, for any even integer i, we can show the equations also hold for $i + 1$.

Hence, for all integers m,

$$(rs^{2a+cm+kc-2c}rs^{a-cm})^2 = 1 \quad \text{and}$$
$$(rs^{2a-cm}rs^{a+cm+kc-2c})^2 = 1.$$

1. Proof of the Case $c = 2$

$$F^{a-4,a,a+2k} = \langle r, s | r^2, rs^{a-4}rs^a rs^{a+2k} \rangle$$

For $F^{a-4,a,a+2k}$, then $n = 3a + 2k - 4$ and $d = 2$ where $(2, k) = 1$. If we can show that $s^{2n} = s^{6a+4k-8} = 1$, then $F^{a-4,a,a+2k} \cong H^{a-4,a,a+2k} = \langle r, s | r^2, s^{6a+4k-8}, rs^{a-4}rs^a rs^{a+2k} \rangle$.

- For all integers m,

$$\begin{aligned}(rs^{2a+2m+2k-4}rs^{a-2m})^2 &= 1 \text{ and} \\ (rs^{2a-2m}rs^{a+2m+2k-4})^2 &= 1 \quad \text{by III.}\end{aligned}$$

- Using $m = a$ in the above equations, we have

$$\begin{aligned} 1 &= (rs^{2a-2a}rs^{a+2a+2k-4})^2 \\ &= (rs^0rs^{3a+2k-4})^2 \\ &= (s^{3a+2k-4})^2 \\ &= s^{6a+4k-8}. \end{aligned}$$

2. Proof of the Case $c = 3$

$$F^{a-6,a,a+3k} = \langle r, s | r^2, rs^{a-6}rs^ars^{a+3k} \rangle$$

For $F^{a-6,a,a+3k}$, $n = 3a + 3k - 6$ and $d = 3$ where $(2, k) = 1$. If we can show that $s^{2n} = s^{6a+6k-12} = s^{-6a-6k+12}$, or $s^{12a+12k-24} = 1$, then we have enough to show

$$F^{a-6,a,a+3k}/C_2 \cong H^{a-6,a,a+3k} = \langle r, s | r^2, s^{6a+6k-12}, rs^{a-6}rs^ars^{a+3k} \rangle.$$

- For all integers m,

$$\begin{aligned} (rs^{2a+3m+3k-6}rs^{a-3m})^2 &= 1 \text{ and} \\ (rs^{2a-3m}rs^{a+3m+3k-6})^2 &= 1 \quad \text{by III.} \end{aligned}$$

- Substituting $m = a$ in the above equations gives

$$\begin{aligned} 1 &= (rs^{a+3a+3k-6}rs^{2a-3a})^2 \\ &= s^{4a+3k-6}rs^{-a}rs^{4a+3k-6}rs^{-a}r \\ &= s^{4a+3k-6}(s^{a+3k}rs^{a-6})s^{4a+3k-6}(s^{a+3k}rs^{a-6}) \\ &= s^{5a+6k-6}rs^{6a+6k-12}rs^{a-6} \\ &= s^{6a+6k-12}rs^{6a+6k-12}r. \end{aligned}$$

Thus, $rs^{6a+6k-12}r = s^{-6a-6k+12}$, and $s^{6a+6k-12} = rs^{-6a-6k+12}r$.

- We know $rs^{a-6}rs^ars^{a+3k} = 1$ and $rs^{6a+6k-12}r = s^{-6a-6k+12}$ so,

$$\begin{aligned} s^{-6a-6k+12} &= (rs^{a-6}rs^ars^{a+3k})(s^{-6a-6k+12}) \\ &= rs^{a-6}rs^a.rs^{-6a-6k+12}.s^{a+3k} \\ &= rs^{a-6}rs^{7a+6k-12}rs^{a+3k} \\ &= rs^{a-6}.rs^{6a+6k-12}.s^ars^{a+3k} \\ &= rs^{-5a-6k+6}rs^ars^{a+3k} \\ &= rs^{-6a-6k+12}.s^{a-6}rs^ars^{a+3k} \\ &= s^{6a+6k-12}rs^{a-6}rs^ars^{a+3k} \\ &= s^{6a+6k-12}. \end{aligned}$$

Thus, $s^{-6a-6k+12} = s^{6a+6k-12}$ and $s^{6a+6k-12}$ is central, so

$$s^{12a+12k-24} = 1.$$

- $F^{a-6,a,a+3k}/C_2 \cong H^{a-6,a,a+3k}$ where $(a,3) = 1$.

Consider $\langle x \rangle$ where $x = s^{6a+6k-12}$. Obviously it is a subgroup of the kernel of the homomorphism from F to H, and since

$$rxr = rs^{6a+6k-12}r = s^{6a+6k-12} = x$$

$$\text{and} \quad s^{-1}xs = x,$$

then $\langle x \rangle$ is the kernel.

We have shown that $s^{4n} = s^{12a+12k-24} = 1$ and $s^{6a+6k-12}$ generates the kernel of the homomorphism. Thus, either $F^{a-6,a,a+3k} \cong H^{a-6,a,a+3k}$ or $F^{a-6,a,a+3k}/C_2 \cong H^{a-6,a,a+3k}$. Since $(2,k) = 1$, then it cannot be that $a - 6 \equiv a \equiv a + 3k \pmod 6$. Also,

$$(a-6-a, a-(a+3k), 3) = (-6, -3k, 3) = 3,$$

so, by Theorem 3.3 of [6], $H^{a-6,a,a+3k}$ is finite and has Schur multiplicator C_2.

We now know $F^{a-6,a,a+3k}$ is finite and as it has a 2-generator, 2-relator presentation, it has deficiency 0 and, by Corollory 1.2 of [31], a trivial multiplicator. Thus, $F^{a-6,a,a+3k} \ncong H^{a-6,a,a+3k}$, so it must be such that, when a is not a multiple of 3,

$$F^{a-6,a,a+3k}/C_2 \cong H^{a-6,a,a+3k}.$$

3. Proof of the Case $c = 4$

$$F^{a-8,a,a+4k} = \langle r, s | r^2, rs^{a-8}rs^a rs^{a+4k}\rangle$$

For $F^{a-8,a,a+4k}$, $n = 3a+4k-8$ and $d = 4$ where $(2, k) = 1$. We want to prove that $rs^{-6a-8k+16}rs^{6a+8k-16}rs^{6a+8k-16}r = s^{-6a-8k+16}$, $s^{24a+32k-64} = 1$ and $s^{12a+16k-32}$ is central. Given this, we could show that the kernel of the natural homomorphism from F to H is generated by $s^{6a+8k-16}$ and $rs^{6a+8k-16}r$ and is isomorphic to Q_8.

- $rs^{6a+8k-16}r \sim s^4$ by I.
- For all integers m,

$$\begin{aligned}(rs^{2a+4m+4k-8}rs^{a-4m})^2 &= 1 \text{ and}\\ (rs^{2a-4m}rs^{a+4m+4k-8})^2 &= 1 \quad \text{by III.}\end{aligned}$$

- Setting $m = a$ and $m = 0$ in the previous equations, we obtain

$$\begin{aligned}rs^{-2a}rs^{5a+4k-8}rs^{-2a}rs^{5a+4k-8} &= 1 \quad \text{and}\\ rs^{2a+4k-8}rs^a rs^{2a+4k-8}rs^a &= 1.\end{aligned}$$

So, as $rs^{2a}r = s^8rs^{2a+4k-8}rs^{-4k}$ then

$$
\begin{aligned}
1 &= rs^{-2a}rs^{5a+4k-8}rs^{-2a}rs^{5a+4k-8} \\
&= (s^{4k}rs^{-2a-4k+8}rs^{-8})s^{5a+4k-8}(s^{4k}rs^{-2a-4k+8}rs^{-8})s^{5a+4k-8} \\
&= s^{4k}rs^{-2a-4k+8}rs^{5a+8k-16}rs^{-2a-4k+8}rs^{5a+4k-16} \\
&= rs^{-2a-4k+8}rs^{5a+8k-16}rs^{-2a-4k+8}rs^{5a+8k-16} \\
&= rs^{-2a-4k+8}rs^{5a+8k-16}(s^{a}rs^{2a+4k-8}rs^{a})s^{5a+8k-16} \\
&= rs^{-2a-4k+8}rs^{6a+8k-16}rs^{2a+4k-8}rs^{6a+8k-16}.
\end{aligned}
$$

We also know that $rs^{6a+8k-16}r \sim s^4$ and, because a must be odd to ensure $(a-8, a, a+4k) = 1)$, then $rs^{6a+8k-16}r \sim s^{2a+4k-6}$. Thus,

$$
\begin{aligned}
1 &= rs^{-2a-4k+8}rs^{6a+8k-16}rs^{2a+4k-8}rs^{6a+8k-16} \\
&= rs^{2}rs^{6a+8k-16}rs^{-2}rs^{6a+8k-16}
\end{aligned}
$$

and $s^{-2}rs^{6a+8k-16}rs^2 = rs^{-6a-8k+16}r$.

- We know a must be odd, so $s^{6a+8k-14}$ is a multiple of 4. Therefore, from $s^{-2}rs^{6a+8k-16}rs^2 = rs^{-6a-8k+16}r$ and $rs^{6a+8k-16}r \sim s^4$, we obtain

$$
\begin{aligned}
rs^{-6a-8k+16}rs^{6a+8k-16}rs^{6a+8k-16}r &= s^{-6a-8k+16} \quad \text{and} \\
rs^{6a+8k-16}rs^{6a+8k-16}rs^{-6a-8k+16}r &= s^{-6a-8k+16}. \qquad (4.63)
\end{aligned}
$$

- We have

$$
\begin{aligned}
s^{-6a-8k+16}rs^{6a+8k-16}rs^{6a+8k-16} &= rs^{-6a-8k+16}r \quad \text{so,} \\
s^{6a+8k-16}rs^{6a+8k-16} &= rs^{6a+8k-16}rs^{-6a-8k+16}r.
\end{aligned}
$$

Alternatively,

$$
\begin{aligned}
s^{6a+8k-16}rs^{6a+8k-16}rs^{-6a-8k+16} &= rs^{-6a-8k+16}r \quad \text{so,} \\
s^{6a+8k-16}rs^{6a+8k-16} &= rs^{-6a-8k+16}rs^{6a+8k-16}r.
\end{aligned}
$$

Hence,

$$\begin{aligned} rs^{6a+8k-16}rs^{-6a-8k+16}r &= rs^{-6a-8k+16}rs^{6a+8k-16}r \\ s^{12a+16k-32} &= rs^{12a+16k-32}r, \end{aligned}$$

and $s^{12a+16k-32}$ is central.

Also,

$$\begin{aligned} rs^{6a+8k-16}rs^{-6a-8k+16}r &= (rs^{6a+8k-16}rs^{-6a-8k+16}r)^{-1} \\ s^{6a+8k-16}rs^{6a+8k-16} &= s^{-6a-8k+16}rs^{-6a-8k+16} \\ s^{12a+16k-32} &= rs^{-12a-16k+32}r. \end{aligned}$$

Thus, $s^{12a+16k-32} = s^{-12a-16k+32}$ and $s^{24a+32k-64} = 1$.

- Since we have that $rs^{-6a-8k+16}rs^{6a+8k-16}rs^{6a+8k-16}r = s^{-6a-8k+16}$, $s^{24a+32k-64} = 1$ and $s^{12a+16k-32}$ is central, we need only check that $\{s^{6a+8k-16}, rs^{6a+8k-16}r\}$ generates the kernel of the homomorphism from F to H. Let $x = s^{6a+8k-16}$ and $y = rs^{6a+8k-16}r$, and consider $\langle x, y\rangle$. Obviously, $\langle x, y\rangle$ is a subgroup of the kernel. We also have $rxr = y$, $ryr = x$ and $s^{-1}xs = x$, leaving only to test $s^{-1}ys$ to show that $\langle x, y\rangle$ is the kernel.

Using $m = a + k - 2$ in $(rs^{2a+4m+4k-8}rs^{a-4m})^2 = 1$, we have

$$rs^{6a+8k-16}rs^{-3a-4k+8}rs^{6a+8k-16}rs^{-3a-4k+8} = 1$$

and

$$s^a rs^{6a+8k-16}rs^{-a} = s^{4a+4k-8}rs^{-6a-8k+16}rs^{2a+4k-8}.$$

We also know $rs^{6a+8k-16}r \sim s^4$, so

$$\begin{aligned} s^a rs^{6a+8k-16}rs^{-a} &= s^{4a+4k-8}rs^{-6a-8k+16}rs^{2a+4k-8} \\ &= rs^{-6a-8k+16}rs^{6a+8k-16}. \end{aligned}$$

There are two cases, as a is an odd number.

(a) $a \equiv 1 \pmod 4$

Here, $a+1 \equiv 2 \pmod 4$.

Thus,

$$\begin{aligned} rs^{6a+8k-16}r &= s^{a+1}rs^{-6a-8k+16}rs^{-a-1} \quad \text{and,} \\ s^{-1}rs^{6a+8k-16}rs &= s^{a}rs^{-6a-8k+16}rs^{-a}. \end{aligned}$$

Using this, we find

$$\begin{aligned} s^{-1}rs^{6a+8k-16}rs &= s^{a}rs^{-6a-8k+16}rs^{-a} \\ &= rs^{-6a-8k+16}rs^{6a+8k-16} \\ &= y^{-1}x. \end{aligned}$$

(b) $a \equiv 3 \pmod 4$

Now, $a+1 \equiv 0 \pmod 4$.

Thus,

$$\begin{aligned} rs^{6a+8k-16}r &= s^{a+1}rs^{6a+8k-16}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a+8k-16}rs &= s^{a}rs^{6a+8k-16}rs^{-a}, \end{aligned}$$

so,

$$\begin{aligned} s^{-1}rs^{6a+8k-16}rs &= s^{a}rs^{6a+8k-16}rs^{-a} \\ &= s^{-6a-8k+16}rs^{6a+8k-16}r \\ &= x^{-1}y. \end{aligned}$$

Hence, $\{x, y\}$ generates the kernel. Also, x and y both have order dividing 4, $y^{-1}xy = x^{-1}$ from 4.63 and $x^2 = y^2$ since $s^{12a+16k-32}$ is central, so $\langle x, y\rangle$ is a homomorphic image of Q_8, which has derived length 2. It is left to show $\langle x, y\rangle \cong Q_8$.

Consider the group

$$G^{a,b,c} = \langle r, s | r^2, s^8, rs^a rs^b rs^c\rangle,$$

a homomorphic image of $F^{a,b,c}$. Here, $G^{a,b,c} \cong G^{a',b',c'}$, where a', b' and c' are a, b and c modulo 8. Using $F^{a-8,a,a+4k}$ for the case $d = 4$, then a is odd and $a' \in \{1, 3, 5, 7\}$. Thus, we are left with only four cases for $G^{a-8,a,a+4k}$. As $(2, k) = 1$, then k is odd, and we have $G^{1,1,5}$, $G^{3,3,7}$, $G^{5,5,1}$ and $G^{7,7,3}$. Using GAP, we obtain that each of these groups has derived length 4, and $F^{a-8,a,a+4k}$ must have derived length of at least 4.

From Theorem 3.5 of [3], we know that all groups $H^{a,b,c}$ are finite metabelian groups when $(a, b, c) = 1$, $n \neq 0$ and $(d, 6) \neq 6$. As a is odd and $d = 4$, then $H^{a-8,a,a+4k}$ is finite metabelian and, therefore, has derived length 2. This implies that $\langle x, y\rangle$, the kernel of the natural homomorphism from $F^{a-8,a,a+4k}$ to $H^{a-8,a,a+4k}$, must have derived length at least 2. Thus, $\langle x, y\rangle \cong Q_8$.

4. When $(a, c) \neq 1$

   According to the $F^{a,b,c}$ conjecture, we must have $(a, b, c) = 1$ to ensure proper results. Consider $F^{a-2c,a,a+kc}$. Here, $s^{2n} = s^{6a+2kc-4c}$ and $d = c$ when $(2, k) = 1$. When $(a, c) \neq 1$ for $c \in \{2, 3, 4\}$, then we have $(a - 2c, a, a + kc) \neq 1$ and either of two cases

   (a) a is a multiple of c or

   (b) $c = 4$ and a is a multiple of 2.

   If a is a multiple of c, then all of $a - 2c$, a and $a + kc$ are divisible by c and, as such, are not co-prime. If we consider $F^{a-2c,a,a+kc}$ where $a = ci$ for some integer i, then using $m = i$ in $(rs^{2a+cm+kc-2c}rs^{a-cm})^2 = 1$ gives

$$
\begin{aligned}
1 &= (rs^{2a+ci+kc-2c}rs^{a-ci})^2 \\
&= (rs^{2a+a+kc-2c}rs^{a-a})^2 \\
&= (rs^{3a+kc-2c}r)^2 \\
&= rs^{6a+2kc-4c}r,
\end{aligned}
$$

   and so, $s^{2n} = s^{6a+2kc-4c} = 1$.

We find that where a is a multiple of c, $F^{a-2c,a,a+kc} \cong H^{a-2c,a,a+kc}$.

We just need to look at the case where $c = 4$ and $a = 2i$ for some odd integer i. Using $m = i$ in $(rs^{2a-4m}rs^{a+4m+4k-8})^2 = 1$ gives

$$\begin{aligned} 1 &= (rs^{2a-4i}rs^{a+4i+4k-8})^2 \\ &= (rs^{2a-2a}rs^{a+2a+4k-8})^2 \\ &= (s^{3a+4k-8})^2 \\ &= s^{6a+8k-16}, \end{aligned}$$

and $s^{2n} = s^{6a+8k-16} = 1$. Hence, $F^{a-8,a,a+4k} \cong H^{a-8,a,a+4k}$ where $a = 2i$ for i odd.

Thus, where $c \in \{2,3,4\}$ and $(a-2c, a, a+kc) \neq 1$, we find that $F^{a-2c,a,a+kc} \cong H^{a-c,a,a+kc}$.

□

4.7 $F^{a-jc,a,a+kc}$ for $a, c, j, k \in \mathbb{Z}$ with $(j, k) = 1$

The difficulties we encountered in trying to modify our proof of the $F^{a,b,c}$ conjecture for the groups $F^{a-c,a,a+kc}$ with $a, c, k \in \mathbb{Z}$ to one for the groups $F^{a-2c,a,a+kc}$ for $a, c, k \in \mathbb{Z}$ with $(2, k) = 1$ gave us a good indication of what to expect for our last generalisation.

For the groups $F^{a-jc,a,a+kc}$ for $a, c, j, k \in \mathbb{Z}$ with $(j, k) = 1$, we still needed to be able to prove two steps in order to use the same following arguments for the cases, $c = 2$, $c = 3$ and $c = 4$, the first of which was relatively easily determined. By the same form of induction for the second step as for our previous groups, we found we could obtain a proof for all multiples of j, $m = lj$ for some integer l,

$$\begin{aligned} (rs^{2a+md+kd-jd}rs^{a-md})^2 &= 1 \quad \text{and} \\ (rs^{2a-md}rs^{a+md+kd-jd})^2 &= 1. \end{aligned}$$

However, we needed these relation sequences to be true for all integers m, not only multiples of j. Previously, we had been able to show they held for the rest of the integers because while proving the equations for m, we also proved the case $m - k - j$. However, in this earlier proof, $j = 2$, so while m was even, $m - k - 2$ was odd and this was enough. Here, $(j, k) = 1$, so where m is a multiple of j, $m - k - j$ is neither a multiple of j nor of k, and we have not determined the truth of the relation sequences for all integers. Thus, we needed another induction proof to consider including multiples of k. Once that was determined, however, the fact that j and k are co-prime allowed us to show the relation sequence was true for all integers m.

As groups of the form, $F^{a-jc,a,a+kc}$ for $a, c, j, k \in \mathbb{Z}$ with $(j, k) = 1$, actually encapsulate all groups $F^{a,b,c}$, our proof of this case finished our study of the $F^{a,b,c}$ conjecture. The proof is contained in the next chapter.

Chapter 5

Proof of the $F^{a,b,c}$ Conjecture

In our investigation of the $F^{a,b,c}$ conjecture, we found it easier to consider these groups when written as

$$F^{a-jd,a,a+kd} = \langle r, s | r^2, rs^{a-jd}rs^a rs^{a+kd} \rangle,$$

for some $j, k \in \mathbb{Z}$ where $(j, k) = 1$.

Beginning with the original form,

$$F^{a,b,c} = \langle r, s | r^2, rs^a rs^b rs^c \rangle,$$

it is obvious that $F^{a,b,c} = F^{c,a,b}$ and, for $F^{c,a,b}$, we have

$$\begin{aligned} n &= a + b + c, \\ d &= (c - a, a - b) \quad \text{and} \\ s^{2n} &= s^{2a+2b+2c}. \end{aligned}$$

When considering $F^{c,a,b}$ with $d = (c - a, a - b)$, then for some integers j and k, it must be that

$$a - c = jd \text{ and } b - a = kd \text{ with } (j, k) = 1.$$

Thus, $c = a - jd$ and $b = a + kd$, and we can write any $F^{a,b,c}$ equivalently as

$$F^{a-jd,a,a+kd} = \langle r,s|r^2, rs^{a-jd}rs^a rs^{a+kd}\rangle, (j,k) = 1.$$

We will use this notation throughout.

Before we can give our proof of the conjecture, some preliminary results and lemmas, which form the building blocks of our proof, must be stated.

For $F^{a-jd,a,a+kd}$ with $(j,k) = 1$, we have

$$\begin{aligned} n &= a - jd + a + a + kd \\ &= 3a + kd - jd \quad \text{and} \\ s^{2n} &= s^{6a+2kd-2jd}. \end{aligned}$$

Note that in $F^{a-jd,a,a+kd}$, we have

$$\begin{aligned} rs^{a-jd}r &= s^{-a-kd}rs^{-a}, \\ rs^a r &= s^{jd-a}rs^{-a-kd} \quad \text{and} \\ rs^{a+kd}r &= s^{-a}rs^{jd-a}. \end{aligned}$$

Hence, we obtain the simple relations

$$\begin{aligned} rs^{2a-2jd}r &= (rs^{a-jd}r)^2 \\ &= s^{-a-kd}rs^{-2a-kd}rs^{-a}, \end{aligned} \tag{5.1}$$

$$\begin{aligned} rs^{2a-jd}r &= (rs^{a-jd}r)(rs^a r) \\ &= s^{-a-kd}rs^{jd-2a}rs^{-a-kd} \quad \text{and} && (5.2) \\ &= (rs^a r)(rs^{a-jd}r) \\ &= s^{jd-a}rs^{-2a-2kd}rs^{-a}, && (5.3) \end{aligned}$$

$$\begin{aligned} rs^{2a}r &= (rs^a r)^2 \\ &= s^{jd-a}rs^{-2a-kd+jd}rs^{-a-kd}, \end{aligned} \tag{5.4}$$

$$
\begin{aligned}
rs^{2a+kd-jd}r &= (rs^{a-jd}r)(rs^{a+kd}r) \\
&= s^{-a-kd}rs^{-2a}rs^{jd-a} \quad \text{and} && (5.5) \\
&= (rs^{a+kd}r)(rs^{a-jd}r) \\
&= s^{-a}rs^{-2a-kd+jd}rs^{-a}, && (5.6)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a+kd}r &= (rs^{a}r)(rs^{a+kd}r) \\
&= s^{jd-a}rs^{-2a-kd}rs^{jd-a} \quad \text{and} && (5.7) \\
&= (rs^{a+kd}r)(rs^{a}r) \\
&= s^{-a}rs^{2jd-2a}rs^{-a-kd}, && (5.8)
\end{aligned}
$$

$$
\begin{aligned}
rs^{2a+2kd}r &= (rs^{a+kd}r)^2 \\
&= s^{-a}rs^{jd-2a}rs^{jd-a}, && (5.9)
\end{aligned}
$$

$$
\begin{aligned}
rs^{jd}r &= (rs^{a}r)(rs^{jd-a}r) \\
&= s^{jd-a}rs^{-kd}rs^{a+kd} \quad \text{and} && (5.10) \\
&= (rs^{jd-a}r)(rs^{a}r) \\
&= s^{a}rs^{kd+jd}rs^{-a-kd}, && (5.11)
\end{aligned}
$$

$$
\begin{aligned}
rs^{kd}r &= (rs^{a+kd}r)(rs^{-a}r) \\
&= s^{-a}rs^{kd+jd}rs^{a-jd} \quad \text{and} && (5.12) \\
&= (rs^{-a}r)(rs^{a+kd}r) \\
&= s^{a+kd}rs^{-jd}rs^{jd-a}, && (5.13)
\end{aligned}
$$

$$
\begin{aligned}
rs^{kd+jd}r &= (rs^{a+kd}r)(rs^{jd-a}r) \\
&= s^{-a}rs^{jd}rs^{a+kd} \quad \text{and} && (5.14) \\
&= (rs^{jd-a}r)(rs^{a+kd}r) \\
&= s^{a}rs^{kd}rs^{jd-a}. && (5.15)
\end{aligned}
$$

So,

$$\begin{aligned} rs^{2a-jd}r &= s^{-a-kd}rs^{jd-2a}rs^{-a-kd} \\ &= s^{-a-kd}(s^{a}rs^{2a+2kd}rs^{a-jd})s^{-a-kd} \quad \text{from 5.2 and 5.3} \\ &= s^{-kd}rs^{2a+2kd}rs^{-kd-jd}, \end{aligned} \tag{5.16}$$

$$\begin{aligned} rs^{2a+kd-jd}r &= s^{-a}rs^{-2a-kd+jd}rs^{-a} \\ &= s^{-a}(s^{a-jd}rs^{2a}rs^{a+kd})s^{-a} \quad \text{from 5.6 and 5.5} \\ &= s^{-jd}rs^{2a}rs^{kd}, \end{aligned} \tag{5.17}$$

$$\begin{aligned} rs^{2a+kd}r &= s^{jd-a}rs^{-2a-kd}rs^{jd-a} \\ &= s^{jd-a}(s^{a+kd}rs^{2a-2jd}rs^{a})s^{jd-a} \quad \text{from 5.7 and 5.8} \\ &= s^{kd+jd}rs^{2a-2jd}rs^{jd}. \end{aligned} \tag{5.18}$$

From these numerous equations, we can form and prove the necessary lemmas.

Lemma 5.1 In the groups $F^{a-jd,a,a+kd}$ with $j,k \in \mathbb{Z}$, then

$$rs^{6a+2kd-2jd}r \sim s^{d}.$$

Proof. Using the equations 5.16, 5.17 and 5.18, we find

$$\begin{aligned} rs^{6a+2kd-2jd}r &= (rs^{2a+kd-jd}r)(rs^{2a-jd}r)(rs^{2a+kd}r) \\ &= s^{-jd}rs^{6a+2kd-2jd}rs^{jd} \quad \text{and} \end{aligned}$$

$$\begin{aligned} rs^{6a+2kd-2jd}r &= (rs^{2a-jd}r)(rs^{2a+kd}r)(rs^{2a+kd-jd}r) \\ &= s^{-kd}rs^{6a+2kd-2jd}rs^{kd}. \end{aligned}$$

Since $(j,k)=1$, then $xj+yk=1$ for some integers x and y, and

$$\begin{aligned}
s^{-d}rs^{6a+2kd-2jd}rs^{d} &= s^{-(xj+yk)d}rs^{6a+2kd-2jd}rs^{(xj+yk)d}\\
&= s^{-xjd}.s^{-ykd}rs^{6a+2kd-2jd}rs^{ykd}.s^{xjd}\\
&= s^{-xjd}rs^{6a+2kd-2jd}rs^{xjd}\\
&= rs^{6a+2kd-2jd}r.
\end{aligned}$$

□

Lemma 5.2 In $F^{a-jd,a,a+kd}$, for all integers $l \geq 0$,

$$\begin{aligned}
(rs^{2a+(lj)d+kd-jd}rs^{a-(lj)d})^2 &= 1 \quad \text{and}\\
(rs^{2a-(lj)d}rs^{a+(lj)d+kd-jd})^2 &= 1.
\end{aligned}$$

Proof. Proof by induction on l

Base step

$l=0$

$$\begin{aligned}
& rs^{2a+kd-jd}rs^{a}rs^{2a+kd-jd}rs^{a}\\
={}& rs^{2a+kd-jd}(s^{jd-a}rs^{-a-kd})s^{2a+kd-jd}rs^{a}\\
={}& rs^{a+kd}rs^{a-jd}rs^{a}\\
={}& 1
\end{aligned}$$

$$\begin{aligned}
& rs^{2a}rs^{a+kd-jd}rs^{2a}rs^{a+kd-jd}\\
={}& rs^{2a}rs^{a+kd-jd}(s^{jd}rs^{2a+kd-jd}rs^{-kd})s^{a+kd-jd} && \text{from 5.17}\\
={}& rs^{2a}rs^{a+kd}rs^{2a+kd-jd}rs^{a-jd}\\
={}& rs^{2a}(s^{-a}rs^{jd-a})s^{2a+kd-jd}rs^{a-jd}\\
={}& rs^{a}rs^{a+kd}rs^{a-jd}\\
={}& 1
\end{aligned}$$

$l = 1$

$$\begin{aligned}
& rs^{2a+kd}rs^{a-jd}rs^{2a+kd}rs^{a-jd} \\
= \;& rs^{2a+kd}(s^{-a-kd}rs^{-a})s^{2a+kd}rs^{a-jd} \\
= \;& rs^{a}rs^{a+kd}rs^{a-jd} \\
= \;& 1
\end{aligned}$$

$$\begin{aligned}
& rs^{2a-jd}rs^{a+kd}rs^{2a-jd}rs^{a+kd} \\
= \;& rs^{2a-jd}(s^{-a}rs^{jd-a})s^{2a-jd}rs^{a+kd} \\
= \;& rs^{a-jd}rs^{a}rs^{a+kd} \\
= \;& 1
\end{aligned}$$

Inductive step

Assume for $0 \leq i < l$,

$$\begin{aligned}
(rs^{2a+(ij)d+kd-jd}rs^{a-(ij)d})^2 &= 1 \quad \text{and} \\
(rs^{2a-(ij)d}rs^{a+(ij)d+kd-jd})^2 &= 1.
\end{aligned}$$

Since we have shown it to be true for $l \in \{0, 1\}$, we can assume $l \geq 2$. Consider $i = l$, with $l \geq 2$. We know $0 \leq l - 2 < l$, so

$$\begin{aligned}
& (rs^{2a+(l-2)jd+kd-jd}rs^{a-(l-2)jd})^2 \\
= \;& (rs^{2a+ljd+kd-3jd}rs^{a-ljd+2jd})^2 \\
= \;& 1
\end{aligned}$$

and

$$\begin{aligned}
& (rs^{2a-(l-2)jd}rs^{a+(l-2)jd+kd-jd})^2 \\
= \;& (rs^{2a-ljd+2jd}rs^{a+ljd+kd-3jd})^2 \\
= \;& 1.
\end{aligned}$$

Also, $0 < l-1 < l$, so

$$\begin{aligned} & (rs^{2a+(l-1)jd+kd-jd} rs^{a-(l-1)jd})^2 \\ = & (rs^{2a+ljd+kd-2jd} rs^{a-ljd+jd})^2 \\ = & 1 \end{aligned}$$

and

$$\begin{aligned} & (rs^{2a-(l-1)jd} rs^{a+(l-1)jd+kd-jd})^2 \\ = & (rs^{2a-ljd+jd} rs^{a+ljd+kd-2jd})^2 \\ = & 1. \end{aligned}$$

We need some additional equations for our proof. As $(j,k) = 1$, then $(l-1)j - k$ is not a multiple of j and we cannot assume that either

$$\begin{aligned} & (rs^{2a-((l-1)j-k)d} rs^{a+((l-1)j-k)d+kd-jd})^2 \\ = & (rs^{2a-ljd+kd+jd} rs^{a+ljd-2jd})^2 \\ = & 1 \end{aligned}$$

or

$$\begin{aligned} & (rs^{2a+((l-1)j-k)d+kd-jd} rs^{a-((l-1)j-k)d})^2 \\ = & (rs^{2a+ljd-2jd} rs^{a-ljd+kd+jd})^2 \\ = & 1. \end{aligned}$$

Using our inductive hypothesis, however, we can form the proofs for these necessary equations. We have

$$\begin{aligned}
r &= s^{kd}rs^{a-jd}rs^{jd}rs^{-a-kd}, \quad \text{from 5.10} \\
1 &= (rs^{a+ljd+kd-2jd}rs^{2a-ljd+jd})^2, \\
1 &= (rs^{-a+ljd-2jd}rs^{-2a-ljd-kd+3jd})^2
\end{aligned}$$

and

$$1 = (rs^{2a+ljd+kd-2jd}rs^{a-ljd+jd})^2,$$

so,

$$\begin{aligned}
& rs^{2a-ljd+kd+jd}rs^{a+ljd-2jd}r \\
= \; & rs^{2a-ljd+kd+jd}rs^{a+ljd-2jd}.r. \\
= \; & rs^{2a-ljd+kd+jd}.rs^{a+ljd+kd-2jd}r.s^{a-jd}rs^{jd}rs^{-a-kd} \\
= \; & rs^{kd}rs^{-a-ljd-kd+2jd}.rs^{-a+ljd-2jd}r.s^{jd}rs^{-a-kd} \\
= \; & rs^{kd}rs^{a-jd}rs^{a-ljd+2jd}.rs^{2a+ljd+kd-2jd}r.s^{-a-kd} \\
= \; & rs^{kd}rs^{a-jd}rs^{jd}rs^{-2a-ljd-kd+2jd}rs^{-2a+ljd-kd-jd} \\
= \; & rs^{-a}rs^{jd-a}rs^{-2a-ljd-kd+2jd}rs^{-2a+ljd-kd-jd} \\
= \; & s^{-a-ljd+2jd}rs^{-2a+ljd-kd-jd}.
\end{aligned}$$

From

$$\begin{aligned}
r &= s^{a+kd}rs^{a-jd}rs^{a}, \\
r &= s^{jd-a}rs^{-a-kd}rs^{-a}, \\
1 &= (rs^{2a+ljd+kd-2jd}rs^{a-ljd+jd})^2, \\
1 &= (rs^{-2a+ljd-kd-jd}rs^{-a-ljd+2jd})^2
\end{aligned}$$

and

$$1 = (rs^{2a-ljd+kd+jd}rs^{a+ljd-2jd})^2,$$

we obtain

$$
\begin{aligned}
& rs^{a-ljd+kd+jd}rs^{2a+ljd-2jd}r \\
= \;& rs^{a-ljd+kd+jd}rs^{2a+ljd-2jd}.r. \\
= \;& rs^{a-ljd+kd+jd}.r.s^{3a+ljd+kd-2jd}rs^{a-jd}rs^{a} \\
= \;& rs^{-ljd+kd+2jd}rs^{-a-kd}.rs^{2a+ljd+kd-2jd}r.s^{a-jd}rs^{a} \\
= \;& rs^{-ljd+kd+2jd}.rs^{-2a+ljd-kd-jd}r.s^{-2a-ljd-kd+2jd}rs^{ljd-2jd}rs^{a} \\
= \;& rs^{a+kd}rs^{2a-ljd+kd+jd}.rs^{-a-kd}r.s^{ljd-2jd}rs^{a} \\
= \;& .rs^{a+kd}r.s^{3a-ljd+kd}rs^{a+ljd-2jd}rs^{a} \\
= \;& s^{-a}.rs^{2a-ljd+kd+jd}rs^{a+ljd-2jd}r.s^{a} \\
= \;& s^{-2a-ljd+2jd}rs^{-a+ljd-kd-jd}.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
(rs^{2a-ljd+kd+jd}rs^{a+ljd-2jd})^2 &= 1 \quad \text{and} \\
(rs^{2a+ljd-2jd}rs^{a-ljd+kd+jd})^2 &= 1.
\end{aligned}
$$

Now, we can consider $i = l$.

Using

$$
\begin{aligned}
rs^{kd+jd}r &= s^{a}rs^{kd}rs^{jd-a}, \quad \text{from 5.15} \\
1 &= (rs^{a+ljd-2jd}rs^{2a-ljd+kd+jd})^2, \\
1 &= (rs^{-a+ljd-kd-jd}rs^{-2a-ljd+2jd})^2 \\
&\text{and} \\
1 &= (rs^{2a+ljd+kd-2jd}rs^{a-ljd+jd})^2,
\end{aligned}
$$

we have

$$
\begin{aligned}
& rs^{2a-ljd}rs^{a+ljd+kd-jd}r \\
= \;& rs^{2a-ljd}(rs^{a+ljd-2jd}r)(rs^{kd+jd}r) \\
= \;& rs^{-kd-jd}rs^{-a-ljd+2jd}.rs^{-a+ljd-kd-jd}r.s^{kd}rs^{jd-a} \\
= \;& rs^{-kd-jd}rs^{a}rs^{a-ljd+kd+jd}rs^{2a+ljd+kd-2jd}rs^{jd-a} \\
= \;& rs^{-kd-jd}(s^{jd-a}rs^{-a-kd})s^{a-ljd+kd+jd}rs^{2a+ljd+kd-2jd}rs^{jd-a} \\
= \;& rs^{-a-kd}rs^{-ljd+jd}.rs^{2a+ljd+kd-2jd}r.s^{jd-a} \\
= \;& rs^{-a-kd}rs^{-a}rs^{-2a-ljd-kd+2jd}rs^{-2a+ljd} \\
= \;& s^{-a-ljd-kd+jd}rs^{-2a+ljd},
\end{aligned}
$$

and, from

$$
\begin{aligned}
rs^{-jd}r &= s^{a+kd}rs^{-kd-jd}rs^{-a}, \quad \text{from 5.11} \\
1 &= (rs^{a-ljd+jd}rs^{2a+ljd+kd-2jd})^2, \\
1 &= (rs^{-a-ljd+2jd}rs^{-2a+ljd-kd-jd})^2 \\
\text{and} & \\
1 &= (rs^{2a-ljd}rs^{a+ljd+kd-jd})^2,
\end{aligned}
$$

we find

$$
\begin{aligned}
& rs^{2a+ljd+kd-jd}rs^{a-ljd}r \\
= \;& rs^{2a+ljd+kd-jd}(rs^{a-ljd+jd}r)(rs^{-jd}r) \\
= \;& rs^{jd}rs^{-a+ljd-jd}rs^{-a-ljd+2jd}rs^{-kd-jd}rs^{-a} \\
= \;& rs^{jd}rs^{-a+ljd-jd}.rs^{-a-ljd+2jd}r.s^{-kd-jd}rs^{-a} \\
= \;& rs^{jd}rs^{a+kd}rs^{a+ljd-2jd}rs^{2a-ljd}rs^{-a} \\
= \;& rs^{jd}(s^{-a}rs^{jd-a})s^{a+ljd-2jd}rs^{2a-ljd}rs^{-a} \\
= \;& rs^{jd-a}rs^{ljd-jd}.rs^{2a-ljd}r.s^{-a} \\
= \;& rs^{jd-a}rs^{-a-kd}rs^{-2a+ljd}rs^{-2a-ljd-kd+jd} \\
= \;& s^{-a+ljd}rs^{-2a-ljd-kd+jd}.
\end{aligned}
$$

Thus, by induction, for all integers $l \geq 0$,

$$\begin{aligned}(rs^{2a+(lj)d+kd-jd}rs^{a-(lj)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj)d}rs^{a+(lj)d+kd-jd})^2 &= 1.\end{aligned}$$

□

Lemma 5.3 In $F^{a-jd,a,a+kd}$, for all integers l,

$$\begin{aligned}(rs^{2a+(lj)d+kd-jd}rs^{a-(lj)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj)d}rs^{a+(lj)d+kd-jd})^2 &= 1.\end{aligned}$$

Proof. Let us consider an integer $l < 0$. Using $l = -i$ for an integer $i > 0$, we have

$$\begin{aligned}&(rs^{2a+(lj)d+kd-jd}rs^{a-(lj)d})^2 \\ =\ &(rs^{2a-ijd+kd-jd}rs^{a+ijd}r)^2 \\ =\ &(rs^{2a-((i+1)j-k)d}rs^{a+((i+1)j-k)d+kd-jd})^2\end{aligned}$$

and

$$\begin{aligned}&(rs^{2a-(lj)d}rs^{a+(lj)d+kd-jd})^2 \\ =\ &(rs^{2a+ijd}rs^{a-ijd+kd-jd}r)^2 \\ =\ &(rs^{2a+((i+1)j-k)d+kd-jd}rs^{a-((i+1)j-k)d})^2.\end{aligned}$$

Thus, a proof of $(i+1)j-k$ is equivalent to one of lj. Obviously, as $i > 0$, then $i+2 > 0$ and so, the two expressions equal the identity for $l = i+2$ according to our induction proof. During the proof of lj, however, we found that the two expressions were also trivial for $(l-1)j-k$. Thus, for $l = i+2$, we have the equations true for $(i+2-1)j-k = (i+1)j-k$, as required, and the proof holds for all negative integers as well. □

Lemma 5.4 In $F^{a-jd,a,a+kd}$, for all integers l and $m \geq 0$,

$$\begin{aligned}(rs^{2a+(lj-mk)d+kd-jd}rs^{a-(lj-mk)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj-mk)d}rs^{a+(lj-mk)d+kd-jd})^2 &= 1.\end{aligned}$$

Proof. Proof by induction on $m \geq 0$

Let l be an integer so we know from our previous inductive proof that both

$$\begin{aligned} & (rs^{2a+(lj)d+kd-jd}rs^{a-(lj)d})^2 \\ = \ & 1, \\ & (rs^{2a-(lj)d}rs^{a+(lj)d+kd-jd})^2 \\ = \ & 1 \end{aligned}$$

and

$$\begin{aligned} & (rs^{2a+((l-1)j-k)d+kd-jd}rs^{a-((l-1)j-k)d})^2 \\ = \ & (rs^{2a+ljd-2jd}rs^{a-ljd+kd+jd})^2 \\ = \ & 1, \\ & (rs^{2a-((l-1)j-k)d}rs^{a+((l-1)j-k)d+kd-jd})^2 \\ = \ & (rs^{2a-ljd+kd+jd}rs^{a+ljd-2jd})^2 \\ = \ & 1. \end{aligned}$$

We also have the same true for $l+1$, so

$$\begin{aligned}(rs^{2a+(l+1)jd+kd-jd}rs^{a-(l+1)jd})^2 &= (rs^{2a+ljd+kd}rs^{a-ljd-jd})^2 \\ &= 1, \\ (rs^{2a-(l+1)jd}rs^{a+(l+1)jd+kd-jd})^2 &= (rs^{2a-ljd-jd)}rs^{a+ljd+kd})^2 \\ &= 1\end{aligned}$$

and

$$\begin{aligned}(rs^{2a+(lj-k)d+kd-jd}rs^{a-(lj-k)d})^2 &= (rs^{2a+ljd-jd}rs^{a-ljd+kd})^2\\ &= 1,\\ (rs^{2a-(lj-k)d}rs^{a+(lj-k)d+kd-jd})^2 &= (rs^{2a-ljd+kd}rs^{a+ljd-jd})^2\\ &= 1.\end{aligned}$$

Induction on $m \geq 0$:

Base step

$m = 0$

$$\begin{aligned}&(rs^{2a-(lj-0)d}rs^{a+(lj-0)d+kd-jd})^2\\ =\ &(rs^{2a-ljd}rs^{a+ljd+kd-jd})^2\\ =\ &1\end{aligned}$$

and

$$\begin{aligned}&(rs^{2a+(lj-0)d+kd-jd}rs^{a-(lj-0)d})^2\\ =\ &(rs^{2a+ljd+kd-jd}rs^{a-ljd})^2\\ =\ &1.\end{aligned}$$

$m = 1$

$$\begin{aligned}&(rs^{2a-(lj-k)d}rs^{a+(lj-k)d+kd-jd})^2\\ =\ &(rs^{2a-ljd+kd}rs^{a+ljd-jd})^2\\ =\ &1\end{aligned}$$

and

$$\begin{aligned}&(rs^{2a+(lj-k)d+kd-jd}rs^{a-(lj-k)d})^2\\ =\ &(rs^{2a+ljd-jd}rs^{a-ljd+kd})^2\\ =\ &1.\end{aligned}$$

Inductive step

Assume for $0 \leq i < m$,

$$\begin{aligned}(rs^{2a+(lj-ik)d+kd-jd}rs^{a-(lj-ik)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj-ik)d}rs^{a+(lj-ik)d+kd-jd})^2 &= 1.\end{aligned}$$

Since we have shown it to be true for $m \in \{0,1\}$, we can assume $m \geq 2$. Given, $0 < m-1 < m$, we know

$$\begin{aligned}&(rs^{2a+(lj-(m-1)k)d+kd-jd}rs^{a-(lj-(m-1)k)d})^2 \\ &= (rs^{2a+ljd-mkd+2kd-jd}rs^{a-ljd+mkd-kd})^2 \\ &= 1\end{aligned}$$

and

$$\begin{aligned}&(rs^{2a-(lj-(m-1)k)d}rs^{a+(lj-(m-1)k)d+kd-jd})^2 \\ &= (rs^{2a-ljd+mkd-kd}rs^{a+ljd-mkd+2kd-jd})^2 \\ &= 1.\end{aligned}$$

Also, since we assumed l to be an integer, we can assume the above equations for $(l-1)j$ and $(l+1)j$ as well. Hence,

$$\begin{aligned}&(rs^{2a+(l-1)jd-mkd+2kd-jd}rs^{a-(l-1)jd+mkd-kd})^2 \\ =\ &(rs^{2a+ljd-mkd+2kd-2jd}rs^{a-ljd+mkd-kd+jd})^2 \\ =\ &1\end{aligned}$$

and

$$\begin{aligned}&(rs^{2a-(l-1)jd+mkd-kd)}rs^{a+(l-1)jd-mkd+2kd-jd})^2 \\ =\ &(rs^{2a-ljd+mkd-kd+jd}rs^{a+ljd-mkd+2kd-2jd})^2 \\ =\ &1,\end{aligned}$$

$$
\begin{aligned}
& \left(rs^{2a+(l+1)jd-mkd+2kd-jd}rs^{a-(l+1)jd+mkd-kd}\right)^2 \\
= & \left(rs^{2a+ljd-mkd+2kd}rs^{a-ljd+mkd-kd-jd}\right)^2 \\
= & \ 1
\end{aligned}
$$

and

$$
\begin{aligned}
& \left(rs^{2a-(l+1)jd+mkd-kd)}rs^{a+(l+1)jd-mkd+2kd-jd}\right)^2 \\
= & \left(rs^{2a-ljd+mkd-kd-jd}rs^{a+ljd-mkd+2kd}\right)^2 \\
= & \ 1.
\end{aligned}
$$

Consider $i = m$.

Using

$$
\begin{aligned}
r &= s^{kd}rs^{a-jd}rs^{jd}rs^{-a-kd}, \quad \text{from 5.13} \\
1 &= \left(rs^{a+ljd-mkd+2kd-jd}rs^{2a-ljd+mkd-kd}\right)^2, \\
1 &= \left(rs^{-a+ljd-mkd+kd-jd}rs^{-2a-ljd+mkd-2kd+2jd}\right)^2
\end{aligned}
$$

and

$$
1 = \left(rs^{2a+ljd-mkd+2kd-jd}rs^{a-ljd+mkd-kd}\right)^2,
$$

we obtain

$$
\begin{aligned}
& rs^{2a-(lj-mk)d}rs^{a+(lj-mk)d+kd-jd}r \\
= \;& rs^{2a-ljd+mkd}rs^{a+ljd-mkd+kd-jd}.r. \\
= \;& rs^{2a-ljd+mkd}rs^{a+ljd-mkd+2kd-jd}rs^{a-jd}rs^{jd}rs^{-a-kd} \\
= \;& rs^{2a-ljd+mkd}.rs^{a+ljd-mkd+2kd-jd}r.s^{a-jd}rs^{jd}rs^{-a-kd} \\
= \;& rs^{kd}rs^{-a-ljd+mkd-2kd+jd}.rs^{-a+ljd-mkd+kd-jd}r.s^{jd}rs^{-a-kd} \\
= \;& rs^{kd}rs^{a-jd}rs^{a-ljd+mkd-kd+jd}.rs^{2a+ljd-mkd+2kd-jd}r.s^{-a-kd} \\
= \;& rs^{kd}rs^{a-jd}rs^{jd}rs^{-2a-ljd+mkd-2kd+jd}rs^{-2a+ljd-mkd} \\
= \;& rs^{-a}rs^{jd-a}rs^{-2a-ljd+mkd-2kd+jd}rs^{-2a+ljd-mkd} \\
= \;& s^{-a-ljd+mkd-kd+jd}rs^{-2a+ljd-mkd} \\
= \;& s^{-a-(lj-mk)d-kd+jd}rs^{-2a+(lj-mk)d},
\end{aligned}
$$

and so,

$$(rs^{2a-(lj-mk)d}rs^{a+(lj-mk)d+kd-jd})^2 = 1.$$

As l is an arbitrary integer, we can assume the above is true for $l+1$, and thus,

$$
\begin{aligned}
& (rs^{2a-((l+1)j-mk)d}rs^{a+((l+1)j-mk)d+kd-jd})^2 \\
= \;& (rs^{2a-ljd+mkd-jd}rs^{a+ljd-mkd+kd})^2 \\
= \;& 1.
\end{aligned}
$$

From

$$
\begin{aligned}
r &= s^{kd+jd}rs^{-a-kd}rs^{-jd}rs^{a}, \quad \text{from 5.11} \\
1 &= (rs^{2a+ljd-mkd+2kd}rs^{a-ljd+mkd-kd-jd})^2, \\
1 &= (rs^{-2a+ljd-mkd+jd}rs^{-a-ljd+mkd-kd})^2
\end{aligned}
$$

and

$$1 = (rs^{a+ljd-mkd+kd-jd}rs^{2a-ljd+mkd})^2,$$

we have

$$\begin{aligned}
& rs^{a-(lj-mk)d}rs^{2a+(lj-mk)d+kd-jd}r \\
= \;& rs^{a-ljd+mkd}rs^{2a+ljd-mkd+kd-jd}.r. \\
= \;& rs^{a-ljd+mkd}.rs^{2a+ljd-mkd+2kd}r.s^{-a-kd}rs^{-jd}rs^{a} \\
= \;& rs^{kd+jd}rs^{-2a-ljd+mkd-2kd}.rs^{-2a+ljd-mkd+jd}r.s^{-jd}rs^{a} \\
= \;& rs^{kd+jd}rs^{-a-kd}rs^{2a-ljd+mkd-jd}.rs^{a+ljd-mkd+kd-jd}r.s^{a} \\
= \;& rs^{kd+jd}rs^{-a-kd}rs^{-jd}rs^{-a-ljd+mkd-kd+jd}rs^{-a+ljd-mkd} \\
= \;& rs^{a+kd}rs^{a-jd}rs^{-a-ljd+mkd-kd+jd}rs^{-a+ljd-mkd} \\
= \;& s^{-2a-ljd+mkd-kd+jd}rs^{-a+ljd-mkd} \\
= \;& s^{-2a-(lj-mk)d-kd+jd}rs^{-a+(lj-mk)d},
\end{aligned}$$

and so,

$$(rs^{2a+(lj-mk)d+kd-jd}rs^{a-(lj-mk)d})^2 = 1.$$

Hence, for all integers l and $m \geq 0$,

$$\begin{aligned}
(rs^{2a+(lj-mk)d+kd-jd}rs^{a-(lj-mk)d})^2 &= 1 \quad \text{and} \\
(rs^{2a-(lj-mk)d}rs^{a+(lj-mk)d+kd-jd})^2 &= 1.
\end{aligned}$$

□

Lemma 5.5 In $F^{a-jd,a,a+kd}$, for all integers l and $m \geq 0$,

$$\begin{aligned}
(rs^{2a+(lj+mk)d+kd-jd}rs^{a-(lj+mk)d})^2 &= 1 \quad \text{and} \\
(rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd})^2 &= 1.
\end{aligned}$$

Proof. Proof by induction on $m \geq 0$

Base step: $m = 0$

$$\begin{aligned}
(rs^{2a-(lj+0)d}rs^{a+(lj+0)d+kd-jd})^2 &= (rs^{2a-ljd}rs^{a+ljd+kd-jd})^2 \\
&= 1
\end{aligned}$$

and

$$\begin{aligned}(rs^{2a+(lj+0)d+kd-jd}rs^{a-(lj+0)d})^2 &= (rs^{2a+ljd+kd-jd}rs^{a-ljd})^2 \\ &= 1.\end{aligned}$$

Inductive step

Assume for $0 \leq i < m$,

$$\begin{aligned}(rs^{2a+(lj+ik)d+kd-jd}rs^{a-(lj+ik)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj+ik)d}rs^{a+(lj+ik)d+kd-jd})^2 &= 1.\end{aligned}$$

Since we have shown it to be true for $m = 0$, we can assume $m \geq 1$.

We know $0 \leq m - 1 < m$, so

$$\begin{aligned}&(rs^{2a+(lj+(m-1)k)d+kd-jd}rs^{a-(lj+(m-1)k)d})^2 \\ &= (rs^{2a+ljd+mkd-jd}rs^{a-ljd-mkd+kd})^2 \\ &= 1\end{aligned}$$

and

$$\begin{aligned}&(rs^{2a-(lj+(m-1)k)d}rs^{a+(lj+(m-1)k)d+kd-jd})^2 \\ &= (rs^{2a-ljd-mkd+kd}rs^{a+ljd+mkd-jd})^2 \\ &= 1.\end{aligned}$$

Also, since we assumed l to be an integer, we can assume the above equations for $(l-1)j$ as well. Thus, given $0 \leq m - 1 < m$, we know

$$\begin{aligned}&(rs^{2a+(l-1)jd+mkd-jd}rs^{a-(l-1)jd-mkd+kd)})^2 \\ &= (rs^{2a+ljd+mkd-2jd}rs^{a-ljd-mkd+kd+jd})^2 \\ &= 1\end{aligned}$$

and

$$
\begin{aligned}
&(rs^{2a-(l-1)jd-mkd+kd)}rs^{a+(l-1)jd+mkd-jd})^2 \\
&= (rs^{2a-ljd-mkd+kd+jd}rs^{a+ljd+mkd-2jd})^2 \\
&= 1.
\end{aligned}
$$

Consider $i = m$.

From

$$
\begin{array}{rcl}
r & = & s^{-kd-jd}rs^{-a}rs^{jd}rs^{a+kd}, \quad \text{from 5.11} \\
1 & = & (rs^{2a+ljd+mkd-2jd}rs^{a-ljd-mkd+kd+jd})^2, \\
1 & = & (rs^{-2a+ljd+mkd-kd-jd}rs^{-a-ljd-mkd+2jd})^2 \\
\text{and} & & \\
1 & = & (rs^{a+ljd+mkd-jd}rs^{2a-ljd-mkd+kd})^2
\end{array}
$$

we have

$$
\begin{array}{rl}
= & rs^{a-(lj+mk)d}rs^{2a+(lj+mk)d+kd-jd}r \\
= & rs^{a-ljd-mkd}rs^{2a+ljd+mkd+kd-jd}.r. \\
= & rs^{a-ljd-mkd}.rs^{2a+ljd+mkd-2jd}r.s^{-a}rs^{jd}rs^{a+kd} \\
= & rs^{-kd-jd}rs^{-2a-ljd-mkd+2jd}.rs^{-2a+ljd+mkd-kd-jd}r.s^{jd}rs^{a+kd} \\
= & rs^{-kd-jd}rs^{-a}rs^{2a-ljd-mkd+kd+jd}.rs^{a+ljd+mkd-jd}r.s^{a+kd} \\
= & rs^{-kd-jd}rs^{-a}rs^{jd}rs^{-a-ljd-mkd+jd}rs^{-a+ljd+mkd} \\
= & rs^{a-jd}rs^{a}rs^{-a-ljd-mkd+jd}rs^{-a+ljd+mkd} \\
= & s^{-2a-ljd-mkd-kd+jd}rs^{-a+ljd+mkd},
\end{array}
$$

and so,

$$(rs^{2a+(lj+mk)d+kd-jd}rs^{a-(lj+mk)d})^2 = 1.$$

As l is an arbitrary integer, we can assume the above is true for $l-1$, and thus,

$$
\begin{aligned}
& (rs^{2a+((l-1)j+mk)d+kd-jd}rs^{a-((l-1)j+mk)d})^2 \\
= & (rs^{2a+ljd+mkd+kd-2jd}rs^{a-ljd-mkd+jd})^2 \\
= & 1.
\end{aligned}
$$

From

$$
\begin{aligned}
r &= s^{-kd}rs^{a+kd}rs^{-jd}rs^{jd-a}, \quad \text{from 5.10} \\
1 &= (rs^{a+ljd+mkd-jd}rs^{2a-ljd-mkd+kd})^2, \\
1 &= (rs^{-a+ljd+mkd}rs^{-2a-ljd-mkd-kd+jd})^2 \\
\text{and} & \\
1 &= (rs^{2a+ljd+mkd+kd-2jd}rs^{a-ljd-mkd+jd})^2,
\end{aligned}
$$

we have

$$
\begin{aligned}
& rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd}r \\
= & rs^{2a-ljd-mkd}rs^{a+ljd+mkd+kd-jd}.r. \\
= & rs^{2a-ljd-mkd}.rs^{a+ljd+mkd-jd}r.s^{a+kd}rs^{-jd}rs^{jd-a} \\
= & rs^{-kd}rs^{-a-ljd-mkd+jd}.rs^{-a+ljd+mkd}r.s^{-jd}rs^{jd-a} \\
= & rs^{-kd}rs^{a+kd}rs^{a-ljd-mkd}.rs^{2a+ljd+mkd+kd-2jd}r.s^{jd-a} \\
= & rs^{-kd}rs^{a+kd}rs^{-jd}rs^{-2a-ljd-mkd-kd+2jd}rs^{-2a+ljd+mkd} \\
= & rs^{-a-kd}rs^{-a}rs^{-2a-ljd-mkd-kd+2jd}rs^{-2a+ljd+mkd} \\
= & s^{-a-ljd-mkd-kd+jd}rs^{-2a+ljd+mkd},
\end{aligned}
$$

and so,

$$
(rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd})^2 = 1.
$$

Hence, for all integers l and $m \geq 0$,

$$\begin{aligned}(rs^{2a+(lj+mk)d+kd-jd}rs^{a-(lj+mk)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd})^2 &= 1.\end{aligned}$$

□

Lemma 5.6 For all integers l and m,

$$\begin{aligned}(rs^{2a+(lj+mk)d+kd-jd}rs^{a-(lj+mk)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd})^2 &= 1.\end{aligned}$$

Proof. We know that for all integers l and $m \geq 0$,

$$\begin{aligned}(rs^{2a+(lj+mk)d+kd-jd}rs^{a-(lj+mk)d})^2 &= 1, \\ (rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd})^2 &= 1, \\ (rs^{2a+(lj-mk)d+kd-jd}rs^{a-(lj-mk)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj-mk)d}rs^{a+(lj-mk)d+kd-jd})^2 &= 1.\end{aligned}$$

Thus, it holds for both m and $-m$ and, for all l and m,

$$\begin{aligned}(rs^{2a+(lj+mk)d+kd-jd}rs^{a-(lj+mk)d})^2 &= 1 \quad \text{and} \\ (rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd})^2 &= 1.\end{aligned}$$

□

Lemma 5.7 For all integers i,

$$\begin{aligned}(rs^{2a+id+kd-jd}rs^{a-id})^2 &= 1 \quad \text{and} \\ (rs^{2a-id}rs^{a+id+kd-jd})^2 &= 1.\end{aligned}$$

Proof. Since $(j, k) = 1$, there exists integers x and y such that $xj + yk = 1$. Thus, for any integer i, we have $ixj + iyk = i$. Setting $l = ix$ and $m = iy$,

we have

$$\begin{aligned}(rs^{2a+id+kd-jd}rs^{a-id})^2 &= (rs^{2a+ixjd+iykd+kd-jd}rs^{a-ixjd-iykd})^2 \\ &= (rs^{2a+(ixj+iyk)d+kd-jd}rs^{a-(ixj+iyk)d})^2 \\ &= (rs^{2a+(lj+mk)d+kd-jd}rs^{a-(lj+mk)d})^2 \\ &= 1\end{aligned}$$

and

$$\begin{aligned}(rs^{2a-id}rs^{a+id+kd-jd})^2 &= (rs^{2a-ixjd-iykd}rs^{a+ixjd+iykd+kd-jd})^2 \\ &= (rs^{2a-(ixj+iyk)d}rs^{a+(ixj+iyk)d+kd-jd})^2 \\ &= (rs^{2a-(lj+mk)d}rs^{a+(lj+mk)d+kd-jd})^2 \\ &= 1.\end{aligned}$$

Hence, for all integers i,

$$\begin{aligned}(rs^{2a+id+kd-jd}rs^{a-id})^2 &= 1 \quad \text{and} \\ (rs^{2a-id}rs^{a+id+kd-jd})^2 &= 1.\end{aligned}$$

□

As well as new lemmas, we also require some results from former works, which we shall state without proof.

Lemma 5.8 (Campbell, Coxeter and Robertson [3, Lemma 2.1])

$$\begin{aligned}F^{a,b,c} &= F^{b,c,a} = F^{c,a,b} \\ &= F^{-c,-b,-a} = F^{-b,-a,-c} = F^{-a,-c,-b} \\ &\cong F^{a,c,b} = F^{c,b,a} = F^{b,a,c} \\ &= F^{-b,-c,-a} = F^{-c,-a,-b} = F^{-a,-b,-c}\end{aligned}$$

From this, it can be seen that one need only consider cases where $n \geq 0$ and $a \geq b \geq c$. We also require two additional theorems, one from Campbell, Coxeter and Robertson's paper of 1977, and another from a paper by Campbell and Robertson of 1981.

Theorem 5.9 (Campbell, Coxeter and Robertson [3, Theorem 3.5]) If $(a, b, c) = 1$ and $n \neq 0$, then $H^{a,b,c}$ is a finite metabelian group if, and only if, a, b and c are not equivalent modulo 6.

Theorem 5.10 (Campbell and Robertson [6, Theorem 3.3]) Where $(a, b, c) = 1$, if $a \equiv b \equiv c \pmod 6$, then $H^{a,b,c}$ is infinite. Otherwise, $H^{a,b,c}$ is finite and the Schur multiplicator is

$$\begin{array}{cl} 1 & \text{if } (a-b, b-c, 3) = 1 \\ C_2 & \text{if } (a-b, b-c, 3) = 3. \end{array}$$

Having outlined all the necessary lemmas and equations, we are in a position to restate the conjecture and form our proof. However, we will begin with an additional result obtained from our lemmas for those groups $F^{a,b,c}$ where $(a, b, c) \neq 1$.

Theorem 5.11 Suppose $(a, b, c) \neq 1$ with $n = a + b + c \neq 0$, then

$$F^{a,b,c} \cong H^{a,b,c} \quad \text{for } d \leq 5.$$

Proof. According to the $F^{a,b,c}$ conjecture, we must have $(a, b, c) = 1$ to ensure proper results. Using the notation $F^{a-jd,a,a+kd}$ with $(j, k) = 1$, we have $s^{2n} = s^{6a+2kd-2jd}$. Consider $d \in \{1, 2, 3, 4, 5\}$, where $(a-jd, a, a+kd) = t \neq 1$.

$$\begin{aligned} t &= (a - jd, a, a + kd) \\ &= (jd, a, kd) \\ &= (a, (jd, kd)) \\ &= (a, d(j, k)) \\ &= (a, d) \quad \text{as } (j, k) = 1 \end{aligned}$$

Thus, t divides d and $u = (t, d) = t$. Obviously where $d = 1$, we cannot have a $t \neq 1$ that divides d. So, for $d \in \{2, 3, 4, 5\}$ with $t \neq 1$, then $(a, d) \neq 1$ and either of two cases

1. a is a multiple of d or
2. $d = 4$ and a is a multiple of 2.

If a is a multiple of d, then all of $a - jd$, a and $a + kd$ are divisable by d and, as such, are not co-prime. If we consider $F^{a-jd,a,a+kd}$ where $a = md$ for some integer m, then using $i = m$ in $(rs^{2a+id+kd-jd}rs^{a-id})^2 = 1$, our result from Lemma 5.7 gives

$$\begin{aligned} 1 &= (rs^{2a+md+kd-jd}rs^{a-md})^2 \\ &= (rs^{2a+a+kd-jd}rs^{a-a})^2 \\ &= (rs^{3a+kd-jd}r)^2 \\ &= rs^{6a+2kd-2jd}r, \end{aligned}$$

and so, $s^{2n} = s^{6a+2kd-2jd} = 1$.

We find that where a is a multiple of d, $F^{a-jd,a,a+kd} \cong H^{a-jd,a,a+kd}$.

We just need to look at the case where $d = 4$ and $a = 2m$ for some odd integer m. Using $i = m$ in $(rs^{2a-4i}rs^{a+4i+4k-4j})^2 = 1$ gives

$$\begin{aligned} 1 &= (rs^{2a-4m}rs^{a+4m+4k-4j})^2 \\ &= (rs^{2a-2a}rs^{a+2a+4k-4j})^2 \\ &= (s^{3a+4k-4j})^2 \\ &= s^{6a+8k-8j}, \end{aligned}$$

and $s^{2n} = s^{6a+8k-8j} = 1$. Hence, $F^{a-4j,a,a+4k} \cong H^{a-4j,a,a+4k}$ where $a = 2m$ for m odd.

Thus, where $d \in \{2, 3, 4, 5\}$ and $(a - jd, a, a + kd) \neq 1$, we find that

$$F^{a-jd,a,a+kd} \cong H^{a-d,a,a+kd}.$$

□

We move on to stating our proof for the $F^{a,b,c}$ conjecture.

The $F^{a,b,c}$ Conjecture: (Campbell, Coxeter and Robertson [3, §12]) Suppose $(a, b, c) = 1$ with $n = a + b + c \neq 0$, and let

$$\theta : F^{a,b,c} \to H^{a,b,c}$$

be the natural homomorphism. Setting $N = ker\theta$ and $d = (a-b, b-c)$, then

- $N = 1$ if $d = 1$,
- $N = 1$ if $d = 2$,
- $N \cong C_2$ if $d = 3$,
- $N \cong Q_8$ if $d = 4$, and
- $N \cong SL(2, 5)$ if $d = 5$.

Proof. For the group $F^{a,b,c}$, we will use the equivalent form, $F^{a-jd,a,a+kd}$ for $j, k \in \mathbb{Z}$ with $(j, k) = 1$.

- From Lemma 5.8, we know, for $F^{a-jd,a,a+kd}$, we can assume without loss of generality that

  $$a - jd \leq a \leq a + kd,$$

  and thus, d, j and k must all have the same sign. If they are all negative, setting

  $$d' = -d, j' = -j \text{ and } k' = -k$$

  gives

  $$a - jd = a - j'd' \text{ and } a + kd = a + k'd'.$$

  As such, $F^{a-jd,a,a+kd} = F^{a-j'd',a,a+k'd'}$ where $d', j', k' \geq 0$, and so, we can assume

  $$d \geq 0, j \geq 0 \text{ and } k \geq 0.$$

- A proof of the case $d = 1$ as well as an alternate proof were given by Campbell and Robertson in [5] and [6]. For completeness, we provide another for this case using our discovered characteristics of the groups $F^{a,b,c}$.

  When $d = 1$, the groups have the form

$$F^{a-j,a,a+k} = \langle r, s | r^2, rs^{a-j}rs^a rs^{a+k} \rangle,$$

  for integers $j \geq 0$ and $k \geq 0$ where $(j, k) = 1$, with

$$\begin{aligned} n &= a - j + a + a + k \\ &= 3a + k - j. \end{aligned}$$

  If we can show that $s^{2n} = s^{6a+2k-2j} = 1$ in $F^{a-j,a,a+k}$, then we have proved

$$F^{a-j,a,a+k} \cong H^{a-j,a,a+k} = \langle r, s | r^2, s^{6a+2k-2j}, rs^{a-j}rs^a rs^{a+k} \rangle.$$

  From Lemma 5.7, for all integers i, we have

$$(rs^{2a+i+k-j}rs^{a-i})^2 = 1 \text{ and } (rs^{2a-i}rs^{a+i+k-j})^2 = 1,$$

  and using $i = a$ in the first equation, we obtain

$$\begin{aligned} 1 &= (rs^{2a+a+k-j}rs^{a-a})^2 \\ &= (rs^{3a+k-j}rs^0)^2 \\ &= (s^{3a+k-j})^2 \\ &= s^{6a+2k-2j} \\ &= s^{2n}. \end{aligned}$$

  Thus, $F^{a-j,a,a+k} \cong H^{a-j,a,a+k}$.

- The proof for $d = 2$ follows similarly to our proof of $d = 1$. Here, for

$j \geq 0$ and $k \geq 0$,

$$F^{a-2j,a,a+2k} = \langle r, s | r^2, rs^{a-2j}rs^a rs^{a+2k} \rangle,$$

where $(j,k) = 1$, with

$$\begin{aligned} n &= a - 2j + a + a + 2k \\ &= 3a + 2k - 2j \quad \text{and} \\ d &= ((a-2j) - a, a - (a+2k)) = 2. \end{aligned}$$

If we can show that $s^{2n} = s^{6a+4k-4j} = 1$ in $F^{a-2j,a,a+2k}$, then we will have proved

$$F^{a-2j,a,a+2k} \cong H^{a-2j,a,a+2k} = \langle r, s | r^2, s^{6a+4k-4j}, rs^{a-2j}rs^a rs^{a+2k} \rangle.$$

From Lemma 5.7, we obtain

$$(rs^{2a+2i+2k-2j}rs^{a-2i})^2 = 1 \text{ and } (rs^{2a-2i}rs^{a+2i+2k-2j})^2 = 1$$

for all integers i. Substituting $i = a$ into the second equation, we have

$$\begin{aligned} 1 &= (rs^{2a-2a}rs^{a+2a+2k-2j})^2 \\ &= (rs^0 rs^{3a+2k-2j})^2 \\ &= (s^{3a+2k-2j})^2 \\ &= s^{6a+4k-4j} \\ &= s^{2n}. \end{aligned}$$

Thus, $F^{a-2j,a,a+2k} \cong H^{a-2j,a,a+2k}$.

- Assume $d = 3$. Then, for $j \geq 0$ and $k \geq 0$ with $(j,k) = 1$, the groups have the form

$$F^{a-3j,a,a+3k} = \langle r, s | r^2, rs^{a-3j}rs^a rs^{a+3k} \rangle,$$

and we have

$$\begin{aligned} n &= a-3j+a+a+3k \\ &= 3a+3k-3j \quad \text{and} \\ d &= ((a-3j)-a, a-(a+3k)) = 3. \end{aligned}$$

To show,

$$F^{a-3j,a,a+3k}/C_2 \cong H^{a-3j,a,a+3k} = \langle r, s | r^2, s^{6a+6k-6j}, rs^{a-3j}rs^{a}rs^{a+3k} \rangle,$$

we are required to prove

$$s^{2n} = s^{6a+6k-6j} = s^{-6a-6k+6j} \quad \text{or} \quad s^{12a+12k-12j} = 1.$$

Lemma 5.7 with $d = 3$ gives us

$$(rs^{2a+3i+3k-3j}rs^{a-3i})^2 = 1 \quad \text{and} \quad (rs^{2a-3i}rs^{a+3i+3k-3j})^2 = 1$$

for all integers i. By substituting $i = a$, the second equation becomes

$$\begin{aligned} 1 &= (rs^{a+3a+3k-3j}rs^{2a-3a})^2 \\ &= s^{4a+3k-3j}rs^{-a}rs^{4a+3k-3j}rs^{-a}r \\ &= s^{4a+3k-3j}(s^{a+3k}rs^{a-3j})s^{4a+3k-3j}(s^{a+3k}rs^{a-3j}) \\ &= s^{5a+6k-3j}rs^{6a+6k-6j}rs^{a-3j} \\ &= s^{6a+6k-6j}rs^{6a+6k-6j}r. \end{aligned}$$

Thus, $rs^{6a+6k-6j}r = s^{-6a-6k+6j}$ and $s^{6a+6k-6j} = rs^{-6a-6k+6j}r$.

Using $rs^{6a+6k-6j}r = s^{-6a-6k+6j}$ with $rs^{a-3j}rs^{a}rs^{a+3k}$, an original relator, we find

$$\begin{aligned}
s^{-6a-6k+6j} &= (rs^{a-3j}rs^{a}rs^{a+3k})(s^{-6a-6k+6j}) \\
&= rs^{a-3j}rs^{a}.rs^{-6a-6k+6j}.s^{a+3k} \\
&= rs^{a-3j}rs^{7a+6k-6j}rs^{a+3k} \\
&= rs^{a-3j}.rs^{6a+6k-6j}.s^{a}rs^{a+3k} \\
&= rs^{-5a-6k+3j}rs^{a}rs^{a+3k} \\
&= rs^{-6a-6k+6j}.s^{a-3j}rs^{a}rs^{a+3k} \\
&= s^{6a+6k-6j}rs^{a-3j}rs^{a}rs^{a+3k} \\
&= s^{6a+6k-6j}.
\end{aligned}$$

Thus, $s^{-6a-6k+6j} = s^{6a+6k-6j}$, $s^{6a+6k-6j}$ is central and $s^{12a+12k-12j} = 1$, as required.

Consider $\langle x \rangle$ where $x = s^{6a+6k-6j}$. Obviously it is a subgroup of the kernel of the homomorphism from F to H and, since

$$rxr = rs^{6a+6k-6j}r = s^{6a+6k-6j} = x \quad \text{and} \quad s^{-1}xs = x,$$

then $\langle x \rangle$ is the kernel. We know from Theoreom 5.11 that if 3 divides a, then $F^{a-3j,a,a+3k} \cong H^{a-3j,a,a+3k}$.

We have shown that $s^{4n} = s^{12a+12k-12j} = 1$ and $s^{6a+6k-6j}$ generates the kernel of the homomorphism. Thus, either $F^{a-3j,a,a+3k} \cong H^{a-3j,a,a+3k}$ or $F^{a-3j,a,a+3k}/C_2 \cong H^{a-3j,a,a+3k}$. Since $(j,k) = 1$, then it cannot be that $a - 3j \equiv a \equiv a + 3k \pmod 6$. Also,

$$(a - 3j - a, a - (a + 3k), 3) = (-3j, 3k, 3) = 3,$$

so, by Theorem 5.10, $H^{a-3j,a,a+3k}$ is finite and has Schur multiplicator C_2.

We now know $F^{a-3j,a,a+3k}$ is finite and as $F^{a-3j,a,a+3k}$ has a 2-generator, 2-relator presentation, it has deficiency 0 and, by Corollory 1.2 of [31], a trivial multiplicator. Thus, $F^{a-3j,a,a+3k} \not\cong H^{a-3j,a,a+3k}$, and it must be such that, when a is not a multiple of 3,

$$F^{a-3j,a,a+3k}/C_2 \cong H^{a-3j,a,a+3k}.$$

- The case $d = 4$ requires a bit more work than the first 3 cases, as we need to show the kernel is isomorphic to the group Q_8. With $d = 4$, the groups take the form

$$F^{a-4j,a,a+4k} = \langle r, s | r^2, rs^{a-4j}rs^a rs^{a+4k} \rangle,$$

where $j \geq 0$, $k \geq 0$ and $(j,k) = 1$, and we have

$$\begin{aligned} n &= a - 4j + a + a + 4k \\ &= 3a + 4k - 4j \quad \text{and} \\ d &= ((a - 4j) - a, a - (a + 4k)) = 4. \end{aligned}$$

We want to show that $rs^{-6a-8k+8j}rs^{6a+8k-8j}rs^{6a+8k-8j}r = s^{-6a-8k+8j}$, $s^{24a+32k-32j} = 1$ and $s^{12a+16k-16j}$ is central in $F^{a-4j,a,a+4k}$. Given this, if we show the kernel of the natural homomorphism from F to H is generated by $s^{6a+8k-8j}$ and $rs^{6a+8k-8j}r$, we would then have enough to prove that the kernel is, in fact, isomorphic to Q_8.

From Lemma 5.1 with $d = 4$, we find that $rs^{6a+8k-8j}r \sim s^4$. Also, the results obtained from Lemma 5.7 with $d = 4$ become

$$(rs^{2a+4i+4k-4j}rs^{a-4i})^2 = 1 \quad \text{and} \quad (rs^{2a-4i}rs^{a+4i+4k-4j})^2 = 1$$

for all integers i. Setting $i = a$ in the second equation and $i = 0$ in the first results in

$$\begin{aligned} rs^{-2a}rs^{5a+4k-4j}rs^{-2a}rs^{5a+4k-4j} &= 1 \quad \text{and} \\ rs^{2a+4k-4j}rs^a rs^{2a+4k-4j}rs^a &= 1. \end{aligned}$$

So, as $rs^{2a}r = s^{4j}rs^{2a+4k-4j}rs^{-4k}$ from 5.17, then

$$\begin{aligned}
1 &= rs^{-2a}rs^{5a+4k-4j}rs^{-2a}rs^{5a+4k-4j} \\
&= (s^{4k}rs^{-2a-4k+4j}rs^{-4j})s^{5a+4k-4j}(s^{4k}rs^{-2a-4k+4j}rs^{-4j})s^{5a+4k-4j} \\
&= s^{4k}rs^{-2a-4k+4j}rs^{5a+8k-8j}rs^{-2a-4k+4j}rs^{5a+4k-8j} \\
&= rs^{-2a-4k+4j}rs^{5a+8k-8j}rs^{-2a-4k+4j}rs^{5a+8k-8j} \\
&= rs^{-2a-4k+4j}rs^{5a+8k-8j}(s^{a}rs^{2a+4k-4j}rs^{a})s^{5a+8k-8j} \\
&= rs^{-2a-4k+4j}rs^{6a+8k-8j}rs^{2a+4k-4j}rs^{6a+8k-8j}.
\end{aligned}$$

It must be the case that a is odd, as we would have $(a-4j, a, a+4k) \neq 1$ otherwise. We also know that $rs^{6a+8k-8j}r \sim s^4$ so, given that 4 cannot divide $2a$, we have

$$rs^{6a+8k-8j}r \sim s^{2a+4k-4j+2}.$$

Thus,

$$\begin{aligned}
1 &= rs^{-2a-4k+4j}rs^{6a+8k-8j}rs^{2a+4k-4j}rs^{6a+8k-8j} \\
&= rs^{2}rs^{6a+8k-8j}rs^{-2}rs^{6a+8k-8j}
\end{aligned}$$

and $s^{-2}rs^{6a+8k-8j}rs^{2} = rs^{-6a-8k+8j}r$.

Again, using that fact that a must be odd, we find that $6a+8k-8j$ is not a multiple of 4. Therefore,

$$\begin{aligned}
s^{-6a-8k+8j}rs^{6a+8k-8j}rs^{6a+8k-8j} &= rs^{-6a-8k+8j}r \quad \text{and} \\
s^{6a+8k-8j}rs^{6a+8k-8j}rs^{-6a-8k+8j} &= rs^{-6a-8k+8j}r.
\end{aligned}$$

From these, we additionally obtain

$$\begin{aligned}
s^{6a+8k-8j}rs^{6a+8k-8j} &= rs^{6a+8k-8j}rs^{-6a-8k+8j}r \quad \text{and} \\
s^{6a+8k-8j}rs^{6a+8k-8j} &= rs^{-6a-8k+8j}rs^{6a+8k-8j}r
\end{aligned}$$

and hence,

$$\begin{aligned} rs^{6a+8k-8j}rs^{-6a-8k+8j}r &= rs^{-6a-8k+8j}rs^{6a+8k-8j}r \\ s^{12a+16k-16j} &= rs^{12a+16k-16j}r. \end{aligned}$$

Thus, $s^{12a+16k-16j}$ is central.

Also,

$$\begin{aligned} rs^{6a+8k-8j}rs^{-6a-8k+8j}r &= (rs^{6a+8k-8j}rs^{-6a-8k+8j}r)^{-1} \\ s^{6a+8k-8j}rs^{6a+8k-8j} &= s^{-6a-8k+8j}rs^{-6a-8k+8j} \\ s^{12a+16k-16j} &= rs^{-12a-16k+16j}r. \end{aligned}$$

Thus, $s^{12a+16k-16j} = s^{-12a-16k+16j}$ and $s^{24a+32k-32j} = 1$.

We have all of $rs^{-6a-8k+8j}rs^{6a+8k-8j}rs^{6a+8k-8j}r = s^{-6a-8k+8j}$, $s^{24a+32k-32j} = 1$ and $s^{12a+16k-16j}$ is central, and we need only check that $\{s^{6a+8k-8j}, rs^{6a+8k-8j}r\}$ generates the kernel of the homomorphism from F to H. Let $x = s^{6a+8k-8j}$ and $y = rs^{6a+8k-8j}r$, and consider $\langle x, y\rangle$. Obviously, $\langle x, y\rangle$ is a subgroup of the kernel.

It is easily seen that $rxr = y$, $ryr = x$ and $s^{-1}xs = x$, and it is left to consider $s^{-1}ys$ to show $\langle x, y\rangle$ is the kernel.

Using $i = a + k - j$ in $(rs^{2a+4i+4k-4j}rs^{a-4i})^2 = 1$, we have

$$1 = rs^{6a+8k-8j}rs^{-3a-4k+4j}rs^{6a+8k-8j}rs^{-3a-4k+4j}$$

so,

$$s^a rs^{6a+8k-8j}rs^{-a} = s^{4a+4k-4j}rs^{-6a-8k+8j}rs^{2a+4k-4j}.$$

We also know $rs^{6a+8k-8j}r \sim s^4$, so

$$\begin{aligned} s^a rs^{6a+8k-8j}rs^{-a} &= s^{4a+4k-4j}rs^{-6a-8k+8j}rs^{2a+4k-4j} \\ &= rs^{-6a-8k+8j}rs^{6a+8k-8j}. \end{aligned}$$

There are two cases, as a must be an odd integer.

1. $a \equiv 1 \pmod 4$
   Here, $a+1 \equiv 2 \pmod 4$.
   Thus,

$$\begin{aligned} rs^{6a+8k-8j}r &= s^{a+1}rs^{-6a-8k+8j}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a+8k-8j}rs &= s^{a}rs^{-6a-8k+8j}rs^{-a}. \end{aligned}$$

   Given this, we find

$$\begin{aligned} s^{-1}rs^{6a+8k-8j}rs &= s^{a}rs^{-6a-8k+8j}rs^{-a} \\ &= rs^{-6a-8k+8j}rs^{6a+8k-8j} \\ &= y^{-1}x. \end{aligned}$$

2. $a \equiv 3 \pmod 4$
   Now, $a+1 \equiv 0 \pmod 4$.
   Thus,

$$\begin{aligned} rs^{6a+8k-8j}r &= s^{a+1}rs^{6a+8k-8j}rs^{-a-1} \quad \text{and} \\ s^{-1}rs^{6a+8k-8j}rs &= s^{a}rs^{6a+8k-8j}rs^{-a}, \end{aligned}$$

   and so,

$$\begin{aligned} s^{-1}rs^{6a+8k-8j}rs &= s^{a}rs^{6a+8k-8j}rs^{-a} \\ &= s^{-6a-8k+8j}rs^{6a+8k-8j}r \\ &= x^{-1}y. \end{aligned}$$

Hence, $\{x, y\}$ generates the kernel. Also, x and y both have order 4, $y^{-1}xy = x^{-1}$ and $x^2 = y^2$ since $s^{12a+16k-16j}$ is central. So, $\langle x, y\rangle$ is a homomorphic image of Q_8, which has derived length 2, and it is left to show $\langle x, y\rangle \cong Q_8$.

Consider the group

$$G^{a,b,c} = \langle r, s | r^2, s^8, rs^a rs^b rs^c\rangle,$$

a homomorphic image of $F^{a,b,c}$. Here, $G^{a,b,c} \cong G^{a',b',c'}$, where a', b' and c' are a, b and c modulo 8. Using $F^{a-4j,a,a+4k}$ for $(j,k) = 1$, then a is odd and $a' \in \{1, 3, 5, 7\}$. Thus, we are left with only 12 cases for $G^{a-8,a,a+4k}$. When j is even, then k is odd and we have $G^{1,1,5}$, $G^{3,3,7}$, $G^{5,5,1}$ and $G^{7,7,3}$. Where k is even, j must be odd and we have the cases, $G^{5,1,1}$, $G^{7,3,3}$, $G^{1,5,5}$ and $G^{3,7,7}$. Where both j and k are odd, we are left with the final four cases, $G^{5,1,5}$, $G^{7,3,7}$, $G^{1,5,1}$ and $G^{3,7,3}$. Using GAP, we find that each of these groups has derived length 4 and so, $F^{a-4j,a,a+4k}$ must have derived length of at least 4.

By Theorem 5.9, the groups $H^{a,b,c}$ are finite metabelian when $(a, b, c) = 1$, $n \neq 0$ and $(d, 6) \neq 6$. As a is odd and $d = 4$, then $H^{a-4j,a,a+4k}$ is finite metabelian and, therefore, has derived length 2. This implies that $\langle x, y\rangle$, the kernel of the natural homomorphism from $F^{a-4j,a,a+4k}$ to $H^{a-4j,a,a+4k}$, must have derived length at least 2. Thus, $\langle x, y\rangle \cong Q_8$.

- The proof of the case $d = 5$ was given by Havas and Robertson [21], and is found in Appendix B. Their proof of $d = 5$ could not be extended for $d = 2$, $d = 3$ or $d = 4$ as it requires that $(d, 2n) = 1$, a statement true only when $d = 1$ or $d = 5$. From our results, we were unable to obtain a proof for this last case using similar techniques to our proofs of the other cases.

□

Appendix A

Corrected Proof of Lemma 3.3

In Campbell, Coxeter and Robertson's paper of 1977 [3], which first outlined the $F^{a,b,c}$ conjecture, a proof was given for a lemma regarding the derived group $K^{a,b,c}$ of $H^{a,b,c}$, a homomorphic image of $F^{a,b,c}$. The lemma was then used to completely determine the order and structure of the groups $H^{a,b,c}$, which, should the $F^{a,b,c}$ conjecture be proved true, would then determine the groups $F^{a,b,c}$.

The proof of this lemma has since been found invalid, and we begin by stating the lemma and outlining the problem with the original proof. A corrected proof, based on the proof of Theorem 3.3 from Campbell and Robertson's paper of the following year [4], follows.

A.1 Lemma 3.3 and the Original Proof

The subgroup $K^{a,b,c}$ of $H^{a,b,c}$ is defined as being generated by the set

$$\{x_i | x_i = s^{i-1} r s^{n-i+1}, i \in \{1, 2, \ldots, n\}, n = a + b + c\}.$$

Lemma 3.1 of [3] had shown that $K^{a,b,c}$ was the derived group of $H^{a,b,c}$, while Lemma 3.2 gave a presentation for $K^{a,b,c}$. For simplicity, we use the notation

$x_i^{\epsilon_i}$, where for $i \equiv j_1 \pmod{n}$ and $i \equiv j_2 \pmod{2n}$,

$$x_i = \begin{cases} x_n & \text{if } j_1 = 0; \\ x_{j_1} & \text{if } j_1 \neq 0. \end{cases} \quad \text{and} \quad \epsilon_i = \begin{cases} 1 & \text{if } 1 \leq j_2 \leq n; \\ -1 & \text{if } n+1 \leq j_2 \leq 2n-1 \text{ or } j_2 = 0. \end{cases}$$

The presentation for $K^{a,b,c}$ is then given as

$$K^{a,b,c} = \langle x_1, x_2, \ldots, x_n | x_{i+a}^{\epsilon_{i+a}} = x_i^{\epsilon_i} x_{i+a+b}^{\epsilon_{i+a+b}}, 1 \leq i \leq n \rangle.$$

Lemma 3.3 states that $K^{a,b,c}$ is abelian if $(a, b, c) = 1$.

The original proof begins by showing that for any x_i, we have both $x_i \sim x_{i+a}$ and $x_i \sim x_{i+b}$. An inductive proof is then attempted to show that $x_i \sim x_{i+sa+tb}$ for integers $s, t \geq 0$. As a, b and c are co-prime, then any integer j can be written as

$$\begin{aligned} j &= j(\alpha a + \beta b + \gamma c) \\ &= j(\alpha - \gamma)a + j(\beta - \gamma)b + j\gamma(a + b + c) \end{aligned}$$

for some integers α, β and γ, and therefore, $j \equiv j(\alpha - \gamma)a + j(\beta - \gamma)b \pmod{n}$. With the result of the inductive proof, using $s = j(\alpha - \gamma)$ and $t = j(\beta - \gamma)$, then we have

$$x_i \sim x_{i+sa+tb} = x_{i+j},$$

and thus, $K^{a,b,c}$ is abelian.

The problem, however, lies within the inductive proof. In the inductive hypothesis, it was assumed that $x_i \sim x_{i+sa+tb}$ holds for $0 \leq s + t \leq k$, and the relation

$$x_{i+sa+tb}^{\epsilon_{i+sa+tb}} = x_{i+sa+(t-1)b}^{\epsilon_{i+sa+(t-1)b}} x_{i+(s-1)a+(t-1)b}^{-\epsilon_{i+(s-1)a+(t-1)b}}$$

was then used to show it held for the sum, $s + t = k + 1$. This step, however, did not take into account the cases where either s or t was 0. For example, consider $t = 0$. Then, $s = k + 1$, and the proof would require the relation

$$x_{i+sa}^{\epsilon_{i+sa}} = x_{i+sa+(-1)b}^{\epsilon_{i+sa+(-1)b}} x_{i+(s-1)a+(-1)b}^{-\epsilon_{i+(s-1)a+(-1)b}}.$$

However, as the induction stipulated both $s \geq 0$ and $t \geq 0$, then it cannot be assumed that either

$$x_i \sim x_{i+sa+(-1)b}^{\epsilon_{i+sa+(-1)b}} \quad \text{or} \quad x_i \sim x_{i+(s-1)a+(-1)b}^{\epsilon_{i+(s-1)a+(-1)b}},$$

and the inductive step does not work.

Although the proof of this lemma is incorrect, the actual lemma is true, and the results based on it still hold. A revision of the proof is now given.

A.2 The Corrected Proof

This version of the proof for Lemma 3.3 in [3] is based on the proof of Theorem 3.3 of [4]. We shall first state three lemmas necessary in our revised proof.

Lemma A.1 In the group $K^{a,b,c}$, if, for the integer j and all integers i, we have $x_i \sim x_{i+j}$, then $x_i \sim x_{i-j}$.

Proof. Since $x_i \sim x_{i+j}$ holds for all integers i taking the subscripts modulo n, then it must hold for $i-j$ and thus, $x_{i-j} \sim x_{i-j+j} = x_i$. □

Lemma A.2 If, for the integers s and t, we have $x_i \sim x_{i+sa+tb}$ for all integers i, then $x_i \sim x_{i-ta-sb}$ in the group $K^{a,b,c}$.

Proof. We have each of the relations

$$\begin{aligned}
x_{i+sa+tb}^{\epsilon_{i+sa+tb}} &= x_{i+sa+(t-1)b}^{\epsilon_{i+sa+(t-1)b}} x_{i+(s-1)a+(t-1)b}^{-\epsilon_{i+(s-1)a+(t-1)b}} \\
x_{i+sa+tb}^{\epsilon_{i+sa+tb}} &= x_{i+(s+1)a+(t+1)b}^{-\epsilon_{i+(s+1)a+(t+1)b}} x_{i+(s+1)a+tb}^{\epsilon_{i+(s+1)a+tb}} \\
x_{i+sa+tb}^{\epsilon_{i+sa+tb}} &= x_{i+sa+(t+1)b}^{\epsilon_{i+sa+(t+1)b}} x_{i+(s-1)a+tb}^{\epsilon_{i+(s-1)a+tb}}
\end{aligned}$$

By their symmetry, if we have $x_i \sim x_{i+sa+tb}$, then $x_i \sim x_{i-ta-sb}$. □

Lemma A.3 If, for the integers s and t, we have $x_i \sim x_{i+sa+tb}$ for all integers i, then $x_i \sim x_{i+ta+sb}$ in the group $K^{a,b,c}$.

Proof. If $x_i \sim x_{i+sa+tb}$, then by Lemma A.2, $x_i \sim x_{i-ta-sb}$, and from Lemma A.1, then $x_i \sim x_{i+ta+sb}$. $\square$

Theorem A.4 (Campbell and Robertson [3, Lemma 3.3])

$$K^{a,b,c} = \langle x_1, x_2, \ldots, x_n | x_{i+a}^{\epsilon_{i+a}} = x_i^{\epsilon_i} x_{i+a+b}^{\epsilon_{i+a+b}}, 1 \leq i \leq n \rangle$$

is abelian if $(a, b, c) = 1$.

Proof. We start by showing $x_i \sim x_{i+a}$ and $x_i \sim x_{i+b}$ for an integer i. A relation of the presentation is

$$x_{i+a}^{\epsilon_{i+a}} = x_i^{\epsilon_i} x_{i+a+b}^{\epsilon_{i+a+b}}, \quad \text{so} \quad x_{i+a+b}^{\epsilon_{i+a+b}} = x_i^{-\epsilon_i} x_{i+a}^{\epsilon_{i+a}}.$$

We also have

$$x_{i+n+a}^{\epsilon_{i+n+a}} = x_{i+n}^{\epsilon_{i+n}} x_{i+n+a+b}^{\epsilon_{i+n+a+b}},$$

which can also be written as

$$\begin{aligned} x_{i+a}^{-\epsilon_{i+a}} &= x_i^{-\epsilon_i} x_{i+a+b}^{-\epsilon_{i+a+b}} \\ x_{i+a+b}^{\epsilon_{i+a+b}} &= x_{i+a}^{\epsilon_{i+a}} x_i^{-\epsilon_i}. \end{aligned}$$

Thus,

$$x_i^{-\epsilon_i} x_{i+a}^{\epsilon_{i+a}} = x_{i+a}^{\epsilon_{i+a}} x_i^{-\epsilon_i}$$

and $x_i \sim x_{i+a}$.

A similar argument, using the relations,

$$x_i^{\epsilon_i} = x_{i-a}^{\epsilon_{i-a}} x_{i+b}^{\epsilon_{i+b}} \quad \text{and} \quad x_{i+n}^{\epsilon_{i+n}} = x_{i+n-a}^{\epsilon_{i+n-a}} x_{i+n+a+b}^{\epsilon_{i+n+a+b}},$$

shows that $x_i \sim x_{i+b}$.

Let T_i be the triple $(i, i+a, i+a+b)$ of subscripts modulo n of x for the relation

$$x_{i+a}^{\epsilon_{i+a}} = x_i^{\epsilon_i} x_{i+a+b}^{\epsilon_{i+a+b}}.$$

Now consider x_j for some j. If $x_j \sim x_u$ and $x_j \sim x_v$ for $u, v \in T_i$, and where the third element of the triple is w, then we can write x_w as a product of x_u and x_v, and $x_j \sim x_w$ as well.

Now, let A be the set $\{j | x_i \sim x_{i+j} \text{ for all } 1 \leq i \leq n\}$. Since we have shown $x_i \sim x_{i+a}$ and $x_i \sim x_{i+b}$, then both $a \in A$ and $b \in A$. Obviously, $x_i \sim x_i$, and we have $x_i \sim x_{i+a}$, so by our earlier remark and from triple $T_i = (i, i+a, i+a+b)$, then $a+b \in A$. To show all the elements of $K^{a,b,c}$ commute with one another and the group is abelian, we need to show all of $1, 2, \ldots, n \in A$.

Using the argument of the original proof, since $(a, b, c) = 1$, there exist integers α, β and γ such that any integer j can be written as

$$\begin{aligned} j &= j(\alpha a + \beta b + \gamma c) \\ &= j(\alpha - \gamma)a + j(\beta - \gamma)b + j\gamma(a + b + c) \end{aligned}$$

so, $j \equiv j(\alpha - \gamma)a + j(\beta - \gamma)b \pmod{n}$. It would suffice then to prove that $sa + tb \in A$ for all $s, t \in \mathbb{Z}$ since, for each $j = 1, 2, \ldots, n$, using $s = j(\alpha - \gamma)$ and $t = j(\beta - \gamma)$, then $j \in A$. Thus, $K^{a,b,c}$ would be shown to be abelian.

Our induction proof of $x_i \sim x_{i+sa+tb}$ for $s, t \in \mathbb{Z}$ is on k, the maximum of $|s|$ and $|t|$. For $k = 0$, both $s = 0$ and $t = 0$, and obviously, $x_i \sim x_i$. For the inductive hypothesis, assume the two elements commute for $max\{|s|, |t|\} \leq k$. Considering $max\{|s|, |t|\} = k + 1$, from Lemma A.3, we have only four cases:

(i) $t = k + 1$, $-k + 1 \leq s \leq k$

Here, $t - 1 = k$ and $-k \leq s - 1 \leq k - 1$, so by the inductive hypothesis,

$$x_i \sim x_{i+sa+(t-1)b} \quad \text{and} \quad x_i \sim x_{i+(s-1)a+(t-1)b},$$

and as

$$x_{i+sa+tb}^{\epsilon_{i+sa+tb}} = x_{i+sa+(t-1)b}^{\epsilon_{i+sa+(t-1)b}} x_{i+(s-1)a+(t-1)b}^{-\epsilon_{i+(s-1)a+(t-1)b}},$$

then $x_i \sim x_{i+sa+tb}$ and $sa + tb \in A$.

(ii) $t = k + 1, s = k + 1$

From case (i), we know the relationship holds for $t = k+1$ and $s = k$, and using Lemma A.3, we thus have shown it for the case $t = k$ and $s = k+1$. Our inductive hypothesis allows us to assume it is true for $t = k$ and $s = k$, so using

$$\begin{aligned} x_{i+sa+tb}^{\epsilon_{i+sa+tb}} &= x_{i+sa+(t-1)b}^{\epsilon_{i+sa+(t-1)b}} x_{i+(s-1)a+(t-1)b}^{-\epsilon_{i+(s-1)a+(t-1)b}} \\ x_{i+(k+1)a+(k+1)b}^{\epsilon_{i+(k+1)a+(k+1)b}} &= x_{i+(k+1)a+kb}^{\epsilon_{i+(k+1)a+kb}} x_{i+ka+kb}^{-\epsilon_{i+ka+kb}}, \end{aligned}$$

the fact that x_i commutes with both terms on the right hand side shows $x_i \sim x_{i+sa+tb}$ and $sa + tb \in A$.

(iii) $t = k+1, s = -k$

From case (i) and Lemma A.3, we have $x_i \sim x_{i+(k+1)a+(-k+1)b}$, and from the hypothesis, we know $x_i \sim x_{i+ka-kb}$. Thus, using the relation

$$x_{i+(k+1)a-kb}^{\epsilon_{i+(k+1)a-kb}} = x_{i+(k+1)a+(-k+1)b}^{\epsilon_{i+(k+1)a+(-k+1)b}} x_{i+ka-kb}^{\epsilon_{i+ka-kb}},$$

then $x_i \sim x_{i+(k+1)a-kb}$. Again, using Lemma A.3, $x_i \sim x_{i+(-k)a+(k+1)b}$ and $sa + tb \in A$.

(iv) $t = k+1, s = -k-1$

From case (iii), we have $x_i \sim x_{i+(k+1)a+(-k)b}$, and using Lemma A.2, we obtain $x_i \sim x_{i+ka+(-k-1)b}$. As there exists the relation

$$x_{i+(k+1)a+(-k-1)b}^{\epsilon_{i+(k+1)a+(-k-1)b}} = x_{i+(k+1)a+(-k)b}^{\epsilon_{i+(k+1)a+(-k)b}} x_{i+ka+(-k-1)b}^{\epsilon_{i+ka+(-k-1)b}},$$

then $x_i \sim x_{i+(k+1)a+(-k-1)b}$. Also, by Lemma A.3, $x_i \sim x_{i+(-k-1)a+(k+1)b}$. Hence, $sa + tb \in A$.

So, by induction, $x_i \sim x_{i+sa+tb}$ and $sa + tb \in A$ for all integers s and t. Thus, $K^{a,b,c}$ is abelian. $\square$

Appendix B

Proof of the $F^{a,b,c}$ Conjecture for $d = 5$

Here, we give the proof of the case $d = 5$ of the $F^{a,b,c}$ conjecture as it is the only case we have not been able to prove using our results. This proof was given by G. Havas and E. F. Robertson in a 2005 paper [21].

B.1 G. Havas and E. F. Robertson's proof

B.1.1 Introduction

Coxeter defined the groups $F^{a,b,c}$ by

$$F^{a,b,c} = \langle r, s | r^2, rs^a rs^b rs^c \rangle.$$

These arose because some of the groups have Cayley graphs which are '0-symmetric' or 'faithful'. Campbell, Coxeter and Robertson investigated the groups $F^{a,b,c}$ in [3] and, after determining the structure of various subclasses, made 'the $F^{a,b,c}$ conjecture' which we state after some preliminaries.

Define $n = a + b + c$ and $d = (a - b, b - c)$. The structure of the groups

$$H^{a,b,c} = \langle r, s | r^2, s^{2n}, rs^a rs^b rs^c \rangle$$

is completely determined in Section 3 of [3]. Provided $(a, b, c) = 1$, $n \neq 0$

and $(d, 6) \neq 6$, the groups $H^{a,b,c}$ are finite metabelian groups. If $d \geq 6$ the groups $F^{a,b,c}$ are infinite.

The $F^{a,b,c}$ conjecture is as follows. Suppose $(a, b, c) = 1$ and let

$$\theta : F^{a,b,c} \to H^{a,b,c}$$

be the natural homomorphism. Let $N = ker\theta$. Then

$N = 1$ if $d = 1$,

$N = 1$ if $d = 2$,

$N \cong C_2$ if $d = 3$,

$N \cong Q_8$ if $d = 4$,

$N \cong SL(2, 5)$ if $d = 5$.

Here we present a proof that the conjecture holds when $d = 5$. The proof was suggested by studying small cases using the ACE enumerator [15], as available in GAP [16]. The proof of the conjecture in the cases $d = 2, 3$ and 4 is quite different in nature from that presented in this paper since in these cases $(d, 6) \neq 1$.

B.1.2 Proof of the Conjecture when $d = 5$

In what follows we assume that $d = 5$ and $N = ker\theta$. First we indicate the strategy behind our proof by breaking the proof into a number of steps.

Step 1. s^{2n} commutes with rs^5r.

Step 2. s^{10n} is central in $F^{a,b,c}$.

Step 3. $e = s^{2n}$, $f = rs^{2n}r$ generate N.

Step 4. $e^5, f^5, (ef)^3$ and $(fe^2)^2$ are central in N.

Step 5. Put $M = \langle e^5, f^5, (ef)^3, (fe^2)^2 \rangle$. Then $N/M \cong A_5$.

Step 6. N is perfect.

Step 7. M is contained in the multiplier of A_5.

Step 8. $N \cong SL(2, 5)$.

We proceed to prove each of these steps in turn. We will use the notation $a \sim b$ to mean that a commutes with b.

Proof of Step 1. From $r^2 = 1$ and $rs^a rs^b rs^c = 1$ we have

$$(s^a rs^b)(s^{-c} rs^{-b}) = (rs^{-c} r)(rs^a r) = rs^{a-c} r.$$

Hence $s^a(rs^{b-c}r)s^{-b} = rs^{a-c}r$.

Similarly $s^b(rs^{c-a}r)s^{-c} = rs^{b-a}r$ and $s^c(rs^{a-b}r)s^{-a} = rs^{c-b}r$. From the first and third of these we have $s^{2a}(rs^{b-a}r)s^{-b-c} = rs^{a-c}r$, and using the second of the three relations

$$s^{2a+b}(rs^{c-a}r)s^{-b-2c} = rs^{a-c}r.$$

Hence

$$s^{2a+b}s^{b+2c}(rs^{a-c}r)s^{-2a-b}s^{-b-2c} = rs^{a-c}r$$

showing that $s^{2n} \sim rs^{a-c}r$. Similarly $s^{2n} \sim rs^{b-a}r$ so, since $5 = d = (a - c, b - a)$, $s^{2n} \sim rs^5 r$.

See also Lemma 1.1 of [7].

Proof of Step 2. Since $a \equiv b \equiv c \pmod 5$ we have $n \equiv 3a \pmod 5$ so $n \equiv 0 \pmod 5$ if and only if $5|(a, b, c)$ showing that n is coprime to 5. From (1), $s^{2n} \sim rs^5 r$ so $s^5 \sim rs^{2n}r$. Hence $s^{10n} \sim rs^5 r$ and $s^{10n} \sim rs^{2n}r$. Since $(5, 2n) = 1$, we have $s^{10n} \sim rsr$. We now see that $s^{10n} \sim rs^a r$, so $s^{10n} \sim s^{-c}rs^{-b}$, showing that $s^{10n} \sim r$ and so s^{10n} is central in $F^{a,b,c}$.

See also Theorem 2.6 of [7].

Proof of Step 3. To prove that $\langle e, f\rangle = N$ we need to show that $N = \langle e\rangle^F = \langle e, f\rangle$. Put $\widehat{N} = \langle e, f\rangle$. Then $rer = f \in \widehat{N}$ and $s^{-1}es = e \in \widehat{N}$. Also $rfr = e \in \widehat{N}$. It remains to consider $s^{-1}fs$.

Now $s^5 \sim rs^{2n}r$ so, if $a \equiv b \equiv c \equiv 1 \pmod 5$, $s^{2n-1} \sim rs^{2n}r$. Hence

$$s^{-1}rs^{2n}rs = s^{-2n}.rs^{2n}r.s^{2n} = e^{-1}fe.$$

Similarly if $a \equiv b \equiv c \equiv 2 \pmod 5$, $s^{-1}rs^{2n}rs = e^{-3}fe^3$, while $a \equiv b \equiv c \equiv 3 \pmod 5$ gives $s^{-1}rs^{2n}rs = e^{-2}fe^2$ and $a \equiv b \equiv c \equiv 4 \pmod 5$ gives $s^{-1}rs^{2n}rs = e^{-4}fe^4$.

Proof of Step 4. First we need a lemma.

Lemma B.1 (i) s^{2n} commutes with $rs^{2n}rs^{2n}r$.

(ii) s^{2n} commutes with $rs^{2n}rs^{4n}rs^{2n}r$.

Proof. (i) s^{2n} commutes with $rs^a rs^b r$ since it commutes with s^c. Since $a \equiv b \equiv c \pmod 5$ we see that

$$2n - a \equiv a + 2b + 2c \equiv 0 \pmod 5$$

so $s^{2n} \sim rs^{2n-a}r$.

Similarly $s^{2n} \sim rs^{2n-b}r$ so

$$s^{2n} \sim rs^{2n-a}r.rs^a rs^b r.rs^{2n-b}r = rs^{2n}rs^{2n}r.$$

(ii) $rs^{2n}rs^{4n}rs^{2n}r = (rs^{2n}rs^{2n}r)^2$.

We need to check that $e^5, f^5, (ef)^3$ and $(fe^2)^2$ are central in N. The first two are easy since $e^5 = s^{10n}$ which is central in N by (2). Also $f^5 = rs^{10n}r$. But s^{10n} is central in $F^{a,b,c}$ by (2) so $f^5 = s^{10n}$ which is central in N.

Before proving the final two elements are central we prove another lemma.

Lemma B.2 $(s^{2n}r)^6 = (rs^{2n}rs^{4n})^2$.

Proof.

$$\begin{aligned}
(s^{2n}r)^6 &= s^{2n}.rs^{2n}rs^{2n}r.s^{2n}.rs^{2n}rs^{2n}r \\
&= rs^{2n}rs^{2n}r.rs^{2n}rs^{2n}r.s^{4n} \\
&= rs^{2n}rs^{4n}rs^{2n}rs^{4n} \\
&= (rs^{2n}rs^{4n})^2
\end{aligned}$$

Hence the lemma is proved.

By Lemma B.2 we see that $(ef)^3 = (fe^2)^2$ so to prove these elements central it suffices to examine one of them.

$$\begin{aligned} e(fe^2)^2 &= s^{2n}rs^{2n}rs^{4n}rs^{2n}rs^{4n} \\ &= rs^{2n}rs^{4n}rs^{2n}rs^{6n} \\ &= (fe^2)^2e \end{aligned}$$

Also

$$\begin{aligned} f(fe^2)^2 &= rs^{2n}r.rs^{2n}rs^{4n}rs^{2n}rs^{4n} \\ &= rs^{4n}rs^{4n}rs^{2n}rs^{4n} \end{aligned}$$

But

$$\begin{aligned} (fe^2)^2f &= rs^{2n}rs^{4n}rs^{2n}rs^{4n}.rs^{2n}r \\ &= rs^{4n}rs^{4n}rs^{2n}rs^{4n} \end{aligned}$$

Hence $f(fe^2)^2 = (fe^2)^2f$ as required.

Proof of Step 5. Certainly M is a normal subgroup of N since its generators are central. However

$$N/M \cong \langle e, f | e^5, f^5, (ef)^3, (fe^2)^2 \rangle \cong A_5$$

Proof of Step 6. To prove that N is perfect we add the relation $e \sim f$ and prove that $e = f = 1$.

Now $e \sim f$ gives $s^{2n} \sim rs^{2n}r$. But we also have $s^{2n} \sim rs^5r$ by (1) so, since $(2n, 5) = 1$, we have $s^{2n} \sim rsr$.

However $r = s^a rs^b rs^c$ and s^{2n} commutes with the right hand side so $s^{2n} \sim r$ proving that s^{2n} is central.

Also $rs^{2n}r = s^{2n}$ so $e = f$. That $s^{2n} = 1$ now follows from Theorem 3.3 of [6]. this proves that N is perfect.

Proof of Step 7. We have $M \leq Z(N)$ and $M \leq N'$. Also $N/M \cong A_5$, so $M = M(A_5) = C_2$.

Proof of Step 8. Follows from what has been proved above.

Bibliography

[1] J. J. Andrews and M. L. Curtis. Free groups and handlebodies. *Proceedings of the American Mathematical Society*, 16:192–195, 1965.

[2] D. G. Arrell and E. F. Robertson. A modified Todd-Coxeter algorithm. In M. D. Atkinson, editor, *Computational Group Theory*, pages 27–32, London, 1984. (Durham, 1982), Academic Press.

[3] C. M. Campbell, H. S. M. Coxeter, and E. F. Robertson. Some families of finite groups having two generators and two relations. *Proceedings of the Royal Society. London. Series A. Mathematical, Physical and Engineering Sciences*, 357(1691):423–438, 1977.

[4] C. M. Campbell and E. F. Robertson. Classes of groups related to $F^{a,b,c}$. *Proceedings of the Royal Society of Edinburgh. Section A. Mathematics*, 78(3-4):209–218, 1977/78.

[5] C. M. Campbell and E. F. Robertson. On 2-generator 2-relation soluble groups. *Proceedings of the Edinburgh Mathematical Society. Series II*, 23(3):269–273, 1980.

[6] C. M. Campbell and E. F. Robertson. Groups related to $F^{a,b,c}$ involving Fibonacci numbers. In C. Davis, B. Grunbaum, and F. A. Sherk, editors, *The geometric vein: the Coxeter Festschrift*, pages 569–576. Springer, New York, 1981.

[7] C. M. Campbell and E. F. Robertson. On the $F^{a,b,c}$ conjecture. *Mitteilungen aus dem Mathematischen Seminar Giessen*, 23(164):25–36, 1984.

[8] J. J. Cannon, L. A. Dimino, G. Havas, and J. M. Watson. Implementation and analysis of the Todd-Coxeter algorithm. *Mathematics of Computation*, 27:463–490, 1973.

[9] J. H. Conway. Advanced problem #5327. *American Mathematical Monthly*, 72:915, 1965.

[10] J. H. Conway. Solution to advanced problem #5327. *American Mathematical Monthly*, 74:91–93, 1967.

[11] H. S. M. Coxeter, R. Frucht, and D. Powers. *Zero-symmetric graphs: Trivalent Graphical Regular Representations of Groups*. Academic Press, New York, U.S.A., 1981.

[12] H. Felsch. Programmierung der Restklassenabzählung einer Gruppe nach untergruppen. *Numerische Mathematik*, 3:250–256, 1961.

[13] V. Felsch, L. Hippe, and J. Neubüser. *GAP – Groups, Algorithms, and Programming, Version 4.4: Package ITC*. The GAP Group, 2004. (`http://www.gap-system.org`).

[14] R. M. Foster. *The Foster census*. Charles Babbage Research Centre, Winnipeg, MB, 1988. R. M. Foster's census of connected symmetric trivalent graphs, With a foreword by H. S. M. Coxeter, With a biographical preface by Seymour Schuster, With an introduction by I. Z. Bouwer, W. W. Chernoff, B. Monson and Z. Star, Edited and with a note by Bouwer.

[15] G. Gamble, A. Hulpke, G. Havas, and C. Ramsay. *GAP – Groups, Algorithms, and Programming, Version 4.4: Package ACE*. The GAP Group, 2004. (`http://www.gap-system.org`).

[16] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2005. (`http://www.gap-system.org`).

[17] G. Havas and C. Ramsay. Advanced Coset Enumerator: ACE version 3.001, 2001. (`http://www.itee.uq.edu.au/~cram/ace3001.tar.gz`).

[18] G. Havas and C. Ramsay. Experiments in coset enumeration. In W. M. Kantor and A. Seress, editors, *Groups and computation, III (Columbus, OH, 1999)*, volume 8 of *Ohio State University Mathematical Research Institute Publications*, pages 183–192. de Gruyter, Berlin, 2001.

[19] G. Havas and C. Ramsay. Proof Extraction After Coset Enumeration: PEACE version 1.100, 2003. (`http://www.csee.uq.edu.au/~havas/peace1v1.tar.gz`).

[20] G. Havas and C. Ramsay. On proofs in finitely presented groups. In C. M. Campbell, M. R. Quick, E. F. Robertson, and G. C. Smith, editors, *Groups – St Andrews* 2005 *(St. Andrews, 2005)*, London Mathematical Society Lecture Note Series, Cambridge, 2006. Cambridge University Press. (to appear) (also at `http://www.itee.uq.edu.au/~havas/opigsta.pdf`).

[21] G. Havas and E. F. Robertson. The $F^{a,b,c}$ conjecture is true, I. 2005. (`http://turnbull.dcs.st-and.ac.uk/circa/Preprints/fabcF.pdf`).

[22] G. Higman. A finitely generated infinite simple group. *Journal of the London Mathematical Society. Second Series*, 26:61–64, 1951.

[23] A.-R. Jamali. Computing with simple groups: Maximal subgroups and presentations. Ph.D. thesis, University of St. Andrews, St. Andrews, United Kingdom, 1988.

[24] J. Leech. Coset enumeration on digital computers. *Proceedings of the Cambridge Philosophical Society*, 59:257–267, 1963.

[25] E. H. Moore. Concerning the abstract groups of order $k!$ and $1/2k!$ holohedrically isomorphic with the symmetric and alternating substitution-groups on k letters. *Proceedings of the London Mathematical Society (1)*, 28:357–366, 1897.

[26] J. Neubüser. An elementary introduction to coset table methods in computational group theory. In C. M. Campbell and E. F. Robertson,

editors, *Groups—St. Andrews 1981 (St. Andrews, 1981)*, volume 71 of *London Mathematical Society Lecture Note Series*, pages 1–45, Cambridge, 1982. Cambridge University Press.

[27] M. Perkel. Groups of type $F^{a,b,-c}$. *Israel Journal of Mathematics*, 52(1-2):167–176, 1985.

[28] F. Spaggiari. On certain classes of finite groups. *Ricerche di Matematica*, 46(1):31–43, 1997.

[29] J. A. Todd and H. S. M. Coxeter. A practical method for enumerating cosets of a finite abstract group. *Proceedings of the Edinburgh Mathematical Society*, 5:26–34, 1936.

[30] H. F. Trotter. A machine program for coset enumeration. *Canadian Mathematical Bulletin. Bulletin Canadien de Mathématiques*, 7:357–368, 1964.

[31] J. Wiegold. The schur multiplier: an elementary approach. In C. M. Campbell and E. F. Robertson, editors, *Groups—St. Andrews 1981 (St. Andrews, 1981)*, volume 71 of *London Mathematical Society Lecture Note Series*, pages 137–159, Cambridge, 1982. Cambridge University Press.