UTS UNIVERSITY OF TECHNOLOGY SYDNEY

On the complexity of epimorphism problems for finitely generated groups.

by Qing (Jerry) Shen

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Under the supervision of
Supervisor: Murray Elder
Co-Supervisors: Anthony Dooley and Kane Townsend

University of Technology Sydney
Faculty of Science

February 2025

Certificate of Original Authorship

I, Qing (Jerry) Shen, declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the Faculty of Science at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Signature: Production Note:
Signature removed prior to publication.

Date: 13 February 2025

Abstract

The *epimorphism problem* for groups asks whether, given two groups G (domain) and H (target), does there exists a surjective homomorphism from G to H. While related to the isomorphism problem, it was shown to be undecidable for nilpotent groups, which is a decidable class for the isomorphism problem.

Friedl and Löh (2021, Confl. Math.) proved that the epimorphism problem is decidable when the target is either a direct product of an abelian and a finite group or a virtually cyclic group. Based on results from Remeslennikov (1979, Sibirsk. Mat. Zh.), they further conjectured that the problem is undecidable for the full class of virtually abelian groups. In this thesis, we establish that the problem is NP-complete for the same target classes, while also extending the known subclasses of virtually abelian groups for which it remains decidable and NP-complete. Additionally, we introduce an alternative approach to investigating the decidability of the epimorphism problem for virtually abelian groups in full generality. To achieve this, we prove that two related integer matrix problems, which arise from a reduction of the epimorphism problem for the decidable classes, are in P, and show a third problem is related to the general class of virtually abelian groups.

We also examine the epimorphism problem for fixed finite targets. Specifically, we show that the problem is NP-complete when the target is a dihedral group of order not a power of 2. This result complements the work of Kuperberg and Samperton [18], who established that the problem is NP-complete when the target is a non-abelian finite simple group.

Finally, we collate a list of results on the epimorphism problem, completing the known complexity classifications for the epimorphism problem to the best of the author's knowledge.

Acknowledgements

I would like to express my gratitude to my co-supervisors, Professor Anthony Dooley and Dr. Kane Townsend, the former for introducing me to the world of mathematical research, and the latter for the many great discussions we had. I am also deeply grateful to my collaborator from the University of Stuttgart, Dr. Armin Weiß, for his valuable ideas and insights. Additionally, I want to thank my partner, Kai Lun Tung, for her support throughout my thesis. Finally, I extend my appreciation to my principal supervisor, Professor Murray Elder, for his guidance and feedback throughout this journey, without whom none of this would have been possible.

Contents

1 Introduction

Dehn [7] first proposed the three foundational group problems, the *word problem*, *conjugacy problem*, and *isomorphism problem* in 1911. It is well known that these problems are undecidable in general, beginning with the word problem [4, 21, 22], from which the undecidability of the other two follows.

Closely related to the isomorphism problem is the *epimorphism* problem, which asks whether there exists an epimorphism from one group to another (where an epimorphism in the category of groups is a surjective homomorphism). Remeslennikov [25] demonstrated that the undecidability of the epimorphism problem persists even under significant restrictions on the classes of groups in 1979. Specifically, he proved that the epimorphism problem is undecidable for nilpotent groups of class at least 2, where this result was established via Hilbert's Tenth Problem. However, nilpotent groups were soon shown to be decidable for the isomorphism problem by Grunewald and Segal [14] in 1980. In a sense, this suggests that the epimorphism problem is more difficult than the isomorphism problem under specific conditions.

Possibly because of this, the epimorphism problem has received limited attention in computational or algorithmic group theory. Recently, Friedl and Löh [12] investigated the problem when the target group is virtually abelian, demonstrating that the problem is decidable when the target is either virtually cyclic or a direct product of an abelian group and a finite group. These results establish decidability without providing complexity bounds, meaning that the corresponding algorithms do not give considerations to efficiency. On the other hand, practical algorithmic approaches also exist, such as in the work of Holt and Plesken [15], who studied epimorphisms from finitely presented groups to simple groups of order up to one million, as well as epimorphisms from a domain group G to a quotient group of the target.

The focus of this thesis is to approach the epimorphism problem from a complexity theory perspective. This requires the development of algorithms which do not use infinitely recursive methods, that is algorithms that run potentially infinitely which are frequently used in decidability results. Unlike decidability results, complexity analysis requires determining the upper bounds for the exact time or space of resources needed for an algorithm to compute a solution. While complexity classifications do not always lead to practical algorithms in a computational sense, since worst-case scenarios must be accounted for, they provide a structured way to assess the relative difficulty of a problem.

For example, by the work of Kuperberg and Samperton [18] on epimorphisms from certain 3-manifold groups to finite non-abelian simple groups, it is implied that the epimorphism problem from a finitely presented group to a fixed finite non-abelian simple group is NP-hard. This is one of the conditions for a problem to be NP-complete, a well-understood and one of the most studied complexity classes, closely related to the $\mathsf{P} = \mathsf{NP}$ problem [5].

In this thesis, we extend these results using techniques involving equations over groups and computational problems with integer matrices. These methods yield new insights into both the computational complexity and decidability of the epimorphism problem for the classes considered by Friedl and Löh, as well as extended generalisations of those classes.

We also provide new classes of groups for fixed finite targets, complementing the work of Kuperberg and Samperton. Additionally, we compile various results on the epimorphism problem that have not been previously documented, and provide either complexity bounds or a decidability result. Finally, we propose a generalisation of previously used methods that suggests a potential framework for investigating the decidability of the epimorphism problem in the broader class of virtually abelian groups.

1.1 Structure and Key Results

In Chapter 2 we provide the basics of group theory, complexity theory and other standard tools which are used throughout this thesis, we refer readers to Section 2.1 for the definition and notation on complexity which will be used when referring to the results.

With the exception of Section 4.1 which provides some preliminary results for the epimorphism testing, each chapter uses distinct techniques and can be read independently, when used in conjunction with Chapter 2. In each of chapters from 3 – 7, we establish one of our theorems.

The first original result provided is the solving of integer matrices problems, which are used in later epimorphism testing. This problem arises naturally by considering a normal subgroup of our virtually abelian target group. We begin by defining the relevant matrix problems.

Notation For $d \in \mathbb{N}$, let $[1, d] := \{1, 2, \ldots, d\}$. For $m, n \in \mathbb{N}$, write $\mathbb{Z}^{m\times n}$ for the set of all $m \times n$ integer matrices. Given $M \in \mathbb{Z}^{m\times n}$ and $\ell \in [1, m]$, let $M|_\ell$ denote the submatrix consisting of the bottom ℓ rows of M.

We refer to an $n \times 1$ matrix as an *n-vector*, and a matrix (resp. n-vector) whose entries are integers as an *integer matrix* (resp. *integer n-vector*). For an integer matrix M, we let $\mathrm{span}(M)$ denote the set of all $\mathbb{Z}$-linear combinations of the columns of M, we now define the following two integer matrix problems.

Problem: MatrixSubspanA
Input: A triple (A, d, ℓ) where A is an $m \times n$ integer matrix, $d, \ell \in \mathbb{N}$ with $\ell \in [0, n-1]$.
Question: Do there exist integer n-vectors $v_1, \ldots, v_d$ such that $Av_i = 0$ for $i \in [1, d]$ and for the $n \times d$ matrix V whose columns are $v_1, \ldots, v_d$, $\mathrm{span}((V|_\ell)^T) = \mathbb{Z}^d$?

Problem: MatrixSubspanB
Input: A triple (A, b, ℓ) where $A \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$, $\ell \in \mathbb{N}$ with $\ell \in [0, n-1]$.
Question: Does there exist an n-vector ν such that $A\nu + b = 0$ and $\mathrm{span}((\nu|_\ell)^T) = \mathbb{Z}^d$?

We then prove the following in Chapter 3.

Theorem A. MatrixSubspanA *and* MatrixSubspanB *are in* P.

Using this result, we build upon the work of Friedl and Löh [12] by determining the complexity of the epimorphism problem for subclasses of virtually abelian targets that they demonstrated to be decidable, we then generalise the complexity result by expanding the subclasses. While Friedl and Löh [12] remarked that the algorithm they proposed to demonstrate decidability "will have ridiculous worst-case complexity", we provide an approach which can be shown to have non-deterministic polynomial time complexity. In particular, we establish the following result in Chapter 4.

Theorem B. *The epimorphism problem from finitely presented groups to the following target classes is* NP*-complete:*

1. *Direct products of abelian and finite groups.*
2. *Virtually cyclic groups.*
3. *Semi-direct products of a free abelian group N and a finite group Q, where the action of Q on N is restricted in a specific way, as described in Definition 2.80.*

From here, we shift focus and use different techniques. Supplementing the results of Kuperberg and Samperton [18] that imply the epimorphism to certain fixed finite groups is NP-hard, we demonstrate that the same result applies when the target is a finite dihedral group of order not a power of 2. Again, using systems of equations over groups, but with different techniques distinct from those used in the previous chapter. Thus, we prove the following in Chapter 5.

Theorem C. *Let $n > 1$ be an integer that is not a power of 2, and let D_{2n} denote the dihedral group of order $2n$. Then, the epimorphism problem from finitely presented groups to the group D_{2n} is* NP*-hard.*

In addition, we also present a collection of results related to epimorphism, some of which follow directly from existing work, while others address problems that are widely regarded as decidable by 'folklore'. These results may be considered more straightforward than those in the previous theorems.

By applying the work of Razborov [24] on equations in free groups, we demonstrate that the epimorphism problem from finitely presented groups to finitely generated free groups is decidable, though no complexity bounds are currently known for this problem. We also formalise the results of Kuperberg and Samperton [18] within the context of the epimorphism problem.

Furthermore, following Friedl and Löh [12] we confirm that the epimorphism problem for finitely generated abelian targets is decidable and, moreover, lies in P. Finally, we present a generalised result that plays a key role in the proof of Theorem C. We consolidate them as the following in Chapter 6.

Theorem D. *The epimorphism problem from finitely presented groups to the following target classes has the corresponding result.*

1. *Finite rank free groups as the target is decidable.*
2. *A fixed non-abelian finite simple group as the target is* NP*-complete.*
3. *Finitely generated abelian groups as the target is in* P*.*
4. *Under the following three conditions for groups A and B*
   - *A is a finitely generated abelian group*
   - *B is a finite group with a trivial centre*
   - *the epimorphism problem from a finitely presented group to B is* NP*-hard.*

   A fixed group $B \times A$ as the target is NP*-complete.*

Finally, Friedl and Löh [12] conjectured that the epimorphism problem for virtually abelian targets, in general, is undecidable, drawing an analogy to Hilbert's Tenth problem, which was the method employed in Remeslennikov [25]. We establish an intermediary result concerning the following matrix problem, which, if shown to be decidable, would imply the decidability of the epimorphism problem for virtually abelian targets. Let $\mathrm{GL}_{\mathsf{Fin}}(d, \mathbb{Z})$ denote all torsion elements of $\mathrm{GL}(d, \mathbb{Z})$.

Problem: MatrixSubspanC
Input: A tuple $(\{A_0, \dots, A_k\}, \{M_0, \dots, M_k\}, B, d, \ell)$, where $A_i \in \mathbb{Z}^{m \times n}$, $M_0 = I \in \mathbb{Z}^{d \times d}$, $M_i \in \mathrm{GL}_{\mathsf{Fin}}(d, \mathbb{Z})$ for $i \in [1, k]$, $B \in \mathbb{Z}^{m \times d}$, and $d, \ell \in \mathbb{N}$ with $\ell \in [0, n-1]$.
Question: Do there exist integer n-vectors $v_1, \dots, v_d$, and a matrix $V = \begin{pmatrix} v_1 & \cdots & v_d \end{pmatrix} \in \mathbb{Z}^{n \times d}$ such that

$$\sum_{i=0}^{k} A_i((M_i V^T)^T) + B = 0$$

and $\mathrm{span}((V|_\ell)^T) = \mathbb{Z}^d$?

Based on this problem, we prove the following in Chapter 7.

Theorem E. *If* MatrixSubspanC *is decidable, then the epimorphism problem from finitely presented groups to virtually abelian groups is decidable.*

1.2 Attribution of results

Theorems A, B, C and D are joint work with my supervisor, Murray Elder and Dr. Armin Weiß, who visited the University of Technology Sydney in January 2023, a preprint is available at [10]. Theorem E is a natural progression of the method used to prove Theorem B, in a more generalised setting.

2 Preliminaries

In this chapter, we introduce the basic notations and definitions used throughout the thesis. Each section provides the necessary background and notation as follows: complexity theory is covered in Section 2.1, group theory in Section 2.2, and group extensions in Section 2.3, the later will only see use in Chapters 4 and 7. Finally, we define the specific classes of groups of interest in Section 2.4.

Let $\mathbb{P}$ denote the set of all prime numbers. Let $\mathbb{N}$ and $\mathbb{N}_+$ represent the sets of natural numbers (including and excluding 0, respectively). For $a, b \in \mathbb{Z}$ with $a < b$, the notation $[a, b]$ denotes the set of integers from a to b, that is

$$[a, b] = \{a, a + 1, \ldots, b - 1, b\}.$$

If $X = \{x_1, \ldots, x_n\}$ is a set, then $X^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\}$ represents the set of letters in biection with X such that

$$X \cap X^{-1} = \varnothing.$$

2.1 Complexity

In this section, we provide background on decision and computational problems, along with the relevant definitions and notations. All problems are presented in natural language rather than in a formal language designed for a Turing machine. For formal definitions, see [2, 33]. Our examples are those relevant to decision problems for groups, we refer readers to Sections 2.2 and 2.3 for definitions relevant to these examples.

A *decision problem* is a problem with a binary output, typically a 'Yes' or 'No' answer, while a *computational problem* involves producing a specified output. As previously noted, all inputs and outputs are assumed to take their natural form, for example, matrices are represented as lists of binary integers, and group presentations are represented using alphabets of letters. For other forms of relative complexity results, we use the concept of an oracle (a theoretical black box).

Polynomial time reductions, introduced here, will be used to show that problems are NP-hard in Chapter 6. For other types of reductions, we use the notation of oracles.

Definition 2.1. A decision (resp. computation) problem Prob is said to be *decidable* if there exists a terminating algorithm that can determine a correct output for every instance of Prob.

Remark 2.2. A decision (resp. computation) problem is considered decidable if there exists a terminating algorithm that correctly decides it. One way to achieve this is as follows, a problem can also be shown to be decidable by using two *infinitely recursive* algorithms, A and B, running in parallel, with the following properties:

- A guarantees a correct 'Yes' output but runs indefinitely if the answer is 'No'
- B guarantees a correct 'No' output but runs indefinitely if the answer is 'Yes'.

Since either the answer is 'Yes' or 'No', running both algorithms simultaneously ensures that one will eventually halt, providing the correct solution (see Remark 2.23).

Definition 2.3. P is the class of all decision problems that can be solved by a deterministic algorithm in polynomial time. NP is the class of all decision problems for which a solution can be verified by a non-deterministic algorithm in polynomial time.

Remark 2.4. To show a problem is in NP, it suffices to demonstrate that a solution can be *verified* in polynomial time. Specifically, if a solution exists, we can 'guess' a correct solution and provide an algorithm that verifies this guess in polynomial time (see Example 4.2). This means that the 'guess' has to be an input length which can be calculated in polynomial time, and thus cannot exceed polynomial space.

We now introduce the concept of a polynomial time reduction, which demonstrates that if a problem A can be reduced to B in polynomial time, then B is at least as hard as A. An alphabet is a finite set. For an alphabet Σ, we write Σ^* for the set of all finite words over Σ, including the empty string ε.

Definition 2.5. Let A and B be problems with inputs $A, B \in \{0,1\}^*$, respectively. The problem A is said to be *polynomial-time reducible* to B, denoted $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$, if there exists a polynomial-time function $f\colon \{0,1\}^* \to \{0,1\}^*$ that transforms inputs for A into inputs for B such that A is a solution to A if and only if $f(A)$ is a solution to B.

Example 2.6. Let problem A be the problem of deciding if an epimorphism exists from a finitely presented group to a fixed dihedral group, and problem B be the problem of deciding if there exists a solution to a system of equations over a fixed dihedral group.

If given a input for A, in the form of a finite presentation for a group G, and we are able to construct a system of equations such that the system of equation has a solution if and only if there exists an epimorphism from G to the fixed dihedral group then $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$. This process is the focus of Chapter 5.

Definition 2.7. A problem Prob is NP-*hard* if every problem in NP is polynomially reducible to Prob. A problem is NP-*complete* if it is both NP-hard and in NP.

Theorem 2.8 ([33, Theorem 7.36])**.** *For decision problems* A, B*, if* A *is* NP*-hard and* $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$*, then* B *is* NP*-hard.*

Remark 2.9. To prove this, we take an input from A and construct a corresponding instance in B in polynomial time, ensuring that there is a solution to the original input in A if and only if there exists a solution in B for the constructed problem. This process is demonstrated in Chapter 6.

2.1.1 Oracles

Next, we introduce the concept of an oracle.

Definition 2.10. An *oracle* for a problem Prob is an abstract computational device that provides the solution to Prob in a single computational step. We may think of the oracle as a *black box* where its internal workings are unspecified, but it returns correct outputs for all valid inputs.

In other words, an oracle can instantly solve a specific problem in a single computational step. They are used to analyse the relative complexity of problems. An oracle can be seen as a more generalised form of a reduction, with the two being equivalent under certain strict conditions. The author finds it useful to analyse problems from both perspectives (reductions and oracles) when assessing complexity of problems relative to other problems. Oracles are used in Chapter 7 to show that the decidability of certain problems are dependent upon other problems.

Definition 2.11. A *complexity class* is a collection of decision problems that can be solved or verified by algorithms subject to specific resource bounds, such as time or space, measured as functions of the input size.

Definition 2.12. Let A and B be decision problems, and let C be a complexity class. If, given an oracle that solves B, we can solve A within the resource limits of C, then we write $\mathsf{A} \in \mathsf{C}^{\mathsf{B}}$.

Example 2.13. Let problem WP be the word problem, see Definition 2.21, and ZMP be the centre membership problem for G with a generating set X, that is, given a word $w \in (X \cup X^{-1})^*$, decide if $w \in Z(G)$.

Assume we have an oracle for WP. To determine whether a word w lies in the centre $Z(G)$, it suffices to verify that w commutes with each generator of G. For each $x \in X$, construct the commutator $wxw^{-1}x^{-1}$ and query the oracle for WP to check whether it represents the identity. This construction has size $(2|w| + 2)|X|$, which is polynomial in the length of the presentation of G and the word w. Hence $\mathsf{ZMP} \in \mathsf{P}^{\mathsf{WP}}$.

Now, let problem WO be the problem of deciding if a word $w \in (X \cup X^{-1})^*$ has order less than or equal to n in G. Again, assume we have an oracle for WP, we enumerate each word w by calculating w^i for $i \in [1, n]$, then calling the oracle for WP. This process has maximum size $|w|^n$, and thus is exponential time to process. Therefore, we have $\mathsf{WO} \in \mathsf{EXP}^{\mathsf{WP}}$, where EXP is the complexity class of all decision problems decidable with a exponential-time algorithms.

Remark 2.14. The concepts of oracles and reductions are equivalent under specific conditions. Let A and B be decision problems. If $\mathsf{A} \in \mathsf{P}^{\mathsf{B}}$, this means that A can be solved in polynomial time with access to an oracle for B.

If, when solving A, the procedure is in polynomial time and the oracle for B is called only once, then we can compute an instance of B from an instance of A in polynomial time. This is equivalent to the claim that $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$.

The reverse direction is trivial: if $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$, then there exists a polynomial time function that transforms an input for A into an input for B. We then call the oracle for B, which shows that $\mathsf{A} \in \mathsf{P}^{\mathsf{B}}$.

That is,

- If $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$, then $\mathsf{A} \in \mathsf{P}^{\mathsf{B}}$.
- If $\mathsf{A} \in \mathsf{P}^{\mathsf{B}}$, then it is not necessarily true that $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$.
- If $\mathsf{A} \in \mathsf{P}^{\mathsf{B}}$ and solving A involves only one use of the oracle for B, then $\mathsf{A} \leq_{\mathsf{P}} \mathsf{B}$.

2.2 Groups

In this section, we establish notation and basic conventions for group theory.

Notation. For a group G, we denote its *identity* by 1_G or simply 1 when the context is clear. For specific groups, such as abelian groups or S_3 (the symmetric group on three letters), where identity notation may differ, we note these differences explicitly. We write $H \leq G$ to indicate that H is a *subgroup* of G and $N \trianglelefteq G$ to indicate that N is a *normal* subgroup of G. For $a, b \in G$, the *commutator* of a and b is $[a, b] = aba^{-1}b^{-1}$, and the *commutator subgroup* $[G, G]$ is the subgroup generated by all such commutators. If u, v are two different ways to represent the same element of G, we write $u =_G v$.

For $d, n \in \mathbb{N}_+$, G^d denotes the direct product of d copies of G, and F_d denotes the free group of rank d. The symbol C_∞ represents the infinite cyclic group, and C_n denotes the cyclic group of order n. We denote the additive group of integers by $\mathbb{Z}$ (with identity 0)

and write $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z} \cong C_\infty$ and $\mathbb{Z}_n \cong C_n$, we use cyclic groups to denote abelian groups multiplicatively and $\mathbb{Z}$ additively. Furthermore, a free abelian group of rank d is equivalent to C_∞^d multiplicatively or $\mathbb{Z}^d$ additively.

2.2.1 Words, Presentations and System of Equations

We begin with the concept of a word over a set of alphabets, which is a standard way to describe group elements, as discussed in [20]. If X is a generating set for a group G, then each word formed from $X \cup X^{-1}$ represents an element of G. However, this representation is not necessarily unique. By defining words in a group in addition with variables we form equations over a group. Using the ideas of equations over a group we will investigate epimorphism targets for certain subclasses of virtually abelian groups in Chapter 4, free groups in Chapter 6, and fixed finite groups in Chapter 5, in Chapter 7 we generalise equations over a group even further to investigate a more generalised targets for epimorphism problem.

Definition 2.15. The *normal closure* of a subset R in a group G is the smallest normal subgroup of G containing R.

Definition 2.16. Let X be a set. A finite sequence $(x_1, \ldots, x_n)$ with $x_i \in X$ is called a *word* over X, denoted $x_1 \cdots x_n$. The set of all words over X is denoted X^*. For a word w, $w(x_1, \ldots, x_n)$ indicates that w is a word over $\{x_1, \ldots, x_n\}$. If $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$ are disjoint finite sets, then $w(X, Y)$ indicates a word $w \in (X \cup Y)^*$. We use the following notation interchangeably

$$w(X,Y), \quad w(x_1,\ldots,x_n,Y), \quad w(X,y_1,\ldots,y_m) \quad \text{or} \quad w(x_1,\ldots,x_n,y_1,\ldots,y_m).$$

The notation $|w|_{x_1}$ counts the occurrences of the letter x_1 in the word w.

Lemma 2.17 ([26, Statement 2.1.5])**.** *Let G be a group with a generating set X, and let F_X be the free group of rank $|X|$ with X as generators. Then there exists a normal subgroup N of F_X such that $G \cong F_X/N$.*

By Lemma 2.17 every group can be represented by a free group quotiented by a normal subgroup. Thus, we now introduce the well-established concept of a *presentation* for a group. It is standard practice for a group G to be described as a free group on a generating set X, quotiented by the normal closure of a set R in G. This gives a presentation denoted by $G = \langle X \mid R \rangle$. If $r \in R \subseteq (X \cup X^{-1})^*$, then

$$r(x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}) = 1_G.$$

It is not assumed that $X = \{x_1, \ldots, x_n\}$ is a minimal generating set for G. A group is said to be finitely generated if X is finite, and finitely presented if both X and R are finite. Throughout this thesis, we assume all groups are finitely presented.

Definition 2.18. Given a finite presentation $\langle X \mid R \rangle$, the following are called *Tietze transformations*:

1. **Adding a set of relations:** Replace $\langle X \mid R \rangle$ by $\langle X \mid R \cup S \rangle$, where S is a subset of the normal closure of R.
2. **Removing a set of relations:** Replace $\langle X \mid R \rangle$ by $\langle X \mid R \setminus S \rangle$, where S is in the normal closure of $R \setminus S$.
3. **Adding a set of generators:** Replace $\langle X \mid R \rangle$ by $\langle X \cup Y \mid R \cup S \rangle$, where $Y \cap F_X = \varnothing$ is a new set of symbols given by some $w_y \in (X \cup X^{-1})^*$ and $S = \{y^{-1} w_y \mid y \in Y\}$.

4. **Removing a set of generators:** Replace $\langle X \mid R\rangle$ by $\langle X \setminus Y \mid R \setminus S\rangle$, where $Y \subseteq X$ such that $S = \{y^{-1}w_y \mid y \in Y\}$ for $w_y \in ((X \setminus Y) \cup (X \setminus Y)^{-1})^*$.

Tietze [36] first proved the equivalent form of the following well-known lemma. We use this lemma to illustrates the distinction between a decision problem and an existence problem.

Lemma 2.19 ([20, Chapter 2 Proposition 2.1])**.** *Two finitely presented groups are isomorphic if and only if it is possible to pass from one to the other by a finite sequence of Tietze transformations.*

Example 2.20. Let D_{2n} be the dihedral group of order $2n$. It is well known that if $c > 1$ is odd, then the D_{4c} is isomorphic to $D_{2c} \times C_2$. This can be shown through Tietze transformation. Let the two groups be presented as follows

$$\begin{aligned} D_{4c} &\cong \left\langle s, t \mid s^2, t^{2c}, stst \right\rangle \\ D_{2c} \times C_2 &\cong \left\langle a, d \mid a^2, d^c, adad \right\rangle \times \left\langle b \mid b^2 \right\rangle \\ &\cong \left\langle a, b, d \mid a^2, d^c, adad, b^2, [a,b], [b,d] \right\rangle. \end{aligned}$$

Then the following sequence of Tietze transformations proves the isomorphism. First we note some relevant consequences of the existing relations for D_{4c} which will be used in the Tietze transformations.

- By the relation s^2, this implies $s = s^{-1}$.
- By the relation $stst$, this implies $st = t^{-1}s$, and $st^2st^2 = st^2t^{-2}s = s^2 = 1$.
- By the previous two implications $[t^c, s] = t^cst^{-c}s^{-1} = t^cst^{-c}s = t^ct^cs^2 = t^{2c}s^2 = 1$.

Begin with the presention for D_{4c}

1. Add generator b, and relation bt^{-c} by rule (3).
2. Add relations $b^2, [b,s], [t,b]$ by rule (1). These are valid relations as $b^2 = t^{2c}$, $[b,s] = [t^c, s]$, and $[t,b] = [t,t^c]$. The group is now presented as
$$\left\langle s, t, b \mid s^2, t^{2c}, stst,\ bt^{-c}, b^2, [b,s], [b,t] \right\rangle.$$

Note From here, when we add a generator x such that $xw_x^{-1} = 1$ for some w_x on existing generators, we write $x = w_x$. Similarly, when adding relations, if adding a relation r follows as a consequence of $r = w$ for some word on the existing generators where $w = 1$, then we write $r = w$. Thus, for the above, to add b, we write: Add generator $b = t^c$. To add the relation b^2, we write: Add relation $b^2 = t^{2c}$.

3. Add generator $d = t^2$ and relations equivalent to $d^c = t^{2c}$, $sdsd = st^2st^2$, and $[b,d] = [b,t^2]$. The group is now presented as
$$\left\langle s, t, b, d \mid s^2, t^{2c}, stst, 1, bt^{-c}, b^2, [b,s], [b,t], dt^{-2}, d^c, sdsd, [b,d] \right\rangle.$$
4. Add relations equivalent to $t = bd^{(c+1)/2}$ as $t = t^{2c+1} = t^ct^{c+1}$, $b = t^c$ and $t^{c+1} = t^{2(c+1)/2} = d^{(c+1)/2}$. The group is now presented as
$$\left\langle s, t, b, d \mid s^2, t^{2c}, stst, 1, bt^{-c}, b^2, [b,s], [b,t], 1, dt^{-2}, d^c, sdsd, [b,d], tb^{-1}d^{-(c+1)/2} \right\rangle.$$
5. Remove the following relations by rule (2):
   - dt^{-2} by the relations $tb^{-1}d^{-(c+1)/2}$, b^2, and d^c. That is, $dt^{-2} = d(bd^{(c+1)/2})^{-2} = db^{-2}d^{-c-1} = db^2d^{-c}d^{-1} = dd^{-1} = 1$. From here we omit this calculation and provide only the relevant relations.

- t^{2c} by the relations bt^{-c} and b^2.
- $ststst$ by the relations $tbd^{-(c+1)/2}$, $[s,b]$, $[b,d]$, $sdsd$ and b^2.
- $[b,t]$ by the relation bt^{-c}.

The group is now presented as

$$\left\langle s,t,b,d \mid s^2, 1, bt^{-c}, b^2, [b,s], 1, d^c, sdsd, [b,d], tb^{-1}d^{-(c+1)/2} \right\rangle.$$

6. Rename generator s as a.
7. Remove generator t and relation $tb^{-1}d^{-(c+1)/2}$. The group is now presented as

$$\left\langle a,b,d \mid a^2,\ d^c,\ adad,\ b^2,\ [a,b],\ [b,d] \right\rangle.$$

Thus, the two groups are isomorphic.

Definition 2.21. Let $G = \langle X \mid R \rangle$ and $H = \langle Y \mid U \rangle$ be a finitely presented groups, where X is a finite set of generators and R is a finite set of relations.

The *word problem* asks that, given a word w over the generators X, is w equivalent to the identity in G?

The *isomorphism problem* asks that, give two group presentations for groups G and H, is $G \cong H$?

Remark 2.22. It is well known that the word problem is undecidable, by the work of Markov [21], Boone [4], and Novikov [22] for some finitely presented group. Thus, given a generating set X for a group G, for $x_1, x_2 \in X$, we are not able to confirm if $x_1 =_G x_2$, and so when we write down an arbitrary list of symbols X from which we have a finite set of relations $R \subseteq (X \cup X^{-1})^*$ to build a presentation $\langle X \mid R \rangle$ we cannot insist X is a subset of G.

Remark 2.23 (non-terminating algorithms)**.** Lemma 2.19 provides a method to relate the structures of two equivalent group presentations, assuming their underlying groups are isomorphic. It guarantees the existence of a finite sequence of Tietze transformations connecting the presentations but does not offer a constructive procedure for finding them.

However, it ensures a non-terminating process for verifying whether one presentation can be transformed into the other. Running this in parallel with a non-terminating process for checking non-isomorphism would yield decidability in this class of groups.

This process is demonstrated by Segal [31] for polycyclic by finite groups (a group with a finitely generated normal subgroup that is polycyclic which has a finite quotient), and Dahmani and Guirardel [6] for hyperbolic groups.

A more concrete demonstration of this dual simultaneous non-terminating process, is the following well-known procedure for deciding the word problem in residually finite groups. We omit justifications and only provide the procedure.

Let G be a residually finite group. If $g, h \in G$ and Γ is a finite group, then $g = h$ if and only if for every homomorphism $\kappa\colon G \to \Gamma$, we have $\kappa(g) = \kappa(h)$. Thus, we run the following procedures simultaneously:

1. List all possible words given by the relations in G.
2. For every finite group Γ, and every homomorphism $\kappa\colon G \to \Gamma$, check if $\kappa(g) = \kappa(1)$.

Either we attain the word by procedure (1), or we attain an homomorphism κ such that $\kappa(g) \neq \kappa(1)$ by procedure (2). Procedure (1) tells us the element is the identity, procedure (2) tells us the element is not the identity.

Remark 2.24 (Undecidability of isomorphism problems)**.** Given a finitely presented group G with a presentation $\langle X \mid R \rangle$, and a word $w \in (X \cup X^{-1})^*$, create a new group $G_w = \langle X \mid R \cup \{w\} \rangle$. This means G_w is G modified so that w is forced to be the identity element.

Then it follows that $G \cong G_w$ if and only if $w =_G 1$. This means we can always create a group to solve the word problem.

This reduction shows that a solution to the isomorphism problem could be used to solve the word problem. As the word problem is undecidable, the isomorphism problem must also be undecidable.

The following provides the definition and notation for a system of equations over a group.

Definition 2.25. Let G be a group, $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$ and $\mathcal{G} = \{g_1, \ldots, g_s\}$ where $g_i \in G$ for $i \in [1, s]$. An *equation* over a group G is a word

$$u(\mathcal{G}, \mathbb{X}) \quad \text{or} \quad u(g_1, \ldots, g_s, X_1, X_1^{-1} \ldots, X_n, X_n^{-1})$$

where $g_i \in \mathcal{G}$ are called *constants*, and $\mathbb{X}$ are called *variables*. We can denote the equation as $u(\mathcal{G}, \mathbb{X})$, and an equation without constants is denoted $u(\mathbb{X})$.

A *system of equations* $(u_i)_{[1,m]}$ over a group G is a finite list of equations $u_i(g_1, \ldots, g_s, \mathbb{X})$ for $i \in [1, m]$. A system of equations *without constants* is a list of equations of the form $u_i(\mathbb{X})$ for $i \in [1, m]$. A system of equations is simply referred to as equations where the context is clear.

A *solution* to a system of equations is a map $\sigma \colon \mathbb{X} \to G$ defined by $\sigma(X_i) = h_i$ and $\sigma(X_i^{-1}) = h_i^{-1}$ for some $h_i \in G$, $i \in [1, n]$, such that

$$u_i(g_1, \ldots, g_s, \sigma(X_1), \sigma(X_1^{-1}), \ldots, \sigma(X_n), \sigma(X_n^{-1})) =_G 1 \quad \text{for all} \quad i \in [1, m].$$

Note that if G is a finitely generated group with a finite inverse-closed generating set $\mathcal{Y} = \{y_1, \ldots, y_s\}$, we may write any equation over G as $u(\mathcal{Y}, \mathbb{X})$. The following demonstrates a system of equations over a fixed group and a possible solution.

Example 2.26. Consider the dihedral group of order 10, let

$$D_{10} = \left\langle s, t \mid s^2, t^5, stst, 1 \right\rangle.$$

Then a system of equations over D_{2n} with variables $\{X, X^{-1}, Y, Y^{-1}, Z, Z^{-1}\}$ and constants $\{s, t\}$, may look like

$$\begin{aligned} u_1(s, t, X, X^{-1}, Y, Y^{-1}, Z, Z^{-1}) &= sXsYtttZ \\ u_2(s, t, X, X^{-1}, Y, Y^{-1}, Z, Z^{-1}) &= YZ \\ u_3(s, t, X, X^{-1}, Y, Y^{-1}, Z, Z^{-1}) &= XsYtttsZ. \end{aligned}$$

A possible valid solution $\sigma \colon \{X, Y, Z\} \to D_{2n}$ would be:

$$\sigma \colon \begin{cases} X \mapsto t^2; & X^{-1} \mapsto t^3 \\ Y \mapsto s; & Y^{-1} \mapsto s \\ Z \mapsto s; & Z^{-1} \mapsto s. \end{cases}$$

Thus our equations now take the form:

$$\begin{aligned} \sigma(u_1) &= st^2ssttts = st^2ttts = ss = 1 \\ \sigma(u_2) &= ss = 1 \\ \sigma(u_3) &= t^2ssttsss = t^2ttt = 1. \end{aligned}$$

The following definition and lemma provide a way to connect solving a system of equations with finding a homomorphism between two group presentations.

Definition 2.27. Let $A = \{a_1, \ldots, a_n\}$ be a set and H a monoid. A map $\psi\colon A \to H$ is a *monoid homomorphism*. The *induced* monoid homomorphism $\psi'\colon (A \cup A^{-1})^* \to H$ is defined by

$$\psi'(a_{i_1}^{\epsilon_1} \cdots a_{i_s}^{\epsilon_s}) = \psi(a_{i_1})^{\epsilon_1} \cdots \psi(a_{i_s})^{\epsilon_s},$$

where $\epsilon_i = \pm 1$. By convention, we refer to the induced map ψ' as ψ.

Lemma 2.28 (von Dyck's lemma [3, Lemma 2.1])**.** *If G is presented by*

$$G = \langle g_1, \ldots, g_n \mid r_1, \ldots, r_m \rangle,$$

where $r_i = r_i(g_1, \ldots, g_n)$, and $\psi\colon \{g_1, \ldots, g_n\} \to H$ is a set map to a group H, then ψ extends to a homomorphism from G to H if and only if

$$r_i(\psi(g_1), \ldots, \psi(g_n)) =_H 1 \quad \textit{for all} \quad i \in [1, m].$$

Remark 2.29. Here, we show the above lemma connects equations over a group to testing if a homomorphism exists between two groups, and that it is undecidable in general.

Given a domain group and a finite presentation

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

and a target group H. By Lemma 2.28 if there exists a set map $\psi\colon \{x_1, \ldots, x_n\} \to H$, such that ψ extends to a homomorphism if and only if for all relations $r_i(x_1, \ldots, x_n)$ for $i \in [1, m]$, we have

$$r_i(\psi(x_1), \psi(x_1^{-1}), \ldots, \psi(x_n), \psi(x_n^{-1}) =_H 1.$$

Then we can instead view this question as the problem if there exists a system of equations over the group H. First we define a way to construct system of equations from words in H, let $\zeta\colon \{x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}\}^* \to \{X_1, X_1^{-1} \ldots, X_n, X_n^{-1}\}^*$ be defined by

$$\zeta\colon x_j \mapsto X_j, \quad x_j^{-1} \mapsto X_j^{-1}$$

That is, for the system of equations described by

$$u_i(X_1, X_1^{-1} \ldots, X_n, X_n^{-1})$$

for $i \in [1, m]$, it follows that for a solution $\sigma\colon \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\} \to H$

$$u_i(\sigma(X_1), \sigma(X_1^{-1}, \ldots, \sigma(X_n), \sigma(X_n^{-1}) =_H 1$$

if and only if

$$r_i(\psi(x_1), \psi(x_1^{-1}), \ldots, \psi(x_n), \psi(x_n^{-1})) =_H 1$$

where $\sigma(X_j) = \psi(x_j)$. $\sigma(X_j) =_H 1$ if and only if $\psi(x_j) =_H$.

Roman' kov [27] proved that the endomorphic reducibility problem is undecidable for free nilpotent groups of class 9 or higher. This result follows from the undecidability of Diophantine equations in these groups, which is linked to Hilbert's Tenth Problem. It follows from this result that it is undecidable whether we may determine if a solution exists for a finite system of equations over such groups.

We now show an example of this process.

Example 2.30. Following the process in Remark 2.29, consider the problem of determining whether there exists a homomorphism from

$$G = \langle x, y, z \mid x^4, y^3, xyz \rangle$$

to the symmetric group

$$S_3 = \langle s, t \mid s^2, t^3, stst \rangle.$$

We require a set map $\psi\colon G \to S_3$ which extends to a homomorphism such that

$$\begin{aligned} \psi(x)\psi(x)\psi(x)\psi(x) &= 1 \\ \psi(y)\psi(y)\psi(y) &= 1 \\ \psi(x)\psi(y)\psi(z) &= 1 \end{aligned}$$

To find such a homomorphism, we define a mapping $\zeta\colon \{x, y, z\} \to \{X, Y, Z\}$, which translates the relations in G into a system of equations with variables X, Y, Z, by

$$\zeta\colon \begin{cases} x^4 & \mapsto \zeta(x)\zeta(x)\zeta(x)\zeta(x) = X^4 \\ y^3 & \mapsto \zeta(y)\zeta(y)\zeta(y) = Y^3 \\ xyz & \mapsto \zeta(x)\zeta(y)\zeta(z) = XYZ. \end{cases}$$

A valid, non-trivial solution $\sigma\colon \{X, Y, Z\} \to S_3$ is given by:

$$\sigma\colon \begin{cases} X \mapsto s \\ Y \mapsto t \\ Z \mapsto st. \end{cases}$$

We can use this to define a set map $\psi\colon G \to S_3$ by

$$\psi\colon \begin{cases} \psi(x) & \mapsto \sigma(X) = s \\ \psi(y) & \mapsto \sigma(Y) = t \\ \psi(z) & \mapsto \sigma(Z) = st \end{cases}$$

using Lemma 2.28 we can verify this extends to a homomorphism as

$$\begin{aligned} \psi(x)\psi(x)\psi(x)\psi(x) &= s^2s^2 = 1 \\ \psi(y)\psi(y)\psi(y) &= t^3 = 1 \\ \psi(x)\psi(y)\psi(z) &= stst = 1. \end{aligned}$$

This demonstrates the relationship between homomorphism testing and equations over a group. Note additionally that this homomorphism is also surjective, this will be a relevant point for Chapter 5.

2.2.2 Finitely Generated Abelian Groups

In this subsection, we provide the basic facts and definitions regarding the structure of abelian groups. We extend this discussion to computation problems concerning abelian groups in subsection 2.2.3. Let $n \in \mathbb{N}_+$ and denote the quotient group $\mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}_n$. We begin with some basic results on finite abelian groups.

Lemma 2.31 ([11, Theorem 9.5])**.** *$\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and is isomorphic to $\mathbb{Z}_{mn}$ if and only if* $\gcd(m, n) = 1$.

Corollary 2.32 ([11, Corollary 9.6])**.** $\prod_{i=1}^{k} \mathbb{Z}_{n_i} \cong \mathbb{Z}_{\prod_{i=1}^{k} n_i}$ *if and only if* $\gcd(n_1, \ldots, n_k) = 1$.

Remark 2.33. Thus, any $\mathbb{Z}_n$ can be rewritten uniquely (up to commutation) as $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{c_1}} \times \cdots \times \mathbb{Z}_{p_k^{c_k}}$ for $p_1, \ldots, p_k \in \mathbb{P}$ and $c_1, \cdots, c_k \in \mathbb{N}_+$.

Definition 2.34. The *rank* of a free abelian group G is the cardinality of its minimal generating set.

As we assume all groups to be finitely generated, we may also assume abelian groups to have finite rank. We now present the following normal forms for any abelian group.

Definition 2.35. Let G be a finitely generated abelian group, where $p_1, \ldots, p_r \in \mathbb{P}$ and $d, c_1, \ldots, c_r \in \mathbb{N}$, and suppose

$$G \cong \mathbb{Z}^d \times \mathbb{Z}_{p_1^{c_1}} \times \cdots \times \mathbb{Z}_{p_r^{c_r}}.$$

The right-hand side is called the *prime factor form* of G, and $p_i^{c_i}$ are the *prime factors* of G.

Similarly, let $d, a_1, \ldots, a_s \in \mathbb{N}$ with $a_i > 1$ for all i and $a_i \mid a_{i+1}$ for $1 \leq i \leq k-1$, and suppose

$$G \cong \mathbb{Z}^d \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_s}.$$

The right-hand side is called the *invariant factor form* of G, and a_i are the *invariant factors* of G.

The following well-known result demonstrates that the invariant factor form and prime factor form of a finitely generated abelian group is unique.

Theorem 2.36 (Structure Theorem [16, Theorem 2.6])**.** *Let G be a finitely generated abelian group. Then there exists a unique list $d, a_1, \ldots, a_k \in \mathbb{N}$ such that*

$$G \cong \mathbb{Z}^d \times \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_k},$$

where:

1. *$d \geq 0$ and $a_i > 1$ for all i*
2. *$a_i \mid a_{i+1}$ for $1 \leq i \leq k-1$.*

When used with Corollary 2.32, we have the following corollary.

Corollary 2.37. *Let G be a finitely generated abelian group. Then there exist unique values $p_1, \ldots, p_n \in \mathbb{P}$ and $a_1, \ldots, a_n \in \mathbb{N}_+$ such that*

$$G \cong \mathbb{Z}^d \times \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

2.2.3 $\mathbb{Z}$-modules and Integer Matrices

Let R be a ring. An R-module is a generalisation of a vector space, and $\mathbb{Z}$-modules are synonymous with abelian groups (under additive notation). Thus, abelian groups can be represented using integer matrices. We use $\mathbb{Z}$-modules to analyse the structure of abelian subgroups of larger non-abelian groups. In this section, we provide the necessary definitions and facts regarding $\mathbb{Z}$-modules.

Example 2.38. Any abelian group can be regarded as a $\mathbb{Z}$-module. For instance, the additive group $\mathbb{Z}/n\mathbb{Z}$ is a $\mathbb{Z}$-module. However, since $\mathbb{Z}$ is not a field, it is not a vector space: multiplicatively, most elements of $\mathbb{Z}$ do not have inverses other than ± 1.

To illustrate this, consider matrices in $\mathbb{R}^{3\times 3}$:

$$\begin{pmatrix} 1/3 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1/4 \end{pmatrix} \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Such inverses exist in $\mathbb{R}^{3\times 3}$, but no analogous multiplicative inverses exist in $\mathbb{Z}^{3\times 3}$, since $1/2, 1/3, 1/4 \notin \mathbb{Z}$.

This illustrates that R-modules generalise the concept of vector spaces to arbitrary rings R, where the existence of multiplicative inverses is not guaranteed.

Definition 2.39. We call a matrix with integer entries an *integer matrix*. For $m, n \in \mathbb{N}$, $\mathbb{Z}^{m\times n}$ denotes the set of all $m \times n$ integer matrices. For $M \in \mathbb{Z}^{m\times n}$ and $\ell \in \mathbb{N}$, $M|_\ell \in \mathbb{Z}^{\ell\times n}$ is the matrix consisting of the bottom ℓ rows of M. Specifically, the i-th row of $M|_\ell$ is the $(m-\ell+i)$-th row of M. An $n \times 1$ matrix is called an *n-vector*.

Definition 2.40. $\mathbb{Z}^d$ denotes the $\mathbb{Z}$-module with basis $\{e_1, \ldots, e_d\}$, where each basis element $e_i \in \mathbb{Z}^d$ is defined by $e_i = (a_1 \ \ldots \ a_d)^T$ with $a_i = 1$ and $a_j = 0$ for $j \neq i$.

The following assertion is stated without proof.

Lemma 2.41. *Every finitely generated abelian group is a $\mathbb{Z}$-module.*

Abelian groups are considered in both additive and multiplicative notation. We use multiplicative notation is used when elements are represented as words on the generators, particularly when the group is viewed as a subgroup of a larger, not necessarily abelian group (for example, virtually abelian groups); additive notation is used for the analogy with $\mathbb{Z}$-modules. The following provides a natural isomorphism between an abelian group in its multiplicative form (as a subgroup of a larger group) and its equivalent $\mathbb{Z}$-module.

Definition 2.42. Let $N = \langle x_1, \ldots, x_d \rangle$ be a free abelian group of rank d. The *natural isomorphism* $\phi\colon N \to \mathbb{Z}^d$ is defined by the map

$$\phi\colon x_i \mapsto e_i,$$

extending to the isomorphism

$$\phi\colon x_1^{c_1} \cdots x_d^{c_d} \mapsto c_1 e_1 + \cdots + c_d e_d.$$

Definition 2.43. A *$\mathbb{Z}$-linear combination* of d-vectors $u_1, \ldots, u_n \in \mathbb{Z}^d$ is any d-vector of the form

$$x = c_1 u_1 + \cdots + c_n u_n,$$

where $c_1, \ldots, c_n \in \mathbb{Z}$.

Definition 2.44. We call the set of all $\mathbb{Z}$-linear combinations of $u_1, \ldots, u_n \in \mathbb{Z}^d$ the *span* of $u_1, \ldots, u_n$, which we denote by $\operatorname{span}(u_1, \ldots, u_n)$. If $M \in \mathbb{Z}^{m\times n}$, we let $\operatorname{span}(M)$ denote the span of the *columns* of M.

For $b \in \mathbb{Z}^m$, we define $\operatorname{span}_b(M)$ to be the set of all m-vectors $x \in \mathbb{Z}^m$ of the form $x = y + b$ for some $y \in \operatorname{span}(M)$.

One powerful tool when working with integer matrices is the Smith normal form. Here, we provide the basic definitions and facts regarding the Smith normal form and show how it is used to attain a canonical form for abelian groups.

Definition 2.45 (Smith Normal Form and 1-count)**.** Let $A \in \mathbb{Z}^{m\times n}$, with $K \in \mathrm{GL}(m,\mathbb{Z})$, $L \in \mathrm{GL}(n,\mathbb{Z})$, and $D \in \mathbb{Z}^{m\times n}$ such that

$$D = \left(\begin{array}{c|c} M & 0 \\ \hline 0 & 0 \end{array}\right),$$

where M is a diagonal matrix of the form

$$M = \begin{pmatrix} \mathfrak{d}_1 & 0 & \cdots & 0 \\ 0 & \mathfrak{d}_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathfrak{d}_r \end{pmatrix}$$

for some $0 \le r \le \min(m,n)$, with each $\mathfrak{d}_i > 0$, satisfying $\mathfrak{d}_i \mid \mathfrak{d}_{i+1}$ for all $i \in [1, r-1]$, and the *rank* of D is denoted $\mathrm{rank}(D) = r$.

If $A = KDL$, then we call D the *Smith normal form* (SNF) of A, and the triple (K, D, L) an SNF-*triple*.

We denote the number of ones on the diagonal of D as $\text{1-count}(D) = \max\{i \mid \mathfrak{d}_i = 1\}$.

Lemma 2.46 ([32, Proposition 3.2])**.** *For all $A \in \mathbb{Z}^{m\times n}$, the Smith normal form D exists and is unique.*

As the Smith normal form is exists and is unique for all $A \in \mathbb{Z}^{m\times n}$, if D is the Smith normal form of A, then $\mathrm{rank}(A) = \mathrm{rank}(D)$. While the Smith normal form D of $A \in \mathbb{Z}^{m\times n}$ is unique, the accompanying general linear matrices K and L in the decomposition $A = KDL$ are not unique. The following example demonstrates this.

Example 2.47. Consider the matrix

$$A = \begin{pmatrix} 2 & 4 \\ 3 & 5 \end{pmatrix}.$$

We can compute the Smith normal form by the following row and column operations which have equivalent elementary integer matrices.

$$R_1 \to R_1 - R_2 \quad \text{is equivalent to} \quad K_1 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

$$R_2 \to R_2 + 3R_1 \quad \text{is equivalent to} \quad K_2 = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$$

$$R_1 \to -R_1 \quad \text{is equivalent to} \quad K_3 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$C_2 \to C_2 - C_1 \quad \text{is equivalent to} \quad L_1 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

so

$$\begin{aligned}
K_1A &= \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\begin{pmatrix}2 & 4\\ 3 & 5\end{pmatrix} = \begin{pmatrix}2-3 & 4-5\\ 3 & 5\end{pmatrix} = \begin{pmatrix}-1 & -1\\ 3 & 5\end{pmatrix}\\
K_2(K_1A) &= \begin{pmatrix}1 & 0\\ 3 & 1\end{pmatrix}\begin{pmatrix}-1 & -1\\ 3 & 5\end{pmatrix} = \begin{pmatrix}-1 & -1\\ -3+3 & -3+5\end{pmatrix} = \begin{pmatrix}-1 & -1\\ 0 & 2\end{pmatrix}\\
K_3(K_2(K_1A)) &= \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & -1\\ 0 & 2\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}\\
(K_3(K_2(K_1A)))L_1 &= \begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}.
\end{aligned}$$

Thus, let

$$K = K_3K_2K_1 = \begin{pmatrix}2 & -1\\ -3 & 1\end{pmatrix} \quad \text{and} \quad L = L_1 = \begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}$$

and the Smith normal form D of A is

$$D = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}.$$

So (K, D, L) form a SNF-triple .

Alternatively, let

$$K' = \begin{pmatrix}2 & 5\\ 1 & 3\end{pmatrix}, \quad L' = \begin{pmatrix}-9 & -13\\ 2 & 3\end{pmatrix}.$$

Then

$$K'D'L' = \begin{pmatrix}2 & 5\\ 1 & 3\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}\begin{pmatrix}-9 & -13\\ 2 & 3\end{pmatrix} = \begin{pmatrix}2 & 4\\ 3 & 5\end{pmatrix} = A.$$

So (K', D, L') form an alternative SNF-triple .

This shows that the Smith normal form D with 1 and 2 on the diagonal is unique, but the matrices K and L are not uniquely determined.

We now define our computational problem for the Smith normal form. While typically, for an input matrix A, the output is a diagonal matrix D as the Smith normal form, we specify the output as a triple (K, D, L) where $K \in \mathrm{GL}(m, \mathbb{Z})$ and $L \in \mathrm{GL}(n, \mathbb{Z})$. This full specification, including K and L, will be useful in later chapters.

Problem:	SNFProb: Calculating the Smith normal form triple
Input:	An integer matrix $A \in \mathbb{Z}^{m\times n}$.
Output:	A triple (K, D, L) such that $A = KDL$, where $K \in \mathrm{GL}(m, \mathbb{Z})$, $L \in \mathrm{GL}(n, \mathbb{Z})$, and D is the Smith normal form of A.

Theorem 2.48 (Complexity of the Smith Normal Form [17])**.** *On input a matrix $M \in \mathbb{Z}^{m\times n}$,* SNFProb *is computed in polynomial time.*

Remark 2.49. Prior to the work of Kannan and Bachem [17] it was not clear that computing the SNF or SNF-triple of an integer matrix is in polynomial time. In fact it was conjectured that, while the process of multiplying by elementary matrices is relatively easy, the size of intermediate values would exceed a threshold calculable in polynomial time.

Additionally, in several modern algorithms for the calculation of the Smith normal form, the computation of the matrices K and L is generally omitted. However, in [17], the authors explicitly compute these left (K) and right (L) multipliers of D and demonstrate that the process is bounded in polynomial time.

We will now show that obtaining the invariant factor form for an abelian group is polynomial time computable by using the Smith normal form (SNF).

Remark 2.50 (Elementary Linear Algebra Operations)**.** Recall that there are three types of elementary row (or column) operations that we can perform on $M \in \mathbb{Z}^{m\times n}$:

1. Add an integer multiple of one row (or column) of M to another.
2. Interchange two rows (or columns) of M.
3. Multiply a row (or column) of M by -1.

These operations correspond to replacing M with EM for some elementary matrix $E \in \mathrm{GL}(d, \mathbb{Z})$.

Definition 2.51. Let $G = \langle x_1, \ldots, x_d \mid R\rangle$ be an abelian group. Then the relations $r_1, \ldots, r_m \in R$ can be written (additively) as

$$\begin{aligned} r_1 &= c_{1,1}x_1 + \cdots + c_{1,d}x_d = 0 \\ &\vdots \quad \vdots \\ r_m &= c_{m,1}x_1 + \cdots + c_{m,d}x_d = 0, \end{aligned}$$

where $c_{i,j} = |r_i|_{x_j} - |r_i|_{x_j^{-1}}$ (that is, by counting each generator and its inverse in the relation).

Then the *relation matrix* for G is $A \in \mathbb{Z}^{m\times d}$, where

$$A = \begin{pmatrix} c_{1,1} & \cdots & c_{1,d} \\ \vdots & \ddots & \vdots \\ c_{m,1} & \cdots & c_{m,d} \end{pmatrix}.$$

Thus, for $x = (x_1 \ \ldots \ x_d)^T \in \mathbb{Z}^d$, $Ax = 0$ represents our list of relations.

Lemma 2.52. *For any abelian group G and its relation matrix M, elementary matrix operations on M are equivalent to Tietze transformations on the presentation of G.*

Proof. Let $G = \langle X \mid R\rangle$. The i-th row of M corresponds to the i-th relation in R, and the j-th column corresponds to the *count* $c_{i,j} = |r_i|_{x_j} - |r_i|_{x_j^{-1}}$ of the j-th generator. We use additive notation for matrix operations and multiplicative notation for group relations to distinguish the two contexts.

Then:

- Multiplying a row by -1 is equivalent to turning $r_i = 1$ into $r_i^{-1} = 1$.
- Interchanging two rows is equivalent to interchanging the order of two relations.
- Applying $R_i = R_i + aR_j$ for $a \in \mathbb{Z}$ is equivalent to forming the new relation $r_{ij} = r_i r_j^a = 1 \cdot 1 = 1$.
- Multiplying a column by -1 is equivalent to replacing a generator with its inverse.
- Interchanging two columns is equivalent to interchanging the order of two generators in all relations, a permitted Tietze transformation as G is abelian.
- Applying column operations $C_i = C_i + aC_j$ for $a \in \mathbb{Z}$ is equivalent to defining the new generator $g_{ij} = g_i g_j^{-a}$ and then replacing all occurrences of g_i with $g_{ij}g_j^a$, allowing us to remove the redundant generator g_i and retain g_{ij}.

□

We now define the following computation problem on finitely generated abelian groups.

Problem:	AbSTRUC: Computing abelian group structure
Input:	Two sets $X = \{x_1, \ldots, x_n\}, R = \{r_1, \ldots, r_m\}$ forming a abelian group $G = \langle X \mid R \rangle$.
Output:	$(d, \mathfrak{d}_1, \ldots, \mathfrak{d}_\ell) \in \mathbb{Z}^{\ell+1}$ for $0 \leq \ell \leq k$ such that $\mathfrak{d}_i \mid \mathfrak{d}_{i+1}$, so that $G \cong \mathbb{Z}^d \times \mathbb{Z}_{\mathfrak{d}_1} \times \cdots \times \mathbb{Z}_{\mathfrak{d}_\ell}$.

Theorem 2.53. AbSTRUC *is computed in polynomial time.*

Proof. The following procedure computes the solution:

1. Build the relation matrix $M \in \mathbb{Z}^{m \times n}$ for G.
2. Perform SNFProb with input M for the SNF-triple output of (K, D, L).
3. Let $d = m - \text{rank}(D)$ (the number of zeros on the diagonal of D), $\ell = \text{rank}(D) - 1\text{-count}(D)$, and let $\mathfrak{d}_1, \ldots, \mathfrak{d}_\ell$ be the non-1 values on the diagonal of D. Output $(d, \mathfrak{d}_1, \ldots, \mathfrak{d}_\ell)$.

Step (1) is linear on the size of the presentation, by Theorem 2.48, Step (2) is in P, and Step (3) is constant.

We now justify the procedure. By Lemma 2.52 D a relation matrix which corresponds to a presentation for G that shows

$$G \cong \mathbb{Z}^d \times \mathbb{Z}_{\mathfrak{d}_1} \times \cdots \times \mathbb{Z}_{\mathfrak{d}_\ell}.$$

Additionally, by the definition of the Smith normal form, it follows that $\mathfrak{d}_i \mid \mathfrak{d}_{i+1}$. By Lemma 2.46 this process is guaranteed. □

2.3 Group Extensions

In this section, we introduce the concept of a group extension. Informally, a group extension describes how a group G can be constructed from a normal subgroup N and the corresponding quotient group G/N. This structure is referred to as a *group extension*, and it provides a framework for analysing how complex groups are built from simpler components. We now provide the formal definition and several key facts about such extensions.

Definition 2.54 (Group Extension)**.** Let G, N and Q be groups. We say that G is an N *by* Q *extension* if G contains N as a normal subgroup and the quotient G/N is isomorphic to Q. This relationship is represented by the short exact sequence

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow 1,$$

where ι is injective, π is surjective, and $\text{im}(\iota) = \ker(\pi)$.

Definition 2.55. Let G, H, Q be groups. H is a N by Q *group extension* when it contains N as a normal subgroup such that the quotient group G/N is isomorphic to Q. This is generally represented by the short exact sequence

$$1 \to N \xrightarrow{\iota} H \xrightarrow{\pi_Q} Q \to 1$$

where ι is an injective homomorphism, π_Q is a surjective homomorphism, and $\text{im}(f) = \ker(g)$. This sequence describes H as an extension of N by Q.

Definition 2.56. Let G be a group and H a subgroup of G. A *transversal set* (or *set of coset representatives*) for H in G is a subset $T \subseteq G$ such that:

- every right (or left) coset Hg of H in G contains exactly one element of T,

- the union of Hg for all $g \in T$ is G.

A *transversal map* for H in G is a function $s\colon G/H \to G$ that assigns to each coset $Hg \in G/H$ a unique representative $s(Hg) \in T$.

Remark 2.57. In the context of a group extension, where G is an N by Q extension, we define a transversal map $s\colon Q \to G$ directly, without explicitly noting the isomorphism between Q and G/N. We assume the transversal map s is always chosen so that $s(1_Q) = 1_G$.

Definition 2.58. Let G be a group and H a subgroup of G, with a fixed transversal map $s\colon Q \to G$. The *projection* of g onto N, denoted $\pi_{N,s}\colon G \to N$, is defined by $\pi_{N,s}(g) = n$ when g is expressed in the form $g = ns(q)$. Where the context is clear, we denote this projection as π_N.

For any element $g \in G$, the *extension normal form* of g is given by the product $g = ns(q)$ for some $n \in N$ and $q \in Q$.

Lemma 2.59. *Let G be an N by Q extension, and $s\colon Q \to G$ be a fixed transversal map. The extension normal form is unique with respect to the given s.*

Proof. Let $n_1, n_2 \in N$ and $q_1, q_2 \in Q$. Suppose for some $g \in G$ that $g = n_1 s(q_1) = n_2 s(q_2)$. Then, it follows that

$$\begin{aligned} n_1 n_2^{-1} &= s(q_2)s(q_1)^{-1} \\ &= s(q_2 q_1^{-1}) \\ &= s(q), \end{aligned}$$

where $q = q_2 q_1^{-1} \in Q$.

Since N is a normal subgroup, we have $s(q) \in N$, and the only element $q \in Q$ such that $s(q) \in N$ is the identity element 1_Q. Hence, it follows that $n_1 n_2^{-1} = 1_N$, which implies $n_1 = n_2$ and $q_1 = q_2$. □

Definition 2.60. For a group G and two elements $x, y \in G$, the *left conjugation action* of x on y is denoted by ${}^x y$ and defined as ${}^x y = xyx^{-1}$.

Since N is a normal subgroup of H, each $s(q)$ acts on N by conjugation as an inner automorphism. Define a map $\theta_s\colon Q \to \mathrm{Aut}(N)$ by $\theta_s(q) = {}^{s(q)}n$, describing this action. Additionally, because N is normal, for $q_1, q_2 \in Q$, we have

$$Ns(q_1)Ns(q_2) = Ns(q_1)s(q_2),$$

so $s(q_1)s(q_2) = ns(q_1q_2)$ for some $n \in N$. Hence,

$$s(q_1)s(q_2)s(q_1q_2)^{-1} \in N.$$

Define a map $f_s\colon Q \times Q \to N$ by

$$f_s(q_1, q_2) = s(q_1)s(q_2)s(q_1q_2)^{-1}.$$

Definition 2.61. Let G be an N by Q extension. The *extension data* with respect to a fixed transversal map s for G is the pair (θ_s, f_s), where:

- $\theta_s\colon Q \to \mathrm{Aut}(N)$ describes the conjugation action of Q on N
- $f_s\colon Q \times Q \to N$ satisfies $f_s(q_1, q_2) = s(q_1)s(q_2)s(q_1q_2)^{-1}$

for some transversal map $s\colon Q \to G$.

In the case where s is a homomorphism, we have $s(q_1)s(q_2)s(q_1q_2)^{-1} = 1_N$, and we write $f_s = f_1$.

Remark 2.62. If Q is finite and N is finitely generated, then (θ_s, f_s) has a finite description.

Remark 2.63. Given extension data (θ_s, f_s) for an N by Q extension H with transversal s and $g_1, g_2 \in G$ where $g_i = n_i s(q_i)$, the normal form of g_1g_2 can be calculated as follows:

$$\begin{aligned} g_1g_2 &= n_1 s(q_1) n_2 s(q_2) \\ &= n_1 s(q_1) n_2 s(q_1)^{-1} s(q_1) s(q_2) \\ &= \left[n_1 ({}^{s(q_1)}(n_2)) f_s(q_1, q_2)\right] s(q_1q_2). \end{aligned}$$

Definition 2.64. Let G be a N by Q extension with data (θ_s, f_s). For $k \geq 2$, define $\tilde{f}_k\colon Q^k \to N$ by

$$\tilde{f}_k(a_1, \ldots, a_k) = f_s(a_1, a_2) f_s(a_1a_2, a_3) \cdots f_s(a_1 \cdots a_{k-1}, a_k).$$

Example 2.65. Let G be a group represented by an N by Q extension, with data (θ_s, f_s), and Q is a finite group.

Let $w = v_1 \cdots v_n$ be a word over the generators of G. As every element $g \in G$ can be written as $g = ns(q)$ for $n \in N$ we can write

$$w = v_1 \cdots v_m \quad \text{as} \quad n_1 s(q_1) \cdots n_k s(q_k)$$

for $n_1, \ldots, n_k$ and $q_1, \ldots, q_k \in Q$. Following the calculations of Remark 2.63 we have

$$\begin{aligned} & n_1 s(q_1) n_2 s(q_2) \cdots n_\ell s(q_\ell) \cdots n_k s(q_k) \\ &= n_1 ({}^{s(q_1)}n_2)\, (s(q_1)s(q_2)) \cdots n_\ell s(q_\ell) \cdots n_k s(q_k) \\ &= \quad \vdots \\ &= n_1 ({}^{s(q_1)}n_2) \cdots ({}^{s(q_1)\cdots s(q_{\ell-1})}n_\ell)\, (s(q_1) \cdots s(q_\ell)) \cdots n_k s(q_k) \\ &= \quad \vdots \\ &= \left[n_1 ({}^{s(q_1)}n_2) \cdots ({}^{s(q_1)\cdots s(q_{\ell-1})}n_\ell) \cdots ({}^{s(q_1)\cdots s(q_{k-1})}n_k)\right] (s(q_1) \cdots s(q_k)). \end{aligned}$$

As $s(q_i)s(q_j) = f_s(q_i, q_j)s(q_iq_j)$ so the sequence

$$\begin{aligned} & s(q_1)s(q_2)s(q_3) \cdots s(q_k) \\ &= f_s(q_1, q_2) s(q_1q_2) s(q_3) \cdots s(q_k) \\ &= f_s(q_1, q_2) f_s(q_1q_2, q_3) s(q_1q_2q_3) \cdots s(q_k) \\ &= \quad \vdots \\ &= f(q_1, q_2) f_s(q_1q_2, q_3) \cdots f_s(q_1 \cdots q_{k-1}, q_k) s(q_1 \cdots q_k) \end{aligned}$$

and it follows

$$\begin{aligned} & \left[n_1 ({}^{s(q_1)}n_2) \cdots ({}^{s(q_1)\cdots s(q_{k-1})}n_k)\right] (s(q_1) \cdots s(q_k)) \\ &= \left[n_1 ({}^{s(q_1)}n_2) \cdots ({}^{s(q_1)\cdots s(q_{k-1}))}n_k)\right] f_s(q_1, q_2) \cdots f_s(q_1 \cdots q_{k-1}, q_k) s(q_1 \cdots q_k) \\ &= \left[n_1 ({}^{s(q_1)}n_2) \cdots ({}^{s(q_1)\cdots s(q_{k-1}))}n_k)\right] \tilde{f}_k(q_1, \ldots, q_k) s(q_1 \cdots q_k) =_G w. \end{aligned}$$

2.3.1 Semi-direct product and restrictions

Semi-direct products can be viewed as extensions with additional constraints and can be used as an intermediate step when solving difficult problems by limiting extensions to semi-direct products. Here, we outline the basics of semi-direct products.

Definition 2.66. A group G is a *semidirect product* of N by Q, denoted $G = N \rtimes_\theta Q$, if:

- N is a normal subgroup of G
- Q is a subgroup of G
- $N \cap Q = \{1\}$
- $NQ = G$
- There exists a homomorphism $\theta : Q \to \mathrm{Aut}(N)$, called the conjugation action of Q on N, such that for all $q \in Q$ and $n \in N$,

$$\theta(q)(n) = {}^q n.$$

Lemma 2.67. *Let G be an N by Q extension. There exists a transversal map $s\colon Q \to G$ that is a homomorphism if and only if G is a semidirect product of N and Q.*

Proof. Note that when $s\colon Q \to G$ is a homomorphism, $f_s\colon N \times N \to Q$ is defined by $(n_1, n_2) \mapsto 1_Q$ for all $n_1, n_2 \in N$. Thus, $f_s = f_1$.

Assume G is described by the semidirect product $N \rtimes_\theta Q$. Then we can construct an N by Q extension for G with extension data (θ_s, f_1), where s is a homomorphism.

Conversely, if G is an N by Q extension with a transversal map s as a homomorphism, then $s(Q)$ forms a subgroup in G. Thus, for all elements $g \in G$, we can uniquely write $g = ns(q)$ for some $n \in N$ and $q \in Q$.

Since $\pi_Q(g) = q$, by the following calculation:

$$\begin{aligned}\pi(s(q)) &= \pi_Q(s(\pi_Q(g))) \\ &= \pi_Q \circ s \circ \pi_Q(g) \\ &= \pi_Q(g),\end{aligned}$$

we have $\pi_Q(g) = \pi_Q(s(q))$, and hence $\pi_Q(g) = \pi_Q(n)\pi_Q(s(q))$. It follows that $\pi(n) \in \ker(\pi_Q)$. Let $N = \ker(\pi_Q)$; then N is a normal subgroup in G, and $G = Ns(Q)$.

Assume now that $x \in N \cap s(Q)$. Then there exist $n \in N$ and $q \in Q$ such that $x = n = s(q)$. As $n \in \ker(\pi_Q)$, we have $\pi_Q(n) = 1_Q = \pi_Q(s(q))$, which implies $q = 1_Q$. It follows that $N \cap s(Q) = \{1\}$, satisfying all conditions for $G \cong N \rtimes_\theta Q$. □

Remark 2.68 (Notation)**.** Thus, if $G \cong N \rtimes_\theta Q$, it is also an N by Q extension with data (θ_s, f_s). Here, we assume s is the transversal that is a homomorphism, so instead, we write θ_s as θ and f_s as f_1, that is, the data given for a semi-direct product is (θ, f_1).

Remark 2.69. In general, it is not necessary for there to exist a transversal map $s\colon Q \to G$ that is also a homomorphism. Consider the following group:

$$G = \left\langle x, y, t \mid [x, y] = 1, t^2 = x, {}^t a = a^{-1}, {}^t y = y^{-1} \right\rangle.$$

Here $\langle x, y\rangle \cong \mathbb{Z}^2$, and $G/\langle x, y\rangle \cong C_2 = \langle q \mid q^2 = 1\rangle$. This forms a $\mathbb{Z}^2$ by C_2 extension with a transversal map $s\colon Q \to G$ defined by

$$s\colon \begin{cases} 1_Q & \mapsto 1_G \\ q & \mapsto t. \end{cases}$$

Thus, we have extension data (θ_s, f_s), where $\theta_s \colon Q \to \mathrm{Aut}(N)$ can be given by the finite description on the generators x, y such that for all $n \in N$, the map is defined by:

$$\theta_s \colon \begin{cases} 1_Q \mapsto {}^{s(1_Q)}n & : \begin{cases} x \mapsto {}^{s(1_Q)}x = {}^{1_G}x = x \\ y \mapsto {}^{s(1_Q)}y = {}^{1_G}y = y, \end{cases} \\ q \mapsto {}^{s(q)}n & : \begin{cases} x \mapsto {}^{s(q)}x = {}^{t}x = x^{-1} \\ y \mapsto {}^{s(q)}y = {}^{t}y = y^{-1}. \end{cases} \end{cases}$$

The function $f_s \colon Q \times Q \to N$ is defined by:

$$f_s \colon \begin{cases} (1,1) & \mapsto 1_N \\ (1,q) & \mapsto 1_N \\ (q,1) & \mapsto 1_N \\ (q,q) & \mapsto s(q)s(q)s(q^2)^{-1} = t^2 = x. \end{cases}$$

Thus, $f_s \neq f_1$. Note that in general $f(1,1) = f(1,q) = f(q,1) = 1_N$, and so does not need to be provided by the extension data.

2.3.2 Virtually Abelian Groups

Virtually abelian groups are a central focus of this thesis. Here, we establish the fundamental properties and demonstrate that they can be viewed as free abelian by finite extensions.

Definition 2.70. A group is *virtually abelian* if it has a finite index subgroup that is abelian.

Example 2.71. Consider $G \cong \mathbb{Z}^2 \times D_6$, where D_6 is the dihedral group of order 6. In this case, $H \cong \mathbb{Z}^2$ is a subgroup of G with finite index, having 6 unique cosets (that is, $|G/H| = 6$). In general, H does not need to be normal in G.

Definition 2.72. Let G be a group and X a non-empty subset of G. The *normal core* of X in G, denoted $\mathrm{core}_G(X)$, is the intersection of all normal subgroups of G that are contained in X. If H is a subgroup of G, then $\mathrm{core}_G(H) = \bigcap_{g \in G} gHg^{-1}$.

Lemma 2.73. *Let H be a finite index subgroup of G. Then $\mathrm{core}_G(H)$ is a finite index normal subgroup of G.*

Proof. Let $X = \{Ht_1, Ht_2, \ldots, Ht_n\}$ be the set of right cosets of H in G. Define the group action $X \times G \to X$ by $(Ht)g = H(tg)$, this group action can be associated with a permutation σ_g such that:

$$\sigma_g \colon Ht_i \mapsto Ht_j$$

where $H(t_i g) = Ht_j$. Then σ_g is a permutation of X, so $\sigma_g \in S_X$. This gives rise to the homomorphism:

$$\varphi \colon G \to S_X, \quad g \mapsto \sigma_g.$$

We claim that $\ker(\varphi)$ is equal to $\mathrm{core}_G(H)$. To show this, consider $x \in \ker(\varphi)$. Then for all x,

$$\begin{aligned} Ht_i x &= Ht_i, \quad \text{since } \sigma_x = 1_{S_X} \\ t_i x &= H^{-1} Ht_i = Ht_i \\ x &= t_i^{-1} Ht_i. \end{aligned}$$

Thus, $x \in \text{core}_G(H)$, and so $\ker(\varphi) \subseteq \text{core}_G(H)$.

Conversely, consider $x \in \text{core}_G(H)$. Then $x = t_i^{-1} h t_i$ for some $h \in H$. Taking the coset Ht_i, we have

$$\begin{aligned} \sigma_x(Ht_i) &= Ht_i x \\ &= Ht_i(t_i^{-1} h t_i) \\ &= Hht_i \\ &= Ht_i. \end{aligned}$$

Hence, $Ht_i x = Ht_i$, so $x \in \ker(\varphi)$, and it follows that $\ker(\varphi) = \text{core}_G(H)$.

Since $\ker(\varphi)$ is normal, it remains to show that $\ker(\varphi)$ is of finite index in G. By the first isomorphism theorem, we have

$$G/\ker(\varphi) \cong Q,$$

where Q is a subgroup of S_X. Since X is finite, S_X is a finite group, so Q is a finite group. Thus, $\ker(\varphi) = \text{core}_G(H)$ is of finite index in G, and the index is $|Q|$.

□

Lemma 2.74 ([26, p. 4.2.3.])**.** *A subgroup of an abelian group is abelian.*

Lemma 2.75. *Every virtually abelian group is an N by Q extension where N is free abelian and Q is finite.*

Proof. Let H be a finite index abelian subgroup of G, by Theorem 2.36 there exists a free abelian subgroup of finite rank and finite index in G. By Lemma 2.73 taking the normal core of this free abelian subgroup, we obtain a finite index normal subgroup N of G, by Lemma 2.74 this subgroup is free abelian. Therefore, G is an N by Q extension where Q is finite. □

In light of this fact, virtually abelian groups G are viewed as N by Q extensions, where N is a free abelian normal subgroup, and Q is isomorphic to the finite quotient group G/N.

Lemma 2.76. *Let G be an N by Q extension. If N is abelian and s_1, s_2 are two transversal maps $Q \to G$, then for all $q \in Q$ and $n \in N$, we have*

$${}^{s_1(q)}n = {}^{s_2(q)}n.$$

Proof. Note that $Ns_1(q) = Ns_2(q)$, so $s_2(q)s_1(q)^{-1} \in N$. Using the fact that N is abelian, we have

$$\begin{aligned} {}^{s_1(q)}n &= s_1(q) n s_1(q)^{-1} \\ &= s_1(q) n (s_1(q)^{-1} s_2(q)) s_2(q)^{-1} \\ &= (s_1(q) s_1(q)^{-1}) s_2(q) n s_2(q)^{-1} \\ &= {}^{s_2(q)}n. \end{aligned}$$

□

Remark 2.77 (Notation)**.** Let G be an N by Q extension, with extension data (θ_s, f_s). If N is abelian, then the choice of transversal map does not affect the conjugation action. In the case where $f_s = f_1$ and we have a split extension, we further assume that the chosen transversal is a homomorphism.

In light of this, when G is an N by Q extension, and either $G \cong N \rtimes_\theta Q$ or N is abelian, we denote the conjugation action θ_s as θ and so the extension data is (θ, f_s).

Restricted Extensions

In this subsection we define a special class of extensions, this class of extensions will see use in Chapter 4 and can be considered a generalisation of direct products and virtually cyclic groups.

Let $N \cong C_\infty = \langle x \rangle$, the infinite cyclic group. For some $\varphi \in \mathrm{Aut}(N)$

$$\varphi(x) = x^a$$

and there exists x^b such that $\varphi(x^b) = x$, so $x = \varphi(x^b) = \varphi(x)^b = x^{ab}$. Thus $ab = 1$ and it follows $i = j = \pm 1$.

Then $\mathrm{Aut}(\langle x \rangle) = \{\varphi_1, \varphi_2\}$ where φ_1 is the trivial automorphism $x \mapsto x$ and φ_2 is the automorphism defined by $x \mapsto x^{-1}$. We now generalise virtually cyclic groups by defining the following class

Definition 2.78. Define $\mathsf{SpecialExt}$ to be the class of groups which are N by Q extensions which satisfy the following conditions

- N is abelian, Q is finite
- there exists a transversal map $s\colon Q \to G$ and a subset $\mathcal{I} \subseteq Q$, so that:
  - ${}^{q}n = n^{-1}$ for all $n \in N$ when $q \in \mathcal{I}$
  - ${}^{q}n = n$ for all $n \in N$ when $q \in Q \setminus \mathcal{I}$.

In other words, the conjugation action $\theta_s\colon Q \to \mathrm{Aut}(N)$ is completely determined by the subset $\mathcal{I}$:

$$\theta_s(q) = \begin{cases} n \mapsto n^{-1} & q \in \mathcal{I} \\ n \mapsto n & q \in Q \setminus \mathcal{I}. \end{cases}$$

Remark 2.79. It is natural to assume N to be abelian, because if $\mathcal{I} \neq \varnothing$ then N is implied to be abelian.

Let $G \in \mathsf{SpecialExt}$ be an N by Q extension, where N is not required to be abelian. If $\mathcal{I} \neq \varnothing$, then the group is virtually abelian (N is abelian). On the other hand, if $\mathcal{I} = \varnothing$, then $G \cong N \times Q$.

The case where $\mathcal{I} = \varnothing$ is straightforward. For the alternative case, assume $\mathcal{I} \neq \varnothing$. For all $n_1, n_2 \in N$ and some $q \in \mathcal{I}$, we have

$${}^{s(q)}n_1 n_2 = (n_1 n_2)^{-1}.$$

Additionally, we have

$$\begin{aligned} {}^{s(q)}(n_1 n_2) &= s(q)(n_1 n_2)s(q)^{-1} \\ &= s(q)(n_1)s(q)^{-1}s(q)(n_2)s(q)^{-1} \\ &= n_1^{-1}n_2^{-1} \\ &= (n_2 n_1)^{-1}. \end{aligned}$$

Therefore, $n_1 n_2 = n_2 n_1$, and so N is abelian.

Both virtually cyclic groups and groups of the form $\mathbb{Z}^d \times Q$ for $d \in \mathbb{Z}$, where Q is finite, are contained in the class of $\mathsf{SpecialExt}$. We now define the following subclass of semidirect products, which is also contained in $\mathsf{SpecialExt}$.

Definition 2.80. Define $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$ to be the subclass of $\mathsf{SpecialExt}$ having extension data $(\mathcal{I}, f_1)$.

Example 2.81. An example of a group in $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$, but is not virtually (infinite) cyclic or the direct product of an abelian group by a finite group, is

$$H = \left\langle a, b, p, q \mid [a, b],\ p^2,\ q^2,\ [p, q],\ ({}^p a)a^{-1},\ ({}^p b)b^{-1},\ ({}^q a)a,\ ({}^q b)b \right\rangle$$

a semidirect product of $\mathbb{Z}^2$ and the Klein 4-group $C_2 \times C_2 = \langle p, q \rangle$. Here, $\mathcal{I} = \{q, pq\}$.

2.4 Group Classes

In this subsection, we provide a comprehensive list of the classes of groups considered throughout this thesis, along with their input data. We begin with the following result, which is a consequence of the works of Adian [1] and Rabin [23].

Theorem 2.82 ([28, Theorem 12.32])**.** *Given a finitely presented group G, the following decision problems are undecidable, whether G is:*

1. *trivial.*
2. *abelian.*
3. *nilpotent.*
4. *free.*
5. *torsion-free (having no elements of finite order).*
6. *residually finite.*
7. *(has) a decidable word problem.*
8. *(has) a decidable isomorphism problem.*

Then the promise of the class in which our group resides is a necessary input. Additionally, suppose that $\mathsf{EPI}(\mathcal{D}, \mathcal{T})$ is decidable for some finitely presented $\mathcal{D}$ and $\mathcal{T}$, where $\mathcal{T}$ along with its finite presention is given with the additional promise that it belongs to some fixed class. Let $G = \langle x \mid x \rangle$ be a group in $\mathcal{D}$, the trivial group. If for some $H \in \mathcal{T}$ there exists an epimorphism $G \to H$, then H must also be the trivial group. However, this contradicts the first item of Theorem 2.82. Thus, in general, we do not give our target group as a finite presentation. Rather, along with the promise that the group belongs to a fixed class, we also provide data that is natural for that class, given as follows.

Finitely Presented Groups. Let $\mathsf{FinPres}$ denote the class of finitely presented groups. A group $G \in \mathsf{FinPres}$ is given as a pair of sets (X, R), where G is described by the presentation $\langle X \mid R \rangle$.

Finite Groups. Let Fin denote the class of finite groups. A group $Q \in \mathsf{Fin}$ is specified by its multiplication table, with an input size of $|Q|^2$.

Free Groups. Let Free denote the class of free groups. A group $G \in \mathsf{Free}$ is given by an integer $d \in \mathbb{N}_+$ such that $G \cong F_d$.

Abelian Groups. Let Ab denote the class of abelian groups. A group $G \in \mathsf{Ab}$ is specified by a presentation $\langle X \mid R \rangle$ together with the assumption (or promise) that G is abelian. By $\mathsf{AbSTRUC}$, we can compute the invariant factor decomposition of any finitely generated abelian group from its presentation. We denote by FreeAb the subclass of Ab consisting of *free abelian* groups, which are isomorphic to $\mathbb{Z}^d$ and are typically specified by their rank $d \in \mathbb{N}$ rather than by a presentation.

Virtually Abelian Groups. Let VAb denote the class of virtually abelian groups. In this work, we consider only the *infinite* virtually abelian groups, that is, groups with a free abelian normal subgroup of finite index. Such groups can be described by a tuple (d, Q, θ, f_s), where $d \in \mathbb{N}_+$ specifies a free abelian subgroup $N \cong \mathbb{Z}^d$ of rank d, Q is a finite quotient group given by its multiplication table, and (θ, f_s) are the extension data describing G as an N by Q extension.

Virtually Abelian Group Subclasses. By Lemma 2.75, every virtually abelian group G contains a finite-index normal free abelian subgroup $N \cong \mathbb{Z}^d$ with finite quotient $Q \cong G/N$. Hence, throughout we specify virtually abelian targets by their extension data (d, Q, θ, f), where $d \in \mathbb{N}_+$ is the rank of N, Q is finite, and (θ, f) describe G as an N by Q extension. In particular, we do *not* present N via a general abelian (torsion–free×torsion) decomposition, since the torsion can be absorbed into the finite quotient Q. The following subclasses are of particular interest:

- $\mathsf{Ab} \times \mathsf{Fin}$ denotes the class of groups described by a direct product of $N \times Q$, with data $(d, Q, \mathcal{I}, f_1)$ and $\mathcal{I} = \varnothing$.
- $\mathsf{Ab} \rtimes_\theta \mathsf{Fin}$ denotes the class of groups described by semi-direct product of $N \rtimes_\theta Q$, with data (d, Q, θ, f_1).
- VCyc denotes the class of virtually (infinite) cyclic groups, with data $(1, Q, \mathcal{I}, f_s)$.
- $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$ denote the subclass of virtually abelian groups with restricted conjugation action as described in subsection 2.3.2, with data $(d, Q, \mathcal{I}, f_1)$.

3 Integer Matrix Problems

In this chapter, we show that the two decision problems for matrices over integers MatrixSubspanA and MatrixSubspanB are in P. The motivation for these problems will become clear when we apply them to epimorphism testing in the following chapter, and so we prove the following.

Theorem A. MatrixSubspanA *and* MatrixSubspanB *are in* P*.*

The method relies heavily on the Smith normal form of integer matrices. However, it does not depend on the structure theorem for finitely generated abelian groups. This is counterintuitive, as the structure theorem is often used in conjunction with the Smith normal form to analyse the structure of abelian groups. The results will be used to establish the complexity of specific epimorphism problem targets in Chapter 4.

We begin by extending the notation for $\mathbb{Z}$-linear combinations to $\mathbb{Z}_p$-linear combinations. Note that when $p \in \mathbb{P}$, a $\mathbb{Z}_p$-module corresponds to a traditional vector space. Although matrices and vectors over $\mathbb{Z}_p$ appear briefly in certain intermediary lemmas, we do not perform explicit calculations over these fields.

Notation. If $A \in \mathbb{Z}^{m\times n}$, let $[A]_p \in \mathbb{Z}_p^{m\times n}$ denote the matrix with the i,j-th entry as

$$(a_{i,j} \mod p)_{i\in[1,m],j\in[1,n]}$$

where $a_{i,j}$ is the i,j-th entry of A.

For $B \in \mathbb{Z}_p^{m\times n}$, $\mathrm{span}_{\mathbb{Z}_p}(B)$ is the set of all $\mathbb{Z}_p$-linear combinations of the columns of B. That is,

$$\mathrm{span}_{\mathbb{Z}_p}(B) = \left\{ \sum_{i=1}^{n} c_i b_i : c_i \in \mathbb{Z}_p, b_i \text{ are columns of } B \right\}.$$

3.1 Basic Calculations

This section presents preliminary results for integer matrices. We start by outlining several well-known computation processes which are polynomial time, these will serve as a foundation for the computations that follow.

Lemma 3.1. *The following tasks can be performed in polynomial time*

1. *Given integers $a_1, \ldots, a_n \in \mathbb{Z}$, compute $\gcd(a_1, \ldots, a_n)$.*
2. *Given a matrix $A \in \mathrm{GL}(n, \mathbb{Z})$, compute its inverse A^{-1}.*

Proof. For Item 1, the problem of finding the gcd reduces to the Euclidean algorithm, which is in polynomial time; see, for example, [34].

For Item 2, the problem of finding the inverse of an integer matrix is also polynomial time; see, for example, [35]. □

Using the above results with the Smith normal form process, we have the following

Lemma 3.2. *The following procedure can be achieved in polynomial time:*
On input $A \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}^m$

1. *Decide whether there exists $x \in \mathbb{Z}^n$ such that $Ax + b = 0$ (returning 'Yes' or 'No').*
2. *If 'Yes', return $u_1, \ldots, u_k \in \mathbb{Z}^n$ and $c \in \mathbb{Z}^n$ such that for $x \in \mathbb{Z}^n$, $Ax + b = 0$ if and only if $x \in \mathrm{span}_c(u_1, \ldots, u_k)$.*

Proof. The following procedure solves the problem

1. Call SNFProb and output SNF-triple (K, D, L) of A, let $\mathrm{rank}(D) = r$.
2. Let $\mathfrak{b} = -K^{-1}b$, with i-th entry $\mathfrak{b}_i$, and let $\mathfrak{d}_i$ be the i-th non-zero diagonal entry of D.
   - If $\mathfrak{b}_i/\mathfrak{d}_i \notin \mathbb{Z}$ for some $i \in [1, r]$, output 'No'. If $\mathfrak{b}_i \neq 0$ for some $i \in [r+1, m]$, output 'No'.
   - Otherwise, return 'Yes' and assume that $\mathfrak{b}_i/\mathfrak{d}_i \in \mathbb{Z}$ for all $i \in [1, r]$ and $\mathfrak{b}_i = 0$ for all $i \in [r+1, m]$.
3. Denote the i, j-th element of L^{-1} as $l_{i,j}$, and let u_i be the $(r+i)$-th column of L^{-1} for $i \in [1, n-r]$. Set $c_i = \sum_{j=1}^{r} l_{i,j}\mathfrak{b}_j/\mathfrak{d}_j$ for $i \in [1, n]$. Define $k = n - r$ and $c = (c_1 \ \cdots \ c_n)^T$. Output $u_1, \ldots, u_k \in \mathbb{Z}^n$ and $c \in \mathbb{Z}^n$.

By Theorem 2.48 Step (1) is polynomial time, and by Lemma 3.1 Steps (2) and (3) require the inverse of an integer matrix, which is polynomial time. Basic calculations with integers given as binary are also polynomial time, so the entire procedure is polynomial time.

We now justify the correctness of the procedure. We wish to solve $Ax - b = 0$, where $A = KDL$ and $x \in \mathbb{Z}^n$, so

$$DLx - K^{-1}b = 0.$$

Let $y = Lx \in \mathbb{Z}^n$ and $-K^{-1}b = \mathfrak{b} \in \mathbb{Z}^m$, so our equation becomes

$$Dy = \begin{pmatrix} \mathfrak{d}_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & \mathfrak{d}_r & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_r \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_r \\ \vdots \\ \mathfrak{b}_m \end{pmatrix} = \mathfrak{b}. \tag{3.1}$$

From Eq. (3.1) it is clear that for a solution to exist we need $y_i = \mathfrak{b}_i/\mathfrak{d}_i$ for $i \in [1, r]$ and $\mathfrak{b}_{r+1}, \ldots, \mathfrak{b}_m = 0$, and since $y \in \mathbb{Z}^n$, we have the condition to return 'Yes' or 'No' in Step (2).

If 'Yes', let $a_i = \mathfrak{b}_i/\mathfrak{d}_i \in \mathbb{Z}$ for $i \in [1, r]$, so

$$\mathfrak{b} = \begin{pmatrix} a_1\mathfrak{d}_1 & \cdots & a_r\mathfrak{d}_r & 0 & \cdots & 0 \end{pmatrix}^T$$

and in such a case, a solution has the form

$$y = \begin{pmatrix} a_1 & \cdots & a_r & t_{r+1} & \cdots & t_n \end{pmatrix}^T$$

for any $t_i \in \mathbb{Z}$, $i > r$.

Recall that we write $l_{i,j}$ for the i,j-th entry of L^{-1}. Since $Lx = y$, we have

$$\begin{aligned} x &= L^{-1}y \\ &= \begin{pmatrix} l_{1,1} & \cdots & l_{1,n} \\ \vdots & \ddots & \vdots \\ l_{n,1} & \cdots & l_{n,n} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_r \\ t_{r+1} \\ \vdots \\ t_n \end{pmatrix} \\ &= \begin{pmatrix} l_{1,1}a_1 + \cdots + l_{1,r}a_r + l_{1,r+1}t_{r+1} + \cdots + l_{1,n}t_n \\ \vdots \\ l_{n,1}a_1 + \cdots + l_{n,r}a_r + l_{n,r+1}t_{r+1} + \cdots + l_{n,n}t_n \end{pmatrix}. \end{aligned}$$

Let $c_i = \sum_{j=1}^{r} l_{i,j}a_j$ for $i \in [1,n]$, then

$$x = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} + t_{r+1}\begin{pmatrix} l_{1,r+1} \\ \vdots \\ l_{n,r+1} \end{pmatrix} + \cdots + t_n \begin{pmatrix} l_{1,n} \\ \vdots \\ l_{n,n} \end{pmatrix}.$$

Setting u_i to be the $(n-r+i)$-th column of L^{-1} for $i \in [1,k]$, we have shown that for $x \in \mathbb{Z}^n$, $Ax - b = 0$ if and only if $x \in \operatorname{span}_c(u_1, \ldots, u_k)$. □

Lemma 3.3. *Let $U \in \mathbb{Z}^{n\times k}$, $b \in \mathbb{Z}^n$, $\ell \in \mathbb{Z}$, and $c = (b_{n-\ell+1} \ \cdots \ b_n)^T$. Then the following are equivalent*

1. *There exists a matrix $V \in \mathbb{Z}^{n\times d}$ such that $\operatorname{span}((V|_\ell)^T) = \mathbb{Z}^d$ and each column of V lies in $\operatorname{span}_b(U)$.*
2. *There exists a matrix $W \in \mathbb{Z}^{\ell\times d}$ such that $\operatorname{span}(W^T) = \mathbb{Z}^d$ and each column of W lies in $\operatorname{span}_c(U|_\ell)$.*

Proof. Assume there exists a matrix

$$V = \begin{pmatrix} v_1 & \cdots & v_d \end{pmatrix} \in \mathbb{Z}^{n\times d}$$

such that $\operatorname{span}((V|_\ell)^T) = \mathbb{Z}^d$ and each column v_i of V lies in $\operatorname{span}_b(U)$.

For each $i \in [1,d]$, let $w_i \in \mathbb{Z}^\ell$ be the last ℓ entries of v_i and set

$$W = \begin{pmatrix} w_1 & \cdots & w_d \end{pmatrix} \in \mathbb{Z}^{\ell\times d},$$

so $W = V|_\ell$. Since $v_i \in \operatorname{span}_b(U)$, it follows that $w_i \in \operatorname{span}_c(U|_\ell)$, and thus $\operatorname{span}(W^T) = \operatorname{span}((V|_\ell)^T) = \mathbb{Z}^d$.

Conversely, assume there exists a matrix

$$W = \begin{pmatrix} w_1 & \cdots & w_d \end{pmatrix} \in \mathbb{Z}^{\ell\times d}$$

such that $\operatorname{span}(W^T) = \mathbb{Z}^d$ and each column w_i of W lies in $\operatorname{span}_c(U|_\ell)$.

For each $i \in [1,d]$, there exist $\alpha_{i,j} \in \mathbb{Z}$ such that

$$w_i = c + \alpha_{i,1}\tilde{u}_1 + \cdots + \alpha_{i,k}\tilde{u}_k,$$

where $\tilde{u}_j \in \mathbb{Z}^\ell$ are the columns of $U|_\ell$. Define $v_i \in \mathbb{Z}^n$ to be

$$v_i = b + \alpha_{i,1}u_1 + \cdots + \alpha_{i,k}u_k,$$

where $u_j \in \mathbb{Z}^n$ are the columns of U.

Then the matrix

$$V = \begin{pmatrix} v_1 & \cdots & v_d \end{pmatrix}$$

satisfies $V|_\ell = W$. Therefore, $\text{span}((V|_\ell)^T) = \text{span}(W^T) = \mathbb{Z}^d$, and each column of V lies in $\text{span}_b(U)$ by construction. □

3.2 Solving Matrix Problem A

In this section, we demonstrate that MatrixSubspanA can be decided in polynomial time. Recall, the problem is defined as follows:

Problem:	MatrixSubspanA
Input:	A triple (A, d, ℓ) where A is an $m \times n$ integer matrix, $d, \ell \in \mathbb{N}$ with $\ell \in [0, n-1]$.
Question:	Do there exist integer n-vectors $v_1, \ldots, v_d$ such that $Av_i = 0$ for $i \in [1, d]$ and for the $n \times d$ matrix V whose columns are $v_1, \ldots, v_d$, $\text{span}((V|_\ell)^T) = \mathbb{Z}^d$?

To begin, we present two simple observations.

Lemma 3.4. *Let R be either $\mathbb{Z}$ or $\mathbb{Z}_p$, $p \in \mathbb{P}$, $A, B \in R^{m\times n}$ and $L \in \text{GL}(n, R)$. If $A = BL$, then* $\text{span}(A) = \text{span}(B)$.

Proof. Recall that if $L \in \text{GL}(n, R)$, there exists a sequence of elementary matrices $E_1, \ldots, E_k \in R$ such that $E_1 \cdots E_k = L$. Define $B_s = BE_1 \cdots E_s$ for $s \in [1, k]$, and let $B_0 = B$. The three types of elementary matrices correspond to the following operations on B_s

1. Interchanging two columns.
2. Multiplying a column by -1.
3. Adding an integer multiple of one column to another.

It is clear that operations (1) and (2) do not change $\text{span}(B_s)$.

Suppose E_{s+1} replaces b_i with $b_i + cb_j$, where $i \neq j \in [1, n]$, $c \in \mathbb{Z}$, and b_i, b_j are columns of B_{s-1}. Assume $i < j$ without loss of generality.

If $z \in \text{span}(B_s)$, there exist $a_1, \ldots, a_n \in \mathbb{Z}$ such that

$$z = a_1b_1 + \cdots + a_nb_n.$$

Substituting $b_i + cb_j$ for b_i, we have

$$z = a_1b_1 + \cdots + a_i(b_i + cb_j) + \cdots + (a_j - a_ic)b_j + \cdots + a_nb_n,$$

where $a_j - a_ic \in \mathbb{Z}$. Thus, $z \in \text{span}(B_sE_{s+1})$.

Similarly, if

$$z = a_1b_1 + \cdots + a_i(b_i + cb_j) + \cdots + a_jb_j + \cdots + a_nb_n,$$

then

$$z = a_1b_1 + \cdots + a_ib_i + \cdots + (a_j + a_ic)b_j + \cdots + a_nb_n,$$

where $a_j + a_ic \in \mathbb{Z}$. Thus, $z \in \text{span}(B_sE_{s+1})$. This proves $\text{span}(B_s) = \text{span}(B_sE_{s+1})$.

Therefore, all three operations preserve the span. By induction, $\text{span}(B) = \text{span}(BL)$. □

Lemma 3.5. *Let $K \in \mathrm{GL}(\ell, \mathbb{Z})$ and denote the (i,j)-th element as $k_{i,j}$. Then for each $j \in [1,\ell]$, there exist $a_1, \ldots, a_\ell \in \mathbb{Z}$ such that*

$$\begin{aligned} &a_1 k_{1,j} + \cdots + a_\ell k_{\ell,j} = 1, \text{ and} \\ &a_1 k_{1,s} + \cdots + a_\ell k_{\ell,s} = 0 \text{ for } s \in [1,\ell] \text{ and } s \neq j. \end{aligned}$$

Proof. Denote the (i,j)-th element of K^{-1} as $c_{i,j}$. Then

$$\begin{aligned} K^{-1}K &= \begin{pmatrix} c_{1,1} & \cdots & c_{1,\ell} \\ \vdots & \ddots & \vdots \\ c_{\ell,1} & \cdots & c_{\ell,\ell} \end{pmatrix} \begin{pmatrix} k_{1,1} & \cdots & k_{1,\ell} \\ \vdots & \ddots & \vdots \\ k_{\ell,1} & \cdots & k_{\ell,\ell} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^{\ell} c_{1,i}k_{i,1} & \cdots & \sum_{i=1}^{\ell} c_{1,i}k_{i,\ell} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^{\ell} c_{\ell,i}k_{i,1} & \cdots & \sum_{i=1}^{\ell} c_{\ell,i}k_{i,\ell} \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}. \end{aligned}$$

Therefore, for each $j \in [1,\ell]$, we have

$$\begin{aligned} &c_{j,1}k_{1,j} + \cdots + c_{j,\ell}k_{\ell,j} = 1 \\ &c_{s,1}k_{1,s} + \cdots + c_{s,\ell}k_{\ell,s} = 0 \text{ for } s \in [1,\ell] \text{ and } s \neq j. \end{aligned}$$

The result follows for fixed $j \in [1,\ell]$ by setting

$$a_1 = c_{j,1}, \ldots, a_\ell = c_{j,\ell}.$$

□

Recall that for a diagonal matrix in Smith Normal Form $D \in \mathbb{Z}^{\ell \times n}$, 1-count$(D)$ denotes the number of entries equal to 1 on its diagonal (Definition 2.45).

Lemma 3.6. *Let $A \in \mathbb{Z}^{\ell \times n}$ with* SNF*-triple (K, D, L), and $d \in \mathbb{N}_+$. If* 1-count$(D) \geq d$*, then there exists a matrix $V \in \mathbb{Z}^{\ell \times d}$ such that* $\mathrm{span}(V^T) = \mathbb{Z}^d$ *and each column of V lies in* $\mathrm{span}(A)$*.*

Proof. Given $A = KDL$, by Lemma 3.4, we have $\mathrm{span}(A) = \mathrm{span}(KD)$. Since the first d entries along the diagonal of D are 1's, the first d columns of K are in $\mathrm{span}(KD)$. Let $v_1, \ldots, v_d \in \mathbb{Z}^\ell$ be the first d columns of K, so $v_i \in \mathrm{span}(KD) = \mathrm{span}(A)$, and let $V = (v_1 \ \cdots \ v_d)$.

Denote the elements of K as $k_{i,j}$, so $v_j = (k_{1,j} \ \cdots \ k_{\ell,j})^T$ for $j \in [1,d]$. By Lemma 3.5, for each $j \in [1,\ell]$, there exist $a_1, \ldots, a_\ell \in \mathbb{Z}$ such that

$$\begin{aligned} &a_1 k_{1,j} + \cdots + a_\ell k_{\ell,j} = 1 \\ &a_1 k_{1,s} + \cdots + a_\ell k_{\ell,s} = 0 \text{ for } s \in [1,\ell] \text{ and } s \neq j. \end{aligned}$$

That is,

$$a_1 \begin{pmatrix} k_{1,1} \\ \vdots \\ k_{1,j} \\ \vdots \\ k_{1,d} \end{pmatrix} + \cdots + a_\ell \begin{pmatrix} k_{\ell,1} \\ \vdots \\ k_{\ell,j} \\ \vdots \\ k_{\ell,d} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} = e_j,$$

where the vectors $(k_{i,1}, \ldots, k_{i,d})^T$ are the columns of V^T. Thus, we have shown that $e_j \in \mathrm{span}(V^T)$ for each $j \in [1,d]$. Therefore, $\mathrm{span}(V^T) = \mathbb{Z}^d$. □

Lemma 3.7. *Let $p \in \mathbb{P}$, $A \in \mathbb{Z}^{m\times n}$ with* SNF-triple (K, D, L).

- *If* $\operatorname{rank}(D) = 1\text{-count}(D)$, *and there exists* $V \in \mathbb{Z}^{m\times d}$ *such that* $\operatorname{span}(V^T) = \mathbb{Z}^d$ *and the columns of* V *lie in* $\operatorname{span}(A)$, *then* $1\text{-count}(D) \geq d$.
- *If* $\operatorname{rank}([D]_p) = 1\text{-count}([D]_p)$, *and there exists* $W \in \mathbb{Z}_p^{m\times d}$ *such that* $\operatorname{span}_{\mathbb{Z}_p}(W^T) = \mathbb{Z}_p^d$ *and the columns of* W *lie in* $\operatorname{span}_{\mathbb{Z}_p}(\mathbb{Z}_p^d)$,*then* $1\text{-count}([D]_p) \geq d$.

Proof. Let $1\text{-count}(D) = c$. Observe that KD is the $m \times d$ matrix whose first c columns are the first c columns of K, and the remaining $d - c$ columns are $0 \in \mathbb{Z}^m$. Similarly, let $1\text{-count}([D]_p) = c'$, $[K]_p[D]_p$ is the $m \times d$ matrix whose first c' columns are the first c' columns of $[K]_p$, and the remaining $d - c'$ columns are $0 \in \mathbb{Z}_p^m$.

Let R be either $\mathbb{Z}$ or $\mathbb{Z}_p$ and let K, D, L be $[K]_p, [L]_p$ when $R = \mathbb{Z}_p$.

By Lemma 3.4, $\operatorname{span}(A) = \operatorname{span}(KD)$, so the columns of V lie in $\operatorname{span}(KD)$.

Denote v_i as the i-th column of V, and $k_{i,j}$ as the i,j-th element of K. Since $v_i \in \operatorname{span}(KD)$, for $j \in [1, d]$, there exist $t_{j,1}, \ldots, t_{j,c} \in R$ such that

$$v_j = t_{j,1}\begin{pmatrix} k_{1,1} \\ \vdots \\ k_{m,1} \end{pmatrix} + \cdots + t_{j,c}\begin{pmatrix} k_{1,c} \\ \vdots \\ k_{m,c} \end{pmatrix}.$$

Thus,

$$V = \begin{pmatrix} \sum_{i=1}^c t_{1,i}k_{1,i} & \cdots & \sum_{i=1}^c t_{d,i}k_{1,i} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^c t_{1,i}k_{m,i} & \cdots & \sum_{i=1}^c t_{d,i}k_{m,i} \end{pmatrix}.$$

Since $\operatorname{span}(V^T) = R^d$ and $e_1, \ldots, e_d \in \operatorname{span}(V^T)$, for $\ell \in [1, d]$, there exist $\rho_{\ell,1}, \ldots, \rho_{\ell,m} \in R$ such that

$$\begin{aligned} e_\ell &= \rho_{\ell,1}\begin{pmatrix} \sum_{i=1}^c t_{1,i}k_{1,i} \\ \vdots \\ \sum_{i=1}^c t_{d,i}k_{1,i} \end{pmatrix} + \cdots + \rho_{\ell,m}\begin{pmatrix} \sum_{i=1}^c t_{1,i}k_{m,i} \\ \vdots \\ \sum_{i=1}^c t_{d,i}k_{m,i} \end{pmatrix} \\ &= \begin{pmatrix} \rho_{\ell,1}\sum_{i=1}^c t_{1,i}k_{1,i} + \cdots + \rho_{\ell,m}\sum_{i=1}^c t_{1,i}k_{m,i} \\ \vdots \\ \rho_{\ell,1}\sum_{i=1}^c t_{d,i}k_{1,i} + \cdots + \rho_{\ell,m}\sum_{i=1}^c t_{d,i}k_{m,i} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{i=1}^m \rho_{\ell,i}\left(\sum_{j=1}^c t_{1,j}k_{i,j}\right) \\ \vdots \\ \sum_{i=1}^m \rho_{\ell,i}\left(\sum_{j=1}^c t_{d,j}k_{i,j}\right) \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^c t_{1,j}\left(\sum_{i=1}^m \rho_{\ell,i}k_{i,j}\right) \\ \vdots \\ \sum_{j=1}^c t_{d,j}\left(\sum_{i=1}^m \rho_{\ell,i}k_{i,j}\right) \end{pmatrix}. \end{aligned}$$

Since the concatenation of $e_1, \ldots, e_d$ is the $d \times d$ identity matrix, we have

$$\begin{aligned} \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} &= \begin{pmatrix} \sum_{j=1}^c t_{1,j}\left(\sum_{i=1}^m \rho_{1,i}k_{i,j}\right) & \cdots & \sum_{j=1}^c t_{1,j}\left(\sum_{i=1}^m \rho_{d,i}k_{i,j}\right) \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^c t_{d,j}\left(\sum_{i=1}^m \rho_{1,i}k_{i,j}\right) & \cdots & \sum_{j=1}^c t_{d,j}\left(\sum_{i=1}^m \rho_{d,i}k_{i,j}\right) \end{pmatrix} \\ &= \begin{pmatrix} t_{1,1} & \cdots & t_{1,c} \\ \vdots & \ddots & \vdots \\ t_{d,1} & \cdots & t_{d,c} \end{pmatrix}\begin{pmatrix} \sum_{i=1}^m \rho_{1,i}k_{i,1} & \cdots & \sum_{i=1}^m \rho_{d,i}k_{i,1} \\ \vdots & \ddots & \vdots \\ \sum_{i=1}^m \rho_{1,i}k_{i,c} & \cdots & \sum_{i=1}^m \rho_{d,i}k_{i,c} \end{pmatrix}. \end{aligned}$$

Recall from standard linear algebra that for any real-valued matrices $A \in \mathbb{R}^{d\times c}$, $B \in \mathbb{R}^{c\times d}$, we have $\text{rank}(AB) \leq \min\{\text{rank}(A), \text{rank}(B)\}$. Since $\text{rank}(D) = d$, it follows that $c \geq d$. If this is the case where $R = \mathbb{Z}_p$, then we have shown 1-count$([D]_p) \geq 1$, which implies 1-count$(D) \geq 1$. □

Lemma 3.8. *Let $p \in \mathbb{P}$, $A \in \mathbb{Z}^{m\times n}$. If there exists $V \in \mathbb{Z}^{m\times d}$ such that the columns of V lie in* span(A) *and* span$(V^T) = \mathbb{Z}^d$*, then there exists $W \in \mathbb{Z}_p^{m\times d}$ such that the columns of W lie in* span$_{\mathbb{Z}_p}([A]_p)$ *and* span$_{\mathbb{Z}_p}(W^T) = \mathbb{Z}_p^d$.

Proof. Assume there exists $V \in \mathbb{Z}^{m\times d}$ such that the columns of V lie in span(A) and span$(V^T) = \mathbb{Z}^d$. Then there exist $e_1, \ldots, e_d \in \text{span}(V^T) = \mathbb{Z}^d$ and $\tilde{e}_1, \ldots, \tilde{e}_d \in \mathbb{Z}^m$ (the standard basis of dimension m) such that $\tilde{e}_1, \ldots, \tilde{e}_d \in \text{span}(A)$.

Let $V \in \mathbb{Z}^{m\times d}$ be the diagonal matrix with d entries of 1 on the diagonal. Define $W = [V]_p$, where each entry $w_{i,j}$ of W is equal to $v_{i,j} \mod p$.

Then $W^T \in \mathbb{Z}_p^{d\times m}$ is the diagonal matrix with d entries of 1 on the diagonal, and thus span$_{\mathbb{Z}_p}(W^T) = \mathbb{Z}_p^d$. □

Corollary 3.9. *Let $A \in \mathbb{Z}^{m\times n}$, $\min(m, n) \geq d \in \mathbb{N}_+$, and (K, D, L) be an* SNF*-triple for A. If there exists $V \in \mathbb{Z}^{m\times d}$ such that the columns of V lie in* span(A) *and* span$(V^T) = \mathbb{Z}^d$*, then* 1-count$(D) \geq d$.

Proof. If 1-count(D) = rank(D), then Lemma 3.7 proves the claim. Otherwise, 1-count$(D) \neq$ rank(D) which equivalent to 1-count$(D) <$ rank(D).

By Lemma 3.8, for any prime p, there exists $W \in \mathbb{Z}_p^{m\times d}$ such that the columns of W lie in span$_{\mathbb{Z}_p}([A]_p)$ and span$_{\mathbb{Z}_p}(W^T) = \mathbb{Z}_p^d$. Let $c =$ 1-count(D), and let $p \mid \mathfrak{d}_{c+1}$ (the first non-1 diagonal entry of $D \in \mathbb{Z}^{m\times n}$). Then rank$([D]_p) =$ 1-count$([D]_p)$. This gives two cases

1. If there exists $V \in \mathbb{Z}^{m\times d}$ such that the columns of V lie in span(A) and span$(V^T) = \mathbb{Z}^d$, and 1-count$(D) =$ rank(D), then 1-count$(D) \geq d$.
2. If there exists $W \in \mathbb{Z}_p^{m\times d}$ such that the columns of W lie in span$_{\mathbb{Z}_p}([A]_p)$ and span$_{\mathbb{Z}_p}(W^T) = \mathbb{Z}_p^d$, and rank$([D]_p) =$ 1-count$([D]_p)$, then 1-count$([D]_p) \geq d$, which implies 1-count$(D) \geq d$.

□

Proposition 3.10. MatrixSubspanA *is in* P.

Proof. We solve MatrixSubspanA by the following procedure

1. Call the algorithm in Lemma 3.2 on input $A \in \mathbb{Z}^{m\times n}$ and $0 = b \in \mathbb{Z}^m$. If this algorithm returns 'No', return 'No' to MatrixSubspanA.
2. Else, let $u_1, \ldots, u_m, c \in \mathbb{Z}^n$ be the output of the procedure (here $c = 0$). Set $U \in \mathbb{Z}^{n\times m}$ to be the matrix whose i-th column is u_i.
3. Calculate the SNF-triple (K, D, L) of $U|_\ell$, and so $K \in \text{GL}(\ell, \mathbb{Z})$, $L \in \text{GL}(m, \mathbb{Z})$, $D \in \mathbb{Z}^{\ell\times m}$, where $U|_\ell = KDL$.
4. If 1-count$(D) \geq d$, output 'Yes'. Otherwise, if 1-count$(D) < d$, output 'No'.

Step (1) is polynomial time by Lemma 3.2, and Step (2) is a straightforward calculation. Thus, our procedure is polynomial time.

We will now justify the correctness of the procedure.

If 'No' is returned in Step (1), then there does not exist $x \in \mathbb{Z}^n$ which satisfies $Ax = 0$, so we output 'No' for MatrixSubspanA. Thus, we may assume there exists a solution to the procedure in Lemma 3.2, which finds U and c such that $c = 0$ and $Ax = 0$ if and only if $x \in \text{span}(U)$. We then check if there exist $v_1, \ldots, v_d \in \text{span}(U)$ such that for the matrix

$V = (v_1 \ \cdots \ v_d)$, we have $\text{span}((V|_\ell)^T) = \mathbb{Z}^d$. By Lemma 3.3, V exists if and only if there exists $W \in \mathbb{Z}^{\ell \times d}$ such that $\text{span}(W^T) = \mathbb{Z}^d$ and each column of W lies in $\text{span}(U|_\ell)$. Using D of the SNF (K, D, L) calculated in Step (3), by Lemma 3.6 and the contrapositive of Corollary 3.9, such a W exists if and only if 1-count$(D) \geq d$, thus justifying the output in Step (4). □

3.3 Solving Matrix Problem B

In this section, we demonstrate that MatrixSubspanB is decidable in polynomial time. Our method closely follows the approach presented in [12, Proposition 4.2 and Lemma 4.3]. Recall the problem is as follows

Problem:	MatrixSubspanB
Input:	A triple (A, b, ℓ) where $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, $\ell \in \mathbb{N}$ with $\ell \in [0, n-1]$.
Question:	Does there exist an n-vector ν such that $A\nu + b = 0$ and $\text{span}((\nu|_\ell)^T) = \mathbb{Z}^d$?

We now present the following simple observation, which provides a more precise way of expressing MatrixSubspanB.

First, the following simple fact enables us to represent our matrix problem in terms of the greatest common divisor (gcd).

Lemma 3.11. *For $a_1, \ldots, a_s \in \mathbb{Z}$, $\text{span}(\begin{bmatrix} a_1 & \cdots & a_s \end{bmatrix}) = \mathbb{Z}$ if and only if $\gcd(a_1, \ldots, a_s) = 1$.*

Proof. If $\text{span}(\begin{bmatrix} a_1 & \cdots & a_s \end{bmatrix}) = \mathbb{Z}$, then $1 \in \text{span}(\begin{bmatrix} a_1 & \cdots & a_s \end{bmatrix})$, which means there exists $x_1, \ldots, x_s \in \mathbb{Z}$ such that

$$x_1 a_1 + \cdots + x_s a_s = 1.$$

Let $c = \gcd(a_1, \ldots, a_s)$, it follows that $a_i = cb_i$ for $b_i \in \mathbb{Z}$. So

$$c(x_1 b_1 + \cdots + x_1 b_1) = 1$$

and the only integer value for which c can take is 1, thus $\gcd(a_1, \ldots, a_s) = 1$.

Conversely, if $\gcd(a_1, \ldots, a_s) = 1$. Then there exists $x_1, \ldots, x_s$ such that

$$x_1 a_1 + \cdots + x_s a_s = 1.$$

Then $1 \in \text{span}(\begin{bmatrix} a_1 & \cdots & a_s \end{bmatrix})$, and $\text{span}(1) = \mathbb{Z}$. □

It follows that the decision problem MatrixSubspanB can be expressed as follows.

Problem:	MatrixSubspanB
Input:	Given $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, $\ell \in \mathbb{Z}$ with $\ell \in [0, n-1]$.
Question:	Does there exist an integer n-vector $\nu = \begin{bmatrix} \nu_1 & \cdots & \nu_n \end{bmatrix}^T \in \mathbb{Z}^n$ such that $A\nu + b = 0$ and $\gcd(\nu_{n-\ell+1}, \ldots, \nu_n) = 1$?

Next, we present some basic facts about gcd.

Lemma 3.12. *Let $n, k, \ell \in \mathbb{N}_+$, $U \in \mathbb{Z}^{\ell \times k}$ with* SNF*-triple (K, D, L) and $r \in \mathbb{Z}^\ell$. There exists $\mu = (\mu_1 \ \cdots \ \mu_\ell)^T \in \text{span}_r(U) \in \mathbb{Z}^\ell$ such that $\gcd(\mu_1, \ldots, \mu_\ell) = 1$ if and only if there exists $v = (v_1 \ \cdots \ v_\ell)^T \in \text{span}_{K^{-1}r}(D) \in \mathbb{Z}^\ell$ such that $\gcd(v_1, \ldots, v_\ell) = 1$.*

Proof. Assume there exists $\mu = (\mu_1 \ \cdots \ \mu_\ell)^T \in \mathrm{span}_r(U)$ with $\gcd(\mu_1, \ldots, \mu_\ell) = 1$. Let $v = K^{-1}\mu$, so $v \in \mathrm{span}_{K^{-1}r}(K^{-1}U)$. By Lemma 3.4, $\mathrm{span}(K^{-1}U) = \mathrm{span}(D)$, hence $v = (v_1 \ \cdots \ v_\ell)^T \in \mathrm{span}_{K^{-1}r}(D)$. As $v = K^{-1}\mu$ and $K^{-1} \in \mathrm{GL}(\ell, \mathbb{Z})$, K^{-1} can be expressed as a product of elementary matrices $E_1 \cdots E_k = K^{-1}$. Since multiplication by an elementary matrix does not change the gcd, $\gcd(v) = \gcd(\mu) = 1$. □

Lemma 3.13 ([12, Lemma 4.3])**.** *Let $n \in \mathbb{N}_+$, $\mathfrak{d}, c_1, \ldots, c_n \in \mathbb{Z}$ such that $n \geq 2$, $c_i \neq 0$ for some $i \in [2, n]$, and $\gcd(\mathfrak{d}, c_1, \ldots, c_n) = 1$. Then there exists $x \in \mathbb{Z}$ such that*

$$\gcd(x\mathfrak{d} + c_1, c_2, \ldots, c_n) = 1.$$

Lemma 3.14. *For $s, \mathfrak{d}_1, \ldots, \mathfrak{d}_n, b_1, \ldots, b_s \in \mathbb{Z}$ and $\mathfrak{d}_i \mid \mathfrak{d}_{i+1}$ for $i \in [1, n-1]$, there exists $a_1, \ldots, a_s \in \mathbb{Z}$ such that*

$$\gcd(a_1\mathfrak{d}_1 + b_1, \ldots, a_s\mathfrak{d}_s + b_s) = 1$$

if and only if one of the following holds

1. *$b_1, \ldots, b_s = 0$ and $\mathfrak{d}_1 \in \{-1, 1\}$,*
2. *$\gcd(b_1, \ldots, b_s) = 1$,*
3. *$\gcd(b_1, \ldots, b_s) = c > 1$, $\gcd(\mathfrak{d}_1, c) = 1$, and*
   a) *$b_i \neq 0$ for some $i \in [2, s]$,*
   b) *$s = 1$ and $c \equiv 1 \pmod{\mathfrak{d}_1}$,*
   c) *$b_2, \ldots, b_s = 0$ and either $c \equiv 1 \pmod{\mathfrak{d}_1}$ or $\mathfrak{d}_2 \neq 0$.*

Proof. Assume one of the conditions (a)–(c) holds. If $b_i = 0$ and $\mathfrak{d}_1 = \pm 1$ set $a_1 = 1$ and $a_j = 0$ for $j \geq 2$ and if $\gcd(b_1, \ldots, b_s) = 1$ then set $a_i = 0$.

If $\gcd(b_1, \ldots, b_s) = c > 1$ and $\gcd(\mathfrak{d}_1, c) = 1$, we have three subcases.

If $b_i \neq 0$ for some $i \in [2, s]$, then by Lemma 3.13 there exists $x \in \mathbb{Z}$ such that $\gcd(x\mathfrak{d}_1 + b_1, b_2, \ldots, b_s) = 1$. Set $a_1 = x$ and $a_2 = \cdots = a_s = 0$.

If $n = 1$ then $c = \gcd(b_1) = b_1$, and $c \equiv 1 \mod \mathfrak{d}_1$ means $c + \alpha\mathfrak{d}_1 = 1$ for some $\alpha \in \mathbb{Z}$. Setting $a_1 = -\alpha$ gives $\gcd(a_1\mathfrak{d}_1 + b_1) = a_1\mathfrak{d}_1 + b_1 = 1$.

If $b_2 = \cdots = b_s = 0$ then $c = \gcd(b_1, 0, \ldots, 0) = b_1$. So if $c \equiv 1 \mod \mathfrak{d}_1$ then again we have $a_1 = \alpha \in \mathbb{Z}$ so that $\alpha b_1 + \mathfrak{d}_1 = 1$. If $\mathfrak{d}_2 \neq 0$ then $\mathfrak{d}_1 \mid \mathfrak{d}_2$ and $\gcd(\mathfrak{d}_1, c) = 1$ implies $\gcd(\mathfrak{d}_1, b_1, \mathfrak{d}_2) = 1$ with $\mathfrak{d}_2, b_1 \neq 0$. By Lemma 3.13 there exists $x \in \mathbb{Z}$ so that $\gcd(x\mathfrak{d}_1 + b_1, \mathfrak{d}_2) = 1$. Set $a_1 = x, a_2 = 1, a_3 = \cdots = a_s = 0$.

Conversely assume there exist $a_1, \ldots, a_s \in \mathbb{Z}$ such that

$$\gcd(a_1\mathfrak{d}_1 + b_1, \ldots, a_s\mathfrak{d}_s + b_s) = 1. \tag{3.2}$$

If $b_i = 0$ for $i \in [1, s]$, since $\mathfrak{d}_i \mid \mathfrak{d}_{i+1}$ for $i \in [1, s-1]$ we get $\gcd(a_1\mathfrak{d}_1, \ldots, a_s\mathfrak{d}_s) > |\mathfrak{d}_1|$, contradicting Eq. (3.2). Thus we must have condition (a) or $b_i \neq 0$ for some $i \in [1, s]$. If $b_i \neq 0$ for some $i \in [1, s]$, either condition (b) holds or $\gcd(b_1, \ldots, b_s) = c > 1$.

If $f = \gcd(\mathfrak{d}_1, c) \neq 1$ then f divides every b_i and $\mathfrak{d}_i$, so no choice of $a_i \in \mathbb{Z}$ can satisfy Eq. (3.2). Thus we must have $\gcd(\mathfrak{d}_1, c) = 1$.

Assume condition (c)(i) does not hold. Then either $s = 1$ or $s > 1$ and $b_i = 0$ for $i \in [2, s]$.

If $s = 1$ then Eq. (3.2) becomes $1 = \gcd(a_1\mathfrak{d}_1 + b_1) = a_1\mathfrak{d}_1 + b_1 = a_1\mathfrak{d}_1 + c$ since $c = b_1$, and we have condition (c)(ii).

Else $s > 1$. If $\mathfrak{d}_2 = 0$ then $\mathfrak{d}_i = 0$ for $i > 2$, and since $b_i = 0$ for $i \in [2, s]$, Eq. (3.2) becomes $1 = \gcd(a_1\mathfrak{d}_1 + b_1, 0, \ldots, 0) = a_1\mathfrak{d}_1 + b_1$ so $c \equiv 1 \mod \mathfrak{d}_1$ and we have condition (c)(iii).

□

Proposition 3.15. MatrixSubspanB *is in* P.

Proof. We solve MatrixSubspanB by the following procedure. Given $A \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$, $\ell \in \mathbb{Z}$ where $\ell \in [0, n-1]$

1. Call the algorithm in Lemma 3.2 on input $A \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}^m$. If this algorithm returns 'No', return 'No' to MatrixSubspanB.
2. Otherwise, let $u_1, \ldots, u_m \in \mathbb{Z}^n$ and $c' = (c'_1 \ \cdots \ c'_n)^T \in \mathbb{Z}^n$ be the output of this algorithm. Set $U \in \mathbb{Z}^{n\times m}$ to be the matrix whose i-th column is u_i.
3. Compute the SNF (K, D, L) of $U|_\ell \in \mathbb{Z}^{\ell\times m}$, and so $K \in \mathrm{GL}(\ell, \mathbb{Z})$, $L \in \mathrm{GL}(m, \mathbb{Z})$, $D \in \mathbb{Z}^{\ell\times m}$ with diagonal entries $\mathfrak{d}_i$ for $i \in [1, \ldots, \mathrm{rank}(D)]$, and $U|_\ell = KDL$. Set
   - $\mathfrak{d}_i = 0$ for $i \in [\mathrm{rank}(D) + 1, \ell]$,
   - $c = (c_1 \ \cdots \ c_\ell) = K^{-1}(c'_{n-\ell+1} \ \cdots \ c'_n) \in \mathbb{Z}^\ell$.
4. Return 'Yes' if one of the following conditions holds, and 'No' otherwise
   a) $c_1, \ldots, c_\ell = 0$ and $\mathfrak{d}_1 \in \{-1, 1\}$,
   b) $\gcd(c_1, \ldots, c_\ell) = 1$,
   c) $\gcd(c_1, \ldots, c_\ell) = f > 1$, $\gcd(\mathfrak{d}_1, f) = 1$, and
      i. $c_i \neq 0$ for some $i \in [2, \ell]$,
      ii. $\ell = 1$ and $f \equiv 1 \pmod{\mathfrak{d}_1}$,
      iii. $c_2, \ldots, c_\ell = 0$ and ($f \equiv 1 \pmod{\mathfrak{d}_1}$ or $\mathfrak{d}_2 \neq 0$).

Step (1) is polynomial time by Lemma 3.2, Step (3) is polynomial time by Theorem 2.48, and Step (4) is polynomial time by Lemma 3.1.

If 'No' is returned in Step (1), then there does not exist $x \in \mathbb{Z}^n$ which satisfies $Ax+b = 0$, so we output 'No' for MatrixSubspanB. Thus, we may assume there exists a solution to the procedure in Lemma 3.2, which finds U and c' such that $Ax + b = 0$ if and only if $x \in \mathrm{span}_{c'}(U)$.

Let $r = (c'_{n-\ell+1} \ \ldots \ c'_n)^T \in \mathbb{Z}^\ell$. We then check if there exists $\nu \in \mathrm{span}_{c'}(U)$ such that $\gcd(\nu_1, \ldots, \nu_n) = 1$. By Lemma 3.3, ν exists if and only if there exists $\mu = (\mu_1 \ \cdots \ \mu_\ell)^T \in \mathrm{span}_r(U|_\ell) \in \mathbb{Z}^\ell$ such that $\gcd(\mu_1, \ldots, \mu_\ell) = 1$.

By Lemma 3.12, such a μ exists if and only if there exists $v = (v_1 \ \cdots \ v_\ell)^T \in \mathrm{span}_{K^{-1}r}(D)$ such that $\gcd(v_1, \ldots, v_\ell) = 1$. Since $c = K^{-1}r$, all elements in $\mathrm{span}_c(D)$ take the form $a_1\mathfrak{d}_1 + c_1, \ldots, a_\ell\mathfrak{d}_\ell + c_\ell$ for $a_1, \ldots, a_\ell \in \mathbb{Z}$. Checking if such a v exists is equivalent to checking if there exist $a_1, \ldots, a_\ell \in \mathbb{Z}$ such that $\gcd(a_1\mathfrak{d}_1 + c_1, \ldots, a_\ell\mathfrak{d}_\ell + c_\ell) = 1$. This is solved in Step (4) by Lemma 3.14. □

Proof of Theorem A. The result is immediate from Propositions 3.10 and 3.15. □

4 Virtually Abelian Targets

As previously noted, the epimorphism problem is undecidable in general. For instance, if G_1 is the trivial group, then an epimorphism exists if and only if G_2 is also trivial. However, it is well known that determining whether a group is trivial is itself undecidable, see Theorem 2.82. Additionally, the result that the epimorphism problem for nilpotent groups is undecidable is notable and unexpected because nilpotent groups share structural similarities with abelian groups, for which the epimorphism problem is more tractable and is shown to be in P in Chapter 6.

Using the results from the previous chapter, in this chapter for the classes which Friedl and Löh [12] showed to be decidable, which they acknowledged "will have ridiculous worst-case complexity" for their proposed algorithm, we instead are able to show the same target classes lies in NP. Thus, we prove the following.

Theorem B. *The epimorphism problem from finitely presented groups to the following target classes is* NP*-complete:*

1. *Direct products of abelian and finite groups.*
2. *Virtually cyclic groups.*
3. *Semi-direct products of a free abelian group N and a finite group Q, where the action of Q on N is restricted in a specific way, as described in Definition 2.80.*

Items (1) and (2) are the classes of virtually abelian groups which are shown to be decidable in [12] which we show to be in NP-complete, and (3) is a generalisation to a larger subclass of virtually abelian groups.

Notation. Given $\mathcal{D}, \mathcal{T}$, two classes of groups. The *epimorphism problem* from $\mathcal{D}$ to $\mathcal{T}$, denoted $\mathsf{EPI}(\mathcal{D}, \mathcal{T})$, is the following decision problem.

Problem:	Epimorphism Problem - $\mathsf{EPI}(\mathcal{D}, \mathcal{T})$
Input:	Finite descriptions for groups $G \in \mathcal{D}$ and $H \in \mathcal{T}$
Question:	Does there exist an epimorphism from G to H?

We refer to $G \in \mathcal{D}$ as the *domain group* and $H \in \mathcal{T}$ as the *target group* for the problem.

The finite description for a group depends on its class and can be found in Chapter 2 and Section 2.4. In the special case where $\mathcal{T} = \{H\}$ is a singleton, we write $\mathsf{EPI}(\mathcal{D}, \mathrm{H})$ for the epimorphism problem from a class $\mathcal{D}$ to a fixed group H, this will be relevant in Chapter 5. In this case, the input consists solely of a finite description for $G \in \mathcal{D}$.

In the following section, we set the notation and prove the preliminary results for epimorphism problem which will be relevant in later chapters.

4.1 Preliminary Results

We begin with the epimorphism problem where finite group targets are given by their multiplication tables. In [15, Chapter 7], Holt and Plesken considered the computational problem of finding epimorphisms onto various classes of finite groups, though without

providing an explicit estimate of complexity, and Friedl and Löh [12, Proposition 5.2] showed that $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Fin})$ is decidable.

Here, we observe that $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Fin})$ is, in fact, in NP.

Lemma 4.1. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Fin})$ *is in* NP.

Proof. On input a presentation $\langle g_1, \dots, g_n \mid r_1, \dots, r_m \rangle$ for $G \in \mathsf{FinPres}$, non-deterministically specify values $\tau(g_i) \in Q$ for each $i \in [1, n]$.

Verify that τ defines a homomorphism from G to H using Lemma 2.28 by checking that each relation is sent to 1_Q via the multiplication table for Q.

To verify that τ is a surjection, proceed as follows. Fix a copy of Q and 'mark' each $q_j \in Q$ that satisfies $\tau(g_i) = q_j$ for some $i \in [1, n]$. While not all of Q is marked, scan the multiplication table for Q to find $q_i, q_j, q_k \in Q$ such that $q_i q_j = q_k$, where q_i and q_j are marked but q_k is not, and then mark q_k. If τ is a surjection, then each $q \in Q$ will eventually be marked, as every element of Q is the image of some product of generators. Thus, the process terminates with all of Q marked.

Each of the above steps takes polynomial time in the size of n, $\sum_{i=1}^{m} |r_i|$, and the size of the multiplication table for Q (which is $O(|Q|^2)$). □

Example 4.2 (Finite target epimorphism)**.** Let G be a group with the presentation

$$G = \left\langle x_1, x_2, x_3, x_4 \mid x_1 x_2 x_3 x_4,\ x_1^2,\ x_1 x_2^n x_3 \right\rangle$$

and D_6 be the dihedral group of order 6 with the presentation

$$D_6 = \left\langle s, t \mid s^2,\ t^3,\ stst \right\rangle$$

this group is given as its full multiplication table which we omit for brevity. Then we can 'guess' the following set map

$$\psi\colon \begin{cases} x_1 \mapsto s \\ x_2 \mapsto t \\ x_3 \mapsto s \\ x_4 \mapsto t^{-1} \end{cases}$$

verify that ψ extends to a homomorphism via the following calculation

$$\begin{aligned} \psi(x_1)\psi(x_2)\psi(x_3)\psi(x_4) &= stst^{-1} = 1 \\ \psi(x_1)^2 &= s^2 = 1 \\ \psi(x_1)\psi(x_2)^3\psi(x_3) &= st^n s = s^2 = 1. \end{aligned}$$

To check surjectivity we fix a copy of D_6 with the elements $\{1, s, t, t^2, st, st^2\}$. We then 'mark off' each element as follows

$$\begin{aligned} \psi(x_1) &= s \\ \psi(x_2) &= t \\ \psi(x_1)\psi(x_2) &= st \\ \psi(x_2)\psi(x_2) &= t^2 \\ \psi(x_1)\psi(x_3) &= s^2 = 1 \\ \psi(x_1)\psi(x_2)\psi(x_2) &= st^2. \end{aligned}$$

Thus, ψ is an epimorphism. Note that this is a similar process to that which is observed in Example 2.30, as $D_6 \cong S_3$. The main differences are that we do not explicitly define a system of equations, and we check for surjection here.

Remark 4.3. This procedure cannot be used for targets that are infinite groups. While the surjection can always be verified in polynomial time, the 'guessed' image cannot be guaranteed to be polynomial bounded as a word on the original generators. Thus, we cannot guarantee a polynomial time verification process.

4.1.1 (Q, τ)-presentation

In this subsection, we provide a useful way to present a domain group when considering the epimorphism problem with a target involving an extension with a finite group Q as the quotient.

Definition 4.4 ((Q, τ)-presentation)**.** Let G be a finitely presented group, Q a finite group, and $\tau\colon G \to Q$ an epimorphism from G to Q. We call $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ a (Q, τ)-presentation for G if

1. $\mathcal{X}, \mathcal{Y}, \mathcal{R}$ are finite.
2. $\mathcal{X} \subseteq G$ and $\tau|_{\mathcal{X}}\colon \mathcal{X} \to Q$ is a bijection.
3. The subgroup $\ker(\tau)$ is generated by $\mathcal{Y}$.

Lemma 4.5. *There is an algorithm which takes as input*

1. a finite presentation $\langle g_1, \dots, g_n \mid r_1, \dots, r_m \rangle$ for a group G,

2. a multiplication table for a finite group Q,

3. a list $(q_1, \dots, q_n) \in Q^n$ defining an epimorphism $\tau\colon G \to Q$ by $\tau(g_j) = q_j$, $j \in [1, n]$,

and outputs a (Q, τ)-presentation for G which has size polynomial in $(n + m + |Q|)$ and runs in time polynomial in $(n + m + |Q|)$.

Proof. Our procedure is as follows. Initialise $\Lambda = \mathcal{X} = \mathcal{Y} = \varnothing$, $\mathcal{G} = \{g_1, \dots, g_n\}$, and $\mathcal{R} = \{r_1, \dots, r_m\}$.

1. Set $\mathcal{G} = \mathcal{G} \cup \mathcal{G}^{-1}$ and $\mathcal{R} = \mathcal{R} \cup \{g_i g_i^{-1} : i \in [1, n]\}$.
2. For each $g \in \mathcal{G}$, if $\tau(g) = q \notin \Lambda$, set $\Lambda = \Lambda \cup \{q\}$, $\mathcal{X} = \mathcal{X} \cup \{x_q\}$, and $\mathcal{R} = \mathcal{R} \cup \{x_q g^{-1}\}$. Since τ is an epimorphism, Λ becomes a generating set for Q, and $\tau(x_q) = q$ for each $x_q \in \mathcal{X}$.
3. While $\Lambda \neq Q$
   a) Scan the multiplication table for Q to find a triple (p_1, p_2, q) where $p_1, p_2 \in \Lambda$, $p_1 p_2 = q$, and $q \in Q \setminus \Lambda$ (such a q must exist as Λ is a generating set for Q).
   b) Set $\Lambda = \Lambda \cup \{q\}$, $\mathcal{X} = \mathcal{X} \cup \{x_q\}$, and $\mathcal{R} = \mathcal{R} \cup \{x_{p_1} x_{p_2} x_q^{-1}\}$.

   Since elements are added to Λ only when new ones are discovered, and each iteration strictly increases its size until $\Lambda = Q$, the loop terminates. When the loop terminates, $\Lambda = Q$, and the set $\mathcal{X}$ is in bijection with Q. At this stage, $G = \langle \mathcal{X} \cup \mathcal{G} \mid \mathcal{R} \rangle$ with $\tau(x_q) = q$ for every $x_q \in \mathcal{X}$.
4. For each $g_i \in \mathcal{G}$ and pair $(p, q) \in Q \times Q$, if $\tau(x_p g_i x_q) =_Q 1$, set $\mathcal{Y} = \mathcal{Y} \cup \{y_{p,i,q}\}$ and $\mathcal{R} = \mathcal{R} \cup \{x_p g_i x_q y_{p,i,q}^{-1}\}$. We now have the presentation $\langle \mathcal{X} \cup \mathcal{Y} \cup \mathcal{G} \mid \mathcal{R} \rangle$ for G.
5. For each $i \in [1, n]$, since $\tau(g_i) \in Q$, it follows that $x_{\tau(g_i)} \in \mathcal{X}$ and $\tau(x_{\tau(g_i)}) = \tau(g_i)$. From this, $\tau(x_{\tau(g_i)^{-1}} g_i x_{1_Q}) = 1_Q$, which implies $y_{\tau(g_i)^{-1}, g_i, 1_Q} \in \mathcal{Y}$ and $y_{\tau(g_i)^{-1}, g_i, 1_Q} =_G x_{\tau(g_i)^{-1}} g_i x_{1_Q}$. Using a Tietze transformation, remove g_i from the generating set and replace each occurrence of g_i in every relation with

$$x_{\tau(g_i)} y_{\tau(g_i)^{-1}, g_i, 1_Q}.$$

   After processing all $i \in [1, n]$, we obtain the presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G.

The time complexity and output length for each step are as follows

1. Takes $|\mathcal{G}| = n$ steps. Setting $\mathcal{G} = \mathcal{G} \cup \mathcal{G}^{-1}$ requires $2n$ steps.

2. Takes $2n$ steps, adding at most $|Q|$ letters to Λ, $\mathcal{X}$, and at most $|Q|$ words of length 2 to $\mathcal{R}$.
3. The while loop iterates at most $|Q|$ times. Each iteration scans at most $|Q|^2$ entries of the multiplication table and adds at most $|Q|$ letters to $\Lambda, \mathcal{X}$ and at most $|Q|$ words of length 3 to $\mathcal{R}$.
4. Takes $2n\,|Q|^2$ steps, adding at most $2n\,|Q|^2$ letters to $\mathcal{Y}$ and at most $2n\,|Q|^2$ words of length at most 4 to $\mathcal{R}$.
5. Takes $2n$ steps, increasing the length of relators by at most a factor of 2 (replacing g_i by a word of length 2).

To show that $\mathcal{Y}$ is a generating set for $\ker(\tau)$, suppose an element in $\ker(\tau)$ is written as

$$w = g_{i_1} g_{i_2} \cdots g_{i_k} \in (\mathcal{G} \cup \mathcal{G}^{-1})^*.$$

with $\tau(w) = 1_Q$. Let $q_{i_1}, \ldots, q_{i_{k-1}} \in Q$ such that $q_1 = \tau(g_{i_1})^{-1}$ and $q_{i_j} = \tau(x_{q_{j-1}}^{-1} g_{i_j})^{-1}$ for $j \in [2, k-1]$ (recall that $\tau(x_q) = q$ for each $x_q \in \mathcal{X}$). Then

$$w = g_{i_1} \left(x_{q_1} x_{q_1}^{-1}\right) g_{i_2} \left(x_{q_2} x_{q_2}^{-1}\right) \cdots \left(x_{q_{k-1}} x_{q_{k-1}}^{-1}\right) g_{i_k}$$

so

$$\begin{aligned}
\tau(w) &= \tau(g_{i_1} x_{q_1}) \tau(x_{q_1}^{-1} g_{i_2} x_{q_2}) \tau(x_{q_2}^{-1} g_{i_3} x_{q_3}) \cdots \tau(x_{q_{k-2}}^{-1} g_{i_{k-1}} x_{q_{k-1}}) \tau(x_{q_{k-1}}^{-1} g_{i_k}) \\
&= \tau(y_{1,i_1,q_1}) \tau(y_{q_1^{-1},i_2,q_2}) \cdots \tau(y_{q_{k-2}^{-1},i_{k-1},q_{k-1}}) \tau(x_{q_{k-1}}^{-1} g_{i_k}) \\
&= \tau(x_{q_{k-1}}^{-1} g_{i_k}).
\end{aligned}$$

Since $\tau(w) = 1_Q$, it follows that $\tau(x_{q_{k-1}}^{-1} g_{i_k}) = 1_Q$, so $x_{q_{k-1}}^{-1} g_{i_k} \in \mathcal{Y}$ (given by $y_{q_{k-1}^{-1},i_k,1} = x_{q_{k-1}}^{-1} g_{i_k} x_{1_Q}$). Thus, we have written w as a product of letters from $\mathcal{Y}$, so $\langle \mathcal{Y} \rangle = \ker(\tau)$. □

Remark 4.6. Since we do not assume that $\mathcal{G} \subseteq G$ or that G has a decidable word problem, we do not claim that $\mathcal{Y}$ is a subset of G (it may contain repetitions). However, in the proof of the above lemma, we ensured that $\mathcal{X} \subseteq G$.

4.1.2 Epimorphism into Extensions

In this subsection we give a useful intermediary result for testing epimorphism, for any target group when described by an extension.

Lemma 4.7. *Let $G, N \in \mathsf{FinPres}$, $Q \in \mathsf{Fin}$, and let H be given by an N by Q extension with a fixed transversal map $s\colon Q \to G$. The following are equivalent:*

1. *There exists an epimorphism $\psi\colon G \to H$.*
2. *There exist homomorphisms $\tau\colon G \to Q$ and $\kappa\colon G \to H$ such that*
   a) *τ is surjective.*
   b) *$\kappa(g) = ns(q)$ implies $q = \tau(g)$.*
   c) *For all $n \in N$, there exists $g \in \ker(\tau)$ such that $\kappa(g) = ns(1_Q)$.*

Proof. If $\psi\colon G \to H$ is an epimorphism, then $\tau = \pi_Q \circ \psi$ is also an epimorphism. For each $g \in G$, if $\psi(g) = ns(q)$, then $\tau(g) = \pi_Q(ns(q)) = q$. Thus, $\psi = \kappa$ satisfies condition (b).

Furthermore, if $n \in N$, then since ψ is surjective, there exists $g \in G$ such that $\psi(g) = ns(1_Q)$ and $\tau(g) = \pi_Q(ns(1_Q)) = 1_Q$. Hence, $\psi = \kappa$ satisfies condition (c).

Conversely, assume there exist τ and κ as described in the lemma. Then, for each $ns(q) \in H$, there exists $g_1 \in G$ such that $\tau(g_1) = q$, and hence $\kappa(g_1) = n_1 s(q)$ for some $n_1 \in N$. Additionally, there exists $g_2 \in \ker(\tau)$ such that $\kappa(g_2) = n n_1^{-1} s(1_Q)$.

Therefore, $\kappa(g_1 g_2) = n n_1^{-1} s(1_Q) n_1 s(q) = ns(q)$. Thus, κ is a surjective homomorphism from G to H. □

Remark 4.8. Item (c) in the above lemma may be replaced by

(c') For some (Q,τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G, for all $n \in N$, there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(w) = ns(1_Q)$.

This follows directly from the definition of a (Q,τ)-presentation, that $\ker(\tau) = \langle \mathcal{Y} \rangle$.

Example 4.9 (Necessity of the conditions in Lemma 4.7)**.** Let

$$G = \left\langle x_1, q_1 \mid [x_1, q_1], q_1^2 \right\rangle \cong \mathbb{Z} \times C_2$$

and

$$N = \langle x_2 \rangle \cong \mathbb{Z}, \quad Q = \left\langle q_2 \mid q_2^2 \right\rangle \cong C_2.$$

Then, it is clear that an epimorphism (isomorphism) from G to $N \times Q$ exists.

Consider the epimorphism $\tau\colon G \to Q$ defined by $\tau(x_1) = q_2$ and $\tau(q_1) = 1_Q$. For a homomorphism $\kappa\colon G \to N \times Q$ to satisfy condition (2), for all $n \in N$, there must exist $g \in \ker(\tau) = \{1_G, q_1\}$ such that $\kappa(g) = ns(1_Q) = (n, 1_Q)$. However, this is impossible since $N \times \{1_Q\}$ is infinite.

This example demonstrates that items (a)–(c) are all required. It is not sufficient to have an epimorphism τ and a homomorphism κ that do not satisfy conditions (b) and (c).

Example 4.10 (When no epimorphism exists)**.** Here, we demonstrate a counterintuitive example of when an epimorphism doesn't exist. First, we demonstrate why an epimorphism does not exist. Let

$$G = \left\langle x, y, t \mid [x, y], t^2, txty \right\rangle \cong \mathbb{Z}^2 \rtimes \mathbb{Z}_2$$

and

$$H = \left\langle a, b, q \mid [a, b], [a, q], [b, q], q^2 \right\rangle \cong \mathbb{Z}^2 \times \mathbb{Z}_2.$$

Denote the abelianisation of a group G as G_{ab}, see Section 6.3 and Definition 6.12 for formal definitions and justification of the following claim. If there exists an epimorphism $G \to H$ then there exists an epimorphism from the $G_{ab} \to H_{ab}$.

H is already abelian, and the abelianisation of G can be presented as follows

$$G = \left\langle x, y, t \mid [x, y], t^2, txty \right\rangle$$
$$G_{ab} = \left\langle x, y, t \mid [x, y], t^2, txty, [x, t], [y, t] \right\rangle$$

By the relations $[x,t]$, $[y,t]$ and $txty$ it is implied that $x = y^{-1}$ in this group. Then it can be verified that

$$G_{ab} \cong \left\langle x, t \mid [x, t] = t^2 \right\rangle \cong \mathbb{Z} \times \mathbb{Z}_2.$$

As there cannot exist an epimorphism $\mathbb{Z} \to \mathbb{Z}^2$, it follows that no epimorphism $G_{ab} \to H_{ab} = H$ can exist.

This can also be demonstrated by attempting to find τ and κ as per Lemma 4.7. Here, $Q = \langle q \mid q^2 \rangle$ just so happens to be a subgroup, we assert the following without proof. If an epimorphism $G \to H$ exists, then there must exist an epimorphism $\tau\colon G \to Q$ defined by

$$\tau\colon \begin{cases} x & \mapsto 1 \\ y & \mapsto 1 \\ t & \mapsto q \end{cases}$$

such that there exists a homomorphism $\kappa\colon G \to H$ such that

1. $\kappa(g) = ns(q)$ implies $\tau(g) = q$
2. for all $n \in N$, there exists $g \in \ker(\tau)$ such that $\kappa(g) = ns(1_Q)$.

τ as defined also maximises $\ker(\tau)$. Note that $s(q) = q$, define $\kappa\colon G \to H$ by a set map

$$\kappa\colon \begin{cases} x & \mapsto n_x s(\tau(x)) = \pi_N(x)1_Q \\ y & \mapsto n_y s(\tau(y)) = \pi_N(y)1_Q \\ t & \mapsto n_t s(\tau(t)) = \pi_N(t)q \end{cases}$$

for some $n_x, n_y, n_t \in N$. We already know $q^2 = 1_Q = 1_H$, so for κ to extend to a homomorphism the following must be satisfied

$$\begin{aligned} [n_x, n_y] &= 1_N = 1_H \\ n_t^2 &= 1_N = 1_H \\ n_t n_x n_t n_y &= 1_N = 1_H. \end{aligned}$$

As $n_t^2 = 1_N$, then either $n_t = 1_H$ or $n_t = q$, however, if $n_t = q$ then $s(t) = q^2 = 1$ contradicting Item (1). Then $n_t = 1_H$, this implies $n_t n_x n_t n_y = n_x n_y = 1_H$ which implies $n_x = n_y^{-1}$. This implies $\langle n_x, n_y \rangle \ncong \mathbb{Z}^2$, as $\ker(\tau) = \langle n_x, n_y \rangle$, then this is a contradiction of Item (2).

4.1.3 Calculations when N is Free Abelian

In this subsection, we introduce additional notation and calculations for equations in free abelian groups that will be relevant for all the relevant classes of groups in this chapter.

Definition 4.11 (Commuting equations when N is abelian)**.** Let N be an abelian group, and let u be an equation with variables $\{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$ and a single constant $\mathfrak{c} \in N$. Define the *commuted normal form* of u as the word

$$\mathsf{CNF}(u) = X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mathfrak{c}$$

where $\alpha_i = |u|_{X_i} - |u|_{X_i^{-1}}$.

The following observation is immediate.

Lemma 4.12. *Let N be an abelian group, and let $(u_i)_{[1,m]}$ be a system of equations in N, where each u_i consists of variables $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$ and a single constant. Then $\sigma\colon \mathbb{X} \to N$ is a solution to $(u_i)_{[1,m]}$ if and only if σ is a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$.*

The following is some calculations which we see use in latter sections.

Lemma 4.13. *Let $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$, $N \cong \langle x_1, \ldots, x_d \rangle$ be a free abelian group of rank d, $(\mathfrak{c}_i)_{[1,m]} \in N^m$ a list of constants, and $(u_i)_{[1,m]}$ a system of equations in N, where $u_i \in (\mathbb{X} \cup \mathbb{Y} \cup \mathfrak{c}_i)^*$ with $\mathfrak{c}_i$ appearing exactly once.*

1. *If $\mathfrak{c}_i = 1_N$ for all $i \in [1, m]$, and σ is a solution to the system of equations given by*

$$\sigma\colon \begin{cases} X_j \mapsto x_1^{c_{j,1}} \cdots x_d^{c_{j,d}}, & j \in [1, t] \\ Y_j \mapsto x_1^{c_{t+j,1}} \cdots x_d^{c_{t+j,d}}, & j \in [1, \ell]. \end{cases}$$

then

$$\sigma(u_i) = x_1^{\sum_{j=1}^{t} c_{j,1}\alpha_{i,j} + \sum_{j=1}^{\ell} c_{t+j,1}\beta_{i,j}} \cdots x_d^{\sum_{j=1}^{t} c_{j,d}\alpha_{i,j} + \sum_{j=1}^{\ell} c_{t+j,d}\beta_{i,j}} \tag{4.1}$$

where $\alpha_{(i,j)} = |u_i|_{X_j} - |u_i|_{X_j^{-1}}$ and $\beta_{(i,j)} = |u_i|_{Y_j} - |u_i|_{Y_j^{-1}}$.

2. *If $d = 1$ (i.e., N is infinite cyclic), $\mathfrak{c}_i = x^{\mathfrak{b}_i}$ for $i \in [1, m]$ with each $\mathfrak{b}_i \in \mathbb{Z}$, and σ is a solution to the system of equations given by*

$$\sigma\colon \begin{cases} X_j \mapsto x^{c_j} & j \in [1, t] \\ Y_j \mapsto x^{c_{t+j}} & j \in [1, \ell] \end{cases}$$

then

$$\sigma(u_i) = x^{\sum_{j=1}^{t} c_j \alpha_{(i,j)} + \sum_{j=1}^{\ell} c_{t+j} \beta_{(i,j)}} x^{\mathfrak{b}_i} \tag{4.2}$$

where $\alpha_{i,j} = |u_i|_{X_j} - |u_i|_{X_j^{-1}}$ and $\beta_{i,j} = |u_i|_{Y_j} - |u_i|_{Y_j^{-1}}$.

Proof. By Lemma 4.12, we may assume without loss of generality that each $u_i = \mathsf{CNF}(u_i)$ has the form

$$u_i = X_1^{\alpha_{i,1}} \cdots X_t^{\alpha_{i,t}} Y_1^{\beta_{i,1}} \cdots Y_\ell^{\beta_{i,\ell}} \mathfrak{c}_i.$$

Since σ is a solution, we have

$$\begin{aligned} \sigma(u_i) &= (x_1^{c_{1,1}} \cdots x_d^{c_{1,d}})^{\alpha_{i,1}} \cdots (x_1^{c_{t,1}} \cdots x_d^{c_{t,d}})^{\alpha_{i,t}} \cdots \\ &\quad (x_1^{c_{t+1,1}} \cdots x_d^{c_{t+1,d}})^{\beta_{i,1}} \cdots (x_1^{c_{t+\ell,1}} \cdots x_d^{c_{t+\ell,d}})^{\beta_{i,\ell}} \mathfrak{c}_i \\ &= x_1^{\sum_{j=1}^{t} c_{j,1}\alpha_{i,j} + \sum_{j=1}^{\ell} c_{t+j,1}\beta_{i,j}} \cdots x_d^{\sum_{j=1}^{t} c_{j,d}\alpha_{i,j} + \sum_{j=1}^{\ell} c_{t+j,d}\beta_{i,j}} \mathfrak{c}_i. \end{aligned}$$

If $\mathfrak{c}_i = 1_N$, we obtain Equation (4.1).

If $d = 1$, let $x_1 = x$ and $\mathfrak{c}_i = x^{\mathfrak{b}_i}$ for some $\mathfrak{b}_i \in \mathbb{Z}$. Substituting, we obtain Equation (4.2). □

4.1.4 System of Equations and Matrix Problems

In this subsection, we demonstrate the equivalence between systems of equations over a group N and integer matrix problems. Specifically, we provide a method to convert a system of equations into integer matrix elements and vice versa, under the assumption that the group N is free abelian. The integer matrices correspond to the inputs for the matrix problems discussed in Chapter 3.

Definition 4.14 (System of equations to matrix system)**.** Let

- $d, t, \ell, m \in \mathbb{Z}$,
- $N = \langle x_1, \ldots, x_d \rangle \in \mathsf{FreeAb}$,
- $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$,
- $v_i \in (\mathbb{X} \cup \mathbb{Y})^*$ for $i \in [1, m]$,
- $\mathfrak{c}_i \in N$ with $\mathfrak{c}_i = x_1^{b_{i,1}} \cdots x_d^{b_{i,d}}$ for $i \in [1, m]$,
- $(u_i)_{[1,m]}$ be a system of equations in N, where each equation is of the form $u_i = v_i \mathfrak{c}_i$.

For each $i \in [1, m]$, the commuted normal form (Definition 4.11) of u_i is

$$\mathsf{CNF}(u_i) = X_1^{\alpha_{i,1}} \ldots X_t^{\alpha_{i,t}} Y_1^{\beta_{i,1}} \ldots Y_\ell^{\beta_{i,\ell}} \mathfrak{c}_i.$$

where

$$\alpha_{i,j} = |v_i|_{X_j} - |v_i|_{X_j^{-1}} \quad \text{and} \quad \beta_{i,k} = |v_i|_{Y_k} - |v_i|_{Y_k^{-1}}$$

for $j \in [1, t]$ and $k \in [1, \ell]$.

Define $\mathsf{EqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]})$ to be the triple (A, B, ℓ), with $A \in \mathbb{Z}^{m \times (t+\ell)}$, $B \in \mathbb{Z}^{m \times d}$, where

$$A = \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,t} & \beta_{1,1} & \cdots & \beta_{1,\ell} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{m,1} & \cdots & \alpha_{m,t} & \beta_{m,1} & \cdots & \beta_{m,\ell} \end{pmatrix}, \quad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,d} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,d} \end{pmatrix}.$$

Definition 4.15 (Matrices to system of equations)**.** Given $\ell \in \mathbb{Z}$, matrices $A \in \mathbb{Z}^{m\times n}$ and $B \in \mathbb{Z}^{m\times d}$, where

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}, \quad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,d} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,d} \end{pmatrix},$$

define $\mathsf{MatEqn}(A, B, \ell)$ to be the quintuple $(d, n-\ell, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]})$, where $(u_i)_{[1,m]}$ is a system of equations with variables

$$\{X_1, X_1^{-1}, \ldots, X_{n-\ell}, X_{n-\ell}^{-1}, Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$$

over a free abelian group $N = \langle x_1, \ldots, x_d\rangle$ of rank d, where each u_i is of the form

$$u_i = v_i \mathfrak{c}_i,$$

with

$$v_i = X_1^{a_{i,1}} \cdots X_{n-\ell}^{a_{i,n-\ell}} Y_1^{a_{i,n-\ell+1}} \cdots Y_\ell^{a_{i,n}}$$

and

$$\mathfrak{c}_i = x_1^{b_{i,1}} \cdots x_d^{b_{i,d}} \in N.$$

The following is immediate from the definitions.

Lemma 4.16. *The following computations can be achieved in polynomial time*

1. *On input finite sets $\mathcal{X}, \mathcal{Y}, \mathcal{R} \subseteq (\mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1})^*$, compute* $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$.
2. *On input $d, t, \ell \in \mathbb{Z}$, a system of equations $(u_i)_{[1,m]}$ where each $u_i = v_i\mathfrak{c}_i$, v_i is a word in variables $\{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}, Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$, and $\mathfrak{c}_i = x_1^{b_{i,1}} \cdots x_d^{b_{i,d}}$, compute* $\mathsf{EqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]})$.
3. *On input $A \in \mathbb{Z}^{m\times n}$, $B \in \mathbb{Z}^{m\times d}$, and $\ell \in \mathbb{Z}$, compute* $\mathsf{MatEqn}(A, B, \ell)$.

4.2 Direct Product Targets

In this section, we show that the epimorphism problem from a finitely presented group to the direct product of a free abelian group of rank d and a finite group is in P. We begin by translating the epimorphism problem into the problem EquationsSubspan which is given as follows

Problem:	EquationsSubspan
Input:	A group N, variables $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$, and a finite system of equations over N using variables $\mathbb{X} \cup \mathbb{Y}$.
Question:	Is there a solution $\sigma\colon \mathbb{X} \cup \mathbb{Y} \to N$ such that $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell)\rangle = N$?

Definition 4.17 (Presentation to system of equations)**.** On input a presentation of the form $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R}\rangle$, where $\mathcal{X}, \mathcal{Y}, \mathcal{R}$ are finite, define $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$ to be the set of equations constructed as follows.

Let

- $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_{|\mathcal{X}|}, X_{|\mathcal{X}|}^{-1}\}$,
- $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_{|\mathcal{Y}|}, Y_{|\mathcal{Y}|}^{-1}\}$,

be sets of variables, and let $\zeta\colon \mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1} \to \mathbb{X} \cup \mathbb{Y}$ be the bijection defined as

$$\zeta\colon x_j \mapsto X_j, \quad x_j^{-1} \mapsto X_j^{-1}, \quad y_j \mapsto Y_j, \quad y_j^{-1} \mapsto Y_j^{-1}.$$

Then $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$ is the system of equations $(\zeta(r_i))_{i\in[1,|\mathcal{R}|]}$.

Note that by definition, $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$ is a system of equations without constants.

Lemma 4.18 (Epimorphism onto direct products)**.** *Let $G, N \in \mathsf{FinPres}$ and $Q \in \mathsf{Fin}$. The following are equivalent:*

1. *There exists an epimorphism from G to $N \times Q$.*
2. *There exists an epimorphism $\tau\colon G \to Q$ such that, for some (Q,τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R}\rangle$ of G,* EquationsSubspan *returns 'Yes' on input N and* $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$.

Proof. Assume there exists an epimorphism from G to $N \times Q$. By Lemma 4.7 and Remark 4.8, there exist $\tau\colon G \to Q$ (an epimorphism) and $\kappa\colon G \to N \times Q$ (a homomorphism) such that

(b) $\kappa(g) = (n, s(q))$ implies $q = \tau(g)$,
(c') For all $n \in N$, there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(w) = (n, 1_Q)$.

Let $\sigma = \pi_N \circ \kappa \circ \zeta^{-1}$, where ζ is the bijection defined in Definition 4.17. Then $\sigma\colon \mathbb{X} \cup \mathbb{Y} \to N$ is the map

$$\begin{aligned} \sigma(X) &= \pi_N(\kappa(\zeta^{-1}(X))) = \pi_N(\kappa(x)), & \sigma(X^{-1}) &= \pi_N(\kappa(x))^{-1} \\ \sigma(Y) &= \pi_N(\kappa(\zeta^{-1}(Y))) = \pi_N(\kappa(y)), & \sigma(Y^{-1}) &= \pi_N(\kappa(y))^{-1}. \end{aligned}$$

Since κ is a homomorphism, for each $r \in \mathcal{R}$, we have $\kappa(r) = (1_N, 1_Q)$, which means

$$\sigma(\zeta(r)) = \pi_N(\kappa(r)) = 1_N,$$

verifying that σ is a solution to $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$.

By item (c'), for all $n \in N$, there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(w) = ns(1_Q)$, so $\pi_N(\kappa(w)) = n$. Then there exists $\zeta(w) \in \mathbb{Y}^*$ which satisfies

$$\begin{aligned} \sigma(\zeta(w)) &= \pi_N(\kappa(\zeta^{-1}(\zeta(w)))) \\ &= \pi_N(\kappa(w)) = n \end{aligned}$$

which implies $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell)\rangle = N$. Therefore, EquationsSubspan returns 'Yes'.

Conversely, assume there exists an epimorphism $\tau\colon G \to Q$ such that for some (Q,τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R}\rangle$ for G, EquationsSubspan returns 'Yes' on input N and the system of equations $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$. This means there is a solution $\sigma\colon \mathbb{X} \cup \mathbb{Y} \to N$ such that $\sigma(\zeta(r)) = 1_N$ for each $r \in \mathcal{R}$ and $\left\langle \sigma(Y_1), \ldots, \sigma(Y_{|\mathcal{Y}|})\right\rangle = N$.

Define a set map $\kappa\colon \mathcal{X} \cup \mathcal{Y} \to N \times Q$ by

$$\kappa\colon \begin{cases} x \mapsto (\sigma(X), \tau(x)), & x \in \mathcal{X} \\ y \mapsto (\sigma(Y), \tau(y)), & y \in \mathcal{Y} \end{cases}$$

and extend κ to a monoid homomorphism $\kappa\colon (\mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1})^* \to N \times Q$.

For each $r \in \mathcal{R}$, where $r = v_1 \cdots v_k$ with $v_i \in \mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1}$, we have

$$\begin{aligned} \kappa(r) &= \kappa(v_1) \cdots \kappa(v_k) \\ &= (\sigma(\zeta(v_1)), \tau(v_1)) \cdots (\sigma(\zeta(v_k)), \tau(v_k)) \\ &= (\sigma(\zeta(v_1)) \cdots \sigma(\zeta(v_k)), \tau(v_1) \cdots \tau(v_k)) \\ &= (\sigma(\zeta(r)), \tau(r)) = (1_N, 1_Q), \end{aligned}$$

where $\tau(r) = 1_Q$ since τ is a homomorphism. By Lemma 2.28, κ is a homomorphism from G to $N \times Q$.

For any $g \in G$, there exists $w \in (\mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1})^*$ with $g =_G w$. Then,

$$\kappa(g) = \kappa(w) = (\sigma(w), \tau(w)) = (\sigma(w), \tau(g)).$$

Thus, $\kappa(g) = (n, q)$ implies $q = \tau(g)$.

Since $\left\langle \sigma(Y_1), \ldots, \sigma(Y_{|\mathcal{Y}|}) \right\rangle = N$, for each $n \in N$, there exists $w \in \mathbb{Y}^*$ such that $\sigma(w) = n$. Therefore, for each $n \in N$, there exists $\zeta^{-1}(w) \in \langle \mathcal{Y} \rangle$ such that $\sigma(\zeta(\zeta^{-1}(w))) = \sigma(w) = n$.

Having found homomorphisms τ and κ, and established conditions (a), (b), and (c') as in Lemma 4.7 and Remark 4.8, we have shown the existence of an epimorphism from G to $N \times Q$. □

For the remainder of this section, we assume N is free abelian of finite rank.

Lemma 4.19. *Let*

1. $N \in \mathsf{FreeAb}$ *have rank* d,
2. $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$,
3. $(u_i)_{[1,m]}$ *be a system of equations in* N *without constants, where each* $u_i \in (\mathbb{X} \cup \mathbb{Y})^*$,
4. $(A, 0, \ell) = \mathsf{EqnMat}(d, t, \ell, (u_i)_{[1,m]}, (1_N)_{[1,m]})$.

The following are equivalent:

1. EquationsSubspan *returns 'Yes' on input* N *and* $(u_i)_{[1,m]}$,
2. MatrixSubspanA *returns 'Yes' on input* (A, d, ℓ).

Proof. Let

$$A = \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,t} & \beta_{1,1} & \cdots & \beta_{1,\ell} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{m,1} & \cdots & \alpha_{m,t} & \beta_{m,1} & \cdots & \beta_{m,\ell} \end{pmatrix} \in \mathbb{Z}^{m \times (t+\ell)}.$$

such that for each $i \in [1, m]$

$$\mathsf{CNF}(u_i) = X_1^{\alpha_{i,1}} \cdots X_t^{\alpha_{i,t}} Y_1^{\beta_{i,1}} \cdots Y_\ell^{\beta_{i,\ell}},$$

where

$$\alpha_{i,j} = |u_i|_{X_j} - |u_i|_{X_j^{-1}}, \quad \beta_{i,k} = |u_i|_{Y_k} - |u_i|_{Y_k^{-1}},$$

for $j \in [1, t]$ and $k \in [1, \ell]$.

By definition, EquationsSubspan on input N and $(u_i)_{[1,m]}$ returns 'Yes' if and only if there exists a solution $\sigma \colon \mathbb{X} \cup \mathbb{Y} \to N$ such that

1. σ satisfies $(u_i)_{[1,m]}$,
2. $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle = N$,
3. σ is also a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$ by Lemma 4.12.

We may write the solution as

$$\sigma \colon \begin{cases} X_j \mapsto x_1^{c_{j,1}} \cdots x_d^{c_{j,d}}, \quad X_j^{-1} \mapsto (x_1^{c_{j,1}} \cdots x_d^{c_{j,d}})^{-1} & j \in [1, t] \\ Y_j \mapsto x_1^{c_{t+j,1}} \cdots x_d^{c_{t+j,d}}, \quad Y_j^{-1} \mapsto (x_1^{c_{t+j,1}} \cdots x_d^{c_{t+j,d}})^{-1} & j \in [1, \ell]. \end{cases}$$

for some $c_{j,k} \in \mathbb{Z}$. Let

$$V = \begin{pmatrix} c_{1,1} & \cdots & c_{1,d} \\ \vdots & \ddots & \vdots \\ c_{t+\ell,1} & \cdots & c_{t+\ell,d} \end{pmatrix} \in \mathbb{Z}^{(t+\ell) \times d},$$

for $i \in [1,d]$, let $v_i \in \mathbb{Z}^{t+\ell}$ denote the i-th column of V, and for $i \in [1,\ell]$ let μ_i denote the i-th column of $(V_\ell)^T$.

By Lemma 4.13 and Eq. (4.1), for each $i \in [1,m]$, we have

$$\sigma(u_i) = x_1^{\sum_{j=1}^{t} c_{j,1}\alpha_{i,j} + \sum_{j=1}^{\ell} c_{t+j,1}\beta_{i,j}} \cdots x_d^{\sum_{j=1}^{t} c_{j,d}\alpha_{i,j} + \sum_{j=1}^{\ell} c_{t+j,d}\beta_{i,j}}.$$

Then, for $i \in [1,m]$, $\sigma(u_i) = 1_N$ if and only if

$$\sum_{j=1}^{t} c_{j,k}\alpha_{i,j} + \sum_{j=1}^{\ell} c_{t+j,k}\beta_{i,j} = 0 \tag{4.3}$$

for each $k \in [1,d]$.

Then $\sigma\colon \mathbb{X} \cup \mathbb{Y} \to N$ is a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$ and $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell)\rangle = N$ if and only if

$$\begin{aligned} AV &= \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,t} & \beta_{1,1} & \cdots & \beta_{1,\ell} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{m,1} & \cdots & \alpha_{m,t} & \beta_{m,1} & \cdots & \beta_{m,\ell} \end{pmatrix} \begin{pmatrix} c_{1,1} & \cdots & c_{1,d} \\ \vdots & \ddots & \vdots \\ c_{t+\ell,1} & \cdots & c_{t+\ell,d} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^{t} c_{j,1}\alpha_{1,j} + \sum_{j=1}^{\ell} c_{t+j,1}\beta_{1,j} & \cdots & \sum_{j=1}^{t} c_{j,d}\alpha_{1,j} + \sum_{j=1}^{\ell} c_{t+j,d}\beta_{1,j} \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{t} c_{j,1}\alpha_{m,j} + \sum_{j=1}^{\ell} c_{t+j,1}\beta_{m,j} & \cdots & \sum_{j=1}^{t} c_{j,d}\alpha_{m,j} + \sum_{j=1}^{\ell} c_{t+j,d}\beta_{m,j} \end{pmatrix} \\ &= \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \text{ by Eq. (4.3).} \end{aligned}$$

Equivalently, $\sigma\colon \mathbb{X} \cup \mathbb{Y} \to N$ is a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$ and $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell)\rangle = N$ if and only if $Av_i = 0$ for $i \in [1,d]$ and $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell)\rangle = N$.

Recall the natural isomorphism $\phi\colon N \to \mathbb{Z}^d$ (Definition 2.42). For each $i \in [1,\ell]$, we have

$$\begin{aligned} \varphi(\sigma(Y_i)) &= \varphi(x_1^{c_{t+i,1}} \cdots x_d^{c_{t+i,d}}) \\ &= c_{t+i,1}e_1 + \cdots + c_{t+i,d}e_d = \mu_i. \end{aligned}$$

Then $Av_i = 0$ for $i \in [1,d]$ and $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell)\rangle = N$ if and only if $Av_i = 0$ for $i \in [1,d]$ and, for each $h \in N$, there exists $w \in \mathbb{Y}^*$ such that $\sigma(w) = h$. This holds if and only if $Av_i = 0$ for $i \in [1,d]$ and, for each $z \in \mathbb{Z}^d$, there exists $w \in \mathbb{Y}^*$ such that $\varphi(\sigma(w)) = z$.

Write $\mathsf{CNF}(w) = Y_1^{b_1} \cdots Y_\ell^{b_\ell}$. Then

$$\begin{aligned} z = \varphi(\sigma(w)) &= \varphi(\sigma(Y_1)^{b_1} \cdots \sigma(Y_\ell)^{b_\ell}) \\ &= b_1\mu_1 + \cdots + b_\ell\mu_\ell. \end{aligned}$$

Therefore, $Av_i = 0$ for $i \in [1,d]$ and $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell)\rangle = N$ if and only if $Av_i = 0$ for $i \in [1,d]$ and

$$\operatorname{span}((V|_\ell)^T) = \operatorname{span}(\mu_1, \ldots, \mu_\ell) = \mathbb{Z}^d,$$

which is true if and only if MatrixSubspanA returns 'Yes'. □

Combining the above results with Proposition 3.10, namely, that MatrixSubspanA can be decided in polynomial time, gives the following.

Proposition 4.20. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Ab} \times \mathsf{Fin})$ *is in* NP.

Proof. Let $G \in \mathsf{FinPres}$, $N \in \mathsf{FreeAb}$, and $Q \in \mathsf{Fin}$. Using Lemma 4.18, we may verify the existence of an epimorphism from G to $N \times Q$ by verifying that

(i) there exists an epimorphism $\tau\colon G \to Q$
(ii) for some (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G, the output to $\mathsf{EquationsSubspan}$ is 'Yes' on input N and $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$.

On input $G = \langle \mathcal{G} \mid \mathcal{R} \rangle$, $d \in \mathbb{N}_+$ encoding a free abelian group N of rank d, and a multiplication table encoding a finite group Q, the following procedure solves our problem

1. Guess a set map $\tau\colon \mathcal{G} \to Q$ and verify that it extends to an epimorphism $\tau\colon G \to Q$.
2. Construct a (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$.
3. Construct a system of equations from $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$, denoted as $(u_i)_{[1,m]}$.
4. Construct the triple $(A, 0_{m,d}, |\mathcal{Y}|) = \mathsf{EqnMat}(d, |\mathcal{X}|, |\mathcal{Y}|, (u_i)_{[1,m]}, (1_N)_{[1,m]})$, where $A \in \mathbb{Z}^{m \times (|\mathcal{X}| + |\mathcal{Y}|)}$.
5. Return the output of $\mathsf{MatrixSubspanA}$ on input $(A, d, |\mathcal{Y}|)$.

Step (1) verifies the existence of Condition (i). Steps (1) to (3) build the necessary data to solve Condition (ii). Lemma 4.19 states that to solve $\mathsf{EquationsSubspan}$, we can solve $\mathsf{MatrixSubspanA}$ on input $(A, 0, |\mathcal{Y}|)$ constructed in Step (4). Thus, we solve $\mathsf{MatrixSubspanA}$ in Step (5) and output the solution.

The time complexity of the procedure is as follows

1. We verify the correct τ in NP by Lemma 4.1; this is the only non-deterministic step of our algorithm.
2. A construction of (Q, τ)-presentation in P exists by Lemma 4.5.
3. $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$ is a polynomial-time construction by Lemma 4.16.
4. $\mathsf{EqnMat}(d, |\mathcal{X}|, |\mathcal{Y}|, (u_i)_{[1,m]}, (1_N)_{[1,m]})$ is a polynomial-time construction by Lemma 4.16.
5. $\mathsf{MatrixSubspanA}$ is solved in P by Proposition 3.10.

Thus, our algorithm is in NP. □

4.3 Virtually Cyclic Targets

In this section, we show that the epimorphism problem from a finitely presented group to a virtually cyclic group is in P. We begin by translating the epimorphism problem into an equations problem.

Recall that $\mathsf{SpecialExt}$ (Definition 2.78) refers to the class of N by Q extensions where Q is finite, N is abelian, and there exists a transversal map s and a subset $\mathcal{I} \subseteq Q$ such that

$$\theta_s(q) = \begin{cases} n \mapsto n^{-1} & q \in \mathcal{I} \\ n \mapsto n & q \in Q \setminus \mathcal{I}, \end{cases}$$

and for all $n \in N$,

$${}^{s(q)}n = s(q)ns(q)^{-1} = \begin{cases} n^{-1} & q \in \mathcal{I}, \\ n & q \in Q \setminus \mathcal{I}. \end{cases}$$

The data for a group in $\mathsf{SpecialExt}$ is given as $N \in \mathsf{FreeAb}$, $Q \in \mathsf{Fin}$, and special extension data $(\mathcal{I}, f_s)$. Additionally, as introduced in Definition 2.64, for $k \geq 2$, the notation $\tilde{f}_k\colon Q^k \to N$ is defined as

$$\tilde{f}_k(a_1, \ldots, a_k) = f_s(a_1, a_2) f_s(a_1 a_2, a_3) \cdots f_s(a_1 \cdots a_{k-1}, a_k).$$

The next two definitions introduce some notation that will be useful in the proofs below.

Definition 4.21 (Left A-count)**.** Let A, B be two disjoint sets and $w \in (A \cup B \cup A^{-1} \cup B^{-1})^*$. Write $w = v_1 \cdots v_n$, where $v_i \in A \cup B \cup A^{-1} \cup B^{-1}$. For each $p \in [1, n]$, define:

$$k_p = |v_1 \cdots v_{p-1}|_A - |v_1 \cdots v_{p-1}|_{A^{-1}}$$

called the *left A-count of w at position p*. Define

$$\operatorname{sgn}(w, A, p) = (-1)^{k_p}.$$

The value $\operatorname{sgn}(w, A, p)$ encodes whether the number of letters from A minus the number of letters from A^{-1} (ignoring all letters from B) in the length $p-1$ prefix of w is odd or even.

Definition 4.22. Let $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ be a (Q, τ)-presentation for a group G, and let $\mathcal{I} \subseteq \mathcal{X}$. Define $\mathcal{I}_\mathcal{X} = \{x \in \mathcal{X} \mid \tau(x) \in \mathcal{I}\}$ as the preimage of $\mathcal{I}$ under the bijection $\tau_X \colon \mathcal{X} \to Q$. For $r \in (\mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1})^*$, define $\gamma(r)$ to be the word obtained by raising the p-th letter of r to the power $\operatorname{sgn}(r, \mathcal{I}_\mathcal{X}, p)$ for each $p \in [1, |r|]$.

Example 4.23. If $r = x_1 y_1 x_3^{-2} y_2 x_1^{-1} x_2^{-1} y_1 x_1$ and $\mathcal{I}_\mathcal{X} = \{x_2, x_3\}$, then

$$\gamma(r) = x_1 y_1 x_3^{-1} x_3 y_2 x_1^{-1} x_2^{-1} y_1^{-1} x_1^{-1}.$$

Below is the working table for $\operatorname{sgn}(r, \mathcal{I}_\mathcal{X}, p)$ and the resulting transformation

Letter	p (Position)	k_p	$\operatorname{sgn}(r, \mathcal{I}_\mathcal{X}, p)$	Replaced by
x_1	1	0	1	x_1
y_1	2	0	1	y_1
x_3^{-1}	3	0	1	x_3^{-1}
x_3^{-1}	4	-1	-1	x_3
y_2	5	-2	1	y_2
x_1^{-1}	6	-2	1	x_1^{-1}
x_2^{-1}	7	-2	1	x_2^{-1}
y_1	8	-3	-1	y_1^{-1}
x_1	9	-3	-1	x_1^{-1}

Remark 4.24. The purpose of defining γ in this way will become evident in the proof of Lemma 4.26.

Next, we define a way to construct a system of equations from a presentation, which will be useful for analysing epimorphisms onto the class $\mathsf{SpecialExt}$, analogous to the construction in Definition 4.17 for direct products.

Definition 4.25 (Presentation to system of equations for $\mathsf{SpecialExt}$)**.** Let $H \in \mathsf{SpecialExt}$ be an N by Q extension with special extension data $(\mathcal{I}, f_s)$. Suppose $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ is a (Q, τ)-presentation for a group G, $\mathcal{I} \subseteq \mathcal{X}$, and $\mathbb{X}, \mathbb{Y}$ are alphabets such that $\mathcal{X} \cup \mathcal{X}^{-1}$ is in bijection with $\mathbb{X}$ and $\mathcal{Y} \cup \mathcal{Y}^{-1}$ is in bijection with $\mathbb{Y}$ via the map

$$\zeta \colon x_j \mapsto X_j, \quad x_j^{-1} \mapsto X_j^{-1}, \quad y_j \mapsto Y_j, \quad y_j^{-1} \mapsto Y_j^{-1}.$$

Define $\mathcal{I}_\mathcal{X} = \{x \in \mathcal{X} \mid \tau(x) \in \mathcal{I}\}$ as the preimage of $\mathcal{I}$ under the bijection $\tau|_X \colon \mathcal{X} \to Q$, γ as in Definition 4.22, and $\tilde{f}_k$ as in Definition 2.64.

For $i \in [1, |\mathcal{R}|]$, assume each $r_i \in \mathcal{R}$ has the form

$$r_i = v_{i,1} \ldots v_{i,|r_i|} \quad \text{where} \quad v_{i,j} \in \mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1}.$$

Define $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$ as the system of equations $(u_i)_{[1,|\mathcal{R}|]}$, where

$$u_i = \zeta(\gamma(r_i)) \tilde{f}_{|r_i|}(\tau(v_{i,1}), \ldots, \tau(v_{i,|r_i|})).$$

Note that by definition, $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$ is a system of equations with variables in $\mathbb{X} \cup \mathbb{Y}$ and a single constant. It is clear from the above definitions that this system can be constructed in polynomial time, as each equation size is linear on the size of each relation, with the addition of the $\tilde{f}_{|r_i|}$ function is polynomial time.

We will now show how this system arises in the context of epimorphisms to $\mathsf{SpecialExt}$.

Lemma 4.26. *Let $G \in \mathsf{FinPres}$, $N \in \mathsf{FreeAb}$, $Q \in \mathsf{Fin}$, and $H \in \mathsf{SpecialExt}$, where H is an N by Q extension with special extension data $(\mathcal{I}, f_s)$. The following are equivalent*

1. *There exists an epimorphism from G to H.*
2. *There exists an epimorphism $\tau\colon G \to Q$ such that, for some (Q,τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ of G, $\mathsf{EquationsSubspan}$ returns 'Yes' on input N and $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$.*

Proof. Assume there exists an epimorphism from G to H. By Lemma 4.7 and Remark 4.8, there exist an epimorphism $\tau\colon G \to Q$ and a homomorphism $\kappa\colon G \to H$ such that

(b) $\kappa(g) = ns(q)$ implies $q = \tau(g)$.
(c') For all $n \in N$, there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(w) = ns(1_Q)$.

Here, $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ is a (Q,τ)-presentation for G.

For $r \in \mathcal{R}$, let $r = v_1 \cdots v_k$ with $v_i \in (\mathcal{X} \cup \mathcal{Y}) \cup (\mathcal{X} \cup \mathcal{Y})^{-1}$. For each v_i, we have

$$\kappa(v_i) = \pi_N(\kappa(v_i))s(\tau(v_i)) = \pi_N(\kappa(v_i))s(v_i')$$

where $v_i' = \tau(v_i)$. Since κ is a homomorphism and r is a relation, we obtain

$$1_N = \kappa(r) = \kappa(v_1)\kappa(v_2)\cdots\kappa(v_k) = \pi_N(\kappa(v_1))s(v_1')\pi_N(\kappa(v_2))s(v_2')\cdots\pi_N(\kappa(v_k))s(v_k'). \tag{4.4}$$

Let us first deal with the term $s(v_1')\cdots s(v_k')$ at the end of Eq. (4.4). By definition of the map $f_s\colon Q \times Q \to N$ we have

$$s(v_1')s(v_2') = f_s(v_1', v_2')s(v_1'v_2')$$

then

$$\begin{aligned} s(v_1')s(v_2')s(v_3') = f_s(v_1', v_2')s(v_1'v_2')s(v_3') &= f_s(v_1', v_2')f_s(v_1'v_2', v_3')s(v_1'v_2'v_3') \\ &= \tilde{f}_3(v_1', v_2', v_3')s(v_1'v_2'v_3'). \end{aligned}$$

Repeating this we obtain

$$\begin{aligned} s(v_1')\cdots s(v_k') &= \tilde{f}_k(v_1', \ldots, v_k')s(v_1'\cdots v_k') \\ &= \tilde{f}_k(v_1', \ldots, v_k')s(\tau(v_1\cdots v_k)) \\ &= \tilde{f}_k(v_1', \ldots, v_k')s(\tau(r)) \\ &= \tilde{f}_k(v_1', \ldots, v_k') \end{aligned} \tag{4.5}$$

since $r \in \mathcal{R}$ and τ is a homomorphism so $s(\tau(r)) = s(1_Q) = 1_H$.

Now we will deal with the term

$$\pi_N(\kappa(v_1))[^{s(v_1')}\pi_N(\kappa(v_2))][^{s(v_1')s(v_2')}\pi_N(\kappa(v_3))]\cdots[^{s(v_1')\cdots s(v_k')}\pi_N(\kappa(v_k))]$$

at the start of Eq. (4.4). Recall from Definition 4.22 that $\mathcal{I}_{\mathcal{X}}$ is the preimage of $\mathcal{I} \subseteq Q$ under the bijection $\tau|_X$.

If $v_i \in \mathcal{Y} \cup \mathcal{Y}^{-1}$, then $v_i' = \tau(v_i) = 1_Q$, so conjugation by $s(v_i')$ sends $n \mapsto n$. Furthermore, conjugation by $s(\tau(v_i))$ sends $n \mapsto n$ if $v_i \in \mathcal{X} \setminus \mathcal{I}_{\mathcal{X}}$, and $n \mapsto n^{-1}$ if $v_i \in \mathcal{I}_{\mathcal{X}}$. Thus,

conjugation by $s(v_1')\cdots s(v_{p-1}')$ sends $\pi_N(\kappa(v_p))$ to $\pi_N(\kappa(v_p))^{\mathrm{sgn}(r,\mathcal{I},p)} = \gamma(\pi_N(\kappa(v_p)))$, as defined in Definition 4.22. Therefore

$$\begin{aligned}
&\pi_N(\kappa(v_1))[^{s(v_1')}\pi_N(\kappa(v_2))][^{s(v_1')s(v_2')}\pi_N(\kappa(v_3))]\cdots[^{s(v_1')\cdots s(v_k')}\pi_N(\kappa(v_k))]\\
&= \gamma(\pi_N(\kappa(v_1))\pi_N(\kappa(v_2))\cdots\pi_N(\kappa(v_k)))\\
&= \gamma(\pi_N(\kappa(v_1\cdots v_k)))\\
&= \gamma(\pi_N(r)) = 1_N.
\end{aligned}$$

We have now shown that Eq. (4.4) becomes

$$1_N = \gamma(\pi_N(r))\tilde{f}_k(v_1',\ldots,v_k'). \tag{4.6}$$

Let $\sigma = \pi_N\circ\kappa\circ\zeta^{-1}$, where ζ is the bijection defined in Definition 4.25. Then $\sigma\colon \mathbb{X}\cup\mathbb{Y}\to N$ is the map

$$\begin{aligned}
\sigma(X_i) &= \pi_N(\kappa(\zeta^{-1}(X_i))) = \pi_N(\kappa(x_i)), & \sigma(X_i^{-1}) &= \pi_N(\kappa(x_i))^{-1}\\
\sigma(Y_i) &= \pi_N(\kappa(\zeta^{-1}(Y_i))) = \pi_N(\kappa(y_i)), & \sigma(Y_i^{-1}) &= \pi_N(\kappa(y_i))^{-1}.
\end{aligned}$$

Let γ be as defined in Definition 4.25, for $i\in[1,m]$, the equation u_i is derived from $r_i = v_{i,1}\ldots v_{i,|r_i|}$, where $v_{i,j}\in\mathcal{X}\cup\mathcal{Y}\cup\mathcal{X}^{-1}\cup\mathcal{Y}^{-1}$, and has the form

$$\begin{aligned}
u_i &= \zeta(\gamma(r_i))\tilde{f}_{|r_i|}(\tau(v_{i,1}),\ldots,\tau(v_{i,|r_i|}))\\
&= \gamma(\zeta(r_i))\tilde{f}_{|r_i|}(\tau(v_{i,1}),\ldots,\tau(v_{i,|r_i|})).
\end{aligned}$$

Thus

$$\begin{aligned}
\sigma(u_i) &= \gamma(\pi_N(\kappa(r_i)))\tilde{f}_{|r_i|}(\tau(v_{i,1}),\ldots,\tau(v_{i,|r_i|}))\\
&= 1_N
\end{aligned}$$

by Eq. (4.6), which means σ is a solution to the system.

By item (c'), for all $n\in N$, there exists $w\in(\mathcal{Y}\cup\mathcal{Y}^{-1})^*$ such that $\kappa(w) = ns(1_Q)$, so $\pi_N(\kappa(w)) = n$. Then there exists $\zeta(w)\in\mathbb{Y}^*$ which satisfies

$$\begin{aligned}
\sigma(\zeta(w)) &= \pi_N(\kappa(\zeta^{-1}(\zeta(w))))\\
&= \pi_N(\kappa(w)) = n
\end{aligned}$$

which implies $\langle\sigma(Y_1),\ldots,\sigma(Y_\ell)\rangle = N$. Therefore, EquationsSubspan returns 'Yes'.

Conversely, assume that there exists an epimorphism $\tau\colon G\to Q$ and, for some (Q,τ)-presentation $\langle\mathcal{X}\cup\mathcal{Y}\mid\mathcal{R}\rangle$ for G, there is a solution $\sigma\colon\mathbb{X}\cup\mathbb{Y}\to N$ to the system $\mathsf{PresEqnB}(\tau,\mathcal{X},\mathcal{Y},\mathcal{R},\mathcal{I},f_s)$ such that $\langle\sigma(Y_1),\ldots,\sigma(Y_\ell)\rangle = N$. We will show that there exists a homomorphism $\kappa\colon G\to H$ such that τ,κ satisfy conditions (b) and (c') of Lemma 4.7 and Remark 4.8, thereby proving the existence of an epimorphism from G to H.

Define $\kappa\colon(\mathcal{X}\cup\mathcal{Y}\cup\mathcal{X}^{-1}\cup\mathcal{Y}^{-1})^*\to H$ as the monoid homomorphism induced by the map

$$\kappa(a) = \sigma(\zeta(a))s(\tau(a))$$

for $a\in\mathcal{X}\cup\mathcal{Y}\cup\mathcal{X}^{-1}\cup\mathcal{Y}^{-1}$.

For any $w = v_1\cdots v_n$, where $v_i\in\mathcal{X}\cup\mathcal{Y}\cup\mathcal{X}^{-1}\cup\mathcal{Y}^{-1}$, we have

$$\begin{aligned}
\kappa(w) &= \kappa(v_1)\cdots\kappa(v_n)\\
&= \sigma(\zeta(v_1))s(\tau(v_1))\cdots\sigma(\zeta(v_n))s(\tau(v_n))\\
&= \sigma(\zeta(v_1))s(v_1')\cdots\sigma(\zeta(v_n))s(v_n')
\end{aligned}$$

where $v_i' = \tau(v_i)$. Inserting $s(v_1')\cdots s(v_j')s(v_j')^{-1}\cdots s(v_1')^{-1}$, we obtain

$$\begin{aligned}\kappa(w) &= \sigma(\zeta(v_1))^{s(v_1')}\sigma(\zeta(v_2))^{s(v_1')s(v_2')}\sigma(\zeta(v_3))\cdots{}^{s(v_1')\cdots s(v_{n-1}')}\sigma(\zeta(v_n))s(v_1')\cdots s(v_n')\\ &= \gamma(\sigma(\zeta(v_1))\cdots\sigma(\zeta(v_k)))s(v_1')\cdots s(v_n')\\ &= \gamma(\sigma(\zeta(w)))\tilde{f}_k(v_1',\ldots,v_k')s(\tau(v_1\cdots v_k)) \quad \text{by Eq. (4.5)}\\ &= \gamma(\sigma(\zeta(w)))\tilde{f}_k(v_1',\ldots,v_k')s(\tau(w)).\end{aligned}$$

If $w \in \mathcal{R}$, then $\tau(w) = 1_Q$, so $s(\tau(w)) = 1_H$, and $\gamma(\zeta(w))\tilde{f}_k(v_1',\ldots,v_k') = \zeta(\gamma(w))\tilde{f}_k(v_1',\ldots,v_k')$ is an equation in the system $\mathsf{PresEqnB}(\tau,\mathcal{X},\mathcal{Y},\mathcal{R},\mathcal{I},f_s)$. Applying σ, we have $\kappa(w) = 1_N$. Thus, by Lemma 2.28, κ is a homomorphism.

For $g \in G$, suppose $w \in (\mathcal{X}\cup\mathcal{Y}\cup\mathcal{X}^{-1}\cup\mathcal{Y}^{-1})^*$ spells g. Then

$$\begin{aligned}\kappa(g) = \kappa(w) &= \gamma(\sigma(\zeta(w)))\tilde{f}_k(v_1',\ldots,v_k')s(\tau(w))\\ &= \gamma(\sigma(\zeta(w)))\tilde{f}_k(v_1',\ldots,v_k')s(\tau(g))\\ &= ns(\tau(g))\end{aligned}$$

where

$$n = \gamma(\sigma(\zeta(w)))\tilde{f}_k(v_1',\ldots,v_k') \in N.$$

Thus, condition (b) of Lemma 4.7 is satisfied.

Since $\langle\sigma(Y_1),\ldots,\sigma(Y_\ell)\rangle = N$, for all $n \in N$, there exists $w \in \mathbb{Y}^*$ such that $\sigma(w) = n$. Then, for all $n \in N$, there exists $\zeta^{-1}(w) \in (\mathcal{Y}\cup\mathcal{Y}^{-1})^*$ such that

$$\begin{aligned}\kappa(\zeta^{-1}(w)) &= \sigma(\zeta(\zeta^{-1}(w)))s(\tau(\zeta^{-1}(w)))\\ &= \sigma(w)s(\tau(\zeta^{-1}(w)))\\ &= ns(\tau(\zeta^{-1}(w))).\end{aligned}$$

Because $\ker(\tau) = \langle\mathcal{Y}\rangle$, it follows that $\tau(\zeta^{-1}(w)) = 1_Q$, and so

$$\kappa(\zeta^{-1}(w)) = ns(1_Q).$$

This satisfies condition (c') of Remark 4.8, thereby proving the existence of an epimorphism from G to H. □

For the rest of this section, we assume N is an infinite cyclic group (so H is virtually cyclic).

Recall from Definition 4.14 that $\mathsf{EqnMat}(1,t,\ell,(u_i)_{[1,m]},(\mathfrak{c}_i)_{[1,m]})$ is a triple (A,b,ℓ), where $A \in \mathbb{Z}^{m\times(t+\ell)}$ and $b \in \mathbb{Z}^{m\times 1}$.

Lemma 4.27. *Let*

- *N be an infinite cyclic group $\langle x\rangle$*
- *$\mathbb{X} = \{X_1, X_1^{-1},\ldots,X_t,X_t^{-1}\}$, $\mathbb{Y} = \{Y_1,Y_1^{-1},\ldots,Y_\ell,Y_\ell^{-1}\}$*
- *$(u_i)_{[1,m]}$ be a system of equations over N, where each equation is of the form $u_i = v_i\mathfrak{c}_i$ with $v_i \in (\mathbb{X}\cup\mathbb{Y})^*$ and $\mathfrak{c}_i = x^{b_i} \in N$ is a constant, where $b_i \in \mathbb{Z}$.*

The following are equivalent

1. $\mathsf{EquationsSubspan}$ *returns 'Yes' on input N and $(u_i)_{[1,m]}$*
2. $\mathsf{MatrixSubspanB}$ *returns 'Yes' on input $(A,b,\ell) = \mathsf{EqnMat}(1,t,\ell,(u_i)_{[1,m]},(\mathfrak{c}_i)_{[1,m]})$.*

Proof. Suppose EquationsSubspan returns 'Yes' on input N and $(u_i)_{[1,m]}$. Then there exists a solution $\sigma\colon \mathbb{X} \cup \mathbb{Y} \to N$ given by

$$\sigma\colon \begin{cases} X_j \mapsto x^{f_j} & j \in [1,t] \\ Y_k \mapsto x^{f_{t+k}} & k \in [1,\ell] \end{cases}$$

such that $\langle \sigma(Y_1), \dots, \sigma(Y_\ell) \rangle = N$. By Lemma 4.12, σ is also a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$.

By Lemma 4.13 and Eq. (4.2) we have that, for $i \in [1,m]$

$$\sigma(u_i) = x^{\sum_{j=1}^{t} f_j \alpha_{(i,j)} + \sum_{k=1}^{\ell} f_{t+k} \beta_{(i,k)}} x^{b_i} = 1_N,$$

where

$$\alpha_{(i,j)} = |u_i|_{X_j} - |u_i|_{X_j^{-1}}, \quad \beta_{(i,k)} = |u_i|_{Y_k} - |u_i|_{Y_k^{-1}},$$

for $j \in [1,t]$ and $k \in [1,\ell]$. This holds if and only if

$$\sum_{j=1}^{t} f_j \alpha_{(i,j)} + \sum_{k=1}^{\ell} f_{t+k} \beta_{(i,k)} + b_i = 0. \tag{4.7}$$

Recall from Definition 4.14 that $\mathsf{EqnMat}(1,t,\ell,(u_i)_{[1,m]},(\mathfrak{c}_i)_{[1,m]}) = (A,b,\ell)$, where

$$A = \begin{pmatrix} \alpha_{(1,1)} & \cdots & \alpha_{(1,t)} & \beta_{(1,1)} & \cdots & \beta_{(1,\ell)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{(m,1)} & \cdots & \alpha_{(m,t)} & \beta_{(m,1)} & \cdots & \beta_{(m,\ell)} \end{pmatrix}, \; b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

and let $\nu \in \mathbb{Z}^{t+\ell}$ be the integer $(t+\ell)$-vector $\nu = (f_1 \; f_2 \; \cdots \; f_{t+\ell})^T$. Then

$$\begin{aligned} A\nu + b &= \begin{pmatrix} \alpha_{(1,1)} & \cdots & \alpha_{(1,t)} & \beta_{(1,1)} & \cdots & \beta_{(1,\ell)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{(m,1)} & \cdots & \alpha_{(m,t)} & \beta_{(m,1)} & \cdots & \beta_{(m,\ell)} \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_{t+\ell} \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^{t} f_j \alpha_{(1,j)} + \sum_{j=1}^{\ell} f_{t+j} \beta_{(1,j)} + b_1 \\ \vdots \\ \sum_{j=1}^{t} f_j \alpha_{(m,j)} + \sum_{j=1}^{\ell} f_{t+j} \beta_{(m,j)} + b_m \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{by Eq. (4.7).} \end{aligned} \tag{4.8}$$

Since $\langle \sigma(Y_1), \dots, \sigma(Y_\ell) \rangle = N$, for all $h \in N$, there exists $w \in \mathbb{Y}^*$ such that $\sigma(w) = h$. Thus, for all $z \in \mathbb{Z}$, there exists $w \in \mathbb{Y}^*$ such that $\varphi(\sigma(w)) = z$, where $\phi\colon N \to \mathbb{Z}$ is the natural isomorphism (Definition 2.42.

We have

$$\begin{aligned} z = \varphi(\sigma(w)) &= \varphi(\sigma(Y_1)^{a_1} \cdots \sigma(Y_\ell)^{a_\ell}) \\ &= a_1 f_{t+1} + \cdots + a_\ell f_{t+\ell} \end{aligned}$$

where $a_i = |w|_{Y_i} - |w|_{Y_i^{-1}}$. Thus, $z \in \operatorname{span}(c_{t+1}, \dots, c_n)$, and MatrixSubspanB returns 'Yes' on input $(A,b,\ell) = \mathsf{EqnMat}(1,t,\ell,(u_i)_{[1,m]},(\mathfrak{c}_i)_{[1,m]})$.

Conversely, suppose MatrixSubspanB on input $(A, b, \ell) = \mathsf{EqnMat}(1, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]})$ returns an integer n-vector ν with $A\nu + b = 0$ and $\mathrm{span}((\nu|_\ell)^T) = \mathbb{Z}$. Define $\sigma\colon \mathbb{X} \cup \mathbb{Y} \to N$ by

$$\sigma\colon \begin{cases} X_j \mapsto x^{\nu_j} & j \in [1,t] \\ Y_k \mapsto x^{\nu_{t+k}} & k \in [1,\ell]. \end{cases}$$

Since $\mathrm{span}((\nu|_\ell)^T) = \mathbb{Z}$, every $z \in \mathbb{Z}$ can be expressed as

$$z = a_1\nu_{t+1} + \cdots + a_\ell\nu_{t+\ell}$$

for $a_i \in \mathbb{Z}$. Thus, for each $x^z \in N$, there exists $w = Y_1^{a_1} \cdots Y_\ell^{a_\ell} \in \mathbb{Y}^*$ such that

$$\sigma(w) = x^{a_1\nu_{t+1}+\cdots+a_\ell\nu_{t+\ell}} = x^z$$

which implies $N \subseteq \langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle$.

Since $A\nu + b = 0$, by Definition 4.14, we have $\sigma(u_i) = 1_N$ for $i \in [1, m]$ by the calculation in Eq. (4.8). Therefore, EquationsSubspan returns 'Yes'. □

Combining the above results with Proposition 3.15, namely, that MatrixSubspanB can be decided in polynomial time, gives the following.

Proposition 4.28. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{VCyc})$ *is in* NP.

Proof. Let $G \in \mathsf{FinPres}$ be given by a finite presentation $\langle \mathcal{G} \mid \mathcal{R} \rangle$ and $H \in \mathsf{SpecialExt}$, a virtually cyclic group given by $N = \langle x \rangle$, an infinite cyclic group, a multiplication table for $Q \in \mathsf{Fin}$, and special extension data $(\mathcal{I}, f_s)$. Using Lemma 4.26, we may verify the existence of an epimorphism from G to H by verifying that there exists an epimorphism $\tau\colon G \to Q$, and for some (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G, EquationsSubspan returns 'Yes' on input N and $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$.

On input G, H as above

1. Guess and verify that the set map $\tau\colon \mathcal{G} \to Q$ extends to an epimorphism $\tau\colon G \to Q$ (this is the only non-deterministic step of the algorithm).
2. Construct a (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$, and set $\mathcal{I}_X = \{x \in \mathcal{X} \mid \tau(x) \in \mathcal{I}\}$.
3. Construct a system of equations $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$, denoted $(u_i)_{[1,m]}$, where v_i is an equation without constants, $\mathfrak{c}_i \in N$ is a constant, and $u_i = v_i\mathfrak{c}_i$.
4. Construct the triple $(A, b, |\mathcal{Y}|) = \mathsf{EqnMat}(1, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]})$.
5. Return the solution to EquationsSubspan on input $(A, b, |\mathcal{Y}|)$.

The correctness of this algorithm follows from Lemmas 4.26 and 4.27. The time complexity is as follows

1. Verifying in polynomial time that τ is an epimorphism follows from Lemma 4.1.
2. Constructing a (Q, τ)-presentation is in P by Lemma 4.5, and $\mathcal{I}_\mathcal{X}$ is immediate from the input.
3. Constructing $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$ is in P immediately from the definition.
4. Constructing $\mathsf{EqnMat}(1, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]})$ is in P by Lemma 4.16.
5. MatrixSubspanB is solved in P by Proposition 3.15.

It follows that $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{VCyc})$ is in NP. □

4.4 Inverse Restricted Semi-Direct Targets

Using the results from the previous two sections, we extend the class of virtually abelian targets for which the epimorphism problem from a finitely presented group is decidable.

Recall that $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$ is the class of N by Q extensions such that Q is finite, N is abelian, there exists a transversal map s, and a subset $\mathcal{I} \subseteq Q$ such that $f_s = f_1$. Specifically, for all $n \in N$

$$ {}^{s(q)}n = \begin{cases} n^{-1} & \text{if } q \in \mathcal{I} \\ n & \text{if } q \in Q \setminus \mathcal{I}. \end{cases} $$

We assume that the data for a group in $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$ is given as

- A free abelian group $N \in \mathsf{FreeAb}$
- A finite group $Q \in \mathsf{Fin}$
- Special extension data $(\mathcal{I}, f_1)$, where $f_1(q, p) = 1_N$ for all $q, p \in Q$.

The following theorem summarises the result for $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$.

Proposition 4.29. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin})$ *is in* NP.

Proof. Let $G \in \mathsf{FinPres}$ be given by a finite presentation $\langle \mathcal{G} \mid \mathcal{R} \rangle$ and $H \in \mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$, given by an integer $d \in \mathbb{N}$ encoding $N \in \mathsf{FreeAb}$ of rank d, a multiplication table for $Q \in \mathsf{Fin}$, and special extension data $(\mathcal{I}, f_1)$.

Since $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$ is a subclass of $\mathsf{SpecialExt}$, by Lemma 4.26, we may verify the existence of an epimorphism from G to H by verifying that

(i) there exists an epimorphism $\tau \colon G \to Q$
(ii) for some (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G $\mathsf{EquationsSubspan}$ returns 'Yes' on input N and $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_1)$.

Note that since $f_s = f_1$, $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_1)$ is a system of equations without constants.

The following procedure solves our problem. On input as above

1. Guess a set map $\tau \colon \mathcal{G} \to Q$ and verify it extends to an epimorphism $\tau \colon G \to Q$.
2. Construct a (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$, and set $\mathcal{I}_X = \{x \in \mathcal{X} \mid \tau(x) \in \mathcal{I}\}$.
3. Construct the system of equations without constants $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_1)$, denoted $(u_i)_{[1,m]}$.
4. Return 'Yes' if $\mathsf{MatrixSubspanA}$ on input $(A, 0, |\mathcal{Y}|) = \mathsf{EqnMat}(d, (u_i)_{[1,m]}, (1_N)_{[1,m]})$ returns 'Yes', and 'No' otherwise.

The correctness of the procedure follows from Lemmas 4.19 and 4.26. The time complexity is as follows

1. Step (1) is in NP by Lemma 4.1; this is the only non-deterministic step of our algorithm.
2. We can construct a (Q, τ)-presentation in P by Lemma 4.5, and $\mathcal{I}_\mathcal{X}$ is immediate.
3. Constructing $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_1)$ in P is clear from its definition.
4. Constructing $\mathsf{EqnMat}(d, (u_i)_{[1,m]}, (1_N)_{[1,m]})$ is in P by Lemma 4.16, and $\mathsf{MatrixSubspanA}$ is solved in P by Proposition 3.10.

Thus, our algorithm is in NP. □

Proof of Theorem B. Let $\mathcal{T}$ be one of the three classes as stated. By Propositions 4.20, 4.28 and 4.29, $\mathsf{EPI}(\mathsf{FinPres}, \mathcal{T})$ is in NP. Since each of these classes includes finite groups (specifically, the quotient group Q in all three cases), it follows from the results of Chapters 5 and 6 that $\mathsf{EPI}(\mathsf{FinPres}, \mathcal{T}')$ is NP-hard when $\mathcal{T}'$ is either a fixed dihedral group of order not a power of 2 or a fixed simple non-abelian group. Thus, $\mathsf{EPI}(\mathsf{FinPres}, \mathcal{T})$ is also NP-hard, which means it is NP-complete. □

5 Dihedral Targets

In this chapter we turn our attention to epimorphisms onto a single finite target group. Specifically, we will prove that deciding whether there exists an epimorphism from a finitely presented group onto the dihedral group D_{2n} of order $2n$, where n is not a power of 2, is NP-hard. Combined with Lemma 4.1, this establishes that the epimorphism problem onto such a group is NP-complete.

Theorem C. *Let $n > 1$ be an integer that is not a power of 2, and let D_{2n} denote the dihedral group of order $2n$. Then, the epimorphism problem from finitely presented groups to the group D_{2n} is NP-hard.*

This result complements the work of Kuperberg and Samperton, who proved an analogous result when the target is a non-abelian finite simple group (see Section 6.2). Recall that for $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{D_{2n}})$, the parameter n is not part of the input. Instead, the input consists solely of a finite presentation for the source group.

Our method is to once again relate deciding epimorphism to solving equations in some finitely generated group. We use the result of Goldmann and Russell, who proves the following.

Theorem 5.1 ([13, Theorem 3])**.** *Let H be a finite group. The problem of deciding whether a system of equations over H has a solution is*

1. NP*-complete if H is non-abelian*
2. *in* P *if H is abelian.*

We begin by demonstrating a weaker result for the fixed target S_3, which is isomorphic to D_6, this provides a concrete way to demonstrate how the reduction is performed. We then prove our main result by first addressing the case when n is odd, followed by the case when n has a factor of 4 and is not only a power of 2. Finally, we prove Theorem D and Item 4, which, when used in conjunction with the previously established facts, leads to our result. The following provides a brief overview of the method used.

Remark 5.2. To show NP-hardness, we use a problem which is NP-hard, so in case of Theorem 5.1, D_{2n} is non-abelian, and reduce it to an epimorphism problem. The process of reducing a system of equations to an epimorphism problem into a group G can be summarised as follows.

1. Identify a way to rewrite every element in G in a restricted manner, where each element is represented by a string of restricted generators and variables, with the variables also being constrained.
2. Use this rewriting method to produce what we call a 'normal form' for each system of equations, which consequently has a solution if and only if the original system of equations has a solution.
3. Construct a group from this system of equations in normal form such that if an epimorphism exists, then each generator in this created group must be sent via this epimorphism to a generator of our choosing.
4. Prove that from this constructed group, there exists an epimorphism to G if and only if there exists a solution to the original system of equations.

The chapter has four sections, Section 5.1 is where we demonstrate this reduction for S_3, for which quite easily generalises to D_{2n} for odd n with some minor adjustments in Section 5.2. However, when n is even (and not a power of 2), several conditions break down, and we are unable to find a normal form as we did in the odd case. Thus, we use a new technique by doubling the group from equations to a dihedral group of double the order for epimorphism testing in Section 5.3. Interestingly, this requires n to have a factor of 4. Thus, in Section 5.4 we prove Item 4 of Theorem D which is used to prove the last remaining case.

5.1 Symmetric group of degree three

In this section, we prove that deciding whether there exists an epimorphism from a finitely presented group onto the symmetric group on three elements (S_3) is NP-hard. This is done by reducing the problem of solving a system of equations in S_3 to the epimorphism problem $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{S}_3)$.

Notation. Let $\mathcal{S}_3 = \{(1), (12), (13), (23), (123), (132)\}$ denote the elements of S_3, written in cycle notation, where (1) is the identity element. Multiplication is performed left-to-right; for example, $(12)(123) = (13)$.

Definition 5.3 (S3NF)**.** Let $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$ and $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_{3n}, Y_{3n}^{-1}\}$. Let a monoid homomorphism

$$\mathsf{S3NF}\colon (\mathcal{S}_3 \cup \mathbb{X})^* \to (\{(12), (123)\} \cup \mathbb{Y})^*$$

be defined by

$$\mathsf{S3NF}\colon \begin{cases} X_j & \mapsto Y_{3j-2}[Y_{3j-1}, (123)][Y_{3j}, (123)], \quad j \in [1, n] \\ X_j^{-1} & \mapsto [(123), Y_{3j}][(123), Y_{3j-1}]Y_{3j-2}^{-1}, \quad j \in [1, n] \\ (13) & \mapsto (12)(123) \\ (23) & \mapsto (12)(123)(123) \\ (132) & \mapsto (123)(123). \end{cases}$$

Lemma 5.4. *Let $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_{3n}, Y_{3n}^{-1}\}$, and $(u_i)_{[1,m]}$ be a system of equations over S_3 where each equation $u_i \in (\mathbb{X} \cup \mathcal{S}_3)^*$. Then there exists a solution $\sigma_1\colon \mathbb{X} \to \mathcal{S}_3$ to $(u_i)_{[1,m]}$ if and only if there exists a solution $\sigma_2\colon \mathbb{Y} \to \{(1), (12)\}$ to $(\mathsf{S3NF}(u_i))_{[1,m]}$.*

Proof. We first claim that

$$\{\alpha[\beta, (123)][\gamma, (123)] \mid \alpha, \beta, \gamma \in \{(1), (12)\}\} = \mathcal{S}_3.$$

Evaluating all combinations yields

α	β	γ	$\alpha[\beta, (123)][\gamma, (123)]$
(12)	(12)	(12)	$(12)(132)(132) = (13)$
e	(12)	(12)	$(132)(132) = (123)$
(12)	e	(12)	$(12)(132) = (23)$
e	e	(12)	(132)
(12)	e	e	(12)
e	e	e	e

then

$$[\delta, (123)] = \begin{cases} (132), & \delta = (12) \\ (1), & \delta = (1). \end{cases}$$

Hence, the claim holds.

Now, suppose each equation is given as

$$u_i = u_i(\mathcal{S}_3, \mathbb{X}) = u_i(\mathcal{S}_3, X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}).$$

By the above claim, we can replace each variable X_j with $Y_{3j-2}[Y_{3j-1}, (123)][Y_{3j}, (123)]$, restricting solutions such that each Y_j takes values in $\{(1), (12)\}$. This substitution preserves the set of solutions, as

$$\sigma_1(X_j) = \sigma_2(Y_{3j-2})[\sigma_2(Y_{3j-1}), (123)][\sigma_2(Y_{3j}), (123)].$$

Thus, we can rewrite each u_i into a new word $v_i(\{(12), (123), (132)\}, \mathbb{Y})$

$$v_i = u_i(\mathcal{S}_3, Y_1[Y_2, (123)][Y_3, (123)], \ldots, (Y_{3n-2}[Y_{3n-1}, (123)][Y_{3n}, (123)])^{-1}).$$

Finally, we observe that $\{(12), (123)\}$ generates S_3 and verify

$$\begin{aligned} (13) &= (12)(123) \\ (23) &= (12)(123)(123) \\ (132) &= (123)(123). \end{aligned}$$

Thus, for each i,

$$u_i(\mathcal{S}_3, \mathbb{X}) = v_i(\{(12), (123)\}, \mathbb{Y})$$

which completes the proof. □

Definition 5.5 (Constructing a group presentation from a system of equations over S_3)**.** Let $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_{3n}, Y_{3n}^{-1}\}$, and $(u_i)_{[1,m]}$ be a system of equations over S_3 with $u_i \in (\mathbb{X} \cup \mathcal{S}_3)^*$. Define

$$\lambda \colon \{(12), (123)\}^* \cup \mathbb{Y} \to \{a, g_0, \ldots, g_{3n}\}^*$$

as the monoid homomorphism induced by the bijection

$$\lambda \colon \begin{cases} (123) & \mapsto a \\ (12) & \mapsto g_0 \\ Y_j & \mapsto g_j \\ Y_j^{-1} & \mapsto g_j^{-1}, \quad j \in [1, 3n]. \end{cases}$$

Then $G_{S_3}((u_i)_{[1,m]})$ is the group with presentation

$$G_{S_3}((u_i)_{[1,m]}) = \left\langle a, g_0, \ldots, g_{3n} \mid [g_0, a]a, a^3, g_i^2, [g_i, g_j], \lambda(\mathsf{S3NF}(u_i))_{[1,m]} \right\rangle.$$

Remark 5.6. It is clear that for n a fixed constant, the finite presentation for $\mathsf{S3NF}(n, (u_i)_{[1,m]})$ can be constructed in linear time in the size $k + \sum_{[1,m]} |u_i|$ of the system of equations.

Lemma 5.7. *Let $\mathbb{X} = \{X_1, X_1^{-1}, \dots, X_n, X_n^{-1}\}$, $(u_i)_{[1,m]}$ be a system of equations over S_3 with $u_i \in (\mathbb{X} \cup \mathcal{S}_3)^*$, and let $G_{S_3}((u_i)_{[1,m]})$ be as defined in Definition 5.5. If $\psi\colon G_{S_3}((u_i)_{[1,m]}) \to S_3$ is an epimorphism, then there exist $\alpha \in \{(123), (132)\}$, $\beta \in \{(12), (13), (23)\}$, and $\gamma_i \in \langle\beta\rangle$ for $i \in [1, n]$ such that*

$$\psi\colon \begin{cases} a & \mapsto \alpha \\ g_0 & \mapsto \beta \\ g_i & \mapsto \gamma_i. \end{cases}$$

Proof. Since ψ is a homomorphism, we have

$$\psi([g_0, a]a) = \psi(a^3) = \psi(g_i^2) = \psi([g_i, g_j]) = (1).$$

Thus, $\psi(a)$ is either trivial or has order 3, and $\psi(g_i)$ is either trivial or has order 2 for $i \in [0, n]$.

If $\psi(a) = (1)$, then $\psi(G_{S_3}((u_i)_{[1,m]}))$ has no element of order 3, so ψ cannot be surjective. Therefore, $\psi(a) = \alpha \in \{(123), (132)\}$.

Since $(1) = \psi([g_0, a]a) = \psi(g_0^{-1}a^{-1}g_0aa)$, we have

$$\psi(g_0a^2g_0) = \psi(a).$$

If $\psi(g_0) = (1)$, then $\psi(a)$ would also be trivial, which contradicts surjectivity. Hence, $\psi(g_0) \in \{(12), (13), (23)\}$.

Finally, note that for $\kappa_1, \kappa_2 \in \{(1), (12), (13), (23)\}$, $[\kappa_1, \kappa_2] = (1)$ if and only if $\kappa_1 = \kappa_2$. Since $\psi(g_i)$ commutes with $\psi(g_0)$ for $i \in [1, n]$, we have $\psi(g_i) \in \langle\beta\rangle$, completing the proof. □

Lemma 5.8. *Let $\mathbb{X} = \{X_1, X_1^{-1}, \dots, X_n, X_n^{-1}\}$ and $(u_i)_{[1,m]}$ be a system of equations over S_3 with $u_i \in (\mathbb{X} \cup \mathcal{S}_3)^*$. Then there exists an epimorphism $\psi\colon G_{S_3}((u_i)_{[1,m]}) \to S_3$ if and only if there exists a solution $\sigma\colon \mathbb{X} \to S_3$ to the system $(u_i)_{[1,m]}$.*

Proof. Assume there exists an epimorphism $\psi'\colon G_{S_3}((u_i)_{[1,m]}) \to S_3$. By Lemma 5.4, there exists a solution $\sigma_1\colon \mathbb{X} \to S_3$ to $(u_i)_{[1,m]}$ if and only if the normalized system $(\mathsf{S3NF}(u_i))_{[1,m]}$ has a solution $\sigma_2\colon \mathbb{Y} \to \{(1), (12)\} \subseteq S_3$. We will construct such a solution σ_2.

By Lemma 5.7, if $\psi'\colon G_{S_3}((u_i)_{[1,m]}) \to S_3$ is an epimorphism, then there exist $\alpha \in \{(123), (132)\}$, $\beta \in \{(12), (13), (23)\}$, and $\gamma_i \in \langle\beta\rangle$ for $i \in [1, n]$ such that

$$\psi'\colon \begin{cases} a & \mapsto \alpha \\ g_0 & \mapsto \beta \\ g_i & \mapsto \gamma_i, \quad i \in [1, n]. \end{cases}$$

Let $\varphi \in \mathrm{Aut}(S_3)$ be the automorphism defined by $\varphi(\alpha) = (123)$ and $\varphi(\beta) = (12)$. Define $\psi = \varphi \circ \psi'$, so

$$\psi\colon \begin{cases} a & \mapsto (123) \\ g_0 & \mapsto (12) \\ g_i & \mapsto \gamma_i \in \langle(12)\rangle, \quad i \in [1, n]. \end{cases}$$

Define $\sigma_2\colon \mathbb{Y} \to \{(1), (12)\}$ by

$$\sigma_2(Y_j) = \psi(g_j), \quad \sigma_2(Y_j^{-1}) = \psi(g_j)^{-1}, \quad j \in [1, 3n].$$

Note that since $\sigma_2(Y_j) \in \{(1), (12)\}$, we have $\sigma_2(Y_j^{-1}) = \sigma_2(Y_j)$ for all $j \in [1, 3n]$. Recall that

$$\mathsf{S3NF}(u_i(\mathcal{S}_3, \mathbb{X})) = v_i(\{(12), (123)\}, \mathbb{Y}) = v_i(\{(12), (123)\}, Y_1, \ldots, Y_{3n}).$$

Since ψ is a homomorphism, for each $i \in [1, m]$, we have

$$\begin{aligned}
1 &= \psi(\lambda(\mathsf{S3NF}(u_i))) \\
&= \psi(\lambda(v_i(\{(12), (123)\}, Y_1, \ldots, Y_{3n}))) \\
&= \psi(v_i(\{\lambda(12), \lambda(123)\}, \lambda(Y_1), \ldots, \lambda(Y_{3n}))) \\
&= \psi(v_i(\{g_0, a\}, g_1, \ldots, g_{3n})) \\
&= v_i(\{\psi(g_0), \psi(a)\}, \psi(g_1), \ldots, \psi(g_{3n})) \\
&= v_i(\{(12), (123)\}, \psi(g_1), \ldots, \psi(g_{3n})) \\
&= \sigma_2(v_i(\{(12), (123)\}, Y_1, \ldots, Y_{3n})) \\
&= \sigma_2(\mathsf{S3NF}(u_i)).
\end{aligned}$$

Thus, σ_2 solves $(\mathsf{S3NF}(u_i))_{[1,m]}$.

Now for the reverse implication, assume there exists a solution $\sigma_1 \colon \mathbb{X} \to \mathcal{S}_3$ to the system $(u_i)_{[1,m]}$. By Lemma 5.4, there exists a solution $\sigma_2 \colon \mathbb{Y} \to \{(1), (12)\} \subseteq S_3$ to $(\mathsf{S3NF}(u_i))_{[1,m]}$. Denote $\mathsf{S3NF}(u_i) = v_i$ for $i \in [1, m]$, and as σ_2 is a solution, we have

$$\sigma_2(v_i) = \sigma_2(v_i(\{(12), (123)\}, Y_1, \ldots, Y_{3n})) = 1.$$

Define

$$\psi \colon \{a, g_0, \ldots, g_{3n}\} \to S_3$$

by

$$\psi \colon \begin{cases} a & \mapsto (123), \\ g_0 & \mapsto (12), \\ g_j & \mapsto \sigma_2(Y_j), \quad j \in [1, 3n]. \end{cases}$$

By Lemma 2.28, the monoid homomorphism ψ induces a homomorphism

$$G_{S_3}((u_i)_{[1,m]}) \to S_3$$

if and only if each relation is mapped to (1).

Now check the relations

$$\begin{aligned}
\psi(a^3) &= (123)^3 = (1) \\
\psi(g_j^2) &= (1) \quad \text{for all } j \in [0, 3n] \\
\psi([g_0, a]a) &= (12)(123)^{-1}(12)(123) = (1).
\end{aligned}$$

Finally, note that

$$\psi(\lambda(\mathsf{S3NF}(u_i))) = \psi(\lambda(v_i((12), (123), Y_1, \ldots, Y_{3n}))) = (1),$$

as σ_2 solves $(\mathsf{S3NF}(u_i))_{[1,m]}$. Thus, ψ is a surjective homomorphism. □

Theorem 5.9. $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{S}_3)$ *is* NP*-hard.*

Proof. Recall that to show a problem $A \subseteq \{0,1\}^*$ is NP-hard, we take an existing NP-hard problem $B \subseteq \{0,1\}^*$ and show that B is polynomial-time reducible to A. That is, we find a function $f\colon \{0,1\}^* \to \{0,1\}^*$, computable in polynomial time, such that $w \in B$ if and only if $f(w) \in A$.

In this setting, A is the set of strings encoding finite presentations of a group G, and B is the set of strings encoding systems of equations over a S_3. Thus, $w \in B$ encodes an instance of a system of equations, and $f(w)$ will encode an instance of a group presentation constructed from the data of w.

Given an input system of equations $(u_i)_{[1,m]}$ with variables $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_k, X_k^{-1}\}$ over S_3, construct the group $\mathsf{S3NF}(n, (u_i)_{[1,m]})$ as defined in Definition 5.3. This construction can be performed in polynomial time by Remark 5.6. By Lemma 5.8, a solution to $(u_i)_{[1,m]}$ exists if and only if there exists an epimorphism from $G_{\mathrm{o}}(n, (u_i)_{[1,m]})$ to D_{2n}.

Since S_3 is non abelian, the result follows from Theorem 5.1. □

5.2 Dihedral Odd Case

In this section we generalise the previous result, for $n > 1$ odd, we will show that deciding whether a system of equations over D_{2n} has a solution can be reduced to $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{D_{2n}})$ in polynomial time. This process follows the methods used for S_3 closely with only minor adjustments.

Notation. Let

$$\left\langle s, t \mid s^2,\, t^n,\, ststst \right\rangle$$

be a presentation for D_{2n}. Using these relations, each element of D_{2n} can be expressed uniquely as a word of the form αt^r, where $\alpha \in \{1, s\}$ and $r \in [0, n-1]$.

The following lemma on the automorphism group of dihedral groups will be relevant for both the even and odd case.

Lemma 5.10. *For $r, p \in \mathbb{Z}$, let $\varphi_{r,p}\colon D_{2n} \to D_{2n}$ be the map $s \mapsto st^r$, $t \mapsto t^p$. If $n \geq 3$, then*

$$\mathrm{Aut}(D_{2n}) = \{\varphi_{r,p} \mid r \in [0, n-1],\, p \in [1, n-1],\, \gcd(p, n) = 1\}.$$

Proof. We first show each $\varphi_{r,p}$ is an automorphism.

By definition

$$\varphi_{r,p}(s) = st^r, \quad \varphi_{r,p}(t) = t^p.$$

Checking the relations of D_{2n}, we have

$$(\varphi_{r,p}(s))^2 = (st^r)^2 = st^r\, st^r = t^{-r}t^r = 1,$$
$$(\varphi_{r,p}(t))^n = (t^p)^n = t^{pn} = (t^n)^p = 1^p = 1$$

and

$$\varphi_{r,p}(s)\,\varphi_{r,p}(t)\,\varphi_{r,p}(s)\,\varphi_{r,p}(t) = (st^r)(t^p)(st^r)(t^p) = s^2 = 1.$$

Hence, by Lemma 2.28 $\varphi_{r,p}$ is a homomorphism.

Because $\gcd(p, n) = 1$, there is a unique integer q such that $pq \equiv 1 \pmod{n}$. Hence, for each $k \in \{0, \ldots, n-1\}$,

$$pqk \equiv k \pmod{n}.$$

Define j by $j \equiv qk \pmod{n}$. Since q is the unique modular inverse of p modulo n, j is uniquely determined in $\{0, \ldots, n-1\}$. Also, if

$$j_1 \equiv qk \pmod{n} \quad \text{and} \quad j_2 \equiv qk \pmod{n},$$

then $j_1 \equiv j_2 \pmod{n}$, and since $j_1, j_2 \in \{0, \ldots, n-1\}$, it follows $j_1 = j_2$.

It follows then that, for any $t^k \in D_{2n}$, there is a unique $j \in \{0, \ldots, n-1\}$ such that

$$\varphi_{r,p}(t^j) = t^{jp} = t^{(qk \bmod n)\, p} = t^{qpk} = t^k.$$

Thus, for every t^k there exists t^j such that $\varphi_{r,p} = t^k$, so $\varphi_{r,p}$ is surjective. Because D_{2n} is finite, surjectivity implies injectivity, so $\varphi_{r,p}$ is an isomorphism. Therefore,

$$\{\varphi_{r,p} \mid r \in \{0, \ldots, n-1\},\, p \in \{1, \ldots, n-1\},\, \gcd(p, n) = 1\} \subseteq \mathrm{Aut}(D_{2n}).$$

Let $\psi \in \mathrm{Aut}(D_{2n})$. We claim ψ coincides with some $\varphi_{r,p}$.

- $\psi(t)$ must have order n. The only elements of order n in D_{2n} are t^p with $\gcd(p, n) = 1$. Hence $\psi(t) = t^p$.
- $\psi(s)$ must have order 2 and not lie in the center. If n is odd, the only elements of order 2 are st^r. If n is even, $t^{n/2}$ is central, but s is not. Thus $\psi(s) = st^r$.

Hence, ψ is given by

$$\psi(s) = st^r, \quad \psi(t) = t^p,$$

where $\gcd(p, n) = 1$. This is exactly $\varphi_{r,p}$.

Thus

$$\mathrm{Aut}(D_{2n}) = \{\varphi_{r,p} \mid r \in \{0, \ldots, n-1\},\ p \in \{1, \ldots, n-1\},\ \gcd(p, n) = 1\}.$$

□

Lemma 5.11. *If $n > 1$ is odd, then*

$$D_{2n} = \{\alpha_0\, ({}^{\alpha_1}t) \cdots ({}^{\alpha_n}t) \mid \alpha_i \in \{1, s\}\}.$$

Proof. Since ${}^{\alpha_i}t \in \{t, t^{-1}\}$ for $\alpha_i \in \{1, s\}$, we have

$$\alpha_0\, ({}^{\alpha_1}t) \cdots ({}^{\alpha_n}t) = \alpha_0 t^{n-\ell} t^{-\ell} = \alpha_0 t^{n-2\ell},$$

where $\ell = |\{i \in [1, n] \mid \alpha_i = s\}| \in [0, n]$. Then, using the values in Table 5.1

ℓ	0	1	$\cdots$	$\frac{n-1}{2}$	$\frac{n+1}{2}$	$\cdots$	n
$n - 2\ell$	n	$n-2$	$\cdots$	1	-1	$\cdots$	$-n$
$(n - 2\ell) + n$	0		$\cdots$		$n-1$	$\cdots$	0

Table 5.1: Computing exponents of t in Lemma 5.11

and the fact that $t^n = 1$, we have

$$\{\alpha_0 t^{n-2\ell} \mid \alpha_0 \in \{1, s\}, \ell \in [0, n]\} = \{\alpha_0 t^r \mid \alpha_0 \in \{1, s\}, r \in [0, n-1]\}.$$

This proves the claim. □

Lemma 5.12. *If $n > 1$ is odd, $r \in [0, n-1]$, and $x \in D_{2n}$ commutes with st^r, then $x \in \{1, st^r\}$. In particular $Z(D_{2n}) = \{1\}$.*

Proof. Write $x = \alpha t^\ell$ for $\alpha \in \{1, s\}$ and $\ell \in [0, n-1]$.

If $x = t^\ell$, then

$$[x, st^r] = t^{2\ell} = 1$$

if and only if $\ell = 0$, so $x = 1$.

If $x = st^\ell$, then

$$[x, st^r] = t^{2r-2\ell} = 1$$

if and only if n divides $2(r-\ell)$. Since $r, \ell \in [0, n-1]$, this implies $r = \ell$.

Therefore, $x \in \{1, st^r\}$. For $n > 2$, the centre is trivial because $x \in Z(D_{2n})$ would imply x commutes with both st and st^2, which is only possible for $x = 1$. □

Definition 5.13 (Odd normal form)**.** Let $n > 1$ be an odd integer, $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_k, X_k^{-1}\}$, and $\mathbb{Y} = \{Y_{0,1}, Y_{0,1}^{-1}, \ldots, Y_{n,k}, Y_{n,k}^{-1}\}$. Define

$$\mathsf{ONF}\colon (\mathbb{X} \cup \{s, t, t^{-1}\})^* \to (\mathbb{Y} \cup \{s, t, t^{-1}\})^*$$

to be the monoid homomorphism induced by the set map

$$\mathsf{ONF}\colon \begin{cases} X_j & \mapsto Y_{0,j} \cdot ({}^{Y_{1,j}}t) \cdot ({}^{Y_{2,j}}t) \cdots ({}^{Y_{n,j}}t) \\ X_j^{-1} & \mapsto ({}^{-Y_{n,j}}t) \cdots ({}^{-Y_{1,j}}t) \cdot Y_{0,j}^{-1} \\ s & \mapsto s \\ t & \mapsto t \\ t^{-1} & \mapsto t^{-1}. \end{cases}$$

Lemma 5.14. *Let $n, \mathbb{X}, \mathbb{Y}$, and ONF be as in Definition 5.13, and $(u_i)_{[1,m]}$ be a system of equations in D_{2n}, where each equation $u_i \in (\mathbb{X} \cup \{s, t, t^{-1}\})^*$. Then there exists a solution $\sigma_1\colon \mathbb{X} \to D_{2n}$ to $(u_i)_{[1,m]}$ if and only if there exists a solution $\sigma_2\colon \mathbb{Y} \to \{1, s\} \subseteq D_{2n}$ to $(\mathsf{ONF}(u_i))_{[1,m]}$.*

Proof. For $i \in [1, m]$, each equation is a word $u_i(s, t, t^{-1}, X_1, X_1^{-1}, \ldots, X_k, X_k^{-1})$. By Lemma 5.11, replacing each variable X_j by the word $Y_{0,j}\left({}^{Y_{1,j}}t\right)\cdots\left({}^{Y_{n,j}}t\right) = \mathsf{ONF}(X_j)$ in each equation and restricting $Y_{i,j}$ to take values in $\{1, s\}$ does not change the set of solutions.

Thus, we can rewrite each u_i as $\mathsf{ONF}(u_i)$, and the result follows. □

Definition 5.15 (Group presentation for odd dihedral case)**.** Let $n, \mathbb{X}, \mathbb{Y}, \mathsf{ONF}$, and $(u_i)_{[1,m]}$ be as in Lemma 5.14. Let $\mathcal{G}_{n,k} = \{g_{i,j} \mid i \in [0, n], j \in [1, k]\}$ be a set of $(n+1)k$ distinct letters.

Define $\lambda\colon (\{s, t, t^{-1}\} \cup \mathbb{Y})^* \to (\{a, d, d^{-1}\} \cup \mathcal{G}_{n,k} \cup \mathcal{G}_{n,k}^{-1})^*$ to be the monoid homomorphism induced by the bijection

$$\lambda\colon \begin{cases} s & \mapsto a \\ t & \mapsto d, \\ Y_{i,j} & \mapsto g_{i,j}, \end{cases} \qquad \begin{cases} t^{-1} & \mapsto d^{-1} \\ Y_{i,j}^{-1} & \mapsto g_{i,j}^{-1}, \end{cases} \qquad i \in [0, n], j \in [1, k].$$

Then $G_{\mathrm{o}}(n, (u_i)_{[1,m]})$ is the group with presentation

$$\left\langle \{a, d\} \cup \mathcal{G}_{n,k} \mid \{a^2, d^n, adad, \lambda(\mathsf{ONF}(u_i)), [g, g'], [g, a], g^2 \mid i \in [1, m], g, g' \in \mathcal{G}_{n,k}\} \right\rangle.$$

Remark 5.16. It is clear that for n a fixed constant, the finite presentation for $G_{\mathrm{o}}(n, (u_i)_{[1,m]})$ can be constructed in linear time in the size $k + \sum_{[1,m]} |u_i|$ of the system of equations.

The idea of this construction is so that for any epimorphism from $G_{\mathrm{o}}(n,(u_i)_{[1,m]})$ to D_{2n} we send

- a to s
- d to t
- $g_{i,j}$ to $\{1,s\}$

up to automorphism, if and only if the system of equations has a solution, where φ is an automorphism of D_{2n}. This is the content of the next two lemmas.

Lemma 5.17. *If $\psi\colon G_{\mathrm{o}}(n,(u_i)_{[1,m]}) \to D_{2n}$ is an epimorphism, then there exists $\varphi \in \mathrm{Aut}(D_{2n})$ such that*

$$\psi\colon \begin{cases} a & \mapsto \varphi(s) \\ d & \mapsto \varphi(t) \\ g_{i,j} & \mapsto \gamma_{i,j} \in \langle \varphi(s) \rangle\,; \quad i \in [0,n], j \in [1,k]. \end{cases}$$

Proof. For readability, we denote $G_{\mathrm{o}}(n,(u_i)_{[1,m]})$ as G for this proof.

If $\psi(d) = 1$, then $\psi(G)$ is abelian since it is generated by $\psi(a)$ and $\psi(g_{i,j})$, which all commute. This implies ψ is not surjective onto D_{2n}. Thus, $\psi(d) \neq 1$.

Now suppose $\psi(d)^2 = 1$. Then, since d^n is a relation in G and $n > 1$ is odd, we have

$$1 = \psi(d^n) = \psi(d)(\psi(d)^2)^{(n-1)/2} = \psi(d)$$

a contradiction. Thus, $\psi(d)^2 \neq 1$.

Since a^2 is a relation in G, we have $\psi(a) \in \{1, st^r \mid r \in [0,n-1]\}$, which is the set of all elements of order 2 in D_{2n}. If $\psi(a) = 1$, then by the relation $adad$, we have $\psi(d)^2 = 1$, which is not possible. Hence, $\psi(a) = st^r$ for some $r \in [0,n-1]$.

Since $[g_{i,j}, a]$ is a relation in G for all $g_{i,j} \in \mathcal{G}_{n,k}$, $\psi(g_{i,j})$ commutes with $\psi(a)$. By Lemma 5.12, this implies

$$\langle \psi(a), \psi(g_{0,1}), \ldots, \psi(g_{n,k}) \rangle = \langle \psi(a) \rangle\,.$$

Since $adad$ is a relation in G, if $\psi(d) = \alpha t^p$ with $\alpha \in \{1,s\}$ and $p \in [0,n-1]$, then

$$1 = \psi(adad) = st^r \alpha t^p st^r \alpha t^p = \begin{cases} st^r st^p st^r st^p = t^{-2r+2p}, & \text{if } \alpha = s \\ st^{r+p} st^{r+p} = 1, & \text{if } \alpha = 1. \end{cases}$$

If $\alpha = s$, then $r = p$ and $\psi(d) = \psi(a)$, which would mean ψ is not surjective. Thus, $\alpha = 1$ and $\psi(d) = t^p$ with $p \in [1,n-1]$ (since $\psi(d) \neq 1$).

It follows that $\psi(G) = \langle \psi(a), \psi(t) \rangle = \langle st^r, t^p \rangle$, so we can express any element in $\psi(G)$ as a word in $\{st^r, t^p, t^{-p}\}^*$. Since ψ is surjective onto D_{2n}, we contains t, we have

$$\begin{aligned} t &= (t^p)^{i_0}(st^r)(t^p)^{i_1} \ldots (st^r)(t^p)^{i_{2m}} \quad \text{(the number of } s \text{ letters must be even)} \\ &= t^{-pi_0} t^{-r-pi_1} t^{r+pi_2} t^{-r-pi_3} \ldots t^{-r-pi_{2m-1}} t^{r+pi_{2m}} \\ &= t^{pi_0} t^{-pi_1} t^{pi_2} t^{-pi_3} \ldots t^{-pi_{2m-1}} t^{pi_{2m}} \\ &= (t^p)^{i_0 - i_1 + \cdots + i_{2m}}. \end{aligned}$$

Thus, n divides $1 - px$ for $x = \sum_{j=0}^{2m} (-1)^j i_j \in \mathbb{Z}$, so $\gcd(p,n) = 1$. Then, by Lemma 5.10, there exists $\varphi_{r,p} \in \mathrm{Aut}(D_{2n})$ such that $\varphi_{r,p}(t) = t^p = \psi(d)$ and $\varphi_{r,p}(s) = st^r = \psi(a)$. □

Lemma 5.18. *Let $n > 1$, $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_k, X_k^{-1}\}$, and $(u_i)_{[1,m]}$ with $u_i \in (\{s,t,t^{-1}\} \cup \mathbb{X})^*$ be a system of equations over D_{2n}. There exists an epimorphism $\psi\colon G_{\mathrm{o}}(n,(u_i)_{[1,m]}) \to D_{2n}$ if and only if there exists a solution $\sigma\colon \mathbb{X} \to D_{2n}$ to the system $(u_i)_{[1,m]}$.*

Proof. Assume that there exists an epimorphism $\psi' \colon G_{\mathrm{o}}(n, (u_i)_{[1,m]}) \to D_{2n}$. By Lemma 5.17, there exists $\varphi \in \mathrm{Aut}(D_{2n})$ such that

$$\psi' \colon \begin{cases} a & \mapsto \varphi(s) \\ d & \mapsto \varphi(t) \\ g_{i,j} & \mapsto \gamma'_{i,j} \in \langle \varphi(s) \rangle, \quad i \in [0,n], j \in [1,k]. \end{cases}$$

Letting $\psi = \varphi^{-1} \circ \psi'$, we obtain an epimorphism

$$\psi \colon \begin{cases} a & \mapsto s \\ d & \mapsto t \\ g_{i,j} & \mapsto \gamma_{i,j} \in \langle s \rangle, \quad i \in [0,n], j \in [1,k]. \end{cases}$$

Define $\sigma \colon \mathbb{Y} \to \{1, s\}$ by $\sigma(Y_{i,j}) = \gamma_{i,j}$, $\sigma(Y_{i,j}^{-1}) = \gamma_{i,j}^{-1}$. Since $s^2 = 1$, we have $\sigma(Y_{i,j}) = \sigma(Y_{i,j}^{-1})$, so without loss of generality, assume $\mathbb{Y} = \{Y_{0,1}, \dots, Y_{n,k}\}$. For $i \in [1,m]$, let $v_i \in (\{s, t, t^{-1}\} \cup \mathbb{Y})^*$ such that $\mathsf{ONF}(u_i) = v_i$. Since ψ is a homomorphism, for each relation $\lambda(\mathsf{ONF}(u_i))$ of G_{o}, $i \in [1,m]$, we have

$$\begin{aligned} 1 = \psi(\lambda(\mathsf{ONF}(u_i))) &= \psi(\lambda(v_i(s, t, t^{-1}, Y_{0,1}, \dots, Y_{n,k}))) \\ &= \psi(v_i(a, d, d^{-1}, g_{0,1}, \dots, g_{n,k})) \\ &= v_i(s, t, t^{-1}, \gamma_{0,1}, \dots, \gamma_{n,k}) \\ &= \sigma(v_i(s, t, t^{-1}, Y_{0,1}, \dots, Y_{n,k})) = \sigma(\mathsf{ONF}(u_i)) \end{aligned}$$

so σ solves $(\mathsf{ONF}(u_i))_{[1,m]}$, and the result follows by Lemma 5.14.

Thus,

$$\sigma(v_i(s, t, t^{-1}, Y_{0,1}, \dots, Y_{n,k})) = \sigma(\mathsf{ONF}(u_i)) = 1 \tag{5.1}$$

so σ solves $(\mathsf{ONF}(u_i))_{[1,m]}$, and the result follows by Lemma 5.14.

Conversely, assume there exists a solution to $(u_i)_{[1,m]}$. By Lemma 5.14, there exists a solution $\sigma \colon \mathbb{Y} \to \{1, s\}$ to $(\mathsf{ONF}(u_i))_{[1,m]}$, so for $i \in [1,m]$, if $\mathsf{ONF}(u_i) = v_i$, then

$$\sigma(\mathsf{ONF}(u_i)) = \sigma(v_i(s, t, t^{-1}, \mathbb{Y})) = 1.$$

Define $\psi \colon \{a, d, d^{-1}\} \cup \mathcal{G}_{n,k} \cup \mathcal{G}_{n,k}^{-1} \to D_{2n}$ as the set map

$$\psi \colon \begin{cases} a & \mapsto s \\ d & \mapsto t \\ d^{-1} & \mapsto t^{-1} \\ g_{i,j} & \mapsto \sigma(Y_{i,j}), \qquad g_{i,j} \in \mathcal{G} \\ g_{i,j}^{-1} & \mapsto \sigma(Y_{i,j})^{-1}, \quad g_{i,j} \in \mathcal{G}. \end{cases}$$

Since the other relations in $G_{\mathrm{o}}(n, (u_i)_{[1,m]})$ clearly map to 1 in D_{2n}, by Lemma 2.28, ψ induces a homomorphism from $G_{\mathrm{o}}(n, (u_i)_{[1,m]})$ to D_{2n} if and only if $\psi(\lambda(\mathsf{ONF}(u_i))) = 1$ for all $i \in [1,m]$.

We have

$$\begin{aligned} \psi(\lambda(\mathsf{ONF}(u_i))) &= \psi(\lambda(v_i(s, t, t^{-1}, \mathbb{Y}))) \\ &= v_i(s, t, t^{-1}, \sigma(\mathbb{Y})) = \sigma(v_i(s, t, t^{-1}, \mathbb{Y})) = 1 \quad \text{(by Eq. (5.1))}. \end{aligned}$$

Thus, ψ is a homomorphism, which is surjective since $\psi(G_{\mathrm{o}}(n, (u_i)_{[1,m]})) = \langle s, t \rangle = D_{2n}$. □

5.3 Dihedral Even Case

We now turn to the case where n has a factor of 4, we refer to this simply as the even case. We will use an additional result to prove the case when n has a factor of 2 but not 4. That is, our strategy requires a different proof for the following cases

1. $n = 2^b c$ with $c > 1$ odd and $b > 1$
2. $n = 2c$ with $c > 1$ odd.

For the first case, we will show that deciding whether a system of equations over the dihedral group D_n of order n reduces to $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{D_{2n}})$.

We begin by observing some preliminary facts.

Lemma 5.19. *Let $n > 2$ be even.*

(a) For any element $x \in D_{2n}$, if $x^2 = 1$, then $x \in \{1, t^{n/2}, st^r \mid r \in [0, n-1]\}$.
(b) The centre $Z(D_{2n}) = \{1, t^{n/2}\}$.
(c) If st^a and st^b commute for $0 \leq a \leq b \leq n-1$, then $b = a$ or $b = a + \frac{n}{2}$.

Proof. Recall that every element of D_{2n} can be uniquely expressed as a word αt^r where $\alpha \in \{1, s\}$ and $r \in [0, n-1]$. If $x = st^r$, then $(st^r)^2 = st^r st^r = 1$ for any $r \in [0, n-1]$. If $x = t^r$, then $t^{2r} = 1$ if and only if $r = 0$ or $r = \frac{n}{2}$, which establishes item (a).

Item (b) can be observed by noting that for any $r \in [0, n-1]$

$$[t, st^r] = tst^r t^{-1} t^{-r} s = t^2 \neq 1$$

since $n > 2$ (so no element st^r can be in the centre). Similarly

$$[t^r, s] = t^{2r}$$

so t^r is in the centre if and only if $r = 0$ or $r = \frac{n}{2}$.

For item (c), if st^a and st^b commute, then

$$[st^a, st^b] = st^a st^b t^{-a} st^{-b} s = t^{-a} t^b t^{-a} t^b = t^{2(b-a)}.$$

Thus, $t^{2(b-a)} = 1$, which implies n divides $2(b-a)$. Since $a, b \in [0, n-1]$, it follows that $b - a \leq n - 1$, so $b - a \in \{0, \frac{n}{2}\}$. Therefore, $b = a$ or $b = a + \frac{n}{2}$. □

Notation. We alert the reader to the fact that here we will be using dihedral groups of different sizes. Let

$$D_n = \left\langle s_1, t_1 \mid s_1^2,\, t_1^{n/2},\, s_1 t_1 s_1 t_1 \right\rangle$$
$$D_{2n} = \left\langle s_2, t_2 \mid s_2^2,\, t_2^n,\, s_2 t_2 s_2 t_2 \right\rangle$$

be presentations for the groups D_n and D_{2n}, respectively.

Lemma 5.20. *Let $n = 4c$ where $c \in \mathbb{N}_+$, and*

$$H = \left\{ \alpha_0 \, ({}^{\alpha_1}t_2) \cdots ({}^{\alpha_{n/2}}t_2) \mid \alpha_i \in \{1, s_2, t^{n/2}, s_2 t^{n/2}\} \right\}.$$

Then H is a subgroup of D_{2n} that is isomorphic to D_n.

Proof. Since

$${}^{\alpha_i}t_2 = t_2 \quad \text{for } \alpha_i \in \{1, t_2^{n/2}\} \quad \text{and} \quad {}^{\alpha_i}t_2 = t_2^{-1} \quad \text{for } \alpha_i \in \{s_2, s_2 t_2^{n/2}\}$$

we have

$$\alpha_0 \cdot ({}^{\alpha_1}t_2) \cdots ({}^{\alpha_{n/2}}t_2) = \alpha_0 t_2^{(n/2-\ell)-\ell} = \alpha_0 t_2^{n/2-2\ell}$$

where $\ell = \left|\{i \in [1, \frac{n}{2}] \mid \alpha_i \in \{s_2, s_2 t^{n/2}\}\}\right|$. Thus

$$\begin{aligned} H &= \left\{\alpha_0 t_2^{n/2-2\ell} \mid \alpha_0 \in \{1, s_2, t_2^{n/2}, s_2 t^{n/2}\}, \ell \in [0, \tfrac{n}{2}]\right\} \\ &= \left\{\alpha_0 t_2^{2(n/4-\ell)} \mid \alpha_0 \in \{1, s_2, t_2^{n/2}, s_2 t^{n/2}\}, \ell \in [0, \tfrac{n}{2}]\right\}. \end{aligned}$$

Since $\frac{n}{2}$ is even, as ℓ ranges over $[0, \frac{n}{2}]$, we have the values in Table 5.2.

ℓ	0	1	$\cdots$	$\frac{n}{4}-1$	$\frac{n}{4}$	$\frac{n}{4}+1$	$\cdots$	$\frac{n}{2}-1$	$\frac{n}{2}$
$\frac{n}{4}-\ell$	$\frac{n}{4}$	$\frac{n}{4}-1$	$\cdots$	1	0	-1	$\cdots$	$\frac{-n}{4}+1$	$\frac{-n}{4}$
$(\frac{n}{4}-\ell)+\frac{n}{2}$						$\frac{n}{2}-1$	$\cdots$	$\frac{n}{4}+1$	$\frac{n}{4}$

Table 5.2: Computing exponents of t_2^2 in Lemma 5.20

From these values, and using the fact that $t_2^n = 1$ in D_{2n}, we see that as ℓ ranges over $[0, \frac{n}{2}]$, the term $t_2^{2(n/4-\ell)}$ is equal to a term of the form t_2^{2r} for r ranging over $[0, \frac{n}{2}-1]$, with all values of r realised in this range.

Thus,

$$H = \left\{\alpha_0 t_2^{2r} \mid \alpha_0 \in \{1, s_2, t_2^{n/2}, s_2 t^{n/2}\}, r \in [0, \tfrac{n}{2}-1]\right\},$$

which is a subgroup since it coincides with $\langle s_2, t_2^2\rangle$, and is clearly isomorphic to D_n via the map $s_1 \mapsto s_2$, $t_1 \mapsto t_2^2$. □

Remark 5.21. For $n = 2c$ with c odd, the set H in Lemma 5.20 would not form a subgroup as it would only contain odd powers of t_2. Specifically, the set H would be defined as

$$H = \{\alpha_0 ({}^{\alpha_1}t_2) \cdots ({}^{\alpha_c}t_2) \mid \alpha_i \in \{1, s_2, t^c, s_2 t^c\}\},$$

but the resulting elements would not include all powers of t_2, leading to a failure to form a subgroup. Changing the definition of H to include all words of the form $\alpha_0 ({}^{\alpha_1}t_2) \cdots ({}^{\alpha_n}t_2)$, as in Lemma 5.11, would not help either, as the additional powers would merely repeat existing elements of H, contributing no new distinct powers.

To illustrate this redundancy, consider the table below, which computes the exponents of t_2 for $n = 2c$ with c odd

ℓ	0	1	2	$\cdots$	$\frac{c-3}{2}$	$\frac{c-1}{2}$	$\frac{c+1}{2}$	$\cdots$	$c-1$	c	$c+1$
$\frac{n}{2}-2\ell$	c	$c-2$	$c-4$	$\cdots$	3	1	-1	$\cdots$	$-c+2$	$-c$	$-c-2$
$\frac{n}{2}-2\ell+n$							$n-1$	$\cdots$	$\frac{n}{2}+2$	$\frac{n}{2}$	$c-2$

Table 5.3: Computing exponents of t_2 in Lemma 5.20 when $\frac{n}{2} = c$ is odd.

Consequently, our results in Lemma 5.20 are restricted to cases where $n = 2^b c$ with $b > 1$ and $c > 1$ odd. This restriction ensures the subgroup structure of H and avoids redundancy in the resulting set.

Definition 5.22 (Even normal form)**.** Let $n, k \in \mathbb{N}_+$ with n even, $\mathbb{X} = \{X_1, X_1^{-1}, \dots, X_k, X_k^{-1}\}$, and $\mathbb{Y} = \{Y_{0,1}, Y_{0,1}^{-1}, \dots, Y_{n/2,k}, Y_{n/2,k}^{-1}\}$. Define a monoid homomorphism

$$\mathsf{ENF}\colon (\{s_1, t_1, t_1^{-1}\} \cup \mathbb{X})^* \to (\{s_2, t_2^2, t_2^{-2}\} \cup \mathbb{Y})^*$$

via the set map

$$\mathsf{ENF}\colon \begin{cases} X_j & \mapsto Y_{0,j} \cdot \left(^{Y_{1,j}}t_2\right) \cdots \left(^{Y_{n/2,j}}t_2\right), \quad j \in [1,k] \\ X_j^{-1} & \mapsto \left(^{Y_{n/2,j}}t_2\right) \cdots \left(^{Y_{1,j}}t_2\right) \cdot Y_{0,j}^{-1}, \quad j \in [1,k] \\ s_1 & \mapsto s_2 \\ t_1 & \mapsto t_2^2 \\ t_1^{-1} & \mapsto t_2^{-2}. \end{cases}$$

Lemma 5.23. *Let $n = 2^b c$ where $c > 1$ is odd and $b > 1$, $\mathbb{X}, \mathbb{Y}, \mathsf{ENF}$ as in Definition 5.22, and let $(u_i)_{[1,m]}$ be a system of equations in D_n with each equation $u_i \in (\mathbb{X} \cup \{s_1, t_1, t_1^{-1}\})^*$.*

Then there exists a solution $\sigma_1\colon \mathbb{X} \to D_n$ to $(u_i)_{[1,m]}$ if and only if there exists a solution $\sigma_2\colon \mathbb{Y} \to \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\} \subseteq D_{2n}$ to $(\mathsf{ENF}(u_i))_{[1,m]}$.

Proof. For $i \in [1,m]$, each equation is a word $u_i(s_1, t_1, t_1^{-1}, X_1, X_1^{-1}, \dots, X_k, X_k^{-1})$. By Lemma 5.20, replacing each variable X_j by the word

$$Y_{0,j} \cdot \left(^{Y_{1,j}}t_2\right) \cdots \left(^{Y_{n/2,j}}t_2\right) = \mathsf{ENF}(X_j)$$

in each equation, and restricting $Y_{i,j}$ to take values in $\{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}$, does not change the set of solutions when moving from D_n to D_{2n}. Thus, each u_i can be rewritten as $\mathsf{ENF}(u_i)$, and the result follows. □

Definition 5.24 (Right Nested Commutator)**.** Let x and y be letters. The string

$$[[\dots[[x,y],y],\dots],y]$$

consisting of n copies of the letter y and one copy of the letter x, is called the *right nested commutator* of x and y, repeated n times. This is denoted by $[x,{}_n\, y]$.

Example 5.25.

$$\begin{aligned} [x,{}_4\, y] &= [[[[x,y],y],y],y] \\ &= [[[xyx^{-1}y^{-1},y],y],y] \\ &= [[(xyx^{-1}y^{-1})y(xyx^{-1}y^{-1})^{-1}y^{-1},y],y] \quad \text{and so on.} \end{aligned}$$

Definition 5.26 (Group presentation for $n = 4c$ case)**.** Let $k \in \mathbb{Z}$, $n = 2^b c$, where $c > 1$ is odd and $b > 1$, $\mathbb{X}$, $\mathbb{Y}$, and ENF as in Definition 5.22, and let $(u_i)_{[1,m]}$ be a system of equations in D_n with each equation $u_i \in (\mathbb{X} \cup \{s_1, t_1, t_1^{-1}\})^*$, and

$$\mathcal{G}_{n/2,k} = \{g_{i,j} \mid i \in [0, \tfrac{n}{2}], j \in [1,k]\}$$

be a set of $(\frac{n}{2}+1)k$ distinct letters.

Define $\lambda\colon (\{s_2, t_2^2, t_2^{-2}\} \cup \mathbb{Y})^* \to (\{a, d^2, d^{-2}\} \cup \mathcal{G}_{n/2,k} \cup \mathcal{G}_{n/2,k}^{-1})^*$ as the monoid homomorphism induced by the bijection

$$\lambda\colon \begin{cases} s_2 & \mapsto a \\ t_2 & \mapsto d \\ t_2^{-1} & \mapsto d^{-1} \\ Y_{i,j} & \mapsto g_{i,j}, \quad i \in [0, n/2],\ j \in [1,k] \\ Y_{i,j}^{-1} & \mapsto g_{i,j}^{-1}, \quad i \in [0, n/2],\ j \in [1,k]. \end{cases}$$

Then $G_{\mathrm{e}}(n, (u_i)_{[1,m]})$ is the group with presentation

$$\left\langle \{a,d\} \cup \mathcal{G}_{n/2,k} \mid \{a^2, d^n, adad, [g,g'], [g,a], g^2, [d^c, {}_b\, g]\,, \lambda(\mathsf{ENF}(u_i)) \mid g, g' \in \mathcal{G}_{n/2,k},\ i \in [1,m]\} \right\rangle.$$

Remark 5.27. Similarly to G_{o}, it is clear that for n a fixed constant, the finite presentation for $G_{\mathrm{e}}(n, (u_i)_{[1,m]})$ can be constructed in linear time relative to the size $k + \sum_{[1,m]} |u_i|$ of the system of equations.

Lemma 5.28. *If $n = 2^b c$ where $c > 1$ is odd and $b > 1$, and $\psi\colon G_{\mathrm{e}}(n, (u_i)_{[1,m]}) \to D_{2n}$ is an epimorphism, then there exists $\varphi \in \mathrm{Aut}(D_{2n})$ such that*

$$\psi\colon \begin{cases} a & \mapsto \varphi(s_2) \\ d & \mapsto \varphi(t_2) \\ g_{i,j} & \mapsto \gamma_{i,j} \in \{\varphi(1), \varphi(s_2), \varphi(t_2^{n/2}), \varphi(s_2 t_2^{n/2})\}; \quad i \in [0,n], j \in [1,k]. \end{cases}$$

Proof. For readability, we denote $G_{\mathrm{e}}(n, (u_i)_{[1,m]})$ as G, and as we are exclusively dealing with the dihedral group of order $2n$, we simplify the notation by denoting s_2 and t_2 as s and t, respectively, throughout this proof.

We first claim that there exists $\ell \in [0, \frac{n}{2} - 1]$ such that $\psi(x) \in \{1, t^{n/2}, st^{\ell}, st^{\ell + n/2}\}$ for all $x \in \{a\} \cup \mathcal{G}$. To see this, each $x \in \{a\} \cup \mathcal{G}$ has order 2, so by Lemma 5.19 (a), $\psi(x) \in \{1, t^{n/2}, st^r\}$ for some $r \in [0, n-1]$. Let $M = \{\ell \in [0, n-1] \mid \exists x \in \{a\} \cup \mathcal{G}, \psi(x) = st^{\ell}\}$. If M is empty (so all $x \in \{a\} \cup \mathcal{G}$ satisfy $\psi(x) \in \{1, t^{n/2}\}$), choose any ℓ, and otherwise choose $\ell = \min M$. To see that this is justified, suppose $x, y \in \{a\} \cup \mathcal{G}$ are such that $\psi(x) = st^a, \psi(y) = st^b$ for $0 \le a < b \le n-1$. Since all elements in $\{a\} \cup \mathcal{G}$ pairwise commute, by Lemma 5.19 (c) we have $b = a + \frac{n}{2}$.

Next, we claim $\psi(d)^2 \neq 1$. For contradiction, assume $\psi\colon G \to D_{2n}$ is an epimorphism and $\psi(d)^2 = 1$. By Lemma 5.19 (a), $\psi(d) \in \{1, t^{n/2}, st^p \mid p \in [0, n-1]\}$. If $\psi(d) \in \{1, t^{n/2}\} = Z(D_{2n})$, then $\psi(d)$ commutes with $\psi(x)$ for all $x \in \{a\} \cup \mathcal{G}$, so $\psi(G)$ is abelian, contradicting that ψ is an epimorphism. Thus, $\psi(d) = st^p$ for some $p \in [0, n-1]$.

If $\psi(a) = st^r$, then by the relation $adad$ we have

$$1 = \psi(adad) = st^r st^p st^r st^p = st^r st^p t^{-r} st^{-p} s = [st^r, st^p] = [\psi(a), \psi(d)].$$

This shows that $\psi(a)$ and $\psi(d)$ commute. By Lemma 5.19 (c), $\psi(d) = st^{r \pm n/2}$, and by the first claim $\psi(x)$ has this form or lies in the centre for $x \in \mathcal{G}$, so $\psi(d)$ commutes with $\psi(x)$ for all $x \in \{a\} \cup \mathcal{G}$, making $\psi(G)$ abelian, contradicting that ψ is surjective.

Otherwise, $\psi(a) \in \{1, t^{n/2}\}$. Suppose that $\psi(x) \in \{1, t^{n/2}\}$ for all $x \in \mathcal{G}$. Then $\psi(G)$ is abelian since every element can be expressed in the form $(t^{n/2})^i (\psi(d))^j$. Thus, we may assume there exists some $g \in \mathcal{G}$ with $\psi(g) = st^{\ell}$ for $\ell \in [0, n-1]$.

Then, by the relation $[d^c, {}_b\, g]$, and noting that

$$[st^p, st^{\ell}] = (st^p)(st^{\ell})(t^{-p}s)(t^{-\ell}s) = s^2 t^{-p} t^{\ell} t^{-p} t^{\ell} s^2 = t^{2(\ell - p)}$$

we have

$$\begin{aligned}
1 = \psi([d^c, {}_b\, g]) &= \left[st^p, {}_b\, st^\ell\right] \quad \text{(since } \psi(d)^2 = 1 \text{ and } c \text{ is odd)} \\
&= \left[\cdots[[[[st^p, st^\ell], st^\ell], st^\ell], st^\ell], \cdots, st^\ell\right] \quad (b \text{ times}) \\
&= \left[\cdots[[[t^{2(\ell-p)}, st^\ell], st^\ell], st^\ell], \cdots, st^\ell\right] \quad (b-1 \text{ times}) \\
&= \left[\cdots[[t^{4(\ell-p)}, st^\ell], st^\ell], \cdots, st^\ell\right] \quad (b-2 \text{ times}) \\
&= \left[\cdots[t^{8(\ell-p)}, st^\ell], \cdots, st^\ell\right] \quad (b-3 \text{ times}) \\
&\vdots \\
&= [t^{2^{b-1}(\ell-p)}, st^\ell] \quad (b-(b-1) \text{ times}) \\
&= t^{2^b(\ell-p)}. \qquad (5.2)
\end{aligned}$$

It follows that $n = 2^b c$ divides $2^b(\ell - p)$, and so c divides $\ell - p$. Let $q \in \mathbb{Z}$ such that $\ell - p = qc$.

By the first claim, for any other $g' \in \mathcal{G}$, $\psi(g')$ has the form $1, t^{n/2}, st^\ell$, or $st^{\ell \pm n/2}$, so

$$\psi(G) = \langle \psi(a), \psi(d), \psi(g) \mid g \in \mathcal{G} \rangle = \left\langle t^{n/2}, st^{\ell+qc}, st^\ell \right\rangle.$$

Noting that $\frac{n}{2} > 1$, $x^2 = 1$ for $x \in \{t^{n/2}, (st^\ell)^{\pm 1}, (st^{\ell+qc})^{\pm 1}\}$, and

$$\begin{array}{rlrl}
st^\ell \cdot st^{\ell+qc} &= t^{qc}, & st^{\ell+qc} \cdot st^\ell &= t^{-qc} \\
(st^\ell)^{-1} \cdot st^{\ell+qc} &= t^{qc}, & st^{\ell+qc} \cdot (st^\ell)^{-1} &= t^{-qc} \\
st^\ell \cdot (st^{\ell+qc})^{-1} &= t^{qc}, & st^\ell \cdot (st^{\ell+qc})^{-1} &= t^{-qc} \\
(st^\ell)^{-1} \cdot (st^{\ell+qc})^{-1} &= t^{-qc}, & (st^\ell)^{-1} \cdot (st^{\ell+qc})^{-1} &= t^{qc}.
\end{array}$$

Thus, to spell the element $t \in D_{2n}$ by a word $w \in \{t^{n/2}, (st^\ell)^{\pm 1}, (st^{\ell+qc})^{\pm 1}\}^*$, w must have an even number of s letters, so the word will represent a power of t^c. Since $c > 1$, this is not possible, so ψ is not surjective. Thus, we may assume for the remainder of the proof that $\psi(d)^2 \neq 1$.

By Lemma 5.19 (a), $\psi(d) = t^p$ for $p \in [0, \frac{n}{2} - 1] \cup [\frac{n}{2} + 1, n - 1]$. If $\psi(a) \in \{1, t^{n/2}\}$, then the relation $adad = 1$ in G implies

$$1 = \psi(adad) = \psi(a)\psi(d)\psi(a)\psi(d) = \psi(d)^2$$

which is a contradiction. Thus, $\psi(a) = st^r$ for some $r \in [0, n-1]$. By the first claim, $\psi(g) \in \{1, t^{n/2}, st^r, st^{r \pm n/2}\}$ for all $g \in \mathcal{G}$.

To show $\psi(d) = t^p$ and $\gcd(n, p) = 1$, we first note that

$$\psi(G) = \langle \psi(a), \psi(d), \psi(\mathcal{G}) \rangle \subseteq \left\langle st^r, t^{n/2}, st^{r+n/2}, t^p \right\rangle = \left\langle st^r, t^p, t^{n/2} \right\rangle$$

for some $r \in [0, n-1]$ and $p \in [0, \frac{n}{2} - 1] \cup [\frac{n}{2} + 1, n - 1]$.

Since ψ surjects onto D_{2n} by the hypothesis, we have t is spelled by a word $w \in \{st^r, t^{-r}s, t^p, t^{-p}, t^{n/2}\}^*$, where w has an even number of s occurrences, and after commuting all $t^{n/2}$ factors to the left and applying $(st^r)(st^r) = 1$, w takes the form

$$w = (t^{n/2})^k (t^p)^{i_0} (st^r)^{\epsilon_1} (t^p)^{i_1} \cdots (st^r)^{\epsilon_{2m}} (t^p)^{i_{2m}},$$

where $\epsilon_j \in \{-1, 1\}$ and $k, i_j \in \mathbb{Z}$.

Since

$$(st^r)t^\eta = t^{-\eta}(st^r) \quad \text{and} \quad (st^r)^{-1}t^\eta = t^{-\eta}(st^r)^{-1},$$

for all $\eta \in \mathbb{Z}$, we move all factors $(st^r)^{\epsilon_j}$ to the right, and we obtain

$$\begin{aligned} w &= (t^{n/2})^k (t^p)^{i_0 - i_1 + i_2 - \cdots + i_{2m}} (st^r)^{\epsilon_1 + \cdots + \epsilon_{2m}} \\ &= (t^{n/2})^k (t^p)^y (st^r)^{2z} \\ &= (t^{n/2})^k (t^p)^y \quad (\text{since } (st^r)^2 = 1), \end{aligned}$$

where $y = i_0 - i_1 + i_2 - \cdots + i_{2m}$ and $z = m - |\{j : \epsilon_j = -1\}|$.

Thus, $1 = \frac{kn}{2} + py$. Writing $n = 2^b c$ with $b > 1$, we obtain

$$1 = \tfrac{kn}{2} + py = k2^{b-1}c + py.$$

From this, it follows that $\gcd(p, 2) = 1$ and $\gcd(p, c) = 1$. By induction, $\gcd(p, 2^b c) = 1$.

Thus, $\psi(d) = t^p$ with $\gcd(n, p) = 1$. Let $\varphi = \varphi_{r,p}$ as defined in Lemma 5.10 be an automorphism, and we have

$$\psi\colon \begin{cases} a & \mapsto s_2 t_2^r = \varphi(s_2) \\ d & \mapsto t_2^p = \varphi(t_2) \\ g_{i,j} & \mapsto \gamma_{i,j} \in \{1, t_2^{n/2}, s_2 t_2^r, s_2 t_2^{r+n/2}\}, \quad i \in [0, n], j \in [1, k]. \end{cases}$$

□

Lemma 5.29. *Let $k \in \mathbb{Z}$, $n = 2^b c$ where $c > 1$ is odd and $b > 1$, $\mathbb{X}$, $\mathbb{Y}$, ENF, $(u_i)_{[1,m]}$, and $G_{\mathrm{e}}(n, (u_i)_{[1,m]})$ be as in Definitions 5.22 and 5.26. Then there exists an epimorphism $\psi\colon G_{\mathrm{e}}(n, (u_i)_{[1,m]}) \to D_{2n}$ if and only if there exists a solution $\sigma\colon \mathbb{X} \to D_n$ to the system of equations $(u_i)_{[1,m]}$.*

Proof. Assume that there is an epimorphism $\psi'\colon G_{\mathrm{e}}(n, (u_i)_{[1,m]}) \to D_{2n}$. By Lemma 5.28, there exists $\varphi \in \mathrm{Aut}(D_{2n})$ such that

$$\psi'\colon \begin{cases} a & \mapsto \varphi(s_2) \\ d & \mapsto \varphi(t_2) \\ g_{i,j} & \mapsto \gamma'_{i,j} \in \{\varphi(1), \varphi(s_2), \varphi(t_2^{n/2}), \varphi(s_2 t_2^{n/2})\}; \quad i \in [0, n], j \in [1, k]. \end{cases}$$

Defining $\psi = \varphi^{-1} \circ \psi'$, we obtain an epimorphism

$$\psi\colon \begin{cases} a & \mapsto s_2 \\ d & \mapsto t_2 \\ g_{i,j} & \mapsto \gamma_{i,j} \in \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}; \quad i \in [0, n], j \in [1, k]. \end{cases}$$

Define $\sigma\colon \mathbb{Y} \to \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}$ by $\sigma(Y_{i,j}) = \gamma_{i,j}$ and $\sigma(Y_{i,j}^{-1}) = \gamma_{i,j}^{-1}$. Since $\gamma_{i,j}^2 = 1$ for all $i \in [0, n], j \in [1, k]$, for all $Y_{i,j} \in \mathbb{Y}$, $\sigma(Y_{i,j} = \sigma(Y_{i,j}^{-1}))$, so without loss of generality we can assume $\mathbb{Y} = \{Y_{0,1}, \ldots, Y_{n/2,k}\}$.

For $i \in [1, m]$, let $v_i \in (\{s_2, t_2^2, t_2^{-2}\} \cup \mathbb{Y})^*$ be such that $\mathsf{ENF}(u_i) = v_i$. Since ψ is a homomorphism, for each relator $\lambda(\mathsf{ENF}(u_i))$ of $G_{\mathrm{e}}(n, (u_i)_{[1,m]})$, we have

$$\begin{aligned} 1 &= \psi(\lambda(\mathsf{ENF}(u_i))) = \psi(\lambda(v_i(s_2, t_2^2, t_2^{-2}, Y_{0,1}, \ldots, Y_{n/2,k}))) \\ &= \psi(v_i(a, d^2, d^{-2}, g_{0,1}, \ldots, g_{n/2,k})) \\ &= v_i(s_2, t_2^2, t_2^{-2}, \gamma_{0,1}, \ldots, \gamma_{n/2,k}) \\ &= \sigma(v_i(s_2, t_2^2, t_2^{-2}, Y_{0,1}, \ldots, Y_{n/2,k})) = \sigma(\mathsf{ENF}(u_i)). \end{aligned}$$

Thus, σ solves $(\mathsf{ENF}(u_i))_{[1,m]}$, and the result follows by Lemma 5.23.

Conversely, assume there exists a solution σ to $(u_i)_{[1,m]}$. By Lemma 5.23, there exists a solution $\sigma\colon \mathbb{Y} \to \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}$ to $(\mathsf{ENF}(u_i))_{[1,m]}$. If $\mathsf{ENF}(u_i) = v_i$, then

$$\sigma(\mathsf{ENF}(u_i)) = \sigma(v_i(s_2, t_2^2, t_2^{-2}, \mathbb{Y})) = 1. \tag{5.3}$$

Define $\psi\colon \{a, d, d^{-1}\} \cup \mathcal{G}_{n/2,k} \cup \mathcal{G}_{n/2,k}^{-1} \to D_{2n}$ as

$$\psi\colon \begin{cases} a & \mapsto s_2 \\ d & \mapsto t_2, \qquad d^{-1} \mapsto t_2^{-1} \\ g_{i,j} & \mapsto \sigma(Y_{i,j}), \qquad g_{i,j}^{-1} \mapsto \sigma(Y_{i,j})^{-1}, \qquad g_{i,j} \in \mathcal{G}_{n/2,k}. \end{cases}$$

Using Lemma 2.28 to verify homomorphism, it is clear that for all $g, g' \in \mathcal{G}_{n/2,k}$, the relations a^2, d^n, $adad$, $[g, a]$, $[g, g']$, and g^2 all map to 1 in D_{2n}. Now we check the relation $[d^c, {}_b\, g]$.

If $\psi(g) \in \{1, t_2^{n/2}\}$, then $\psi(g)$ commutes with t_2, and we have $[t^c, \psi(g)] = 1$. Now, consider the case where $\psi(g) = s_2 t_2^r$ with $r \in \{0, \frac{n}{2}\}$.

For this calculation, we denote s_2 and t_2 as s and t, respectively. Noting that $[t^c, st^r] = t^c s t^r t^{-c} t^{-r} s = t^c s t^{-c} s = t^{2c}$, we have

$$\begin{aligned}
\psi([d^c, {}_b\, g]) &= [t^c, {}_b\, st^r] \quad (\text{since } \psi(d)^2 = 1 \text{ and } c \text{ is odd}) \\
&= [\cdots[[[[t^c, st^r], st^r], st^r], st^r], \cdots, st^r] \quad (b \text{ times}) \\
&= \left[\cdots[[[t^{2c}, st^r], st^r], st^r], \cdots, st^r\right] \quad (b-1 \text{ times}) \\
&= \left[\cdots[[t^{4c}, st^r], st^r], \cdots, st^r\right] \quad (b-2 \text{ times}) \\
&= \left[\cdots[t^{8c}, st^r], \cdots, st^r\right] \quad (b-3 \text{ times}) \\
&\vdots \\
&= [t^{2^{b-1}c}, st^r] \quad (b-(b-1) \text{ times}) \\
&= t^{2^b c} = 1.
\end{aligned}$$

(Note that this calculation that shows why we have chosen to write d^c in our nested commutator.)

For ψ to induce a homomorphism $G_{\mathrm{e}}(n, (u_i)_{[1,m]} \to D_{2n})$, it remains to check if $\psi(\lambda(\mathsf{ENF}(u_i))) = 1$ for $i \in [1, m]$. We have

$$\begin{aligned}
\psi(\lambda(\mathsf{ENF}(u_i))) &= \psi(\lambda(v_i(s_2, t_2^2, t_2^{-2}, \mathbb{Y}))) \\
&= v_i(s_2, t_2^2, t_2^{-2}, \sigma(\mathbb{Y})) = \sigma(v_i(s_2, t_2^2, t_2^{-2}, \mathbb{Y})) = 1 \quad (\text{by Eq. (5.3)}).
\end{aligned}$$

Thus, by Lemma 2.28 ψ is a homomorphism, which is surjective since $\psi(G_{\mathrm{e}}(n, (u_i)_{[1,m]})) = \langle s_2, t_2 \rangle = D_{2n}$. □

Theorem 5.30. *Let $n > 1$ be an integer such that either*

- *n is odd, or*
- *$n = 2^b c$ where $b > 1$ and $c > 1$ is odd.*

Then $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{D}_{2\mathrm{n}})$ *is* NP*-hard.*

Proof. In this setting, A is the set of strings encoding finite presentations of a group G, and B is the set of strings encoding systems of equations over a dihedral group. Thus,

$w \in B$ encodes an instance of a system of equations, and $f(w)$ will encode an instance of a group presentation constructed from the data of w.

Let $n > 1$ be an odd integer. Given an input system of equations $(u_i)_{[1,m]}$ with variables $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_k, X_k^{-1}\}$ over D_{2n}, construct the group $G_{\mathrm{o}}(n, (u_i)_{[1,m]})$ as defined in Definition 5.15. This construction can be performed in polynomial time by Remark 5.16. By Lemma 5.18, a solution to $(u_i)_{[1,m]}$ exists if and only if there exists an epimorphism from $G_{\mathrm{o}}(n, (u_i)_{[1,m]})$ to D_{2n}.

Now consider the case where $n = 2^b c$ with $b > 1$ and $c > 1$ odd. Given an input system of equations $(u_i)_{[1,m]}$ with variables $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_k, X_k^{-1}\}$ over D_n, construct the group $G_{\mathrm{e}}(n, (u_i)_{[1,m]})$ as defined in Definition 5.26. This construction can also be performed in polynomial time by Remark 5.27. By Lemma 5.29, a solution to $(u_i)_{[1,m]}$ exists if and only if there exists an epimorphism from $G_{\mathrm{e}}(n, (u_i)_{[1,m]})$ to D_{2n}.

Since D_{2n} is non-abelian for $n > 1$, the result follows from Theorem 5.1. □

Remark 5.31. Note that the case $n = 2c$ is not covered by the even case proof, as Lemmas 5.20 and 5.28 break down for this case. Instead of attempting to modify these lemmas, we take a different approach, as demonstrated in the next section.

5.4 Direct product of abelian and trivial centre

In this section, we prove Item 4 of Theorem D, which will be used to deal with the remaining $n = 2c$ case for dihedral groups. We begin with a well-known fact.

Lemma 5.32. *Let $c > 1$ be odd, then D_{4c} is isomorphic to $D_{2c} \times C_2$.*

Proof. The demonstration in Example 2.20 proves this. □

Recall also that by Lemma 5.12, $Z(D_{2c}) = \{1\}$.

Lemma 5.33. *Let G be a finitely presented group, A an abelian group, and B a group with trivial centre. There exists an epimorphism from $G \times A$ to $B \times A$ if and only if there exists an epimorphism from G to B.*

Proof. Suppose $\kappa\colon G \times A \to B \times A$ is an epimorphism. Recall that $\pi_B\colon B \times A \to B$ is the epimorphism defined by $\pi_B((x, y)) = x$ for all $(x, y) \in B \times A$. Then $\psi = \pi_B \circ \kappa$ is an epimorphism.

For each $z \in A$, $(1, z) \in Z(G \times A)$, so $\psi((1, z)) \in Z(B)$. Since B has trivial centre, $\psi((1, z)) = 1$ for all $z \in A$.

As ψ is an epimorphism, for each $b \in B$, there exists $(x, y) \in G \times A$ such that $\psi((x, y)) = b$. Then,

$$b = \psi((x, y)) = \psi((x, 1))\psi((1, y)) = \psi((x, 1))$$

since $y \in A$ and $\psi((1, y)) = 1$. Thus, ψ restricted to G is an epimorphism.

Conversely, suppose $\tau\colon G \to B$ is an epimorphism. Define $\tau'\colon G \times A \to B \times A$ by $\tau'((x, y)) = (\tau(x), y)$. It is straightforward to verify that τ' is an epimorphism. □

Lemma 5.34 (Direct product with abelian and no centre)**.** *Let A be a finitely generated abelian group and B a finite group with a trivial centre, and* $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B})$ *is* NP*-hard. Then* $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B} \times \mathrm{A})$ *is* NP*-complete.*

Proof. Since B is finite, by Proposition 4.20, $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B} \times \mathrm{A})$ is in NP. We show that it is NP-hard by demonstrating that $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B})$ is polynomial time reducible to $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B} \times \mathrm{A})$. Let $\langle P \mid Q \rangle$ be a finite presentation for A.

Given a finite presentation $\mathcal{P} = \langle X \mid R \rangle$ for a group $G \in \mathsf{FinPres}$, construct a presentation $\mathcal{P}'$ for $G \times A$ by writing

$$\langle X \cup P \mid R \cup Q \cup \{[x, y] \mid x \in X, y \in P\} \rangle .$$

This construction can clearly be done in linear time in the size of $\mathcal{P}$.

By Lemma 5.33, $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B})$ returns 'Yes' on input $\mathcal{P}$ if and only if $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B} \times \mathrm{A})$ returns 'Yes' on input $\mathcal{P}'$. Thus, $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{B} \times \mathrm{A})$ is NP-hard, completing the proof. □

Proof of Theorem C. Theorem 5.30 combined with Lemma 4.1 gives the result for D_{2n} when $n = 2^b c$ with $b = 0$ or $b > 1$, with the case $b = 1$ covered by Lemma 5.34 since D_{4c} is isomorphic to $D_{2c} \times C_2$, and $Z(D_{2c}) = \{1\}$. □

Remark 5.35. Note that D_{2n} is nilpotent if and only if n is a power of 2. It remains unclear whether Theorem C extends to these groups or if there is a way to show $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{D}_{2^k})$ is in P.

6 Other Epimorphism Targets

In this chapter, we prove the remaining items Items 1 to 3 of Theorem D. We do so by invoking established results from the literature that have either not been formally written down or not previously stated within the epimorphism context. These results yield the required decidability or complexity bounds for the corresponding epimorphism problems. The arguments here are more straightforward than in earlier chapters. For completeness, we now record the statements proved below.

Theorem D. *The epimorphism problem from finitely presented groups to the following target classes has the corresponding result.*

1. *Finite rank free groups as the target is decidable.*
2. *A fixed non-abelian finite simple group as the target is* NP*-complete.*
3. *Finitely generated abelian groups as the target is in* P*.*
4. *Under the following three conditions for groups A and B*
   - *A is a finitely generated abelian group*
   - *B is a finite group with a trivial centre*
   - *the epimorphism problem from a finitely presented group to B is* NP*-hard.*

   A fixed group $B \times A$ as the target is NP*-complete.*

For Item 1 we apply the work of Razborov [24] on equations in free groups to show that the epimorphism problem from finitely presented groups to finitely generated free groups is decidable, though without any known complexity bounds. For Item 2 we observe a result of Kuperberg and Samperton [18] is equivalent to the epimorphism problem as defined here. For Item 3 we show that $\mathsf{EPI}(\mathsf{Ab}, \mathsf{Ab})$ is in P, where we utilise the structure theorem for abelian groups (Theorem 2.36), this result is stated to be decidable in [12].

6.1 Epimorphism onto free groups

Notation. Let F_d be the free group of rank d with identity element denoted as $e \in F_d$

Definition 6.1. Let $m, n, d \in \mathbb{N}_+$, $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$, and $(u_i)_{[1,m]}$ a system of equations without constants over F_d, and so each $u_i = u_i(\mathbb{X}) \in \mathbb{X}^*$.

The *rank* of a solution $\sigma \colon \mathbb{X} \to F_d$ is the rank of the free subgroup $\langle \sigma(X_1), \ldots, \sigma(X_n) \rangle$ of F_d.

The *rank* of the system of equations without constants $(u_i)_{[1,m]}$ is the maximum rank over all solutions.

Definition 6.2 (Primitive Element of a Free Group)**.** Let F_d be a free group of rank d with generating set $X = \{x_1, x_2, \ldots, x_d\}$. An element $v \in F_d$ is called a *primitive element* if there exists a automorphism $\varphi \in \mathrm{Aut}(F_d)$ such that

$$\varphi(v) = x_i \quad \text{for some} \quad i \in [1, d].$$

Remark 6.3. Since $\{X_i^{\pm 1} \mapsto e\}$ is a solution to any system without constants, the rank of a solution is at least 0 and at most the number of variables n.

Example 6.4. Let $u = X^{-1}Y^{-1}XYZ^s$ be a system of one equation over F_d. By [30] (see [20, page 51] The only solutions are

$$\{X \mapsto v^i, Y \mapsto v^j, Z \mapsto e\}$$

for some primitive element v. Thus, the rank of this equation is 1.

Theorem 6.5 (Razborov [24, Theorem 3])**.** *Let d be a fixed integer. Given a system of equations $(u_i)_{[1,m]}$ without constants over a free group F_d, there is an algorithm which computes the* rank *of the system of equations.*

Remark 6.6. Note that Razborov's algorithm operates by constructing "Makanin-Razborov diagrams", and the complexity to compute these are not known, though it is conjectured to require at least doubly exponential space (see, for example, [9]), and thus is outside the scope of this thesis.

Lemma 6.7. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Free})$ *is decidable.*

Proof. Assume the input is a finite presentation $\langle g_1, \dots, g_n \mid r_1, \dots, r_m \rangle$ for a group $G \in \mathsf{FinPres}$, and $d \in \mathbb{N}_+$ specifies a target free group of rank d. Let $\mathcal{G} = \{g_1, g_1^{-1}, \dots, g_n, g_n^{-1}\}$ and $\mathbb{X} = \{X_1, X_1^{-1}, \dots, X_n, X_n^{-1}\}$. Perform the following procedure:

1. Fix a free group $H = \langle a_1, \dots, a_d \rangle$.
2. Let $\lambda\colon g_i \mapsto X_i,\ g_i^{-1} \mapsto X_i^{-1}$ induce a monoid homomorphism from words over $\mathcal{G}$ to words over $\mathbb{X}$. Then $(\lambda(r_j))_{[1,m]}$ is a system of equations without constants over F_d, with each $\lambda(r_j) \in \mathbb{X}^*$.
3. Apply Theorem 6.5 with input $(\lambda(r_j))_{[1,m]}$ over the group H, to compute the rank $\mathfrak{r} \in [0, n]$ of the system. If $\mathfrak{r} \geq d$, return 'Yes'; otherwise, return 'No'.

The justification for the procedure is as follows. Let $h_1, \dots, h_n \in H$. By Lemma 2.28, $\{X_i \mapsto h_i, X_i^{-1} \mapsto h_i^{-1} \mid i \in [1, n]\}$ is a solution to $(\lambda(r_j))_{[1,m]}$ if and only if the map induced by $\{g_i \mapsto h_i \mid i \in [1, n]\}$ is a homomorphism from G to H.

If $\mathfrak{r} \geq d$, then there is a homomorphism κ from G onto a subgroup K of H such that K is free of rank $\mathfrak{r}$. The subgroup K has some free basis, say $\{y_1, \dots, y_\mathfrak{r}\}$, and there exists a subgroup $K' = \langle y_1, \dots, y_d \rangle$ of H along with a map $\tau\colon K \to K'$ defined by:

$$\tau(y_i) = \begin{cases} y_i & i \leq d \\ 1 & i > d. \end{cases}$$

Then $\tau \circ \kappa$ is a surjective homomorphism from G to K', and by definition, K' is free of rank d. Note that the procedure finds an epimorphism to some free group of rank d, not necessarily to the original group H.

If $\mathfrak{r} < d$, then there is no epimorphism since an epimorphism $\psi\colon G \to H$ would correspond to a solution to the system of rank d, which contradicts $\mathfrak{r} < d$.

Hence, the procedure correctly decides $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Free})$. □

Remark 6.8. We were unable to prove the analogue of Proposition 4.20 for targets of the form $N \times Q$ when N is a free group of finite rank. While Lemma 4.18 is stated for an arbitrary group N, we could not replicate the strategy of Section 4.2 in this context.

6.2 Epimorphism onto non-abelian finite simple groups

In this section, we observe that Item 2 of Theorem D follows directly from the work of Kuperberg and Samperton. We apply their result directly, and as such we do not

provide formal definitions of certain concepts, such as fundamental groups, 3-manifolds and triangulations, we refer the reader to [29] for rigorous definitions. It is stated in [18] that a finite triangulation is a reasonable and standard input type for these objects.

Definition 6.9. Let Hom be the set of all triangulated homology 3-spheres, given by finite triangulations. From a finite triangulation of a 3-manifold M, one can write down (in linear time) a finite presentation for the fundamental group $\pi_1(M)$ of the manifold.

We now introduce the decision problem as used by Kuperberg and Samperton. [18, Corollary 1.2] prove the following problem is NP-complete.

Problem:	KSHomProb
Input:	Let H be a fixed, finite, non-abelian simple group, $M \in$ Hom and the promise that every non-trivial homomorphism from $\pi_1(M)$ to H is surjective
Output:	Is there a non-trivial homomorphism from $\pi_1(M)$ to H?

Lemma 6.10 ([18, Corollary 1.2])**.** KSHomProb *is* NP*-complete.*

From this result the following is immediate.

Proposition 6.11. *Let G be a fixed, finite, nonabelian group.* EPI(FinPres, G) *is* NP*-hard.*

Proof. On input we are given a finite triangulation for M and the promise that every non-trivial homomorphism from $\pi_1(M)$ to H is surjective. Obtain in linear time a presentation $\langle X \mid R \rangle$ for $\pi_1(M)$.

- If there exists an homorphism from $\pi_1(M) \to G$, i.e. KSHomProb outputs 'Yes', then there exists an epimorphism $\langle X \mid R \rangle \to G$.
- If there does not exist an epimorphism, then it follows there cannot exist homomorphism that has the promise to be surjective, so KSHomProb outputs 'No'.

Thus, we have created a group input ($\langle X \mid R \rangle$), which outputs 'Yes' (resp. 'No') to EPI(FinPres, G) if and only if the original output is 'Yes' (resp. 'No') to KSHomProb on input M. □

6.3 Epimorphism onto Abelian Groups

In this section, we sharpen Proposition 4.20 for the case when the target group is finitely generated abelian (the direct product of a free abelian group with a finite abelian group), and show that the problem EPI(FinPres, Ab) is in P. Given the Structure Theorem for finitely generated abelian groups (Theorem 2.36), the problem is clearly decidable, as noted in [12].

To do this, we reduce the problem to EPI(Ab, Ab), and show that EPI(Ab, Ab) is in P.

Definition 6.12. The *abelianisation* of G denoted G_{ab} is

$$G/[G:G].$$

Remark 6.13. Note that if $\langle X \mid R \rangle$ is a presentation for G, then $\langle X \mid R \cup \{[x,y] : x, y \in X\} \rangle$ is a presentation for G_{ab}, which can clearly be obtained in time linear in the size of $\langle X \mid R \rangle$.

Let $G = \langle \mathcal{X} \mid \mathcal{R} \rangle$, then $\kappa\colon x \mapsto x$ for all $x \in \mathcal{X}$ induces a homomorphism $\kappa\colon G \to G_{ab}$. Moreover, κ is surjective since each $g \in G_{ab}$ can be represented by a word $w \in (\mathcal{X} \cup \mathcal{X}^{-1})^*$, and the element $g' \in G$ spelled by w satisfies $\kappa(g') = g$.

It follows that if $\tau\colon G_{ab} \to H$ is an epimorphism to a group H, then $\psi\colon G \to H$ defined by $\psi(g) = \tau(\kappa(g))$ for all $g \in G$ is an epimorphism. When H is abelian, we have a stronger statement.

Lemma 6.14. *Let $G \in \mathsf{FinPres}$ and $H \in \mathsf{Ab}$. Then there exists an epimorphism $\psi\colon G \to H$ if and only if there exists an epimorphism $\varphi\colon G_{ab} \to H$.*

Proof. One direction is stated above.

For the reverse direction, assume there exists an epimorphism $\psi\colon G \to H$. Let G and G_{ab} be presented as follows:

$$\begin{aligned} G &= \langle x_1, \dots, x_n \mid \mathcal{R} \rangle \\ G_{ab} &= \langle x_1, \dots, x_n \mid \mathcal{R} \cup \{[x_i, x_j]\} \rangle \text{ for } i, j \in [1, n]. \end{aligned}$$

Let $\mathcal{X} = \{x_1, \dots, x_n\}$. Define a set map $\tau\colon G_{ab} \to H$ by $\tau(x_i) = \psi(x_i)$. Since ψ is a homomorphism, we have

$$r(\tau(x_1), \dots, \tau(x_n)) = \psi(r) = 1$$

for all $r \in \mathcal{R}$.

Additionally, since H is abelian we have that

$$[\tau(x_i), \tau(x_j)] = 1$$

for $i, j \in [1, n]$. Thus, τ is a homomorphism by Lemma 2.28.

As ψ is surjective, for all $h \in H$, there exists $w \in (\mathcal{X} \cup \mathcal{X}^{-1})^*$ such that $w =_G g$ and $\psi(g) = h$. Let $g' \in G_{ab}$ be the image of w under the natural abelianisation map (which maps every word to itself under the abelianised group), so $w =_{G_{ab}} g'$. Then,

$$\tau(g') = \tau(w) = \psi(w) = \psi(g) = h.$$

Hence, τ is surjective, and $\tau\colon G_{ab} \to H$ is an epimorphism. □

Thus, to solve $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Ab})$, we can instead solve $\mathsf{EPI}(\mathsf{Ab}, \mathsf{Ab})$.

Lemma 6.15 ([19, Proposition 9.23])**.** *Let G and H be abelian groups. If $\psi\colon G \to H$ is an epimorphism, then*

$$\operatorname{rank}(G) = \operatorname{rank}(H) + \operatorname{rank}(\ker(\psi)).$$

The following technical lemma allows us to check if an epimorphism exists between two finitely generated abelian groups given in invariant forms.

Lemma 6.16. *Let*

$$G \cong \mathbb{Z}^d \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_s} \quad \text{and} \quad H \cong \mathbb{Z}_{c_1} \times \cdots \times \mathbb{Z}_{c_t},$$

with $s, t, a_i, c_j \in \mathbb{N}_+$ such that $c_{i+1} \mid c_i$ and $a_{i+1} \mid a_i$.

Then there exists an epimorphism $\psi\colon G \to H$ if and only if $s \geq t - d$ and $c_{d+i} \mid a_i$ for $i \in [1, t - d]$.

Proof. Let G and H be presented as follows:

$$G = \langle x_1, \ldots, x_{s+d} \mid \{[x_i, x_j], x_k^{a_k} \ ; \ i, j \in [1, s+d], k \in [1, s]\}\rangle$$
$$H = \langle y_1, \ldots, y_t \mid \{[y_i, y_j], y_i^{c_i} \ ; \ i, j \in [1, t]\}\rangle .$$

Assume there is an epimorphism $\psi\colon G \to H$. Then for all $i \in [1, t]$, there exists some $g_i \in G$ such that $\psi(g_i) = y_i$. Thus, $\psi(g_i)^{c_i} = 1_H$, which implies either g_i is of finite order with $g_i^{\ell_i c_i} = 1_G$ for some $\ell_i \in \mathbb{Z}$, or g_i is of infinite order.

First, if $s < t - d$, recall that a map $\tau\colon \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ cannot be an epimorphism if $\gcd(m, n) > 1$. Thus, at most, $\mathbb{Z}^d$ can produce a surjective homomorphism into the first d invariant factors of H. Since ψ exists, we can assume, without loss of generality, that an epimorphism $\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_s} \to \mathbb{Z}_{c_{t-d+1}} \times \cdots \times \mathbb{Z}_{c_t}$ exists. Similarly, as $\mathbb{Z}_a \to \mathbb{Z}_m \times \mathbb{Z}_n$ cannot be an epimorphism if $\gcd(m, n) > 1$, we conclude that $s \geq t - d$.

For g_i of finite order, there must also exist $x_j^{\ell_i c_i} = 1_G$ due to the divisibility property of the torsion generators, which implies $c_{d+i} \mid a_i$ for $i \in [1, t-d]$.

Conversely, assume that $s \geq t - d$ and $c_{d+i} \mid a_i$ for $i \in [1, t-d]$. Construct the following set map $\tau\colon \{x_1, \ldots, x_{s+d}\} \to \{y_1, \ldots, y_t\}$:

$$\tau(x_i) = \begin{cases} y_{d+i} & \text{for } i \in [1, t-d] \\ 1_H & \text{for } i \in [t-d+1, s]\text{; skip this if } s = t-d \\ y_{i-s} & \text{for } i \in [s+1, s+d]. \end{cases}$$

Since $c_{d+i} \mid a_i$, for $i \in [1, t-d]$, we have $\tau(x_i)^{a_i} = y_{d+i}^{\ell_i c_{d+i}}$ for some $\ell_i \in \mathbb{Z}$, and as $y_{d+i}^{c_{d+i}} = 1_H$, it follows that $y_{d+i}^{\ell_i c_{d+i}} = 1_H$. For $i \in [s+1, s+d]$, x_i is of infinite order, so $\psi(x_i)^{c_{i-s}} = y_{i-s}^{c_{i-s}} = 1_H$, and ψ is a homomorphism. Since $a_i \geq c_{d+i}$, ψ is surjective, and thus an epimorphism. □

Lemma 6.17. $\mathsf{EPI}(\mathsf{Ab}, \mathsf{Ab})$ *is in* P.

Proof. Let $G, H \in \mathsf{Ab}$ with free ranks d_1, d_2 respectively, with G being the domain group and H be the target group.

The following procedure solves the problem:

1. Input finite presentations for procedure $\mathsf{AbSTRUC}$, we output the tuples $(d_1, a_1, \ldots, a_s)$ and $(d_2, c_1, \ldots, c_t)$ such that:

$$G \cong \mathbb{Z}^{d_1} \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_s} \quad \text{and} \quad H \cong \mathbb{Z}^{d_2} \times \mathbb{Z}_{c_1} \times \cdots \times \mathbb{Z}_{c_t}$$

   where $a_i \mid a_{i+1}$ for $i \in [1, s-1]$ and $c_i \mid c_{j+1}$ for $j \in [1, t-1]$.
2. If $d_1 < d_2$, output 'No'.
3. Let $b = d_1 - d_2$. If $s \geq t - b$ and $c_{b+i} \mid a_i$ for all $i \in [1, t-b]$, then output 'Yes', otherwise, output 'No'.

Step (1) is performed in polynomial time by Theorem 2.53. Steps (2) and (3) are numerical checks and thus the entire procedure runs in polynomial time.

Step (1) is justified by Theorem 2.36, which allows us to express G and H in its invariant forms. Step (2) ensures that the free rank of G is sufficient to map onto H, as guaranteed by Lemma 6.15. Step (3) is justfied by Lemma 6.16 to ensure that the torsion part of G can map onto the torsion part of H. □

Lemma 6.18. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Ab})$ *is in* P.

Proof. Let $G \in \mathsf{FinPres}$ and $H \in \mathsf{Ab}$. The following procedure solves our problem:

1. Compute a presentation for G_{ab} (the abelianisation of G).
2. If $\mathsf{EPI}(\mathsf{Ab}, \mathsf{Ab})$ on input G_{ab} as the domain group and H as the target group returns 'Yes', return 'Yes'. Otherwise, return 'No'.

Step (1) constructs a finite presentation for G_{ab} in polynomial time, and by Lemma 6.17 Step (2) is in P. □

Proof of Theorem D. Each item is proved as follows.

- Lemma 6.7 gives this item.
- Proposition 6.11 shows that this target is NP-hard, when used in conjunction with Lemma 4.1 gives our NP-complete result.
- Lemma 6.18 gives this result.
- Lemma 5.34 shows that this target is NP-hard, when used in conjunction with Lemma 4.1 gives our NP-complete result.

□

7 Generalised Virtually Abelian Targets

Friedl and Löh [12] conjectured that EPI(FinPres, VAb) is undecidable, based on the undecidability of the "column-generation problem", which was proven undecidable by a reduction to Hilbert's Tenth Problem. This reduction is achieved via the work of Remeslennikov [25], where the following result was proved.

Lemma 7.1 ([25])**.** *Let* $\mathbb{X} = \{X_{1,1}, \dots, X_{n,n}\}$ *be a set of* n^2 *variables. Given a system of* linear equations *with variables in* $\mathbb{X}$*, the problem of whether there exists a solution* $\sigma \colon \mathbb{X} \to \mathbb{Z}$ *such that*

$$\det \begin{pmatrix} \sigma(X_{1,1}) & \sigma(X_{1,2}) & \cdots & \sigma(X_{1,n}) \\ \sigma(X_{2,1}) & \sigma(X_{2,2}) & \cdots & \sigma(X_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma(X_{n,1}) & \sigma(X_{n,2}) & \cdots & \sigma(X_{n,n}) \end{pmatrix} = 1$$

is undecidable.

Despite this, it is unclear if this approach would yield any undecidability or decidability results for EPI(FinPres, VAb). In this chapter, we provide an alternative method to investigate the decidability or complexity of the epimorphism problem for virtually abelian targets. Instead of the above problem, we provide a different problem that is a more complex version of MatrixSubspanA and MatrixSubspanB, which we have shown to be in P. We then show that if the following integer matrix problem is decidable, it implies that EPI(FinPres, VAb) is decidable.

Problem:	MatrixSubspanC
Input:	A tuple $(\{A_0, \dots, A_k\}, \{M_0, \dots, M_k\}, B, \ell)$ where $A_i \in \mathbb{Z}^{m \times n}$, $M_0 = I \in \mathbb{Z}^{d \times d}$, and $M_i \in \mathrm{GL}_{\mathsf{Fin}}(d, \mathbb{Z})$ for $i \in [1, k]$, $B \in \mathbb{Z}^{m \times d}$, $d, \ell \in \mathbb{N}$ with $\ell \in [0, n-1]$.
Question:	Do there exist integer n-vectors $v_1, \dots, v_d$ and the matrix $V = \begin{pmatrix} v_1 & \cdots & v_d \end{pmatrix} \in \mathbb{Z}^{n \times d}$ such that $\sum_{i=0}^{k} A_i((M_i V^T)^T) + B = 0$, and $\mathrm{span}((V\vert_\ell)^T) = \mathbb{Z}^d$?

Thus, by generalising the methods used in Chapter 4, we will prove the following.

Theorem E. *If* MatrixSubspanC *is decidable, then the epimorphism problem from finitely presented groups to virtually abelian groups is decidable.*

From this we propose that to investigate the decidability (resp. complexity) of EPI(FinPres, VAb), one should investigate the decidability (resp. complexity) of MatrixSubspanC.

7.1 Twisted Equations

We begin by generalising the definitions and tools from Chapter 4 for the classes $\mathsf{Ab} \times \mathsf{Fin}$, VCyc, and $\mathsf{Ab} \rtimes_{\pm 1} \mathsf{Fin}$ to encompass all virtually abelian groups. This generalisation

involves extending the definition of a system of equations to incorporate automorphisms on variables, introducing a new method for formulating a system of equations from a (Q, τ)-presentation, and defining a new equation problem through which we reduce the problem of finite presentations to a group described by an extension.

The generalised system of equations include automorphisms acting on variables, analogous to that which is used in Diekert and Elder [8] for equations in free groups.

Definition 7.2. Let G be a group, and let $\Phi = \{\varphi_0, \ldots, \varphi_k\} \leq \mathrm{Aut}(G)$ be a finite subgroup of order $k+1$, where φ_0 is the identity automorphism. Let $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$ be a set of formal variables, and let $\mathcal{G} = \{g_1, \ldots, g_s\}$ with each $g_i \in G$.

A *twisted equation* over G is a word $u \in (\mathcal{G} \cup (\Phi \times \mathbb{X}))^*$, denoted

$$u(\mathcal{G}, \Phi \times \mathbb{X}) = u(g_1, \ldots, g_s, (\varphi_0, X_1), (\varphi_0, X_1^{-1}), \ldots, (\varphi_k, X_n^{-1})).$$

Here each $g_i \in \mathcal{G}$ is called a *constant*, and each pair (φ_p, X_j) is a *twisted variable*.

A *system of twisted equations* over G is a finite list $(u_i)_{i=1}^m$, where each $u_i(\mathcal{G}, \Phi \times \mathbb{X})$ is a twisted equation. We often refer to these collectively as simply "equations" when the context is clear.

A *solution* to such a system is a map $\sigma\colon (\Phi \times \mathbb{X}) \to G$ induced by a map $\sigma_{\mathbb{X}}\colon \mathbb{X} \to G$ defined by

$$\sigma_{\mathbb{X}}(X_j) = h_j, \qquad \sigma_{\mathbb{X}}(X_j^{-1}) = h_j^{-1} \quad \text{for some } h_j \in G,\ j \in [1, n],$$

such that

- for all $p \in [0, k]$ and $j \in [1, n]$, $\varphi_p(\sigma_{\mathbb{X}}(X_j)) = \sigma(\varphi_p, X_j)$; and
- for all $i \in [1, m]$,

$$\sigma(u_i) = u_i(g_1, \ldots, g_s, \sigma(\varphi_0, X_1), \sigma(\varphi_0, X_1^{-1}), \ldots, \sigma(\varphi_k, X_n), \sigma(\varphi_k, X_n^{-1})) =_G 1.$$

Remark 7.3. By the property that $\varphi_p(\sigma_{\mathbb{X}}(X_j)) = \sigma(\varphi_p, X_j)$ for $p \in [0, k]$, $j \in [1, n]$, this implies that σ is uniquely extended from $\sigma_{\mathbb{X}}$. Thus, when describing a solution σ, we can simply define $\sigma_{\mathbb{X}}$ from which it is extended.

Example 7.4. Let $\mathcal{X} = \{x_1, x_2\}$, $H = \langle \mathcal{X} \rangle$ be a free abelian group of rank 2, and $\Phi = \{\varphi_0, \ldots, \varphi_5\}$ where $C_6 \cong \Phi \leq \mathrm{Aut}(H)$, and φ_0 is the trivial automorphism.

Let the automorphisms be described as

$$\begin{array}{lllll}
\varphi_0\colon & x_1 \mapsto x_1 & ; & x_2 \mapsto x_2 \\
\varphi_1\colon & x_1 \mapsto x_1 x_2 & ; & x_2 \mapsto x_1^{-1} \\
\varphi_2\colon & x_1 \mapsto x_2 & ; & x_2 \mapsto x_1^{-1} x_2^{-1} \\
\varphi_3\colon & x_1 \mapsto x_1^{-1} & ; & x_2 \mapsto x_2^{-1} \\
\varphi_4\colon & x_1 \mapsto x_1^{-1} x_2^{-1} & ; & x_2 \mapsto x_1 \\
\varphi_5\colon & x_1 \mapsto x_1^{-1} & ; & x_2 \mapsto x_1 x_2.
\end{array}$$

This set of automorphisms is in bijection with the group $C_6 = \langle a \mid a^6 \rangle$ where $\varphi_i = a^i$ for $i \in [0, 5]$.

For brevity, we omit the inverse variables from the following system of twisted equations. Given a system of twisted equations with variables $\mathbb{X} = \{X, Y, Z\}$ over H

$$\begin{array}{lcllll}
u_1((\mathcal{X} \cup \mathcal{X}^{-1}), (\Phi \times \mathbb{X})) & = & (\varphi_0, X) & (\varphi_1, X) & (\varphi_0, Z) & (x_1^2 x_2^5) \\
u_2((\mathcal{X} \cup \mathcal{X}^{-1}), (\Phi \times \mathbb{X})) & = & (\varphi_2, Z) & (\varphi_0, Z) & & (x_1^{-1}) \\
u_3((\mathcal{X} \cup \mathcal{X}^{-1}), (\Phi \times \mathbb{X})) & = & (\varphi_3, Y) & (\varphi_4, Z) & (\varphi_0, X) & (x_2^{-5}).
\end{array}$$

A possible valid solution σ is extended from $\sigma_{\mathbb{X}}\colon \mathbb{X} \to (\mathcal{X} \cup \mathcal{X}^{-1})^*$ is

$$\sigma_{\mathbb{X}}\colon \begin{cases} X & \mapsto x_1^{-2}x_2^{-3} \\ Y & \mapsto x_1^{-3}x_2^{-8} \\ Z & \mapsto x_2^{-1}. \end{cases}$$

This extends to σ uniquely, as an example for the automorphism φ_1 we have

$$\sigma\colon \begin{cases} (\varphi_1, X) & \mapsto x_1x_2^{-2} \\ (\varphi_1, Y) & \mapsto x_1^5x_2^{-3} \\ (\varphi_1, Z) & \mapsto x_1. \end{cases}$$

Thus, our equations take the form

$$\begin{array}{rcccccl}
\sigma(u_1) & = & \sigma(\varphi_0, X) & \sigma(\varphi_1, X) & \sigma(\varphi_0, Z) & (x_1^2x_2^5) & \\
 & = & \sigma_{\mathbb{X}}(X) & \varphi_1(\sigma_{\mathbb{X}}(X)) & \sigma_{\mathbb{X}}(Z) & (x_1^2x_2^5) & \\
 & = & (x_1^{-2}x_2^{-3}) & \varphi_1(x_1^{-2}x_2^{-3}) & (x_2^{-1}) & (x_1^2x_2^5) & \\
 & = & (x_1^{-2}x_2^{-3}) & (x_1x_2^{-2}) & (x_2^{-1}) & (x_1x_2^6) & = 1 \\
\sigma(u_2) & = & \sigma(\varphi_2, Z) & \sigma(\varphi_0, Z) & & (x_1^{-1}) & \\
 & = & \varphi_2(\sigma_{\mathbb{X}}(Z)) & \sigma_{\mathbb{X}}(Z) & & x_1^{-1} & \\
 & = & \varphi_2(x_2^{-1}) & (x_2^{-1}) & & x_1^{-1} & \\
 & = & (x_1x_2) & (x_2^{-1}) & & (x_1^{-1}) & = 1 \\
\sigma(u_3) & = & \sigma(\varphi_3, Y) & \sigma(\varphi_4, Z) & \sigma(\varphi_0, X) & (x_2^{-5}) & \\
 & = & \varphi_3(\sigma_{\mathbb{X}}(Y)) & \varphi_4(\sigma_{\mathbb{X}}(Z)) & \sigma_{\mathbb{X}}(X) & x_2^{-5} & \\
 & = & \varphi_3(x_1^{-3}x_2^{-8}) & \varphi_4(x_2^{-1}) & (x_1^{-2}x_2^{-3}) & (x_2^{-5}) & \\
 & = & (x_1^3x_2^8) & (x_1^{-1}) & (x_1^{-2}x_2^{-3}) & (x_2^{-5}) & = 1.
\end{array}$$

Confirming that this is a valid solution.

We now define some structure analogous to those found in Section 4.3, in particular Definitions 4.21, 4.22 and 4.25.

Definition 7.5 (twisted-word)**.** Let

- G be a group
- $\Phi \leq \mathrm{Aut}(G)$ be a finite subgroup
- A, B be two disjoint finite sets
- $\rho\colon A \cup A^{-1} \cup B \cup B^{-1} \to G$ be a set map
- $\phi\colon A \to \Phi$ be a set bijection, which naturally induces a monoid homomorphism $\phi\colon A \cup A^{-1} \to \Phi$.

Define $\xi_A\colon (A \cup B \cup A^{-1} \cup B^{-1})^* \to (A \cup A^{-1})^*$, a *letter-erasing* homomorphism as the map induced by

$$\xi_A\colon \begin{cases} a \mapsto a & \forall a \in A \cup A^{-1} \\ b \mapsto \varepsilon & \forall b \in B \cup B^{-1} \end{cases}$$

For $w = v_1 \cdots v_n$ with $v_i \in A \cup B \cup A^{-1} \cup B^{-1}$, let $w_p \in (A \cup A^{-1})^*$ for $p \in [1, n]$ be the word

$$w_p = \xi_A(v_1 \cdots v_p).$$

For w, the *twist-factor* of letter v_i is $\mu_i \in \mathrm{Aut}(G)$, where $\mu_i = \phi(w_i)$.

Define $\Gamma_{(G,\Phi,A,B,\rho,\phi)}\colon (A \cup A^{-1} \cup B \cup B^{-1})^* \to G$ by

$$\Gamma_{(G,\Phi,A,B,\rho,\phi)}\colon v_1v_2 \cdots v_n \mapsto \mu_0(\rho(v_1))\mu_1(\rho(v_2)) \cdots \mu_{n-1}(\rho(v_n)).$$

We call $\Gamma_{(G,\Phi,A,B,\rho,\phi)}(w)$ the *twisted-word* of w.

Example 7.6. Let G be a group, $\{\varphi_0, \varphi_1, \varphi_2\} = \Phi \leq \mathrm{Aut}(G)$ be a finite subgroup such that $\varphi_1^2 = \varphi_2$ and $\varphi_1^3 = \varphi_0$ the trivial automorphism. $\mathcal{X} = \{x_1, x_2, x_3\}$, $\mathcal{Y} = \{y_1, y_2\}$, $\rho\colon \mathcal{X} \cup \mathcal{Y} \to G$ and $\phi\colon \mathcal{X} \to \Phi$ are defined as

$$\rho\colon \begin{cases} x_i & \mapsto g_i, \quad i \in [1,3] \\ y_i & \mapsto g_{i+3}, \quad i \in [1,2] \end{cases}, \quad \phi\colon \begin{cases} x_1 & \mapsto \varphi_1 \\ x_2 & \mapsto \varphi_2 \\ x_3 & \mapsto \varphi_0. \end{cases}$$

For a word $w = x_1x_1y_1x_2y_2$, we first calculate the $\mathcal{X}$-twist-factor $\mu_i = \phi(w_i)$, the calculation for $i \in [0,4]$ is as follows

$$\begin{array}{llll} \mu_0 & = \phi(\xi_{\mathcal{X}}()) & = \phi() & = \varphi_0 \\ \mu_1 & = \phi(\xi_{\mathcal{X}}(x_1)) & = \phi(x_1) & = \varphi_1 \\ \mu_2 & = \phi(\xi_{\mathcal{X}}(x_1x_1)) & = \phi(x_1x_1) & = \varphi_2 \\ \mu_3 & = \phi(\xi_{\mathcal{X}}(x_1x_1y_1)) & = \phi(x_1x_1) & = \varphi_2 \\ \mu_4 & = \phi(\xi_{\mathcal{X}}(x_1x_1y_1x_2)) & = \phi(x_1x_1x_2) & = \varphi_1 \end{array}$$

and the twisted-word of w is

$$\begin{aligned} \Gamma_{(G,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}(x_1x_1y_2x_2y_2) &= \varphi_0(\rho(x_1))\varphi_1(\rho(x_1))\varphi_2(\rho(y_1))\varphi_2(\rho(x_1))\varphi_1(\rho(y_2)) \\ &= \varphi_0(g_1)\varphi_1(g_1)\varphi_2(g_4)\varphi_2(g_2))\varphi_1(g_5). \end{aligned}$$

Lemma 7.7. *Given*

- *G a (Q,τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$*
- *H a virtually abelian group represented by an N by Q extension where $N \cong \mathbb{Z}^d$ and Q is finite, with extension data (θ, f_s)*
- *$\kappa\colon G \to H$ be a homomorphism*

and let

- *$\Phi = \theta(Q)$, and so $\Phi \leq \mathrm{Aut}(N)$ is a finite group*
- *$\rho = \pi_N \circ \kappa$, then $\rho\colon \mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1} \to N$ is a homomorphism*
- *$\phi = \theta \circ \tau$, and so $\phi\colon \mathcal{X} \to \Phi$ is a set bijection*
- *$\Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}\colon (\mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1})^* \to H$ defined as in Definition 7.5.*

For all words $w = v_1 \cdots v_k \in (\mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1})^*$, if $\tau(v_i) = q_i$ then

$$\kappa(w) = \Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}(w)\tilde{f}(\tau(v_1), \ldots, \tau(v_k))s(\tau(w)).$$

Proof. Let $\mu_i = \phi(w_i)$, for a word $w = v_1 \cdots v_k$, where $v_i \in (\mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1})$, by definition

$$\Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}(w) = \mu_0(\rho(v_1))\mu_1(\rho(v_2)) \cdots \mu_{k-1}(\rho(v_k)). \tag{7.1}$$

Recall that by the properties of a (Q,τ)-presentation

- $\tau\colon \mathcal{X} \to Q$ is a set bijection
- if $\kappa(g) = ns(q)$ then $\tau(g) = q$
- $\langle \mathcal{Y} \rangle = \ker(\tau)$.

For a word w, we apply κ and so we get

$$\kappa(w) = \kappa(v_1) \cdots \kappa(v_d)$$

as $\kappa(g) = ns(q)$ implies $\tau(g) = q$ we have

$$\kappa(w) = \pi_N(\kappa(v_1))s(\tau(v_1)) \cdots \pi_N(\kappa(v_k))s(\tau(v_k)) = \rho(v_1)s(\tau(v_1)) \cdots \rho(v_k)s(\tau(v_k)).$$

By noting that for all $n \in N$ and $q \in Q$, $s(q)n = s(q)ns(q)^{-1}s(q) = {}^{s(q)}ns(q)$, then denote $\tau(v_i) = q_i$ and we can perform the following calculation

$$\begin{aligned}
\kappa(w) &= \rho(v_1)s(q_1)\rho(v_2)s(q_2)\rho(v_3)s(q_3)\cdots\rho(v_k)s(q_k)\\
&= \rho(v_1)^{s(q_1)}\rho(v_2)s(q_1)s(q_2)\rho(v_3)s(q_3)\cdots\rho(v_k)s(q_k)\\
&= \rho(v_1)\left({}^{s(q_1)}\rho(v_2)\right)\left({}^{s(q_1)s(q_2)}\rho(v_3)\right)s(q_1)s(q_2)s(q_3)\cdots\rho(v_k)s(q_k)\\
&\;\;\vdots\\
&= \rho(v_1)\left({}^{s(q_1)}\rho(v_2)\right)\left({}^{s(q_1)s(q_2)}\rho(v_3)\right)\cdots\left({}^{s(q_1)\cdots s(q_{k-1})}\rho(v_k)\right)s(q_1)\cdots s(q_k).
\end{aligned}$$

By definition $f(q_i, q_j) = s(q_i)s(q_j)s(q_iq_j)^{-1}$, and using the property that N is abelian, then for all $n \in N$

$$\begin{aligned}
{}^{s(q_i)s(q_j)}n &= s(q_i)s(q_j)ns(q_j)^{-1}s(q_i)^{-1}\\
&= f(q_i,q_j)s(q_iq_j)ns(q_iq_j)^{-1}f(q_i,q_j)^{-1}\\
&= f(q_i,q_j)^{s(q_iq_j)}nf(q_i,q_j)^{-1}\\
&= {}^{s(q_iq_j)}n
\end{aligned} \tag{7.2}$$

and similarly

$$\begin{aligned}
&s(q_1)s(q_2)s(q_3)\cdots s(q_k)\\
&= f(q_1,q_2)s(q_1q_2)s(q_3)\cdots s(q_k)\\
&= f(q_1,q_2)f(q_1q_2,q_3)s(q_1q_2q_3)\cdots s(q_k)\\
&\;\;\vdots\\
&= f(q_1,q_2)f(q_1q_2,q_3)f(q_1q_2q_3,q_4)\cdots f(q_1\cdots q_{k-1},q_k)s(q_1\cdots q_k)\\
&= \tilde{f}_{|w|}(q_1,\ldots,q_k)s(q_1\cdots q_k).
\end{aligned}$$

Thus, we have

$$\kappa(w) = \rho(v_1)\left({}^{s(q_1)}\rho(v_2)\right)\left({}^{s(q_1q_2)}\rho(v_3)\right)\cdots\left({}^{s(q_1\cdots q_{k-1})}\rho(v_k)\right)\tilde{f}_{|w|}(q_1,\ldots,q_k)s(q_1\cdots q_k)$$

as $q_i = \tau(v_i)$, then $q_1q_2\cdots q_i = \tau(v_1v_2\cdots v_i) = \tau(w_i)$, and we have

$$\kappa(w) = \rho(v_1)\left({}^{s(\tau(w_1))}\rho(v_2)\right)\left({}^{s(\tau(w_2))}\rho(v_3)\right)\cdots\left({}^{s(\tau(w_{k-1}))}\rho(v_k)\right)\tilde{f}_{|w|}(q_1,\ldots,q_k)s(q_1\cdots q_k).$$

As $\langle\mathcal{Y}\rangle = \ker(\tau)$, then for any word in $(\mathcal{X}\cup\mathcal{X}^{-1}\cup\mathcal{Y}\cup\mathcal{Y}-1)^*$

$$\tau(w) = \tau(\xi_{\mathcal{X}}(w))$$

and so for all $n \in N$

$${}^{s(\tau(w))}n = {}^{s(\tau(\xi_{\mathcal{X}}(w)))}n = \theta(\tau(\xi_{\mathcal{X}}(w))) = \phi(\xi_{\mathcal{X}}(w))$$

so, for the word w_i

$${}^{s(\tau(w_i))}n = \phi(w_i)(n) = \mu_i(n)$$

where $\mu_i \in \mathrm{Aut}(N)$ is the twist-factor as defined in Example 7.6. Thus

$$\kappa(w) = \mu_0(\rho(v_1))\mu_1\left(\rho(v_2)\right)\mu_2\left(\rho(v_3)\right)\cdots\mu_{k-1}\left(\rho(v_k)\right)\tilde{f}_{|w|}(q_1,\ldots,q_k)s(q_1\cdots q_k)$$

where μ_0 is the trivial automorphism. Then by Eq. (7.1) we have

$$\kappa(w) = \Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}(w)\tilde{f}_{|w|}(q_1,\ldots,q_k)s(q_1\cdots q_k).$$

□

Remark 7.8. Eq. (7.2) highlights why H needs to be virtually abelian, that is if N is not abelian we do not have the fact that ${}^{s(q_i)s(q_j)}n = {}^{s(q_iq_j)}n$. If N was not abelian, we would instead have

$$\begin{aligned} {}^{s(q_i)s(q_j)}n &= s(q_i)s(q_j)ns(q_j)^{-1}s(q_i)^{-1} \\ &= f_s(q_i,q_j)s(q_iq_j)ns(q_iq_j)^{-1}f_s(q_i,q_j)^{-1} \\ &= f_s(q_i,q_j)\left({}^{s(q_iq_j)}n\right)f_s(q_i,q_j)^{-1}. \end{aligned}$$

7.2 Building Twisted Equations

Using Lemma 7.7 as motivation, we define the following way to write a system of twisted equations from a (Q,τ)-presentation, which will be useful for analysing epimorphisms to groups described by an extension with a finite quotient and its extension data, analogous to the construction in Definitions 4.17 and 4.25.

Definition 7.9 (Presentation to system of equations)**.** Given $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R}\rangle$, a (Q,τ)-presentation for a group G, and H an N by Q extension where $N \cong \mathbb{Z}^d$ and Q is finite with extension data (θ, f_s). Let

- $\Phi = \theta(Q)$ and label each automorphism of Φ as φ_p, for $p \in [0, |Q|-1]$ such that φ_0 is the trivial automorphism
- $\rho\colon \mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1} \to H$ be a set map
- $\phi = \theta \circ \tau$, and so $\phi\colon \mathcal{X} \to \Phi$ is a set bijection
- $\mathbb{X} = \{X_1, X_1^{-1} \ldots, X_{|\mathcal{X}|}, X_{|\mathcal{X}|}^{-1}\}$ and $\mathbb{Y} = \{Y_1, Y_1^{-1} \ldots, Y_{|\mathcal{Y}|}, Y_{|\mathcal{Y}|}\}^{-1}$

Define $\Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}$ as in Definition 7.5. For a word $w \in (\mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1})^*$, let ζ be a map from a twisted-word $\Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}(w)$ to a twisted equation via the set map

$$\zeta\colon \begin{cases} \varphi_p(\rho(x_j)) & \mapsto (\varphi_p, X_j) \\ \varphi_p(\rho(x_j^{-1})) & \mapsto (\varphi_p, X_j^{-1}) \\ \varphi_p(\rho(y_j)) & \mapsto (\varphi_p, Y_j) \\ \varphi_p(\rho(y_j^{-1})) & \mapsto (\varphi_p, Y_j^{-1}). \end{cases}$$

For $i \in [1, |\mathcal{R}|]$, assume each $r_i \in \mathcal{R}$ has the form:

$$r_i = v_{i,1} \ldots v_{i,|r_i|} \quad \text{where} \quad v_{i,j} \in \mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1}.$$

Let $\tilde{f}_k$ be as defined in Definition 2.64, define $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$ to be the system of equations $(u_i)_{[1,|\mathcal{R}|]}$, where

$$u_i = \zeta\left(\Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}(r_i)\right)\tilde{f}_{|r_i|}(\tau(v_{i,1}) \cdots \tau(v_{i,|r_i|}))).$$

Example 7.10. Given $\mathcal{X} = \{x_1, x_2, x_3\}$, $\mathcal{Y} = \{y_1, y_2\}$ and G be a (Q,τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R}\rangle$, H be a N by Q extension with data (θ, f_s), $Q = \{q_1, q_2, q_3\} \cong C_3$ such that $q_1^2 = q_2, q_1^3 = q_3 = 1_Q$, and $\tau\colon \mathcal{X} \to Q$ be defined as $\tau\colon x_i \mapsto q_i$. Let

- $\Phi = \theta(Q)$, so $\Phi = \{\theta(q_1), \theta(q_2), \theta(q_3)\}$, as $q_3 = 1_Q$, label $\theta(q_3) = \varphi_0$ and $\theta(q_i) = \varphi_i$ for $i \in \{1,2\}$
- $\rho\colon \mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1} \to H$ be an unspecified set map
- $\phi = \theta \circ \tau$, so $\phi\colon \mathcal{X} \to \Phi \leq \mathrm{Aut}(N)$

$$\phi\colon \begin{cases} x_1 & \mapsto \theta(\tau(x_1)) = \theta(q_1) = \varphi_1 \\ x_2 & \mapsto \theta(\tau(x_2)) = \theta(q_2) = \varphi_2 \\ x_3 & \mapsto \theta(\tau(x_3)) = \theta(q_3) = \varphi_0 \end{cases}$$

- $\mathbb{X} = \{X_1, X_1^{-1} \dots, X_3, X_3^{-1}\}$ and $\mathbb{Y} = \{Y_1, Y_1^{-1} \dots, Y_2, Y_2\}^{-1}$.

For some $r_i \in \mathcal{R}$, let $r_i = x_1x_1y_1x_2y_2$, then by noting that this is the same word as in Example 7.6

$$\begin{aligned} u_i &= \zeta\left(\Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}(x_1x_1y_1x_2y_2)\right)\tilde{f}_5(\tau(x_1),\tau(x_1),\tau(y_1),\tau(x_2),\tau(y_2)) \\ &= \zeta\left(\varphi_0(\rho(x_1))\varphi_1(\rho(x_1))\varphi_2(\rho(y_1))\varphi_2(\rho(x_1))\varphi_1(\rho(y_2))\right)\tilde{f}_5(q_1,q_1,1_Q,q_2,1_Q) \\ &= (\varphi_0, X_1)(\varphi_1, X_1)(\varphi_2, Y_1)(\varphi_2, Y_1)(\varphi_1, Y_2)\tilde{f}_5(q_1,q_1,1_Q,q_2,1_Q). \end{aligned}$$

Next, we define the following equations problem for which we reduce the epimorphism problem to for virtually abelian targets.

Problem:	TwistedEquationSubspan
Input:	A group N, variables $\mathbb{X} = \{X_1, X_1^{-1}, \dots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \dots, Y_\ell, Y_\ell^{-1}\}$, a finite list of automorphisms $\Phi = \{\varphi_0, \dots, \varphi_k\}$ which form a subgroup $\Phi \leq \mathrm{Aut}(N)$, and a finite system of twisted equations over N, each of the form $u_i = v_i\mathfrak{c}_i$ where $v_i \in (\Phi \times (\mathbb{X} \cup \mathbb{Y}))^*$ and $\mathfrak{c}_i \in N$.
Output:	Is there a solution $\sigma\colon (\Phi \times (\mathbb{X} \cup \mathbb{Y})) \to N$ such that $\langle \sigma(\varphi_0, Y_1), \dots, \sigma(\varphi_0, Y_\ell)\rangle = N$?

Lemma 7.11. *Let $G \in$ FinPres, H be a N by Q extension, $N \in$ FreeAb, $Q \in$ Fin with extension data (θ, f_s). The following are equivalent*

1. *There exists an epimorphism from G to H.*
2. *There exists an epimorphism $\tau\colon G \to Q$ such that for some (Q,τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R}\rangle$ for G,* TwistedEquationSubspan *returns 'Yes' on input N and* PresEqnC$(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$.

Proof. We begin by setting some notation for this proof. Let

- $\Phi = \theta(Q)$, and so $\Phi \leq \mathrm{Aut}(N)$ is a finite subgroup
- $\rho = \pi_N \circ \kappa$
- $\phi = \theta \circ \tau$
- $\Gamma_{(N,\Phi,\mathcal{X},\mathcal{Y},\rho,\phi)}$ be as in Definition 7.5, denoted as Γ
- $\tilde{f}_{|r_i|}(\tau(v_{i,1}) \cdots \tau(v_{i,|r_i|})))$ be as in Definition 2.64, denoted as $\tilde{f}_i$.

For $i \in [1, m]$, the equation u_i is derived from $r_i = v_{i,1} \dots v_{i,|r_i|}$, denote

$$\tau(v_{i,j}) = v'_{i,j}, \quad \tilde{v}_{i,j} = v'_{i,1} \cdots v'_{i,j} \quad \text{and} \quad \mu_{i,j} = \phi(\xi_{\mathcal{X}}(\tilde{v}_{i,j})).$$

So each equation $u_i = \zeta(\Gamma(r_i))\tilde{f}_i$, and $\zeta(\Gamma(r_i))$ is equivalent to

$$\begin{array}{lccccc} \zeta(\Gamma(& & & & r_i &)) \\ = \zeta(\Gamma(& v_{i,1} & v_{i,2} & \dots & v_{i,|r_i|} &)) \\ = \zeta(& \phi(\xi_{\mathcal{X}}(\tilde{v}_{i,0}))(\rho(v_{i,1})) & \phi(\xi_{\mathcal{X}}(\tilde{v}_{i,1}))(\rho(v_{i,2})) & \dots & \phi(\xi_{\mathcal{X}}(\tilde{v}_{i,|r_i|-1}))(\rho(v_{i,|r_i|})) &) \\ = \zeta(& \mu_{i,0}(\rho(v_{i,1})) & \mu_{i,1}(\rho(v_{i,2})) & \dots & \mu_{i,|r_i|-1}(\rho(v_{i,|r_i|})) &) \end{array}$$

let $(\varphi_p, V_{i,j}) = \zeta(\varphi_p(\rho(v_{i,j})))$ where φ_0 is the trivial automorphism and $V_{i,j} \in \mathbb{X} \cup \mathbb{Y}$ then we have

$$\zeta(\Gamma(r_i)) = (\mu_{i,0}, V_{i,1})(\mu_{i,1}, V_{i,2}) \cdots (\mu_{i,|r_i|-1}, V_{i,|r_i|}). \tag{7.3}$$

Assume there exists an epimorphism from G to H. By Lemma 4.7 and Remark 4.8, there exist $\tau\colon G \to Q$ (an epimorphism) and $\kappa\colon G \to H$ (a homomorphism) such that

(b) $\kappa(g) = ns(q)$ implies $q = \tau(g)$,

(c') For all $n \in N$, there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(w) = ns(1_Q)$.
Applying the homomorphisms κ to r_i, and by Lemma 7.7 we have

$$\kappa(r_i) = \Gamma(r_i)\ \tilde{f}_i\ s(\tau(r_i))$$

as τ is a homomorphism it follows that $s(\tau(r_i)) = s(1_Q)$, and κ is also a homomorphism this implies

$$\Gamma(r_i)\ \tilde{f}_i\ s(1_Q) = \Gamma(r_i)\ f_i = 1_N \tag{7.4}$$

we will now build a solution which uses this fact.

Let a solution $\sigma\colon (\Phi \times (\mathbb{X} \cup \mathbb{Y})) \to N$ be extended from $\sigma_{\mathbb{X}\cup\mathbb{Y}}\colon \mathbb{X} \cup \mathbb{Y} \to N$ which is defined as

$$\begin{aligned}
\sigma_{\mathbb{X}\cup\mathbb{Y}}(X) &= \pi_N(\kappa(\Gamma^{-1}(\zeta^{-1}(\varphi_0, X)))) = \pi_N(\kappa(x)), \qquad & \sigma_{\mathbb{X}\cup\mathbb{Y}}(X^{-1}) &= \pi_N(\kappa(x^{-1})) \\
\sigma_{\mathbb{X}\cup\mathbb{Y}}(Y) &= \pi_N(\kappa(\Gamma^{-1}(\zeta^{-1}(\varphi_0, Y)))) = \pi_N(\kappa(y)), \qquad & \sigma_{\mathbb{X}\cup\mathbb{Y}}(Y^{-1}) &= \pi_N(\kappa(y^{-1}))
\end{aligned}$$

where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, and by the use of Eqs. (7.3) and (7.4) we have,

$$\begin{array}{lccccccc}
 & \sigma(& & u_i & & & &) \\
= & \sigma(& (\mu_{i,0}, V_{i,1}) & (\mu_{i,1}, V_{i,2}) & \cdots & (\mu_{i,|r_i|-1}, V_{i,|r_i|}) &) & \tilde{f} \\
= & & \mu_{i,0}(\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_{i,1})) & \mu_{i,1}(\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_{i,2})) & \cdots & \mu_{i,|r_i|-1}(\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_{i,|r_i|})) & & \tilde{f} \\
= & & \mu_{i,0}(\pi_N(\kappa(v_{i,1}))) & \mu_{i,1}(\pi_N(\kappa(v_{i,2}))) & \cdots & \mu_{i,|r_i|-1}(\pi_N(\kappa(v_{i,|r_i|}))) & & \tilde{f} \\
= & & \mu_{i,0}(\rho(v_{i,1})) & \mu_{i,1}(\rho(v_{i,2})) & \cdots & \mu_{i,|r_i|-1}(\rho(v_{i,k})) & & \tilde{f} \\
= & \Gamma(& & r_i & & &) & \tilde{f} \\
= & 1_N. & & & & & &
\end{array}$$

verifying that σ is a solution to $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$.

By item (c'), for all $n \in N$, there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(\Gamma(w)) = ns(1_Q)$, so $\pi_N(\kappa(w)) = n$, and if $w \in (\mathcal{Y} \cup \mathcal{Y})^{-1}$ then every twist-factor is equal to the trivial automorphism, so $\Gamma(w) = \rho(w)$. Let $w = v_1 \cdots v_k$ and denote $\zeta(\varphi_0(v_i)) = (\varphi_0, V_i)$ for $V_i \in \mathbb{Y}$, then there exists $\zeta(\Gamma(w)) \in (\varphi_0 \times \mathbb{Y})^*$ which satisfies

$$\begin{array}{lcccccc}
 & \sigma(& & \zeta(\Gamma(w)) & & &) \\
= & \sigma(\zeta(\Gamma(& v_1 & \cdots & v_k &))) & \\
= & \sigma(& (\varphi_0, V_1) & \cdots & (\varphi_0, V_k) &) & \\
= & & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_1) & \cdots & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_k) & & \\
= & & \pi_N(\kappa(v_1)) & \cdots & \pi_N(\kappa(v_k)) & & \\
= & \pi_N(\kappa(& & w & &)) & \\
= & & & n & & &
\end{array}$$

which implies $\langle \sigma(\varphi_0, Y_1), \ldots, \sigma(\varphi_0, Y_\ell) \rangle = N$. Therefore, TwistedEquationSubspan returns 'Yes'.

Conversely, assume there exists an epimorphism $\tau\colon G \to Q$ such that for some (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G, TwistedEquationSubspan returns 'Yes' on input N and the system of equations $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$ and so there is a solution $\sigma\colon (\Phi \times (\mathbb{X} \cup \mathbb{Y})) \to N$ such that to the system of equation $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$ such that $\langle \sigma(\varphi_0, Y_1), \ldots, \sigma(\varphi_0, Y_\ell) \rangle = N$. We will show that there exists a homomorphism $\kappa\colon G \to H$ such that τ, κ satisfy conditions

(b) $\kappa(g) = ns(q)$ implies $q = \tau(g)$
(c') for some (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G, for all $n \in N$, there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(w) = ns(1_Q)$

of Lemma 4.7 and Remark 4.8, thereby proving the existence of an epimorphism from G to H.

Recall that in this case, $\rho\colon (\mathcal{X}\cup\mathcal{Y}\cup\mathcal{X}^{-1}\cup\mathcal{Y}^{-1})\to N$ is an unspecified set map which serves as an intermediary map for $\zeta\colon N\to(\Phi\times(\mathbb{X}\cup\mathbb{Y}))$. Define a map $\kappa\colon(\mathcal{X}\cup\mathcal{X}^{-1}\cup\mathcal{Y}\cup\mathcal{Y}^{-1})^*\to N$ as the extension of the set map

$$\kappa(a)=\sigma(\zeta(\varphi_0(\rho(a))))s(\tau(a))$$

for $a\in\mathcal{X}\cup\mathcal{X}^{-1}\cup\mathcal{Y}\cup\mathcal{Y}^{-1}$. Thus, if $\zeta(\varphi_0(\rho(a)))=(\varphi_0,A)$ for some $A\in\mathbb{X}\cup\mathbb{Y}$

$$\kappa(a)=\sigma_{\mathbb{X}\cup\mathbb{Y}}(A)s(\tau(a)).$$

For a word $w=v_1\cdots v_k$, where $v_1,\ldots,v_k\in(\mathcal{X}\cup\mathcal{X}^{-1}\cup\mathcal{Y}\cup\mathcal{Y}^{-1})$, denote $\zeta(\varphi_0(\rho(v_j)))=(\varphi_0,V_j)$ for $V_j\in\mathcal{X}\cup\mathcal{Y}$ and denote $\tilde{f}_k(s(\tau(v_1),\ldots,s(\tau(v_k)))$ as $\tilde{f}_{|w|}$ for this next calculation, so we have that

$$\begin{array}{rcccl}
\kappa(w)= & \kappa(v_1) & \kappa(v_2) & \cdots & \kappa(v_k)\\
= & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_1)s(\tau(v_1)) & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_2)s(\tau(v_2)) & \cdots & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_k)s(\tau(v_k))\\
= & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_1)s(v_1') & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_2)s(v_2') & \cdots & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_k)s(v_k')\\
= & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_1) & {}^{s(v_1')}\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_2)s(v_1')s(v_2') & \cdots & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_k)s(v_k')\\
= & & & \vdots & \\
= & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_1) & {}^{s(v_1')}\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_2) & \cdots & {}^{s(v_1'\cdots v_{k-1}')}\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_k)\\
& & & & s(v_1')\cdots s(v_k')\\
= & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_1) & {}^{s(\tilde{v}_1)}\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_2) & \cdots & {}^{s(\tilde{v}_{k-1})}\sigma_{\mathbb{X}\cup\mathbb{Y}}(V_k)(\tilde{f}_{|w|})s(\tilde{v}_k)\\
= & \sigma_{\mathbb{X}\cup\mathbb{Y}}(V_1) & \varphi_2(\sigma_{\mathbb{X}\cup\mathbb{Y}})(V_2) & \cdots & \varphi_k(\sigma_{\mathbb{X}\cup\mathbb{Y}})(V_k)(\tilde{f}_{|w|})s(\tau(w))\\
= & \sigma(\varphi_0,V_1) & \sigma(\varphi_2,V_2) & \cdots & \sigma(\varphi_k,V_k)(\tilde{f}_{|w|})s(\tau(w)).
\end{array}\tag{7.5}$$

Then for $r_i\in\mathcal{R}$ of the form $r_i=v_{i,1}\cdots v_{i,|r_i|}$, where for a letter $v_{i,j}$, denote $\zeta(\varphi_0(\rho(v_{i,j})))$ as $(\varphi_0,V_{i,j})$ for $V_{i,j}\in\mathbb{X}\cup\mathbb{Y}$, and it follows by Eq. (7.5) that

$$\begin{array}{rcccl}
\kappa(r_i)= & \kappa(v_{i,1}) & \kappa(v_{i,1}) & \cdots & \kappa(v_{i,|r_i|})\\
= & \sigma(\varphi_0,V_{i,1}) & \sigma(\varphi_{i,2},V_{i,2}) & \cdots & \sigma(\varphi_{i,|r_i|},V_{i,|r_i|})(\tilde{f}_{|r_i|})s(\tau(r_i))\\
= & \sigma(u_i) & & & \\
= & 1_N. & & &
\end{array}$$

Thus, by Lemma 2.28 κ is a homomorphism.

Again using Eq. (7.5), noting additionally now that κ is a homomorphism, then we have

$$\sigma(\varphi_0,V_1)\sigma(\varphi_2,V_2)\cdots\sigma(\varphi_k,V_k)\tilde{f}(s(\tau(v_1),\ldots,s(\tau(v_k)))=n\in N$$

so $\kappa(w)=ns(\tau(w))$, and it follows that condition (b) is satisfied.

Since $\langle\sigma(\varphi_0,Y_1),\ldots,\sigma(\varphi_0,Y_\ell)\rangle=N$, for all $n\in N$, there exists $w\in(\varphi_0\times\mathbb{Y})^*$ such that $\sigma(w)=n$.

Then there exists $\Gamma^{-1}(\zeta^{-1}(w))\in(\mathcal{Y}\cup\mathcal{Y}^{-1})^*$, then

$$\begin{aligned}
\kappa(\Gamma^{-1}(\zeta^{-1}(w)))&=\sigma(\zeta(\Gamma(\Gamma^{-1}(\zeta^{-1}(w))s(\tau(\Gamma^{-1}(\zeta^{-1}(w)))\\
&=\sigma(w)s(\tau(\Gamma^{-1}(\zeta^{-1}(w))))\\
&=\sigma(w)s(1_Q)\\
&=ns(1_Q).
\end{aligned}$$

This satisfies condition (c') of Remark 4.8, thereby proving the existence of an epimorphism from G to H. □

7.3 Equation to Integer Matrices

We now provide a way to construct a list of matrices from a system of twisted equations over a free abelian group, and vice versa.

We begin by some introducing some notation and standard results for general linear groups over integers. Recall that a *torsion element* is an element of finite order.

Notation. Let $\mathrm{GL}_{\mathsf{Fin}}(d,\mathbb{Z})$ denote the subset of $\mathrm{GL}(d,\mathbb{Z})$ consisting only of torsion elements.

Lemma 7.12. *Let $N \cong \mathbb{Z}^d$ be a free abelian group of rank d. Then,* $\mathrm{Aut}(N)$ *is isomorphic to* $\mathrm{GL}(d,\mathbb{Z})$.

Proof. Let $X = \{x_1, \dots, x_d\}$ be a minimal generating set for for $\mathbb{Z}^d$, then for all $\varphi \in \mathrm{Aut}(\mathbb{Z}^d)$, the map φ cts on each generator x_i by sending it to an integer linear combination of the generators

$$\varphi(x_i) = \sum_{j=1}^{d} m_{i,j} x_j.$$

This map defines an integer matrix $M \in \mathbb{Z}^{d\times d}$, where the (i,j)-th entry $m_{i,j}$ is the coefficient of x_j in $\varphi(x_i)$.

We define a map

$$\tilde{\phi}\colon \mathrm{Aut}(\mathbb{Z}^d) \to \mathrm{GL}(d,\mathbb{Z})$$

by sending each automorphism φ to its associated matrix M under this construction, and so

$$M = \begin{pmatrix} m_{1,1} & \cdots & m_{1,d} \\ \vdots & \ddots & \vdots \\ m_{d,1} & \cdots & m_{d,d} \end{pmatrix}.$$

This is a well defined as φ is an automorphism, so $\{\varphi(x_1), \dots, \varphi(x_d)\}$ is a minimal generating set, implying $\det(\tilde{\phi}(\varphi)) = \pm 1$.

For any $M \in \mathrm{GL}(d,\mathbb{Z})$, define a map μ by

$$\mu(x_i) \;=\; \sum_{j=1}^{d} m_{i,j}\, x_j.$$

Since $\det(M) = \pm 1$, then μ is a bijective homomorphism, and so $\mu \in \mathrm{Aut}(\mathbb{Z}^d)$. Thus, set $\mu = \varphi$ and for all $M \in \mathrm{GL}(d,\mathbb{Z})$ there exists $\varphi \in \mathrm{Aut}(\mathbb{Z}^d)$, and $\tilde{\phi}$ is surjective.

As $\tilde{\phi}$ is injective by construction, it follows that $\tilde{\phi}$ is an isomorphism. □

Definition 7.13. Let $N = \langle x_1, \dots, x_d \rangle$ be a free abelian group of rank d and $\varphi \in \mathrm{Aut}(N)$ be automorphism defined by the map

$$\varphi\colon x_i \mapsto x_1^{c_{1,i}} \cdots x_d^{c_{d,i}}.$$

The *natural isomorphism* $\tilde{\phi}\colon \mathrm{Aut}(N) \to \mathrm{GL}(d,\mathbb{Z})$ is defined by the map

$$\tilde{\phi}\colon \varphi \mapsto \begin{pmatrix} c_{1,1} & \cdots & c_{1,d} \\ \vdots & \ddots & \vdots \\ c_{d,1} & \cdots & c_{d,d} \end{pmatrix}$$

as in the above proof.

Example 7.14. Let $N = \langle x_1, x_2 \rangle$ be a free abelian group of rank 2, and $\varphi \in \mathrm{Aut}(N)$ be described by

$$\varphi\colon \begin{cases} x_1 \mapsto x_1^2 x_2^5 \\ x_2 \mapsto x_1 x_2^3. \end{cases}$$

Then natural isomorphism produces the following matrix $M \in \mathrm{GL}(2, \mathbb{Z})$

$$\tilde{\phi}(\varphi) = M = \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix}$$

and

$$\begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}.$$

We now extend Definition 4.11 on the commuted normal form of a system of equations to twisted system of equations.

Definition 7.15 (Commuting twisted equations when N is abelian)**.** Let N be an abelian group, u be an twisted equation with variables $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$ and a list of automorphisms $\Phi = \{\varphi_0, \ldots, \varphi_n\}$, of the form $u = v\mathfrak{c}$ where $v \in (\Phi \times \mathbb{X})^*$ and $\mathfrak{c} \in N$ is a single constant. Define the *commuted normal form* of u as the word

$$\begin{aligned} \mathsf{CNF}(u) = \quad & (\varphi_0, X_1)^{\alpha_{0,1}} \cdots (\varphi_0, X_n)^{\alpha_{0,n}} \\ & (\varphi_1, X_1)^{\alpha_{1,1}} \cdots (\varphi_1, X_n)^{\alpha_{1,n}} \\ & \quad \vdots \\ & (\varphi_k, X_1)^{\alpha_{k,1}} \cdots (\varphi_k, X_n)^{\alpha_{k,n}} \mathfrak{c} \end{aligned}$$

where $\alpha_{i,j} = |u|_{(\varphi_i, X_j)} - |u|_{(\varphi_i, X_j^{-1})}$ for $i \in [0, k], j \in [1, n]$.

Similarly to Lemma 4.12, the following lemma is immediate from the commuting property of abelian groups.

Lemma 7.16. *Let N be an abelian group, and let $(u_i)_{i \in [1,m]}$ be a system of twisted equations in N, where each u_i consists of variables $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$, automorphisms $\Phi = \{\varphi_0, \ldots, \varphi_k\}$ and a single constant. Then $\sigma\colon (\Phi \times \mathbb{X}) \to N$ is a solution to $(u_i)_{i \in [1,m]}$ if and only if σ is a solution to $(\mathsf{CNF}(u_i))_{i \in [1,m]}$.*

We now provide a method to convert a system of twisted equations over an abelian group N into a list of integer matrix elements and vice versa. The integer matrix elements correspond to the inputs for the matrix problems which will be defined after. This is a generalisation of Definitions 4.14 and 4.15

Definition 7.17 (System of equations to matrix system)**.** Let

- $d, t, \ell, m, k \in \mathbb{Z}$
- $N = \langle x_1, \ldots, x_d \rangle \in \mathsf{FreeAb}$
- $\Phi = \{\varphi_0, \varphi_1, \ldots, \varphi_k\}$ a list of finite order automorphisms on N, where φ_0 is the trivial automorphism
- $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$
- $v_i \in (\Phi \times (\mathbb{X} \cup \mathbb{Y}))^*$ be a twisted equation without constants for $i \in [1, m]$
- $\mathfrak{c}_i \in N$ with $\mathfrak{c}_i = x_1^{b_{i,1}} \cdots x_d^{b_{i,d}}$ for $i \in [1, m]$
- $(u_i)_{[1,m]}$ be a system of twisted equations in N, where each equation is of the form $u_i = v_i \mathfrak{c}_i$.

Let $n = t + \ell$, for each $i \in [1, m]$ and $p \in [0, k]$, the commuted normal form (Definition 7.15)

$$\begin{aligned}\mathsf{CNF}(u_i) = \quad & (\varphi_0, X_1)^{c_{i,1,0}} \cdots (\varphi_0, X_t)^{c_{i,t,0}} (\varphi_0, Y_1)^{c_{i,t+1,0}} \cdots (\varphi_0, Y_\ell)^{c_{i,n,0}} \\ & (\varphi_1, X_1)^{c_{i,1,1}} \cdots (\varphi_1, X_t)^{c_{i,t,1}} (\varphi_1, Y_1)^{c_{i,t+1,1}} \cdots (\varphi_1, Y_\ell)^{c_{i,n,1}} \\ & \quad \vdots \\ & (\varphi_k, X_1)^{c_{i,1,k}} \cdots (\varphi_k, X_t)^{c_{i,t,k}} (\varphi_k, Y_1)^{c_{i,t+1,k}} \cdots (\varphi_k, Y_\ell)^{c_{i,n,k}} \mathfrak{c}_i\end{aligned}$$

where

$$c_{(i,j,p)} = |v_i|_{(\varphi_p, X_j)} - |v_i|_{(\varphi_p, X_j^{-1})} \quad \text{for} \quad j \in [1, t]$$

and

$$c_{(i,j,p)} = |v_i|_{(\varphi_p, Y_j)} - |v_i|_{(\varphi_p, Y_j^{-1})} \quad \text{for} \quad j \in [t+1, t+\ell]$$

Define $\mathsf{TwistedEqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi)$ to be the tuple

$$(\{A_0, \ldots, A_k\}, \{M_0, \ldots, M_k\}, B, \ell)$$

with $A_i \in \mathbb{Z}^{m \times (t+\ell)}$, $M_i \in \mathrm{GL}_{\mathsf{Fin}}(d, \mathbb{Z})$, and $B \in \mathbb{Z}^{m \times d}$, where M_i is attained using the natural isomorphism $\tilde{\phi}\colon \mathrm{Aut}(N) \to \mathrm{GL}(d, \mathbb{Z})$ as per Definition 7.13 for $i \in [0, k]$, so we have

$$M_i = \tilde{\phi}(\varphi_i)$$

and

$$A_i = \begin{pmatrix} c_{1,1,i} & \cdots & c_{1,n,i} \\ \vdots & \ddots & \vdots \\ c_{m,1,i} & \cdots & c_{m,n,i} \end{pmatrix}, \quad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,d} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,d} \end{pmatrix}.$$

Definition 7.18 (Matrices to system of equations)**.** Given $\ell \in \mathbb{Z}$, matrices $A_0, \ldots, A_k \in \mathbb{Z}^{m \times n}$, $M_0 = I \in \mathbb{Z}^{d \times d}$, $M_1 \ldots, M_k \in \mathrm{GL}_{\mathsf{Fin}}(d, \mathbb{Z})$ and $B \in \mathbb{Z}^{m \times d}$, where

$$A_i = \begin{pmatrix} a_{1,1,i} & \cdots & a_{1,n,i} \\ \vdots & \ddots & \vdots \\ a_{m,1,i} & \cdots & a_{m,n,i} \end{pmatrix}, \quad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,d} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,d} \end{pmatrix}$$

define $\mathsf{GLMatEqn}(\{A_0, \ldots, A_k\}, \{M_0, \ldots, M_k\}, B, \ell)$ to be the tuple

$$(d, n - \ell, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi)$$

where $(u_i)_{[1,m]}$ is a system of twisted equations with variables

$$\{X_1, X_1^{-1}, \ldots, X_{n-\ell}, X_{n-\ell}^{-1}, Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$$

a list of finite order automorphisms constructed via the natural isomorphism (Definition 7.13)

$$\Phi = \{\tilde{\phi}^{-1}(M_0), \ldots, \tilde{\phi}^{-1}(M_k)\} = \{\varphi_0, \ldots, \varphi_k\}$$

and so φ_0 is the trivial automorphism over a free abelian group $N = \langle x_1, \ldots, x_d \rangle$ of rank d, where each u_i is of the form

$$u_i = v_i \mathfrak{c}_i,$$

where $t = n - \ell$, and has the form

$$\begin{aligned} v_i = \quad & (\varphi_0, X_1)^{a_{i,1,0}} \cdots (\varphi_0, X_t)^{a_{i,t,0}} (\varphi_0, Y_1)^{a_{i,t+1,0}} \cdots (\varphi_0, Y_\ell)^{a_{i,n,0}} \\ & (\varphi_1, X_1)^{a_{i,1,1}} \cdots (\varphi_1, X_t)^{a_{i,t,1}} (\varphi_1, Y_1)^{a_{i,t+1,1}} \cdots (\varphi_1, Y_\ell)^{a_{i,n,1}} \\ & \quad \vdots \\ & (\varphi_k, X_1)^{a_{i,1,k}} \cdots (\varphi_k, X_t)^{a_{i,t,k}} (\varphi_k, Y_1)^{a_{i,t+1,k}} \cdots (\varphi_k, Y_\ell)^{a_{i,n,k}} \end{aligned}$$

and

$$\mathfrak{c}_i = x_1^{b_{i,1}} \cdots x_d^{b_{i,d}} \in N.$$

The following is immediate from the definitions.

Lemma 7.19. *Let $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$ and $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$. Let H be an N by Q extension where $N \cong \mathbb{Z}^d$ and Q is finite, with extension data (θ, f_s). The following computations can be achieved in polynomial time:*

1. *On input finite sets $\mathcal{X}, \mathcal{Y}, \mathcal{R} \subseteq (\mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1})^*$, compute $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$.*
2. *Let $\Phi = \theta \circ \tau$. On input $d, t, \ell \in \mathbb{Z}$, a system of equations $(u_i)_{[1,m]}$ where each $u_i = v_i \mathfrak{c}_i$, and $v_i \in (\Phi \times (\mathbb{X} \cup \mathbb{Y}))^*$ is a twisted equation without constants, and $\mathfrak{c}_i = x_1^{b_{(i,1)}} \cdots x_d^{b_{(i,d)}}$, compute $\mathsf{TwistedEqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi)$.*
3. *On input $A_0, \ldots, A_k \in \mathbb{Z}^{m \times n}$, $M_0, \ldots, M_k \in \mathrm{GL}_{\mathsf{Fin}}(d, \mathbb{Z})$ where $M_0 = I \in \mathbb{Z}^{d \times d}$, $B \in \mathbb{Z}^{m \times d}$, and $\ell \in \mathbb{Z}$, compute $\mathsf{GLMatEqn}(\{A_0, \ldots, A_k\}, \{M_0, \ldots, M_k\}, B, \ell)$.*

Lemma 7.20. *Let*

- *$d, t, \ell, m, k \in \mathbb{Z}$*
- *$N = \langle x_1, \ldots, x_d \rangle \in \mathsf{FreeAb}$*
- *$\{\varphi_0, \varphi_1, \ldots, \varphi_k\} = \Phi \leq \mathrm{Aut}(N)$ is a list of finite order automorphisms on N, where φ_0 is the trivial automorphism and Φ is a subgroup*
- *$\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$*
- *$v_i \in (\Phi \times (\mathbb{X} \cup \mathbb{Y}))^*$ be a twisted equation without constants for $i \in [1, m]$*
- *$\mathfrak{c}_i \in N$ with $\mathfrak{c}_i = x_1^{b_{i,1}} \cdots x_d^{b_{i,d}}$ for $i \in [1, m]$*
- *$(u_i)_{[1,m]}$ be a system of twisted equations in N, where each equation is of the form $u_i = v_i \mathfrak{c}_i$.*

The following are equivalent

- $\mathsf{TwistedEquationSubspan}$ *returns 'Yes' on input N and a system of twisted equations $(u_i)_{[1,m]}$,*
- $\mathsf{MatrixSubspanC}$ *returns 'Yes' on input*

$$(\{A_0, \ldots, A_k\}, \{M_0, \ldots, M_k\}, B, \ell) = \mathsf{TwistedEqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi).$$

Proof. Let

$$\begin{aligned} \mathsf{CNF}(u_i) = \quad & (\varphi_0, X_1)^{a_{i,1,0}} \cdots (\varphi_0, X_t)^{a_{i,t,0}} (\varphi_0, Y_1)^{a_{i,t+1,0}} \cdots (\varphi_0, Y_\ell)^{a_{i,n,0}} \\ & (\varphi_1, X_1)^{a_{i,1,1}} \cdots (\varphi_1, X_t)^{a_{i,t,1}} (\varphi_1, Y_1)^{a_{i,t+1,1}} \cdots (\varphi_1, Y_\ell)^{a_{i,n,1}} \\ & \quad \vdots \\ & (\varphi_k, X_1)^{a_{i,1,k}} \cdots (\varphi_k, X_t)^{a_{i,t,k}} (\varphi_k, Y_1)^{a_{i,t+1,k}} \cdots (\varphi_k, Y_\ell)^{a_{i,n,k}} \ \mathfrak{c}_i \end{aligned} \tag{7.6}$$

for $i \in [1, m]$ where

$$\begin{aligned} a_{(i,j,p)} &= |u_i|_{(\varphi_p, X_j)} - |u_i|_{(\varphi_p, X_j^{-1})} \quad \text{for} \quad j \in [1, t], p \in [0, k] \\ a_{(i,j,p)} &= |u_i|_{(\varphi_p, Y_j)} - |u_i|_{(\varphi_p, Y_j^{-1})} \quad \text{for} \quad j \in [t+1, n], p \in [0, k]. \end{aligned}$$

Let $\tilde{\phi}\colon N \to \mathrm{GL}(d,\mathbb{Z})$ be defined as in Definition 7.13 and so the outputs for $\mathsf{TwistedEqnMat}(d,t,\ell,(u_i)_{[1,m]},(\mathfrak{c}_i)_{[1,m]},\Phi)$ are

$$M_p = \tilde{\phi}(\varphi_p), \quad A_p = \begin{pmatrix} a_{1,1,p} & \cdots & a_{1,n,p} \\ \vdots & \ddots & \vdots \\ a_{m,1,p} & \cdots & a_{m,n,p} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,d} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,d} \end{pmatrix}$$

for $p \in [0,k]$.

Assume $\mathsf{TwistedEquationSubspan}$ returns 'Yes' on input N and $(u_i)_{[1,m]}$. Then there exists a solution $\sigma\colon (\Phi \times (\mathbb{X} \cup \mathbb{Y})) \to N$ which we may write as

$$\sigma_{\mathbb{X}\cup\mathbb{Y}}\colon \begin{cases} X_j \mapsto x_1^{c_{j,1}} \cdots x_d^{c_{j,d}}, \quad X_j^{-1} \mapsto (x_1^{c_{j,1}} \cdots x_d^{c_{j,d}})^{-1} & j \in [1,t] \\ Y_j \mapsto x_1^{c_{t+j,1}} \cdots x_d^{c_{t+j,d}}, \quad Y_j^{-1} \mapsto (x_1^{c_{t+j,1}} \cdots x_d^{c_{t+j,d}})^{-1} & j \in [1,\ell] \end{cases}$$

for some list of $c_{(i,p)} \in \mathbb{Z}$, such that $\langle \sigma(\varphi_0, Y_1), \ldots, \sigma(\varphi_0, Y_\ell) \rangle = N$. By Lemma 7.16, σ is also a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$.

Let

$$V = \begin{pmatrix} c_{1,1} & \cdots & c_{1,d} \\ \vdots & \ddots & \vdots \\ c_{t+\ell,1} & \cdots & c_{t+\ell,d} \end{pmatrix} \in \mathbb{Z}^{(t+\ell)\times d}.$$

Note that $t+\ell = n$, for $i \in [1,d]$, let $v_i \in \mathbb{Z}^{t+\ell}$ denote the i-th column of V, and for $i \in [1,\ell]$ let μ_i denote the i-th column of $(V_\ell)^T$.

Since σ is a solution, we can write in place of the each variable in Eq. (7.6) as

$$\begin{aligned} \sigma(\mathsf{CNF}(u_i)) &= \sigma(\varphi_0, X_1)^{a_{i,1,0}} \cdots \sigma(\varphi_0, X_t)^{a_{i,t,0}} \sigma(\varphi_0, Y_1)^{a_{i,t+1,0}} \cdots \sigma(\varphi_0, Y_\ell)^{a_{i,n,0}} \\ &\quad \sigma(\varphi_1, X_1)^{a_{i,1,1}} \cdots \sigma(\varphi_1, X_t)^{a_{i,t,1}} \sigma(\varphi_1, Y_1)^{a_{i,t+1,1}} \cdots \sigma(\varphi_1, Y_\ell)^{a_{i,n,1}} \\ &\quad \vdots \\ &\quad \sigma(\varphi_k, X_1)^{a_{i,1,k}} \cdots \sigma(\varphi_k, X_t)^{a_{i,t,k}} \sigma(\varphi_k, Y_1)^{a_{i,t+1,k}} \cdots \sigma(\varphi_k, Y_\ell)^{a_{i,n,k}} \, \mathfrak{c}_i \\ &= \varphi_0(x_1^{c_{1,1}} \cdots x_d^{c_{1,d}})^{a_{i,1,0}} \cdots \quad \cdots \quad \cdots \varphi_0(x_1^{c_{t+\ell,1}} \cdots x_d^{c_{t+\ell,d}})^{a_{i,n,0}} \\ &\quad \varphi_1(x_1^{c_{1,1}} \cdots x_d^{c_{1,d}})^{a_{i,1,1}} \cdots \quad \cdots \quad \cdots \varphi_1(x_1^{c_{t+\ell,1}} \cdots x_d^{c_{t+\ell,d}})^{a_{i,n,1}} \\ &\quad \vdots \\ &\quad \varphi_k(x_1^{c_{1,1}} \cdots x_d^{c_{1,d}})^{a_{i,1,k}} \cdots \quad \cdots \quad \cdots \varphi_k(x_1^{c_{t+\ell,1}} \cdots x_d^{c_{t+\ell,d}})^{a_{i,n,k}} \, \mathfrak{c}_i \end{aligned}$$

For $\varphi_p \in \mathrm{Aut}(N)$, we can describe this map by

$$\varphi_p\colon x_1^{c_{j,1}} \cdots x_d^{c_{j,d}} \mapsto x_1^{c'_{j,1}} \cdots x_d^{c'_{j,d}}$$

for $j \in [1, t+\ell]$, and some $c'_{j,1}, \ldots, c'_{j,d} \in \mathbb{Z}$. Let $\tilde{\varphi}_p\colon \mathbb{Z} \to \mathbb{Z}$ describe this map, that is

$$\varphi_p\colon x_1^{c_{j,1}} \cdots x_d^{c_{j,d}} \mapsto x_1^{\tilde{\varphi}_p(c_{j,1})} \cdots x_d^{\tilde{\varphi}_p(c_{j,d})}$$

then, continuing the calculations above, we have

$$\begin{aligned} \sigma(\mathsf{CNF}(u_i)) &= \left(x_1^{\tilde{\varphi}_0(c_{1,1})} \cdots x_d^{\tilde{\varphi}_0(c_{1,d})}\right)^{a_{i,1,0}} \cdots \quad \cdots \quad \cdots \left(x_1^{\tilde{\varphi}_0(c_{t+\ell,1})} \cdots x_d^{\tilde{\varphi}_0(c_{t+\ell,d})}\right)^{a_{i,n,0}} \\ &\quad \left(x_1^{\tilde{\varphi}_1(c_{1,1})} \cdots x_d^{\tilde{\varphi}_1(c_{1,d})}\right)^{a_{i,1,1}} \cdots \quad \cdots \quad \cdots \left(x_1^{\tilde{\varphi}_1(c_{t+\ell,1})} \cdots x_d^{\tilde{\varphi}_1(c_{t+\ell,d})}\right)^{a_{i,n,1}} \\ &\quad \vdots \\ &\quad \left(x_1^{\tilde{\varphi}_k(c_{1,1})} \cdots x_d^{\tilde{\varphi}_k(c_{1,d})}\right)^{a_{i,1,k}} \cdots \quad \cdots \quad \cdots \left(x_1^{\tilde{\varphi}_k(c_{t+\ell,1})} \cdots x_d^{\tilde{\varphi}_k(c_{t+\ell,d})}\right)^{a_{i,n,k}} \mathfrak{c}_i. \end{aligned}$$

Recall that $n = t + \ell$, from the above equation by collating terms for each x_i, $i \in [1, d]$ across each row which is affected by φ_p, $p \in [0, k]$ we get

$$\begin{array}{rl} = & \begin{array}{cccccc} x_1^{\sum_{j=1}^{n} c_{j,1} a_{i,j,0}} & \cdots & \cdots & \cdots & x_d^{\sum_{j=1}^{n} c_{j,d} a_{i,j,0}} & \\ x_1^{\sum_{j=1}^{n} \tilde{\varphi}_1(c_{j,1}) a_{i,j,1}} & \cdots & \cdots & \cdots & x_d^{\sum_{j=1}^{n} \tilde{\varphi}_1(c_{j,d}) a_{i,j,1}} & \\ & & \vdots & & & \\ x_1^{\sum_{j=1}^{n} \tilde{\varphi}_k(c_{j,1}) a_{i,j,k}} & \cdots & \cdots & \cdots & x_d^{\sum_{j=1}^{n} \tilde{\varphi}_k(c_{j,d}) a_{i,j,k}} & x_1^{b_{i,1}} \cdots x_d^{b_{i,d}} \end{array} = 1_N \end{array} \tag{7.7}$$

which implies

$$\sum_{j=1}^{n} c_{j,s} a_{i,j,0} + \sum_{j=1}^{n} \tilde{\varphi}_1(c_{j,s}) a_{i,j,0} + \cdots + \sum_{j=1}^{n} \tilde{\varphi}_k(c_{j,s}) a_{i,j,k} + b_{i,s} = 0 \tag{7.8}$$

for $i, \in [1, m]$, $s \in [1, d]$.

We now make an observation on the matrices as output by $\mathsf{TwistedEqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi)$.

Note that $M_0 = I$, so $(M_0 V^T)^T$, so we begin with $A_0((M_0 V^T)^T) = A_0 V$

$$\begin{aligned} A_0 V &= \begin{pmatrix} a_{1,1,0} & \cdots & a_{1,t,0} & a_{1,t+1,0} & \cdots & a_{1,t+\ell,0} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1,0} & \cdots & a_{m,t,0} & a_{m,t+1,0} & \cdots & a_{m,t+\ell,0} \end{pmatrix} \begin{pmatrix} c_{1,1} & \cdots & c_{1,d} \\ \vdots & \ddots & \vdots \\ c_{t+\ell,1} & \cdots & c_{t+\ell,d} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^{t} c_{j,1}\, a_{1,j,p} + \sum_{j=1}^{\ell} c_{t+j,1}\, a_{1,t+j,p} & \cdots & \sum_{j=1}^{t} c_{j,d}\, a_{1,j,p} + \sum_{j=1}^{\ell} c_{t+j,d}\, a_{1,t+j,p} \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{t} c_{j,1}\, a_{m,j,p} + \sum_{j=1}^{\ell} c_{t+j,1}\, a_{m,t+j,p} & \cdots & \sum_{j=1}^{t} c_{j,d}\, a_{m,j,p} + \sum_{j=1}^{\ell} c_{t+j,d}\, a_{m,t+j,p} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^{n} c_{j,1}\, a_{1,j,p} & \cdots & \sum_{j=1}^{n} c_{j,d}\, a_{1,j,p} \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} c_{j,1}\, a_{m,j,p} & \cdots & \sum_{j=1}^{n} c_{j,d}\, a_{m,j,p} \end{pmatrix}. \end{aligned} \tag{7.9}$$

Recall that $M_p = \tilde{\phi}(\varphi_p)$ and $\varphi_p(x_1^{c_{i,1}} \cdots x_d^{c_{i,d}}) = x_1^{\tilde{\varphi}_p(c_{i,1})} \cdots x_d^{\tilde{\varphi}_p(c_{i,d})}$, it follows that

$$M_p \begin{pmatrix} c_{(1,1)} & \cdots & c_{(n,1)} \\ \vdots & \ddots & \vdots \\ c_{(1,d)} & \cdots & c_{(n,d)} \end{pmatrix} = \begin{pmatrix} \tilde{\varphi}_p(c_{1,1}) & \cdots & \tilde{\varphi}_p(c_{1,d}) \\ \vdots & \ddots & \vdots \\ \tilde{\varphi}_p(c_{t+\ell,1}) & \cdots & \tilde{\varphi}_p(c_{t+\ell,d}) \end{pmatrix}.$$

We now calculate $A_p((M_pV^T)^T)$ for $p \in [1,k]$

$$
\begin{aligned}
&A_p(M_pV^T)^T \\
&= \begin{pmatrix} a_{1,1,p} & \cdots & a_{1,t,p} & a_{1,t+1,p} & \cdots & a_{1,t+\ell,p} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1,p} & \cdots & a_{m,t,p} & a_{m,t+1,p} & \cdots & a_{m,t+\ell,p} \end{pmatrix} (M_p \begin{pmatrix} c_{1,1} & \cdots & c_{t+\ell,1} \\ \vdots & \ddots & \vdots \\ c_{1,d} & \cdots & c_{t+\ell,d} \end{pmatrix})^T \\
&= \begin{pmatrix} a_{1,1,0} & \cdots & a_{1,t,0} & a_{1,t+1,0} & \cdots & a_{1,t+\ell,0} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1,0} & \cdots & a_{m,t,0} & a_{m,t+1,0} & \cdots & a_{m,t+\ell,0} \end{pmatrix} \begin{pmatrix} \tilde{\varphi}_p(c_{1,1}) & \cdots & \tilde{\varphi}_p(c_{1,d}) \\ \vdots & \ddots & \vdots \\ \tilde{\varphi}_p(c_{t+\ell,1}) & \cdots & \tilde{\varphi}_p(c_{t+\ell,d}) \end{pmatrix} \\
&= \begin{pmatrix} \sum_{j=1}^{n} \tilde{\varphi}_p(c_{j,1}) a_{1,j,p} & \cdots & \sum_{j=1}^{n} \tilde{\varphi}_p(c_{j,d}) a_{1,j,p} \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} \tilde{\varphi}_p(c_{j,1}) a_{m,j,p} & \cdots & \sum_{j=1}^{n} \tilde{\varphi}_p(c_{j,d}) a_{m,j,p} \end{pmatrix}.
\end{aligned} \tag{7.10}
$$

Using Eq. (7.8), we note each cell is equal is the i-th row and s-th column of when using Eqs. (7.9) and (7.10)

$$A_0V + A_1(M_1V^T)^T + \cdots + A_k(M_kV^T)^T + B$$

it follows that

$$A_0V + A_1(M_1V^T)^T + \cdots + A_k(M_kV^T)^T + B = 0.$$

Thus, we have shown there exists $V \in \mathbb{Z}^{n\times d}$ such that $\sum_{i=0}^{k} A_i((M_iV^T)^T) + B = 0$. Equivalently,

$$\begin{gathered} \sigma\colon (\Phi \times (\mathbb{X} \cup \mathbb{Y})) \to N \quad \text{is a solution to} \quad (\mathsf{CNF}(u_i))_{[1,m]} \\ \text{and} \quad \langle \sigma(\varphi_0, Y_1), \ldots, \sigma(\varphi_0, Y_\ell) \rangle = N \end{gathered}$$

if and only if

$$\begin{gathered} \textstyle\sum_{i=0}^{k} A_i(M_iV^T)^T + B = 0 \\ \text{and} \quad \langle \sigma(\varphi_0, Y_1), \ldots, \sigma(\varphi_0, Y_\ell) \rangle = N. \end{gathered}$$

Let be the natural isomorphism $\phi\colon N \to \mathbb{Z}^d$ be as defined in Definition 2.42. For each $i \in [1,\ell]$, we set $\mu_i = \phi(\sigma(\varphi_0, Y_i))$ and so

$$\begin{aligned} \phi(\sigma(\varphi_0, Y_i)) &= \phi(x_1^{c_{(t+i,1)}} \cdots x_d^{c_{(t+i,d)}}) \\ &= c_{(t+i,1)}e_1 + \cdots + c_{(t+i,d)}e_d = \mu_i. \end{aligned} \tag{7.11}$$

Then the previous statement is true if and only if

$$\begin{gathered} \textstyle\sum_{i=0}^{k} A_i(M_iV^T)^T + B = 0 \\ \text{and} \\ \text{for all } h \in N, \text{ there exists } w \in (\varphi_0 \times \mathbb{Y})^* \quad \text{such that} \quad \sigma(w) = h \end{gathered}$$

if and only if

$$\begin{gathered} \textstyle\sum_{i=0}^{k} A_i(M_iV^T)^T + B = 0 \\ \text{and} \\ \text{for all } z \in \mathbb{Z}^d, \text{ there exists } w \in (\varphi_0 \times \mathbb{Y})^* \quad \text{such that} \quad \phi(\sigma(w)) = z. \end{gathered}$$

Write $\mathsf{CNF}(w) = (\varphi_0, Y_1)^{b_1} \cdots (\varphi_0, Y_\ell)^{b_\ell}$, and so

$$z = \phi(\sigma(w)) = \phi((\varphi_0, Y_1)^{b_1} \cdots (\varphi_0, Y_\ell)^{b_\ell}) = b_1\mu_1 + \cdots + b_\ell\mu_\ell. \quad \text{by Eq. (7.11)}$$

Then the previous statement is true if and only if

$$\sum_{i=0}^{k} A_i(M_iV^T)^T + B = 0$$
$$\text{and}$$
$$\operatorname{span}(\mu_1, \ldots, \mu_\ell) = \operatorname{span}((V|_\ell)^T) = \mathbb{Z}^d.$$

which is true if and only if $\mathsf{MatrixSubspanC}$ returns 'Yes'. □

Proposition 7.21. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{VAb})$ *is in* $\mathsf{NP}^{\mathsf{MatrixSubspanC}}$

Proof. Let $G \in \mathsf{FinPres}$ be given by a finite presentation $\langle \mathcal{G} \mid \mathcal{R} \rangle$ and $H \in \mathsf{VAb}$, given by an integer $d \in \mathbb{N}$ encoding $N \in \mathsf{FreeAb}$ of rank d, a multiplication table for $Q \in \mathsf{Fin}$, and extension data (θ, f_s).

By Lemma 7.11, we may verify the existence of an epimorphism from G to H by verifying that

(i) there exists an epimorphism $\tau\colon G \to H$
(ii) for some (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G, $\mathsf{TwistedEquationSubspan}$ returns 'Yes' on input N and $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$.

The following procedure solves our problem. On input as above

1. Guess a set map $\tau\colon \mathcal{G} \to Q$ and verify it extends to an epimorphism $\tau\colon G \to Q$. If no such map exists, output 'No'.
2. Construct a (Q, τ)-presentation $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$.
3. Construct the system of equations without constants $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$, denoted $(u_i)_{[1,m]}$ with constants $(\mathfrak{c}_i)_{[1,m]}$.
4. Set $\Phi = \theta(Q)$, return the solution to $\mathsf{MatrixSubspanC}$ on input

$$(\{A_0, \ldots, A_k\}, \{M_0, \ldots, M_k\}, B, \ell) = \mathsf{TwistedEqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi).$$

The correctness of this algorithm follows from Lemmas 7.11 and 7.20. The time complexity is as follows

1. Verifying in polynomial time that τ is an epimorphism follows from Lemma 4.1.
2. Constructing a (Q, τ)-presentation is in P by Lemma 4.5
3. constructing $\mathsf{PresEqnC}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \theta, f_s)$ is in P by Lemma 7.19 and Item 1.
4. Constructing $\mathsf{TwistedEqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi)$ is in P by Lemma 7.19 and Item 2.
5. $\mathsf{MatrixSubspanC}$ is solved in by an oracle.

The time complexity is as follows

1. Step (1) is in NP by Lemma 4.1; this is the only non-deterministic step of our algorithm.
2. We can construct a (Q, τ)-presentation in P by Lemma 4.5, and $\mathcal{I}_\mathcal{X}$ is immediate.
3. Constructing $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_1)$ in P is clear from its definition.
4. Constructing $\mathsf{EqnMat}(d, (u_i)_{[1,m]}, (1_N)_{[1,m]})$ is in P by Lemma 4.16.

Thus, our algorithm is in NP when using an oracle for $\mathsf{MatrixSubspanC}$. □

Proof of Theorem E. The result follows directly from Proposition 7.21. □

7.4 Future Directions and Open Questions

In this section, we discuss several potential directions for further research arising from the results and techniques presented in this thesis.

A natural starting point for investigating whether $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{VAb})$ is decidable is to examine a related problem. We propose a potentially easier problem, $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Ab} \rtimes_\theta \mathsf{Fin})$, as an intermediary point of investigation. This motivates the following matrix problem, and we assert the claim following it without proof.

Problem:	MatrixSubspanD
Input:	A tuple $(\{A_0, \dots, A_k\}, \{M_0, \dots, M_k\}, \ell)$ where $A_i \in \mathbb{Z}^{m \times n}$, $M_0 = I \in \mathbb{Z}^{d \times d}$, and $M_i \in \mathrm{GL}_{\mathsf{Fin}}(d, \mathbb{Z})$ for $i \in [1, k]$, $d, \ell \in \mathbb{N}$ with $\ell \in [0, n-1]$.
Question:	Do there exist integer n-vectors $v_1, \dots, v_d$ and the matrix $V = \begin{pmatrix} v_1 & \cdots & v_d \end{pmatrix} \in \mathbb{Z}^{n \times d}$ such that $\sum_{i=0}^{k} A_i((M_i V^T)^T) = 0$, and $\mathrm{span}((V\|_\ell)^T) = \mathbb{Z}^d$?

Claim 7.22. *If* MatrixSubspanD *is decidable, then* $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Ab} \rtimes_\theta \mathsf{Fin})$ *is decidable.*

Remark 7.23 (Proof sketch)**.** The argument follows the proof of Theorem E with one modification. Since the target is a split extension $H = N \rtimes_\theta Q$, we may choose a transversal map $s \colon Q \to H$ whose associated 2-cocycle satisfies $f_s(p, q) = 1_N$ for all $p, q \in Q$. Consequently

- applying PresEqnC to a (Q, τ)-presentation of G and the extension data (θ, f_s) produces a system of twisted equations for TwistedEquationSubspan with trivial constants, i.e. $\mathfrak{c}_i = 1_N$ for all i; and
- in the construction $\mathsf{GLMatEqn}\big(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}, \Phi\big)$, the matrix $B \in \mathbb{Z}^{m \times d}$ is built from the exponent vectors of the $\mathfrak{c}_i$, so $\mathfrak{c}_i = 1_N$ for all i implies $B = 0$.

Thus MatrixSubspanD is exactly MatrixSubspanC with $B = 0$, and the remainder of the reduction proceeds as in Theorem E.

Then it is natural to ask the following question, when investigating if $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{Ab} \rtimes_\theta \mathsf{Fin})$ (resp. $\mathsf{EPI}(\mathsf{FinPres}, \mathsf{VAb})$) is decidable.

Question 7.24. Is MatrixSubspanD (resp. MatrixSubspanC) decidable?

Section 6.1 investigated epimorphisms onto free groups of finite rank. In light of Remarks 6.6 and 6.8, we pose two open questions.

Question 7.25. Is EquationsSubspan decidable on input a system of equations (without constants) over N when N is a free group of finite rank?

Question 7.26. What is an upper bound for the complexity of computing the rank of a system of equations $(u_i)_{[1,m]}$ without constants over a free group F_d?

Another interesting direction concerns the complexity of $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{G})$ for a fixed finite group G. As noted in Remark 5.35, we encountered particular difficulty in showing that nilpotent dihedral groups were NP-hard. In light of this, consider the following questions.

Question 7.27. Assuming $\mathsf{P} \neq \mathsf{NP}$, and letting G be a fixed finite group.

- Is $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{G})$ in P if and only if G is abelian?
- Is $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{D}_8)$ (the dihedral group of order 8) NP-hard?
- Does the above generalise to finite nilpotent groups? That is, for a nilpotent group G, is $\mathsf{EPI}(\mathsf{FinPres}, \mathrm{G})$ NP-hard?

Finally, we note that the primary emphasis of this thesis has been on varying the target group, another direction is to vary the domain group. Investigating how the structural properties of the domain influence the complexity of epimorphism problems, take for example [18] is interested in restricting the domain group to 3-manifolds.

Overall, this thesis provides a framework for investigating the complexity and decidability of epimorphism testing. Given the relative lack of attention that the epimorphism problem has received, there remain several directions for further investigation. The tools and techniques developed here offer a potential foundation for exploring new decidability results.

References

[1] S. I. Adian. 'Algorithmic unsolvability of problems of recognition of certain properties of groups'. In: *Dokl. Akad. Nauk SSSR (N.S.)* 103 (1955), pp. 533–535.

[2] Sanjeev Arora and Boaz Barak. *Computational complexity.* A modern approach. Cambridge University Press, Cambridge, 2009, pp. xxiv+579. ISBN: 978-0-521-42426-4. DOI: 10.1017/CBO9780511804090.

[3] Katalin A. Bencsáth, Marianna C. Bonanome, Margaret H. Dean and Marcos Zyman. 'Tools: Presentations and Their Calculus'. In: *Lectures on Finitely Generated Solvable Groups.* New York, NY: Springer New York, 2013, pp. 5–7. ISBN: 978-1-4614-5450-2. DOI: 10.1007/978-1-4614-5450-2_2. URL: https://doi.org/10.1007/978-1-4614-5450-2_2.

[4] William W. Boone. 'Certain simple, unsolvable problems of group theory. V, VI'. In: *Indag. Math.* 19 (1957). Nederl. Akad. Wetensch. Proc. Ser. A 60, pp. 22–27, 227–232.

[5] Stephen A. Cook. 'The Complexity of Theorem-Proving Procedures'. In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing (STOC).* ACM, 1971, pp. 151–158. DOI: 10.1145/800157.805047. URL: https://doi.org/10.1145/800157.805047.

[6] François Dahmani and Vincent Guirardel. 'The isomorphism problem for all hyperbolic groups'. In: *Geom. Funct. Anal.* 21.2 (2011), pp. 223–300. ISSN: 1016-443X,1420-8970. DOI: 10.1007/s00039-011-0120-0. URL: https://doi.org/10.1007/s00039-011-0120-0.

[7] M. Dehn. 'Über unendliche diskontinuierliche Gruppen'. In: *Math. Ann.* 71.1 (1911), pp. 116–144. ISSN: 0025-5831,1432-1807. DOI: 10.1007/BF01456932. URL: https://doi.org/10.1007/BF01456932.

[8] Volker Diekert and Murray Elder. 'Solutions to twisted word equations and equations in virtually free groups'. In: *Internat. J. Algebra Comput.* 30.4 (2020), pp. 731–819. ISSN: 0218-1967,1793-6500. DOI: 10.1142/S0218196720500198. URL: https://doi.org/10.1142/S0218196720500198.

[9] Volker Diekert, Claudio Gutierrez and Christian Hagenah. 'The existential theory of equations with rational constraints in free groups is PSPACE-complete'. In: *Inform. and Comput.* 202.2 (2005), pp. 105–140. ISSN: 0890-5401,1090-2651. DOI: 10.1016/j.ic.2005.04.002. URL: https://doi.org/10.1016/j.ic.2005.04.002.

[10] Murray Elder, Jerry Shen and Armin Weiß. *On the complexity of epimorphism testing with virtually abelian targets.* 2025. arXiv: 2501.05283 [math.GR]. URL: https://arxiv.org/abs/2501.05283.

[11] John B. Fraleigh. *A first course in abstract algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967, pp. xvi+447.

[12] Stefan Friedl and Clara Löh. 'Epimorphism testing with virtually Abelian targets'. In: *Confluentes Math.* 13.1 (2021), pp. 61–78. ISSN: 1793-7434.

[13] Mikael Goldmann and Alexander Russell. 'The Complexity of Solving Equations over Finite Groups'. In: *Information and Computation* 178.1 (2002), pp. 253–262. ISSN: 0890-5401. DOI: https://doi.org/10.1006/inco.2002.3173.

[14] Fritz Grunewald and Daniel Segal. 'Some general algorithms. II. Nilpotent groups'. In: *Ann. of Math. (2)* 112.3 (1980), pp. 585–617. ISSN: 0003-486X. DOI: 10.2307/1971092. URL: https://doi.org/10.2307/1971092.

[15] Derek F. Holt and W. Plesken. *Perfect groups*. Oxford Mathematical Monographs. With an appendix by W. Hanrath, Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1989, pp. xii+364. ISBN: 0-19-853559-7.

[16] Thomas W. Hungerford. *Algebra*. Vol. 73. Graduate Texts in Mathematics. Reprint of the 1974 original. Springer-Verlag, New York-Berlin, 1980, pp. xxiii+502. ISBN: 0-387-90518-9.

[17] Ravindran Kannan and Achim Bachem. 'Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix'. In: *SIAM Journal on Computing* 8.4 (1979), pp. 499–507. DOI: 10.1137/0208040.

[18] Greg Kuperberg and Eric Samperton. 'Computational complexity and 3-manifolds and zombies'. In: *Geom. Topol.* 22.6 (2018), pp. 3623–3670. ISSN: 1465-3060,1364-0380. DOI: 10.2140/gt.2018.22.3623. URL: https://doi.org/10.2140/gt.2018.22.3623.

[19] John M. Lee. *Introduction to topological manifolds*. Second. Vol. 202. Graduate Texts in Mathematics. Springer, New York, 2011, pp. xviii+433. ISBN: 978-1-4419-7939-1. DOI: 10.1007/978-1-4419-7940-7. URL: https://doi.org/10.1007/978-1-4419-7940-7.

[20] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Reprint of the 1977 edition. Springer-Verlag, Berlin, 2001, pp. xiv+339. ISBN: 3-540-41158-5. DOI: 10.1007/978-3-642-61896-3. URL: https://doi.org/10.1007/978-3-642-61896-3.

[21] A. A. Markov. 'The theory of algorithms'. In: *Trudy Mat. Inst. Steklov.* 38 (1951), pp. 176–189. ISSN: 0371-9685.

[22] P. S. Novikov. *On the algorithmic unsolvability of the word problem in group theory*. Trudy Mat. Inst. Steklov. no. 44. Izdat. Akad. Nauk SSSR, Moscow, 1955, p. 143.

[23] Michael O. Rabin. 'Recursive unsolvability of group theoretic problems'. In: *Ann. of Math. (2)* 67 (1958), pp. 172–194. ISSN: 0003-486X. DOI: 10.2307/1969933. URL: https://doi.org/10.2307/1969933.

[24] A. A. Razborov. 'Systems of equations in a free group'. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 48.4 (1984), pp. 779–832. ISSN: 0373-2436.

[25] V. N. Remeslennikov. 'An algorithmic problem for nilpotent groups and rings'. In: *Sibirsk. Mat. Zh.* 20.5 (1979), pp. 1077–1081, 1167. ISSN: 0037-4474.

[26] Derek J. S. Robinson. *A course in the theory of groups*. Second. Vol. 80. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, pp. xviii+499. ISBN: 0-387-94461-3. DOI: 10.1007/978-1-4419-8594-1. URL: https://doi.org/10.1007/978-1-4419-8594-1.

[27] V. A. Roman' kov. 'Unsolvability of the problem of endomorphic reducibility in free nilpotent groups and in free rings'. In: *Algebra i Logika* 16.4 (1977), pp. 457–471, 494. ISSN: 0373-9252.

[28] Joseph J. Rotman. *An introduction to the theory of groups*. Third. Allyn and Bacon, Inc., Boston, MA, 1984, pp. x+422. ISBN: 0-205-07963-6.

[29] Jennifer Schultens. *Introduction to 3-manifolds*. Vol. 151. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2014, pp. x+286. ISBN: 978-1-4704-1020-9. DOI: 10.1090/gsm/151. URL: https://doi.org/10.1090/gsm/151.

[30] Marcel-Paul Schützenberger. 'Sur l'équation $a^{2+n} = b^{2+m}c^{2+p}$ dans un groupe libre'. In: *C. R. Acad. Sci. Paris* 248 (1959), pp. 2435–2436. ISSN: 0001-4036.

[31] Dan Segal. 'Decidable properties of polycyclic groups'. In: *Proc. London Math. Soc. (3)* 61.3 (1990), pp. 497–528. ISSN: 0024-6115,1460-244X. DOI: 10.1112/plms/s3-61.3.497. URL: https://doi.org/10.1112/plms/s3-61.3.497.

[32] Charles C. Sims. *Computation with finitely presented groups*. Vol. 48. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 1994, pp. xiii+604. ISBN: 0-521-43213-8. DOI: 10.1017/CBO9780511574702. URL: https://doi.org/10.1017/CBO9780511574702.

[33] Michael Sipser. *Introduction to the Theory of Computation*. Vol. 27. ACM New York, NY, USA, 1996.

[34] Jonathan Sorenson. 'Two fast GCD algorithms'. In: *J. Algorithms* 16.1 (1994), pp. 110–144. ISSN: 0196-6774. DOI: 10.1006/jagm.1994.1006. URL: https://doi.org/10.1006/jagm.1994.1006.

[35] Arne Storjohann. 'On the complexity of inverting integer and polynomial matrices'. In: *Comput. Complexity* 24.4 (2015), pp. 777–821. ISSN: 1016-3328,1420-8954. DOI: 10.1007/s00037-015-0106-7. URL: https://doi.org/10.1007/s00037-015-0106-7.

[36] Heinrich Tietze. 'Über die topologischen Invarianten mehrdimensionaler Mannigfaltigkeiten'. In: *Monatsh. Math. Phys.* 19.1 (1908), pp. 1–118. ISSN: 1812-8076. DOI: 10.1007/BF01736688. URL: https://doi.org/10.1007/BF01736688.