ON THE COMPLEXITY OF EPIMORPHISM TESTING
WITH VIRTUALLY ABELIAN TARGETS

MURRAY ELDER, JERRY SHEN, AND ARMIN WEISS

ABSTRACT. Friedl and Löh (2021, Confl. Math.) prove that testing whether or not there is an epimorphism from a finitely presented group to a virtually cyclic group, or to the direct product of an abelian and a finite group, is decidable. Here we prove that these problems are NP-complete. We also show that testing epimorphism is NP-complete when the target is a restricted type of semi-direct product of a finitely generated free abelian group and a finite group, thus extending the class of virtually abelian target groups for which decidability of epimorphism is known.

Lastly, we consider epimorphism onto a fixed finite group. We show the problem is NP-complete when the target is a dihedral groups of order that is not a power of 2, complementing the work on Kuperberg and Samperton (2018, Geom. Topol.) who showed the same result when the target is non-abelian finite simple.

1. INTRODUCTION

Let $\mathcal{D}, \mathcal{T}$ be classes of groups. The (uniform) *epimorphism problem* from $\mathcal{D}$ to $\mathcal{T}$, denoted $\mathrm{Epi}(\mathcal{D}, \mathcal{T})$, is the following decision problem.

Input: Finite descriptions for groups $G \in \mathcal{D}$ and $H \in \mathcal{T}$
Question: Is there a surjective homomorphism from G to H?

Note that an epimorphism in the category of groups is a surjective homomorphism. We refer to $G \in \mathcal{D}$ as the *domain group* and $H \in \mathcal{T}$ is the *target group* for the problem. If $\mathcal{T} = \{H\}$ is a singleton, we write $\mathrm{Epi}(\mathcal{D}, H)$ for the epimorphism problem from a class $\mathcal{D}$ to the fixed group H, in which case the input is just a finite description for a group $G \in \mathcal{D}$.

Remeslennikov [10] proved for $\mathcal{D}$ the class of non-abelian nilpotent groups, the epimorphism problem from $\mathcal{D}$ to $\mathcal{D}$ is undecidable, via Hilbert's 10th problem. Applying work of Razborov [9, Theorem 3] on equations in free groups, the epimorphism problem from finitely presented groups to finitely generated free groups is decidable, but without any known complexity bounds (see Section 8). Friedl and Löh [3] considered the epimorphism problem from finitely presented groups to virtually abelian groups, proving that the problem is decidable when the target is either a virtually cyclic or the direct product of an abelian group and a finite group. Whilst they claim that the algorithms they consider to establish decidability "will have ridiculous worst-case complexity", in fact we are able to show the following.

Theorem A. The epimorphism problem from finitely presented groups to the following targets 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 of a certain restricted type (see Definition 1.6).

Kuperberg and Samperton [7] considered the special case of epimorphism from certain 3-manifold groups to finite non-abelian simple groups, in the context of more general questions. It follows from their work that the epimorphism problem from a finitely presented group to a fixed finite non-abelian simple group is NP-hard (see Subsection 8.2). Here we show the same result applies when the target is a finite dihedral group of order not a power of 2.

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

For completeness we include the following which collects together known results [7] and some straightforward consequences of known results [9, 6].

Theorem C. The epimorphism problem from finitely presented groups to
(1) finite rank free groups is decidable
(2) a fixed non-abelian finite simple group is NP-complete
(3) a fixed group $B \times A$, where B is a finite non-abelian simple group, or D_{2n} with n odd, and A is abelian, is NP-complete
(4) finitely generated abelian groups is in P.

Reduction to integer matrix problems. We prove Theorem A by reducing the epimorphism problem to the following algebraic problems, which we will show are both in P.

For $d \in \mathbb{N}$ let $[1,d]$ denote the set of integers $\{1,\dots,d\}$. For $m,n,\ell \in \mathbb{N}$ with $\ell \leqslant m$ and M an $m \times n$ matrix, let $M|_\ell$ denote the $\ell \times n$ matrix consisting of the bottom ℓ rows of M. We call an $n \times 1$ matrix an n-*vector*, and a matrix (resp. n-vector) whose entries are integers an *integer matrix* (resp. *integer n-vector*). For an integer matrix M we let $\text{span}(M)$ denote the set of all $\mathbb{Z}$-linear combinations of the columns of M (see Subsection 1.1 for additional notation).

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 $v_1,\dots,v_d$ such that $Av_i = 0$ for $i \in [1,d]$ and for the $n \times d$ matrix V whose columns are $v_1,\dots,v_d$, $\text{span}((V|_\ell)^T) = \mathbb{Z}^d$?

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

Throughout this paper we assume integer matrices are given with entries as binary numbers for the purpose of complexity.

Theorem D. MATRIXSUBSPANA and MATRIXSUBSPANB are in P.

1.1. **Notation and basic facts.**

Complexity. We assume the reader is familiar with the complexity classes of P and NP. A problem is NP-*hard* if every problem in NP is reducible to it in polynomial time, and a decision problem is NP-*complete* if it is both in NP and NP-hard. For all decision problems and algorithms we assume integer structures (eg. matrices, $\mathbb{Z}$-modules) are given by a list of integers in binary, and constants (of a group) are given in unary (on generators).

Matrices, basis, span. Let $\mathbb{Z}^{m \times n}$ denote the set of all $m \times n$ integer matrices (matrices with integer entries), $\mathrm{GL}(n, \mathbb{Z})$ the set of invertible $n \times n$ integer matrices, and $0_{m,n}$ (or 0 when the size is clear) the $m \times n$ matrix with all 0 entries. If $M \in \mathbb{Z}^{m \times n}$, the matrix $M|_\ell \in \mathbb{Z}^{\ell \times n}$ is the matrix consisting of the bottom ℓ rows of M, that is, the matrix whose i-th row is the $(m - \ell + i)$-th row of M. Note that the $\mathbb{Z}$-module $\mathbb{Z}^d$ is identified with $\mathbb{Z}^{d \times 1}$ throughout this paper. A $\mathbb{Z}$-*linear combination* of d-vectors $u_1, \ldots, u_n \in \mathbb{Z}^d$ is a d-vector of the form $x = c_1 u_1 + \cdots + c_n u_n$ for $c_1, \ldots, c_n \in \mathbb{Z}$. The *span* of $u_1, \ldots, u_n$ is the set of all $\mathbb{Z}$-linear combinations of $u_1, \ldots, u_n \in \mathbb{Z}^d$, which we denote by $\mathrm{span}(u_1, \ldots, u_n)$. If $M \in \mathbb{Z}^{m \times n}$ we let $\mathrm{span}(M)$ denote the span of the columns of M. For $b \in \mathbb{Z}^m$ we define $\mathrm{span}_b(M)$ to be the set of all m-vectors of the form $y + b$ for some $y \in \mathrm{span}(M)$.

Words. Let X be a set. We call a finite sequence $(x_1, \ldots, x_n)$ with $x_i \in X$ a *word* over X, and denote it as $x_1 \cdots x_n$. The set of all words over X is denoted X^*. The notation $u(X) = u(x_1, \ldots, x_n)$ stands for a word u over the letters $x_1, \ldots, x_n$. If $Y = \{y_1, \ldots, y_p\}, Z = \{z_1, \ldots, z_q\}$ are sets, then we may write $u(Y, z_1, \ldots, z_q) = u(y_1, \ldots, y_p, z_1, \ldots, z_q) = u(Y, Z)$.

For any set X we let $X^{-1} = \{x^{-1} \mid x \in X\}$ be a set of letters with $X \cap X^{-1} = \emptyset$.

If A is a set, H is a monoid and $\psi \colon A \to H$ is a set map, we define the induced monoid homomorphism from $(A \cup A^{-1})^*$ to H by

$$\psi(a_1^{\epsilon_1} \cdots a_s^{\epsilon_s}) = \psi(a_1)^{\epsilon_1} \cdots \psi(a_s)^{\epsilon_s}$$

where $a_i \in A$ and $\epsilon_i = \pm 1$.

Groups. We use the notation 1_G to denote the identity element of a group G, $[a, b] := aba^{-1}b^{-1}$ for the commutator of two elements a, b of G, and $[G, G]$ the commutator subgroup of G (the subgroup consisting of all products of commutators of elements of G). For a group G and two elements $a, b \in G$, $^b a = bab^{-1}$ denotes the conjugation of a by b. If u, v are two different ways to represent the same element of G, we write $u =_G v$.

We denote the infinite cyclic group as C_∞, the cyclic group of order $n \in \mathbb{N}_+$ as C_n, and the dihedral group of *order* $2n$ as D_{2n}. We denote certain classes of groups as follows:

(1) FinPres is the class of finitely presented groups
(2) Fin is the class of finite groups
(3) FreeAb is the class of free abelian groups of finite rank (groups isomorphic to direct products of finitely many copies of C_∞)
(4) VirtCyclic is the class of virtually cyclic groups
(5) Ab × Fin is the class of groups of the form $N \times Q$ where $N \in$ FreeAb and $Q \in$ Fin
(6) SpecialExt and RestrAbelSemi are restricted classes of extensions to be defined below (Definitions 1.5 and 1.6).

Presentations. A group $G \in$ FinPres is given by a finite presentation $\langle X \mid R \rangle$ where X is a finite set and each $r \in R$ is a word over $X \cup X^{-1}$. We do not assume X is a subset of G, so for example we may have $x, y \in X$ with $x =_G y$, and we do not assume G has decidable word problem, so, *a priori*, given a presentation $\langle X \mid R \rangle$, we have no algorithm to determine whether $x =_G y$ for $x, y \in X$. The following well-known lemma is used repeatedly throughout this paper.

Lemma 1.1 (von Dyck's lemma [1, Lemma 2.1])**.** *If G is presented by $\langle g_1, \ldots, g_n \mid r_1, \ldots, r_m \rangle$ 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 the induced monoid homomorphism $\psi \colon \{g_1^{\pm 1}, \ldots, g_n^{\pm 1}\}^* \to H$ defines a homomorphism from G to H if and only if $r_i(\psi(g_1), \ldots, \psi(g_n)) =_H 1_H$ for $1 \leqslant i \leqslant m$.*

Equations. Let $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$. An *equation* over a group G is a word

$$u(g_1, \ldots, g_s, \mathbb{X})$$

where $g_i \in G$ for $i \in [1, s]$ are called *constants* and $\mathbb{X}$ are called *variables*. A *system of equations* $(u_i)_{[1,m]}$ is a finite list of equations $u_i(g_1, \ldots, g_s, \mathbb{X})$ for $i \in [1, m]$. A *solution* to a system of equations $(u_i)_{[1,m]}$ is a map $\sigma \colon \mathbb{X} \to G$ of the form $\sigma \colon X_i \mapsto h_i, X_i^{-1} \mapsto h_i^{-1}$ for some $h_i \in G$, $i \in [1, n]$ so that

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

A system of equations *without constants* is a list of equations of the form $u_i(\mathbb{X})$ for $i \in [1, m]$. Note that if G is a finitely generated group with finite inverse-closed generating set $\mathcal{Y} = \{y_1, \ldots, y_s\}$, we may write any equation over G as $u(\mathcal{Y}, \mathbb{X})$.

A key step in our reduction from epimorphism to matrix problems is the following decision problem for equations over groups.

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 $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle = N$?

Free abelian groups. A free abelian group of rank $d \in \mathbb{N}_+$ is a group isomorphic to the direct product of d copies of the infinite cyclic group C_∞. Such a group admits the presentation $\langle x_1, \ldots, x_d \mid [x_i, x_j], \forall i, j \in [1, d] \rangle$, which we may write simply as $\langle x_1, \ldots, x_d \rangle$ when the context is understood. It follows that every element of a free abelian group $N \cong \langle x_1, \ldots, x_d \rangle$ can be represented uniquely as a word $x_1^{c_1} \cdots x_d^{c_d}$ for some $c_1, \ldots c_d \in \mathbb{Z}$. It is well known that every free abelian group is a $\mathbb{Z}$-module which we denote by $\mathbb{Z}^d$, with standard basis $\{e_1, \ldots, e_d\}$ where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T \in \mathbb{Z}^d$ with non-zero entry in the i-th position, via the natural isomorphism $\varphi \colon N \to \mathbb{Z}^d$ defined by the set map

$$\varphi \colon x_i \mapsto e_i,$$

extending to the isomorphism

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

Equations over abelian groups. Let u an equation over a group N with variables $\mathbb{X}$ as above and a single constant $\mathfrak{c} \in N$ (possibly with $\mathfrak{c} = 1_N$). Define the *commuted normal form* of u to be the word

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

where $\alpha_i = |u|_{X_i} - |u|_{X_i^{-1}}$ for $i \in [1, n]$. The following observation is immediate.

Lemma 1.2. *Let N be an abelian group, and $(u_i)_{[1,m]}$ 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 σ is a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$.*

Extensions. A group H is said to be an *N by Q extension* if

    (1) N is a normal subgroup of H

    (2) there is an isomorphism $\psi\colon H/N \to Q$.

It follows that the maps $\iota\colon N \to H$ and $\pi_Q\colon H \to Q$ given by given by $\iota\colon n \mapsto n$ and $\pi_Q\colon g \mapsto \psi(gN)$ define an exact sequence

$$\{1\} \to N \overset{\iota}{\to} H \overset{\pi_Q}{\to} Q \to \{1\}.$$

A set $T \subseteq H$ which contains exactly one element of each (right) coset of a subgroup N is called a (right) *transversal* for N in H (note that throughout this paper all cosets will be right cosets). A map $s\colon Q \to H$ is a *transversal map* if $\{s(q) \mid q \in Q\}$ is a transversal, or equivalently if s is injective and $\pi_Q(s(q)) = q$. w.l.o.g we assume s is always chosen so that $s(1_Q) = 1_H$ throughout this article.

Given a fixed transversal map s, every element $g \in H$ can be written uniquely as a product $g = ns(q)$ for some $n \in N$ and $q \in Q$, which we call the *normal form* for g. The map $\pi_N\colon H \to N$ given by $\pi_N(g) = n$ when $g = ns(q)$ is well defined since s is a transversal map. Since N is a normal subgroup of H, each $s(q)$ acts by conjugation on N as an inner automorphism. Define $\theta_s\colon Q \to \mathrm{Aut}(N)$ by $\theta_s\colon q \mapsto {}^{s(q)}n$. Also since 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 $n \in N$, and so $s(q_1)s(q_2)s(q_1q_2)^{-1} \in N$. Define a map $f_s\colon Q \times Q \to N$ by $f_s\colon (q_1, q_2) \mapsto s(q_1)s(q_2)s(q_1q_2)^{-1}$. We call the pair (θ_s, f_s) the *extension data* for the N by Q extension H with respect to a chosen transversal map $s\colon Q \to H$. Clearly if Q is finite and N is finitely generated then (θ_s, f_s) has a finite description.

In the case s is a homomorphism then $s(q_1)s(q_2)s(q_1q_2)^{-1} = 1_N$ and we write $f_s = 1_N$ to denote the trivial map, and H is a semidirect product of N and Q via θ_s. For example, if H is isomorphic to the direct product of a group N and a finite group Q, $s\colon q \mapsto (1, q)$ is a transversal map which is an injective homomorphism so $f_s = 1_N$ and $\theta_s\colon n \mapsto n$, and we may write every element uniquely in the form $ns(q) = (n, q)$.

Virtually abelian groups. A standard argument shows that if H has a finite index abelian subgroup, then it contains a normal finite index abelian subgroup (by taking the *normal core*, see for example [3, Proposition 2.2]). Thus we may view every virtually abelian group H as an N by Q extension where $N \in \mathrm{FreeAb}$ and $Q \in \mathrm{Fin}$.

Remark 1.3 (Action is determined by q when N is abelian)**.** If s_1, s_2 are two transversal maps from Q to H, $Ns_1(q) = Ns_2(q)$ so $s_2(q)^{-1}s_1(q) \in N$. Then since N is abelian we have

$$
{}^{s_2(q)}(n)\left({}^{s_1(q)}(n)\right)^{-1} = s_2(q)ns_2(q)^{-1}s_1(q)n^{-1}s_1(q)^{-1}
$$
$$
= s_2(q)nn^{-1}\left(s_2(q)^{-1}s_1(q)\right)s_1(q)^{-1} = 1_N
$$

which shows that the conjugation action does not depend on the choice of transversal. Thus, when N is abelian we may sometimes write ${}^q n$ rather than ${}^{s(q)}n$, and θ rather than θ_s.

Virtually cyclic groups. If φ is an automorphism of the infinite cyclic group $C_\infty = \langle x \rangle$, there exists $i, j \in \mathbb{Z}$ so that $\varphi(x) = x^i$ and $\varphi(x^j) = x$, so $x = \varphi(x^j) = (\varphi(x))^j = x^{ij}$, which means $i = j = 1$ or $i = j = -1$. Thus $\mathrm{Aut}(\langle x \rangle) = \{n \mapsto n, n \mapsto n^{-1}\}$, so in a C_∞ by Q extension each $q \in Q$ acts as either ${}^q n = n$ for all $n \in C_\infty$ or ${}^q n = n^{-1}$ for all $n \in C_\infty$.

Remark 1.4. Suppose an N by Q extension H has transversal map $s\colon Q \to H$ such that for some $q \in Q$, ${}^{s(q)}(n) = n^{-1}$ for all $n \in N$. Then

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

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

so N is abelian. Thus, if we wish to define a class of N by Q extensions where the action of $q \in Q$ is restricted to being either $^{s(q)}x = x$ for all $x \in N$ or $^{s(q)}x = x^{-1}$ for all $x \in N$ (generalising the class VirtCyclic), then necessarily N must be abelian.

Special abelian extensions. We define two subclasses of virtually abelian groups as follows.

Definition 1.5 (SpecialExt)**.** Define SpecialExt to be the class of N by Q extensions for a group H which satisfy the following conditions:

(1) N is abelian and Q is finite
(2) there is a transversal map $s\colon Q \to H$ and a subset $\mathcal{I} \subseteq Q$ so that
    (a) $^q n = n^{-1}$ for all $n \in N$ when $q \in \mathcal{I}$
    (b) $^q n = n$ for all $n \in N$ when $q \in Q \setminus \mathcal{I}$.

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

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

so we can specify the extension data for $H \in$ SpecialExt by the pair $(\mathcal{I}, f_s)$, which we call the *special extension data* of H. The class SpecialExt includes $\mathrm{Ab} \times \mathrm{Fin}$ (when $\mathcal{I} = \emptyset$ and $f_s = 1_N$) and VirtCyclic (when $N \cong C_\infty$).

Definition 1.6 (RestrAbelSemi)**.** Define RestrAbelSemi to be the subclass of SpecialExt having special extension data $(\mathcal{I}, 1_N)$.

An example of a group in RestrAbelSemi but not VirtCyclic or $\mathrm{Ab} \times \mathrm{Fin}$ is

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

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. Preliminary results

2.1. **Finite targets.** We start by observing that $\mathrm{Epi}(\mathrm{FinPres}, \mathrm{Fin})$ is in NP. We note that Holt and Plesken [5, Chapter 7] considered the computational problem of finding epimorphisms onto various classes of finite groups, without explicitly giving a complexity bound, and Friedl and Löh [3, Proposition 5.2] show that $\mathrm{Epi}(\mathrm{FinPres}, \mathrm{Fin})$ is decidable.

We assume that the input to the problem is a finite presentation $\langle\, g_1, \ldots, g_n \mid r_1, \ldots, r_m \,\rangle$ for the domain group $G \in \mathrm{FinPres}$ and a multiplication table for the target group $Q \in \mathrm{Fin}$.

Lemma 2.1. $\mathrm{Epi}(\mathrm{FinPres}, \mathrm{Fin})$ *is in* NP.

Proof. On input a presentation $\langle\, g_1, \ldots, g_n \mid r_1, \ldots, r_m \,\rangle$ for $G \in \mathrm{FinPres}$, 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 1.1 by checking that each relator is sent to 1_Q using the multiplication table for Q.

To verify that τ is a surjection, we may proceed as follows. Fix a copy of Q and 'mark' each $q_j \in Q$ which satisfies $\tau(g_i) = q_j$ for $i \in [1, n]$. While not all of Q is marked, scan the multiplication table for Q to find $q_i, q_j, q_k \in Q$ so that $q_i q_j = q_k$ with q_i, q_j marked and q_k not marked, then mark q_k. If τ is a surjection then each $q \in Q$ is the image of some product of generators so the process will terminate with all of Q marked.

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

Note that combining Lemma 2.1 with [7, Corollary 1.2] (or Theorem 7.19 below) we immediately have that $\mathrm{Epi}(\mathrm{FinPres}, \mathrm{Fin})$ is NP-complete.

2.2. (Q, τ)-**presentation.** The following is a useful format in which to present a finitely presented domain group when considering epimorphism onto a target which involves a finite group.

Definition 2.2 $((Q, \tau)$-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 2.3. *There is an algorithm which takes input*

(1) a finite presentation $\langle\, g_1, \ldots, g_n \mid r_1, \ldots, r_m \,\rangle$ for a group G
(2) a multiplication table for a finite group Q
(3) a list $(q_1, \ldots, q_n) \in Q^n$ 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 $(n + m + |Q|)$, which runs in time polynomial in $(n + m + |Q|)$.

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

(1) Set $\mathcal{G}$ to be $\mathcal{G} \cup \mathcal{G}^{-1}$ and $\mathcal{R}$ to be $\mathcal{R} \cup \{g_i(g_i^{-1}) : i \in [1, n]\}$.
(2) For each $g \in \mathcal{G}$:
   (a) 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, after this for-loop we have Λ is 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 $\mathcal{R} = \mathcal{R} \cup \{x_{p_1} x_{p_2} x_q^{-1}\}$.
   On termination of this while-loop, we have $\Lambda = Q$ and $\mathcal{X}$ is in bijection with $\Lambda = Q$. As Λ increases in each iteration, the loop is guaranteed to terminate. We have $\langle\, \mathcal{X} \cup \mathcal{G} \mid \mathcal{R} \,\rangle$ presents G, and $\tau(x_q) = q$ for each $x_q \in \mathcal{X}$.
(4) For each $g_i \in \mathcal{G}$ and pair $(p, q) \in Q \times Q$:
   (a) if $\tau(x_p g_i x_q) =_Q 1$, set $\mathcal{Y} = \mathcal{Y} \cup \{y_{p,i,q}\}$, and $\mathcal{R} = \mathcal{R} \cup \{x_p g_i x_q y_{p,i,q}^{-1}\}$.
   After this for-loop have $\langle\, \mathcal{X} \cup \mathcal{Y} \cup \mathcal{G} \mid \mathcal{R} \,\rangle$ presents G.
(5) For each $i \in [1, n]$, we have that $\tau(g_i) \in Q$, which means $x_{\tau(g_i)} \in \mathcal{X}$ and $\tau(x_{\tau(g_i)}) = \tau(g_i)$. From this it follows that $\tau(x_{\tau(g_i)^{-1}} g_i x_{1_Q}) = 1_Q$, which implies $y_{\tau(g_i)^{-1}, g_i, 1_Q} \in \mathcal{Y}$ and $y_{\tau(g_i)^{-1}, g_i, 1_Q} =_G x_{\tau(g_i)^{-1}} g_i x_{1_Q}$. Then we may perform a Tietze transformation to remove g_i from the generating set and replace each occurrence of the letter g_i in each relation by

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

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

The time complexity and output length for each subroutine is as follows.

(1) takes $|\mathcal{G}| = n$ steps, and so from here on setting $\mathcal{G}$ to be $\mathcal{G} \cup \mathcal{G}^{-1}$ gives $2n$ steps when iterating through $\mathcal{G}$.
(2) takes $2n$ steps, and adds at most $|Q|$ letters to $\Lambda, \mathcal{X}$ and $|Q|$ words of length 2 to $\mathcal{R}$.
(3) the while-loop is performed 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, adds at most $2n|Q|^2$ new letters to $\mathcal{Y}$, and adds at most $2n|Q|^2$ new words of length at most 4 to $\mathcal{R}$.

(5) takes $2n$ steps, and all steps combined increase 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 spelled as

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

Let $q_{i_1}, \ldots, q_{i_{k-1}} \in Q$ so 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 $q = \tau(x_q)$ 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 $\langle \mathcal{Y} \rangle = \ker(\tau)$. $\qquad\square$

Remark 2.4. Since we do not assume that $\mathcal{G} \subseteq G$ or that G has decidable word problem, we do not assert that $\mathcal{Y}$ is a subset of G (it may have repetitions), whereas we have ensured that $\mathcal{X} \subseteq G$ in the proof of the above lemma.

2.3. **Epimorphism into extensions.** Recall that if H is an N by Q extension, the map $\pi_Q \colon H \to Q$ is an epimorphism.

Lemma 2.5. *Let $G, N \in$ FinPres, and $Q \in$ Fin and H is given by an N by Q extension and a transversal map s. The following are equivalent:*

(1) *there exists an epimorphism from G to H*
(2) *there exist homomorphisms $\tau \colon G \to Q$, $\kappa \colon G \to H$ 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 an epimorphism. For each $g \in G$ if $\psi(g) = ns(q)$, then $\tau(g) = \pi_Q(ns(q)) = q$ so $\psi = \kappa$ satisfies item (b), and if $n \in N$ then since ψ is surjective there exists $g \in G$ with $\psi(g) = ns(1_Q)$ and $\tau(g) = \pi_Q(ns(1_Q)) = 1_Q$ so $\psi = \kappa$ satisfies item (c).

Conversely, assume there exist τ and κ as described in the lemma. Then for each $ns(q) \in H$ there exists $g_1 \in G$ so that $\tau(g_1) = q$, so $\kappa(g_1) = n_1 s(q)$ for some $n_1 \in N$, and $g_2 \in \ker(\tau)$ so that $\kappa(g_2) = nn_1^{-1} s(1_Q)$. Then $\kappa(g_1 g_2) = nn_1^{-1} s(1_Q) n_1 s(q) = ns(q)$. Therefore, κ is a surjective homomorphism from G to H. $\qquad\square$

Remark 2.6. 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 $\kappa(w) = ns(1_Q)$*

since $\ker(\tau) = \langle \mathcal{Y} \rangle$.

Example 2.7 (Necessity of the conditions in Lemma 2.5)**.** Let $G = \left\langle x_1, q_1 \mid [x_1, q_1], q_1^2 \right\rangle \cong \mathbb{Z} \times \mathbb{Z}_2$, $N = \left\langle x_2 \right\rangle \cong \mathbb{Z}$ and $Q = \left\langle q_2 \mid q_2^2 \right\rangle \cong C_2$. Then clearly an epimorphism (isomorphism) from G to $N \times Q$ exists. Consider the epimorphism $\tau \colon G \to Q$ defined by $\tau(x_1) = q_2, \tau(q_1) = 1_Q$. For a homomorphism $\kappa \colon G \to N \times Q$ to satisfy condition (2), for all $n \in N$ there must exist $g \in \ker(\tau) = \{1_G, q_1\}$ so that $\kappa(g) = ns(1_Q) = (n, 1_Q)$, which is impossible since $N \times \{1_Q\}$ is infinite. This example shows that items (a)–(c) are all required, it is not enough to have an epimorphism τ and a homomorphism κ that do not satisfy (b) and (c).

3. Direct product targets

In this section, we show 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 (defined on page 4).

Definition 3.1 (Presentation to system of equations)**.** On input a presentation of the form $\left\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \right\rangle$ 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 $\zeta \colon \mathcal{X} \cup \mathcal{X}^{-1} \cup \mathcal{Y} \cup \mathcal{Y}^{-1} \to \mathbb{X} \cup \mathbb{Y}$ the bijection

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

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

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

Lemma 3.2 (Epimorphism onto direct products)**.** *Let* $G, N \in \mathrm{FinPres}$ *and* $Q \in \mathrm{Fin}$. *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 $\left\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \right\rangle$ for 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 2.5 and Remark 2.6, 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 $\kappa(w) = (n, 1_Q)$

Define $\sigma \colon \mathbb{X} \cup \mathbb{Y} \to N$ by

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

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

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

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

For each $n \in N$ there exists $w \in (\mathcal{Y} \cup \mathcal{Y}^{-1})^*$ such that $\kappa(w) = (n, 1_Q)$, and for each $n \in N$ there exists $\zeta(w) \in \mathbb{Y}^*$ so that $\sigma(\zeta(w)) = \pi_N(\kappa(w)) = n$, which means $\left\langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \right\rangle = N$, and EQUATIONSSUBSPAN returns 'Yes'.

Conversely, assume there exists an epimorphism $\tau \colon G \to Q$ such that for some (Q, τ)-presentation $\left\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \right\rangle$ for G, EQUATIONSSUBSPAN returns 'Yes' on input N and system of equations $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$, which 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

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

with $\kappa\colon (\mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1})^* \to N$ the induced monoid homomorphism.

Then 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

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

where $\tau(r) = 1_Q$ since τ is a homomorphism, so by Lemma 1.1 κ is a homomorphism from G to N.

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 $\kappa(g) = \kappa(w) = (\sigma(w), \tau(w)) = (\sigma(w), \tau(g))$ so $\kappa(g) = (n, q)$ 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 $\sigma(w) = n$, so for each $n \in N$ there exists $\zeta^{-1}(w) \in \langle \mathcal{Y} \rangle$ so that $\sigma(\zeta(\zeta^{-1}(w))) = \sigma(w) = n$.

Having found homomorphisms τ, κ and established conditions (a), (b) and (c') as in Lemma 2.5 and Remark 2.6, we have shown the existence of an epimorphism from G to $N \times Q$. $\square$

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

Definition 3.3 (System of equations to matrix system). Let

(1) $d, t, \ell, m \in \mathbb{Z}$
(2) $N = \langle x_1, \ldots, x_d \rangle \in \mathrm{FreeAb}$
(3) $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_t, X_t^{-1}\}$, $\mathbb{Y} = \{Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$
(4) $v_i \in (\mathbb{X} \cup \mathbb{Y})^*$ for $i \in [1, m]$
(5) $\mathfrak{c}_i \in N$ with $\mathfrak{c}_i = x_1^{b_{(i,1)}} \cdots x_d^{b_{(i,d)}}$ for $i \in [1, m]$
(6) $(u_i)_{[1,m]}$ 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 (page 4 in Subsection 1.1) 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 $j \in [1, t], k \in [1, \ell]$. Define

$$\mathsf{EqnMat}(d, t, \ell, (u_i)_{[1,m]}, (\mathfrak{c}_i)_{[1,m]}))$$

to be the triple (A, B, ℓ) with $A \in \mathbb{Z}^{m \times (t+\ell)}$, $B \in \mathbb{Z}^{m \times d}$,

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

Definition 3.4 (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

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

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

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

and $\mathfrak{c}_i = x_1^{b(i,1)} \ldots x_d^{b(i,d)} \in N$.

The following is immediate from the definitions.

Lemma 3.5. *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 $(u_i)_{[1,m]}$ with each $u_i = v_i \mathfrak{c}_i$ where v_i is a word in variables $\{X_1, X_1^{-1}, X_t, X_t^{-1}, Y_1, Y_1^{-1}, \ldots, Y_\ell, Y_\ell^{-1}\}$ 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 $A \in \mathbb{Z}^{m \times n}, B \in \mathbb{Z}^{n \times d}$ and $\ell \in \mathbb{Z}$, compute $\mathsf{MatEqn}(A, B, \ell)$.

Lemma 3.6. *Let*
   (1) $N \in \mathrm{FreeAb}$ 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, with 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

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

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

$$\mathsf{CNF}(u_i) = X_1^{\alpha(i,1)} \ldots X_t^{\alpha(i,t)} Y_1^{\beta(i,1)} \ldots Y_\ell^{\beta(i,\ell)}$$

where

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

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

By definition, EQUATIONSSUBSPAN on input N and $(u_i)_{[1,m]}$ returns 'Yes' if and only if there is a solution $\sigma \colon \mathbb{X} \cup \mathbb{Y} \to N$ to $(u_i)_{[1,m]}$ and $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle = N$, where σ is also a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$ by Lemma 1.2.

We may write the solution as

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

for some values $c_{j,k} \in \mathbb{Z}$. 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 direct calculation 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

$$\sum_{j=1}^{t} c_{(j,k)}\alpha_{(i,j)} + \sum_{j=1}^{\ell} c_{(t+j,k)}\beta_{(i,j)} = 0 \tag{3.1}$$

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 $\langle \sigma(Y_1), \dots, \sigma(Y_\ell) \rangle = N$ if and only if

$$
\begin{aligned}
AV &= \begin{pmatrix} \alpha_{(1,1)} & \cdots & \alpha_{(1,t)} & \beta_{(1,1)} & \cdots & \beta_{(1,\ell)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{(m,1)} & \cdots & \alpha_{(m,t)} & \beta_{(m,1)} & \cdots & \beta_{(m,\ell)} \end{pmatrix} \begin{pmatrix} c_{(1,1)} & \cdots & c_{(1,d)} \\ \vdots & \ddots & \vdots \\ c_{(t+\ell,1)} & \cdots & c_{(t+\ell,d)} \end{pmatrix} \\
&= \begin{pmatrix} \sum_{j=1}^{t} c_{(j,1)}\alpha_{(1,j)} + \sum_{j=1}^{\ell} c_{(t+j,1)}\beta_{(1,j)} & \cdots & \sum_{j=1}^{t} c_{(j,d)}\alpha_{(1,j)} + \sum_{j=1}^{\ell} c_{(t+j,d)}\beta_{(1,j)} \\ \vdots & \ddots & \vdots \\ \sum_{j=1}^{t} c_{(j,1)}\alpha_{(m,j)} + \sum_{j=1}^{\ell} c_{(t+j,1)}\beta_{(m,j)} & \cdots & \sum_{j=1}^{t} c_{(j,d)}\alpha_{(m,j)} + \sum_{j=1}^{\ell} c_{(t+j,d)}\beta_{(m,j)} \end{pmatrix} \\
&= \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \text{ by Eq. (3.1),}
\end{aligned}
$$

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

Recall the natural isomorphism $\varphi \colon N \to \mathbb{Z}^d$ (page 4 in Subsection 1.1). 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 $\langle \sigma(Y_1), \dots, \sigma(Y_\ell) \rangle = N$ 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 $\langle \sigma(Y_1), \dots, \sigma(Y_\ell) \rangle = N$ if and only if $Av_i = 0$ for $i \in [1, d]$ and

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

which is true if and only if MATRIXSUBSPANA returns 'Yes'. $\qquad\square$

Combining the above results with the fact that will be proved in Section 6 that MATRIXSUB-SPANA can be decided in polynomial time gives the following.

Theorem 3.7. Epi(FinPres, Ab × Fin) *is in* NP.

Proof. Let $G \in$ FinPres, $N \in$ FreeAb and $Q \in$ Fin. Using Lemma 3.2 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 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 its 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 input MATRIXSUBSPANA on input $(A, d, |\mathcal{Y}|)$.

Step (1) verifies the existence of Condition (i). step (1) to (3) builds the necessary data to solve Condition (ii). Lemma 3.6 states that to solve EQUATIONSSUBSPAN, we can solve MATRIXSUBSPANA on input $(A, 0, |\mathcal{Y}|)$ constructed in step (4). Thus we solve 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 2.1; this is the only non-deterministic step of our algorithm.
(2) A construction of (Q, τ)-presentation in P exists by Lemma 2.3.
(3) $\mathsf{PresEqnA}(\mathcal{X}, \mathcal{Y}, \mathcal{R})$ is a polynomial time construction by Lemma 3.5.
(4) $\mathsf{EqnMat}(d, |\mathcal{X}|, |\mathcal{Y}|, (u_i)_{[1,m]}, (1_N)_{[1,m]})$ is a polynomial time construction by Lemma 3.5.
(5) MATRIXSUBSPANA is solved P by Proposition 6.13 (Subsection 6.1).

Thus, our algorithm is in NP. $\qquad\square$

4. 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 again begin by translating epimorphism to an equations problem.

Recall that SpecialExt is the class of N by Q extensions such that Q is finite, N is abelian, and there exists a transversal map s and a subset $\mathcal{I} \subseteq Q$ so that

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

so for all $n \in N$,

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

We assume the data for a group in SpecialExt is given as a group $N \in$ FreeAb, $Q \in$ Fin and special extension data $(\mathcal{I}, f_s)$.

The next three definitions introduce some notation that will be useful in our proofs below.

Definition 4.1. Let $H \in$ SpecialExt with $N, Q, (\mathcal{I}, f_s)$ as above. For $k \geqslant 2$ define $\tilde{f}_k \colon Q^k \to N$ by

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

Definition 4.2 (Left A-count). Let A, B be two disjoint sets and $w = v_1 \cdots v_n$ with $v_i \in A \cup B \cup A^{-1} \cup B^{-1}$. For each $p \in [1, n]$ let

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

which we call the *left A-count of w at position p*. Define $\mathrm{sgn}(w, A, p) = (-1)^{k_p}$.

The digit $\mathrm{sgn}(w, A, p)$ 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 4.3. Let $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ be a (Q, τ)-presentation for a group G, and let $\mathcal{I} \subseteq \mathcal{X}$, $\mathcal{I}_{\mathcal{X}} = \{x \in \mathcal{X} \mid \tau(x) \in \mathcal{I}\}$ denote the preimage of $\mathcal{I}$ under the bijection $\tau|_{\mathcal{X}} \colon \mathcal{X} \to Q$. 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 of $\mathrm{sgn}(r, \mathcal{I}_{\mathcal{X}}, p)$ for each $p \in [1, |r|]$.

Example 4.4. 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
$$\gamma(r) = x_1 y_1 x_3^{-1} x_3 y_2 x_1^{-1} x_2^{-1} y_1^{-1} x_1^{-1}$$

The purpose of defining γ in this way will become evident in the proof of Lemma 4.6.

Next we define a way to construct a system of equations from a presentation which will be useful for analysing epimorphism onto the class SpecialExt, analogously to the construction in Definition 3.1 for direct products.

Definition 4.5 (Presentation to system of equations for SpecialExt)**.** Let $H \in$ SpecialExt be an N by Q extension with special extension data $(\mathcal{I}, f_s)$, $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ a (Q, τ)-presentation for a group G, $\mathcal{I} \subseteq \mathcal{X}$, $\mathbb{X}, \mathbb{Y}$ alphabets with $\mathcal{X} \cup \mathcal{X}^{-1}$ in bijection with $\mathbb{X}$ and $\mathcal{Y} \cup \mathcal{Y}^{-1}$ in bijection with $\mathbb{Y}$ via
$$\zeta \colon x_j \mapsto X_j, \quad x_j^{-1} \mapsto X_j^{-1}, \quad y_j \mapsto Y_j, \quad y_j^{-1} \mapsto Y_j^{-1},$$
$\mathcal{I}_{\mathcal{X}} = \{x \in \mathcal{X} \mid \tau(x) \in \mathcal{I}\}$ the preimage of $\mathcal{I}$ under the bijection $\tau|_{\mathcal{X}} \colon \mathcal{X} \to Q$, γ as in Definition 4.3, and $\tilde{f}_k$ as in Definition 4.1. For $i \in [1, |\mathcal{R}|]$ assume each $r_i \in \mathcal{R}$ has the form
$$r_i = v_{i,1} \ldots v_{i,|r_i|}$$
with $v_{i,j} \in \mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1}$. Define $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$ to be 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 $\mathbb{X} \cup \mathbb{Y}$ with a single constant. It is clear from the above definitions that it can be written in polynomial time. We will now show how it arises in the context of epimorphism to SpecialExt.

Recall the decision problem EQUATIONSSUBSPAN.

Lemma 4.6. *Let* $G \in$ FinPres, $N \in$ FreeAb, $Q \in$ Fin *and* $H \in$ SpecialExt *where* H *is a* 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 $\langle \mathcal{X} \cup \mathcal{Y} \mid \mathcal{R} \rangle$ for G, 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 2.5 and Remark 2.6, 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 $\kappa(w) = ns(1_Q)$

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

For $r \in \mathcal{R}$ let $r = v_1 \cdots v_k$ with $v_i \in (\mathcal{X} \cup \mathcal{Y}) \cup (\mathcal{X} \cup \mathcal{Y})^{-1}$. Note that 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 have
$$1_N = \kappa(r) = \kappa(v_1)\kappa(v_2)\cdots\kappa(v_k) = \pi_N(\kappa(v_1))s(v_1')\pi_N(\kappa(v_2))s(v_2')\cdots\pi_N(\kappa(v_k))s(v_k').$$

By inserting $s(v_1')^{-1}s(v_1')$ after $\pi_N(\kappa(v_2))$, $s(v_2')^{-1}s(v_1')^{-1}s(v_1')s(v_2')$ after $\pi_N(\kappa(v_3))$ and so on, we obtain
$$1_N = \pi_N(\kappa(v_1))[{}^{s(v_1')}\pi_N(\kappa(v_2))][{}^{s(v_1')s(v_2')}\pi_N(\kappa(v_3))]\cdots[{}^{s(v_1')\cdots s(v_k')}\pi_N(\kappa(v_k))]\ s(v_1')\cdots s(v_k') \tag{4.1}$$

Let us first deal with the term $s(v'_1) \cdots s(v'_k)$ at the end of Eq. (4.1). 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

$$s(v'_1)s(v'_2)s(v'_3) = f_s(v'_1, v'_2)s(v'_1 v'_2)s(v'_3) = f_s(v'_1, v'_2)f_s(v'_1 v'_2, v'_3)s(v'_1 v'_2 v'_3)$$
$$= \tilde{f}_3(v'_1, v'_2, v'_3)s(v'_1 v'_2 v'_3).$$

Repeating this we obtain

$$\begin{aligned}
s(v'_1) \cdots s(v'_k) &= \tilde{f}_k(v'_1, \dots, v'_k)s(v'_1 \cdots v'_k) \\
&= \tilde{f}_k(v'_1, \dots, v'_k)s(\tau(v_1 \cdots v_k)) \\
&= \tilde{f}_k(v'_1, \dots, v'_k)s(\tau(r)) \\
&= \tilde{f}_k(v'_1, \dots, v'_k)
\end{aligned} \tag{4.2}$$

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. (4.1). Recall from Definition 4.3 that $\mathcal{I}_\mathcal{X}$ is the preimage of $\mathcal{I} \subseteq Q$ under the bijection $\tau|_\mathcal{X}$. 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 $n \mapsto n$, and conjugation by $s(\tau(v_i))$ sends $n \mapsto n$ if $v_i \in \mathcal{X} \setminus \mathcal{I}_X$, and $n \mapsto n^{-1}$ if $v_i \in \mathcal{I}_X$. Therefore conjugation by $s(v'_1) \cdots s(v'_{p-1})$ sends $\pi_N(\kappa(v_p))$ to $\pi_N(\kappa(v_p))^{\mathrm{sgn}(r,\mathcal{I},p)} = \gamma(\pi_N(\kappa(v_p)))$ by Definition 4.3, so

$$\begin{aligned}
&\pi_N(\kappa(v_1))[^{s(v'_1)}\pi_N(\kappa(v_2))][^{s(v'_1)s(v'_2)}\pi_N(\kappa(v_3))] \cdots [^{s(v'_1) \cdots s(v'_k)}\pi_N(\kappa(v_k))] \\
&= \gamma(\pi_N(\kappa(v_1))\pi_N(\kappa(v_2)) \cdots \pi_N(\kappa(v_k))) \\
&= \gamma(\pi_N(\kappa(v_1 \cdots v_k))) \\
&= \gamma(\pi_N(r)).
\end{aligned}$$

We have shown that Eq. (4.1) becomes

$$1_N = \gamma(\pi_N(r))\tilde{f}_k(v'_1, \dots, v'_k) \tag{4.3}$$

Let $\sigma = \pi_N \circ \kappa \circ \zeta^{-1}$ where ζ is the bijection as in Definition 4.5. Then $\sigma \colon \mathbb{X} \cup \mathbb{Y} \to N$ is the map

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

For $i \in [1, m]$ the equation u_i is obtained from $r_i = v_{i,1} \dots v_{i,|r_i|}$ with $v_{i,j} \in \mathcal{X} \cup \mathcal{Y} \cup \mathcal{X}^{-1} \cup \mathcal{Y}^{-1}$ of the form

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

so

$$\sigma(u_i) = \gamma(\pi_N(\kappa(r_i)))\tilde{f}_{|r_i|}(\tau(v_{i,1}), \dots, \tau(v_{i,|r_i|})) = 1_N$$

by Eq. (4.3), 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 $\zeta(w) \in \mathbb{Y}^*$ satisfies

$$\sigma(\zeta(w)) = \pi_N(\kappa(\zeta^{-1}(\zeta(w))))$$

$$= \pi_N(\kappa(w)) = n$$

which means $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle = N$, so 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 $\sigma \colon \mathcal{X} \cup \mathcal{Y} \to N$ 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 is a homomorphism $\kappa \colon G \to H$ such that τ, κ satisfy conditions (b) and (c') of Lemma 2.5 and Remark 2.6, thereby proving the existence of an epimorphism from G to H.

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

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

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

Then for any $w = v_1 \ldots v_n$ 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 $v_i' = \tau(v_i)$ as before. Inserting $s(v_1') \cdots s(v_j') s(v_j')^{-1} \cdots s(v_1')^{-1}$ we obtain

$$\begin{aligned}
\kappa(w) &= \sigma(\zeta(v_1))^{s(v_1')} \sigma(\zeta(v_2))^{s(v_1') s(v_2')} \sigma(\zeta(v_3)) \cdots {}^{s(v_1') \cdots s(v_{n-1}')} \sigma(\zeta(v_n)) s(v_1') \cdots s(v_n') \\
&= \gamma(\sigma(\zeta(v_1)) \cdots \sigma(\zeta(v_k))) s(v_1') \cdots s(v_n') \\
&= \gamma(\sigma(\zeta(w))) \tilde{f}_k(v_1', \ldots, v_k') s(\tau(v_1 \cdots v_k)) \quad \text{by Eq. (4.2)} \\
&= \gamma(\sigma(\zeta(w))) \tilde{f}_k(v_1', \ldots, v_k') s(\tau(w)).
\end{aligned}$$

If $w \in \mathcal{R}$ then $\tau(w) = 1_Q$ so $s(\tau(w)) = 1_N$ 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 $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, f_s)$ so applying σ we have $\kappa(w) = 1_N$, so by Lemma 1.1 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

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

where $n = \gamma(\sigma(\zeta(w))) \tilde{f}_k(v_1', \ldots, v_k') \in N$ so condition (b) of Lemma 2.5 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

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

and $\tau(\zeta^{-1}(w)) = 1_Q$ because $\ker(\tau) = \langle \mathcal{Y} \rangle$, so $\kappa(\zeta^{-1}(w)) = n s(1_Q)$ giving condition (c') of Remark 2.6, thus showing there exists an epimorphism from G to H. $\square$

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

Recall from Definition 3.3 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 4.7. *Let*

(1) N be an infinite cyclic group $\langle x \rangle$

(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 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) EQUATIONSSUBSPAN *returns 'Yes' on input* N *and* $(u_i)_{[1,m]}$

(2) 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

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

to $(u_i)_{[1,m]}$ with $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle = N$, which is also a solution to $(\mathsf{CNF}(u_i))_{[1,m]}$ by Lemma 1.2. Then 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

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

for $j \in [1, t], k \in [1, \ell]$, which holds if and only if

$$\sum_{j=1}^t f_j \alpha_{(i,j)} + \sum_{k=1}^\ell f_{t+k} \beta_{(i,k)} + b_i = 0. \tag{4.4}$$

Recall from Definition 3.3 that

$$A = \begin{pmatrix} \alpha_{(1,1)} & \cdots & \alpha_{(1,t)} & \beta_{(1,1)} & \cdots & \beta_{(1,\ell)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{(m,1)} & \cdots & \alpha_{(m,t)} & \beta_{(m,1)} & \cdots & \beta_{(m,\ell)} \end{pmatrix}, \ b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

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

$$\begin{aligned} A\nu + b &= \begin{pmatrix} \alpha_{(1,1)} & \cdots & \alpha_{(1,t)} & \beta_{(1,1)} & \cdots & \beta_{(1,\ell)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{(m,1)} & \cdots & \alpha_{(m,t)} & \beta_{(m,1)} & \cdots & \beta_{(m,\ell)} \end{pmatrix} \begin{pmatrix} f_1 \\ \vdots \\ f_{t+\ell} \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_{t+\ell} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{j=1}^t f_j \alpha_{(1,j)} + \sum_{j=1}^\ell f_{t+j} \beta_{(1,j)} + b_1 \\ \vdots \\ \sum_{j=1}^t f_j \alpha_{(m,j)} + \sum_{j=1}^\ell f_{t+j} \beta_{(m,j)} + b_m \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \text{ by Eq. (4.4).} \end{aligned} \tag{4.5}$$

Since $\langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle = N$, for all $h \in N$ there exists $w \in \mathbb{Y}^*$ such that $\sigma(w) = h$, so for all $z \in \mathbb{Z}$ there exists $w \in \mathbb{Y}^*$ such that $\varphi(\sigma(w)) = z$ where $\varphi \colon N \to \mathbb{Z}$ is the natural isomorphism defined in Subsection 1.1. 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 $a_i = |w|_{Y_i} - |w|_{Y_i^{-1}}$, so $z \in \mathrm{span}(c_{t+1}, \ldots, c_n)$, so 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 $\mathrm{span}((\nu|_\ell)^T) = \mathbb{Z}$ then every $z \in \mathbb{Z}$ can be expressed as

$$z = a_1 \nu_{t+1} + \cdots + a_\ell \nu_{t+\ell}$$

for $a_i \in \mathbb{Z}$, so for each $x^z \in N$ there exists $w = Y_1^{a_1} \cdots Y_1^{\nu_{a_\ell}} \in \mathbb{Y}^*$ so that $\sigma(w) = x^{a_1 \nu_{t+1} + \cdots + a_\ell \nu_{t+\ell}} = x^z$, so $N \subseteq \langle \sigma(Y_1), \ldots, \sigma(Y_\ell) \rangle$. Since $A\nu + b = 0$, by Definition 3.3 we have $\sigma(u_i) = 1_N$ for $i \in [1, m]$ by the calculation in Eq. (4.5), so EQUATIONSSUBSPAN returns 'Yes'. $\qquad \square$

Combining the above results with the fact that will be proved in Section 6 that MATRIXSUBSPANB can be decided in polynomial time gives the following.

Theorem 4.8. Epi(FinPres, VirtCyclic) *is in* NP.

Proof. Let $G \in$ FinPres be given by a finite presentation $\langle \mathcal{G} \mid \mathcal{R} \rangle$ and $H \in$ SpecialExt a virtually cyclic group given by $N = \langle x \rangle$ an infinite cyclic, a multiplication table for $Q \in$ Fin, and special extension data $(\mathcal{I}, f_s)$. Using Lemma 4.6 we may verify the existence of an epimorphism from G to H by verifying that there exists an epimorphism $\tau \colon G \to H$, 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 $(u_i)_{[1, |\mathcal{R}|]}$ 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 $(A, b, |\mathcal{Y}|) = \mathsf{EqnMat}(1, (u_i)_{[1, |\mathcal{R}|]}, (\mathfrak{c}_i)_{[1, |\mathcal{R}|]})$
(5) return the solution to EQUATIONSSUBSPAN on input $(A, b, |\mathcal{Y}|)$.

The correctness of this algorithm follows from Lemmas 4.6 and 4.7. The time complexity is as follows:

(1) verifying in polynomial time that τ is an epimorphism follows from Lemma 2.1
(2) constructing a (Q, τ)-presentation is in P by Lemma 2.3, 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 $\mathsf{EqnMat}(1, (u_i)_{[1, |\mathcal{Y}|]}, (\mathfrak{c}_i)_{[1, |\mathcal{Y}|]})$ is in P by Lemma 3.5
(5) MATRIXSUBSPANB is solved in P by Proposition 6.16 (Subsection 6.2).

It follows that Epi(FinPres, VirtCyclic) is in NP. $\qquad \square$

5. Inverse restricted semi-direct targets

Using results from the previous two sections, we are able to extend the class of virtually abelian targets for which epimorphism from a finitely presented group is decidable, as follows.

Recall that RestrAbelSemi 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 $f_s = 1_N$ and for all $n \in N$,

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

Theorem 5.1. Epi(FinPres, RestrAbelSemi) *is in* NP.

Proof. Let $G \in$ FinPres be given by a finite presentation $\langle\, \mathcal{G} \mid \mathcal{R}\, \rangle$ and $H \in$ RestrAbelSemi given by an integer $d \in \mathbb{N}$ encoding $N \in$ FreeAb of rank d, a multiplication table for $Q \in$ Fin, and special extension data $(\mathcal{I}, 1_N)$.

Since RestrAbelSemi is a subclass of SpecialExt, by Lemma 4.6 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, EQUATIONSSUBSPAN returns 'Yes' on input N and $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, 1_N)$.

Note that since $f_s = 1_N$, $\mathsf{PresEqnB}(\mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}_\mathcal{X}, 1_N)$ 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 $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, 1_N)$ denoted $(u_i)_{[1,m]}$
- (4) return 'Yes' 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 3.6 and 4.6. The time complexity is as follows.

- (1) Step (1) is in NP by Lemma 2.1; this is the only non-deterministic step of our algorithm.
- (2) We can construct a (Q, τ)-presentationin P by Lemma 2.3, and $\mathcal{I}_\mathcal{X}$ is immediate.
- (3) Constructing $\mathsf{PresEqnB}(\tau, \mathcal{X}, \mathcal{Y}, \mathcal{R}, \mathcal{I}, 1_N)$ 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 3.5, and MATRIXSUB-SPANA is solved P by Proposition 6.13 (see Subsection 6.1).

Thus, our algorithm is in NP. $\qquad\square$

Proof of Theorem A. We have shown (modulo Theorem D to be proved in the next section) that Epi(FinPres, $\mathcal{T}$) is in NP for $\mathcal{T} =$ the class of direct products of an abelian and a finite group, the virtually cyclic groups, and RestrAbelSemi. Since each of these classes includes finite groups, NP-completeness follows from [7, Corollary 1.2] or Theorem 7.19. $\qquad\square$

6. PROVING MATRIXSUBSPANA AND MATRIXSUBSPANB ARE IN P

In this section we prove that the integer matrix problems MATRIXSUBSPANA and MATRIX-SUBSPANB can be decided in polynomial time. Recall that throughout this paper, integer matrices are assumed to be given with entries in binary. Throughout this section we let R denote either $\mathbb{Z}$ or $\mathbb{Z}_p$ for some prime p (the ring of integers mod p).

Definition 6.1 (Smith normal form and 1-count). Let $A \in R^{m \times n}$. We call (K, D, L) a *Smith normal form* (SNF) for A if $A = KDL$, $K \in \mathrm{GL}(m, R)$, $L \in \mathrm{GL}(n, R)$, and $D \in R^{m \times n}$ has the form

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

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 $0 \leqslant r \leqslant \min(m,n)$, each $\mathfrak{d}_i \neq 0$ such that $\mathfrak{d}_i \mid \mathfrak{d}_{i+1}$ for all $i \in [1, r-1]$. Note $\mathrm{rank}(D) = r$. When $R = \mathbb{Z}$ we also require $\mathfrak{d}_i > 0$ for $i \in [1, r]$.

We denote the number of units (invertible elements) of R on the diagonal of D as 1-count$(D) = \max\{i \mid \mathfrak{d}_i \in R^*\}$, so if $R = \mathbb{Z}$ then 1-count(D) is the number of 1s on the diagonal, and if $R = \mathbb{Z}_p$ then 1-count(D) is the number of non-zero entries on the diagonal.

Lemma 6.2 ([13, Proposition 3.2]). *If $R = \mathbb{Z}$, then the matrix D in Definition 6.1 is unique.*

Moreover for $A \in R^{m \times n}$ if $(K, D, L), (K'D', L')$ are both Smith normal forms for A then 1-count$(D) =$ 1-count(D'). Note that in many papers the Smith normal form for $A \in \mathbb{Z}^{m \times n}$ is defined just to be the matrix D.

If $A \in \mathbb{Z}_p^{m \times n}$ then (since $\mathbb{Z}_p$ is a field) multiplying left and right by elementary matrices one may easily obtain a Smith normal form for A where diagonal entries of D are either 1 or 0. For $A \in \mathbb{Z}^{m \times n}$ the problem requires more attention.

Theorem 6.3 (Computing SNF; [6]). *The following computational problem is in* P.

    Input: *a matrix $A \in \mathbb{Z}^{m \times n}$*
    Output: *compute $K \in \mathrm{GL}(m, \mathbb{Z}), L \in \mathrm{GL}(n, \mathbb{Z}), D \in \mathbb{Z}^{m \times n}$ such that (K, D, L) is a SNF for A.*

We also observe the following facts. The first is straightforward, and the second can be found in [6].

Lemma 6.4. *The following calculations can be achieved in polynomial time.*

   (1) Given $a_1, \ldots, a_s \in \mathbb{Z}$, calculate $\gcd(a_1, \ldots, a_s)$.
   (2) Given $A \in \mathrm{GL}(n, \mathbb{Z})$, calculate A^{-1}.

Putting the above results together, we have

Lemma 6.5. *The following algorithmic problem can be answered in polynomial time. On input $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$,*

   (1) decide if there exists $x \in \mathbb{Z}^n$ such that $Ax + b = 0$ (returning 'Yes/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 our problem.
   (1) Calculate an SNF (K, D, L) of A and set $r = \mathrm{rank}(D)$.
   (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 $i \in [1, r]$ then output 'No'. If $\mathfrak{b}_i \neq 0$ for some $i \in [r+1, m]$ then output 'No'. Else return 'Yes'. (Thus we may assume from here that $\mathfrak{b}_i/\mathfrak{d}_i \in \mathbb{Z}$ for each $i \in [1, r]$ and $\mathfrak{b}_i = 0$ for each $i \in [r+1, m]$.)
   (3) Denote the (i, j)-element of L^{-1} as $l_{(i,j)}$, u_i the $(r+i)$-th column of L^{-1} for $i \in [1, n-r]$, and $c_i = \sum_{j=1}^{r} l_{(i,j)}\mathfrak{b}_j/\mathfrak{d}_j$ for $i \in [1, n]$. Set $k = n - r$ and $c = (c_1 \ \cdots \ c_n)^T$, and output $u_1, \ldots, u_k \in \mathbb{Z}^n$ and $c \in \mathbb{Z}^n$.

Step (1) takes polynomial time by Theorem 6.3, steps (2) and (3) require the inverse of an integer matrix which can be obtained in polynomial time by Lemma 6.4, and basic calculations with integers written in binary which are polynomial time. Thus, our process takes polynomial time.

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

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

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

$$Dy = \begin{pmatrix} \mathfrak{d}_1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & & \vdots \\ 0 & \cdots & \mathfrak{d}_r & \cdots & 0 \\ \vdots & & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_r \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} \mathfrak{b}_1 \\ \vdots \\ \mathfrak{b}_r \\ \vdots \\ \mathfrak{b}_m \end{pmatrix} = \mathfrak{b}. \tag{6.1}$$

From Eq. (6.1) 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/No' in step (2). If 'Yes', let $a_i = \mathfrak{b}_i/\mathfrak{d}_i \in \mathbb{Z}$ for $i \in [1, r]$, so

$$\mathfrak{b} = (a_1\mathfrak{d}_1 \ \cdots \ a_r\mathfrak{d}_r \ 0 \ \cdots \ 0)^T$$

and in such case a solution has the form

$$y = (a_1 \ \cdots \ a_r \ t_{r+1} \ \cdots \ t_n)^T$$

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

$$x = L^{-1}y$$

$$= \begin{pmatrix} l_{(1,1)} & \cdots & l_{(1,n)} \\ \vdots & \ddots & \vdots \\ l_{(n,1)} & \cdots & l_{(n,n)} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_r \\ t_{r+1} \\ \vdots \\ t_n \end{pmatrix}$$

$$= \begin{pmatrix} l_{(1,1)}a_1 + \cdots + l_{(1,r)}a_r + l_{(1,r+1)}t_{r+1} + \cdots + l_{(1,n)}t_n \\ \vdots \\ l_{(n,1)}a_1 + \cdots + l_{(n,r)}a_r + l_{(n,r+1)}t_{r+1} + \cdots + l_{(n,n)}t_n \end{pmatrix}.$$

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 $x \in \mathrm{span}_c(u_1, \ldots, u_k)$. $\square$

Lemma 6.6. *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 $\mathrm{span}((V|_\ell)^T) = \mathbb{Z}^d$ and each column of V lies in $\mathrm{span}_b(U)$*

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

Proof. Assume there exists a matrix $V = \begin{pmatrix} v_1 & \cdots & v_d \end{pmatrix} \in \mathbb{Z}^{n \times d}$ such that $\mathrm{span}((V|_\ell)^T) = \mathbb{Z}^d$ and each column v_i of V lies in $\mathrm{span}_b(U)$. 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 $v_i \in \mathrm{span}_b(U)$, $w_i \in \mathrm{span}_c(U|_\ell)$, and so $\mathrm{span}(W^T) = \mathrm{span}((V|_\ell)^T) = \mathbb{Z}^d$.

Conversely, assume there exist a matrix $W = \begin{pmatrix} w_1 & \cdots & w_d \end{pmatrix} \in \mathbb{Z}^{\ell \times d}$ such that $\mathrm{span}(W^T) = \mathbb{Z}^d$ and each column w_i of W lies in $\mathrm{span}_c(U|_\ell)$. For each $i \in [1, d]$ there exist $\alpha_{i,j} \in \mathbb{Z}$ so 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 $v_i \in \mathbb{Z}^k$ 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 $V|_\ell = W$ so $\mathrm{span}((V|_\ell)^T) = \mathrm{span}(W^T) = \mathbb{Z}^d$, and each column of V is in $\mathrm{span}_b(U)$ by construction. $\square$

6.1. **Solving MatrixSubspanA.** In this subsection, we show that MATRIXSUBSPANA can be decided in polynomial time. We start with two simple observations. Recall that $R = \mathbb{Z}$ or $\mathbb{Z}_p$.

Lemma 6.7. *Let $A, B \in R^{m \times n}$ and $L \in \mathrm{GL}(n, R)$. If $A = BL$ then $\mathrm{span}(A) = \mathrm{span}(B)$.*

Proof. Recall that if $L \in \mathrm{GL}(n, R)$ then there exists a sequence of elementary matrices $E_1, \ldots, E_k \in R$ such that $E_1 \cdots E_k = L$. Let $B_s = BE_1 \cdots E_s$ for $s \in [1, k]$ and $B_0 = B$. The three types of elementary matrices coincide with 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 $\mathrm{span}(B_s)$.

Suppose E_{s+1} has the effect of replacing b_i by $b_i + cb_j$ for some $i \neq j \in [1, n], c \in \mathbb{Z}$, where b_i, b_j are columns of B_{s-1}. Assume w.l.o.g. $i < j$. If $z \in \mathrm{span}(B_s)$, there exist $a_1, \ldots, a_n \in \mathbb{Z}$ such that $z = a_1b_1 + \cdots a_nb_n$, so

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

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

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 $a_j + a_ic \in R$ so $z \in \mathrm{span}(B_sE_{s+1})$. This proves $\mathrm{span}(B_s) = \mathrm{span}(B_sE_{s+1})$. Thus all three operations preserve the span, so (by induction) $\mathrm{span}(B) = \mathrm{span}(BL)$. $\square$

Lemma 6.8. *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 exists $a_1, \ldots, a_\ell \in \mathbb{Z}$ such that*

$$a_1k_{1,j} + \cdots + a_\ell k_{\ell,j} = 1 \text{ and}$$
$$a_1k_{1,s} + \cdots + a_\ell k_{n,s} = 0 \text{ for } s \in [1, \ell] \text{ and } s \neq j.$$

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

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

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

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

$$c_{j,1}k_{1,j} + \cdots + c_{j,\ell}k_{\ell,j} = 1$$

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

The result follows for fixed $j \in [1,\ell]$ by setting $a_1 = c_{j,1}, \ldots, a_\ell = c_{j,\ell}$. $\square$

Using these facts, we obtain the following.

Lemma 6.9. *Let $A \in \mathbb{Z}^{\ell \times n}$ with SNF (K, D, L), and $d \in \mathbb{N}_+$. If 1-count$(D) \geqslant d$ 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. Since $A = KDL$, by Lemma 6.7 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 6.8, for each $j \in [1,\ell]$ there exists $a_1, \ldots, a_\ell \in \mathbb{Z}$ such that

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

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 $j \in [1,d]$, so $\mathrm{span}(V^T) = \mathbb{Z}^d$. $\square$

If $A \in \mathbb{Z}^{m \times n}$, let $[A]_p \in \mathbb{Z}_p^{m \times n}$ denote the matrix $(a_{i,j} \mod p)_{i \in [1,m], j \in [1,n]}$ 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.

Lemma 6.10. *Let $A \in R^{m \times n}$ with SNF (K, D, L) such that $\mathrm{rank}(D) = $ 1-count(D). If there exists $V \in R^{m \times d}$ such that $\mathrm{span}(V^T) = R^d$ and the columns of V lie in $\mathrm{span}(A)$ then 1-count$(D) \geqslant d$.*

Proof. Let 1-count$(D) = c$, observe that when $R = \mathbb{Z}$ we have KD as the $m \times d$ matrix whose first c columns are the first c columns of K, and remaining $d - c$ columns are $0 \in \mathbb{Z}^m$. In the case $R = \mathbb{Z}_p$, as $\mathbb{Z}_p$ is a field, then w.l.o.g assume all non-0 diagonals of D are 1.

By Lemma 6.7 $\mathrm{span}(A) = \mathrm{span}(KD)$, so the columns of V lie in $\mathrm{span}(KD)$. Denote v_i as the i-th column of V and $k_{i,j}$ as the i,j-th element of K. As $v_i \in \mathrm{span}(KD)$, for $j \in [1,d]$ there exists $t_{j,1}, \ldots, t_{j,c} \in R$ such that

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

and so

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

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

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

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

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

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 $\mathrm{rank}(AB) \leqslant \min\{\mathrm{rank}(A), \mathrm{rank}(B)\}$. Since $\mathrm{rank}(D) = d$ it follows that $c \geqslant d$. $\qquad\square$

Lemma 6.11. *Let p be a prime, $A \in \mathbb{Z}^{m \times n}$. If there exists $V \in \mathbb{Z}^{m \times d}$ such that the columns of V lie in $\mathrm{span}(A)$ and $\mathrm{span}(V^T) = \mathbb{Z}^d$, then there exists $W \in \mathbb{Z}_p^{m \times d}$ such that the columns of W lie in $\mathrm{span}_{\mathbb{Z}_p}([A]_p)$ and $\mathrm{span}_{\mathbb{Z}_p}(W^T) = \mathbb{Z}_p^d$.*

Proof. Assume there exists $V \in \mathbb{Z}^{m \times d}$ such that the columns of V lie in $\mathrm{span}(A)$ and $\mathrm{span}(V^T) = \mathbb{Z}^d$, then there exist $e_1, \ldots, e_d \in \mathrm{span}(V^T) = \mathbb{Z}^d$ and $f_1, \ldots, f_d \in \mathbb{Z}^m$ (the standard basis of dimension m) $f_1, \ldots, f_d \in \mathrm{span}(A)$. So let $V \in \mathbb{Z}^{m \times d}$ be the diagonal matrix with d entries of 1 on the diagonal then as $W = [V]_p$, that is, 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 so $\mathrm{span}(W^T) = \mathbb{Z}_p^d$. $\quad\square$

Corollary 6.12. *Let $A \in \mathbb{Z}^{m \times n}$, $\min(m,n) \geqslant d \in \mathbb{N}_+$, and (K, D, L) is an SNF for A. If there exists $V \in \mathbb{Z}^{m \times d}$ such that the columns of V lie in $\mathrm{span}(A)$ and $\mathrm{span}(V^T) = \mathbb{Z}^d$, then $1\text{-count}(D) \geqslant d$.*

Proof. If $1\text{-count}(D) = \mathrm{rank}(D)$ then Lemma 6.10 proves the claim. Else $1\text{-count}(D) < \mathrm{rank}(D)$.

By Lemma 6.11 for any prime p there will exist $W \in \mathbb{Z}_p^{m \times d}$ such that the columns of W lie in $\mathrm{span}_{\mathbb{Z}_p}([A]_p)$ and $\mathrm{span}_{\mathbb{Z}_p}(W^T) = \mathbb{Z}_p^d$. Let $c = 1\text{-count}(D)$ and $p \mid \mathfrak{d}_{c+1}$ (the first non-1 diagonal entry of $D \in \mathbb{Z}^{m \times n}$) and so $\mathrm{rank}([D]_p) = 1\text{-count}([D]_p)$. This gives two cases.

   (1) If there exists $V \in \mathbb{Z}^{m \times d}$ such that the columns of V lie in $\mathrm{span}(A)$ and $\mathrm{span}(V^T) = \mathbb{Z}^d$ and $1\text{-count}(D) = \mathrm{rank}(D)$, then $1\text{-count}(D) \geqslant d$.

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

$\square$

Proposition 6.13. MATRIXSUBSPANA *is in* P.

Proof. Recall that MATRIXSUBSPANA asks the following: given $A \in \mathbb{Z}^{m \times n}$, $d, \ell \in \mathbb{Z}$ where $0 \leqslant \ell < n$, does there exist $v_1, \ldots, v_d \in \mathbb{Z}^n$ such that $Av_i = 0$ for $i \in [1, d]$ and for the matrix $V = (v_1 \; \cdots \; v_d)$ we have $\mathrm{span}((V|_\ell)^T) = \mathbb{Z}^d$?

We solve MATRIXSUBSPANA by the following procedure:

(1) call the algorithm in Lemma 6.5 on input $A \in \mathbb{Z}^{m \times n}$ and $0 = b \in \mathbb{Z}^m$
(2) if this algorithm returns 'No', return 'No' to MATRIXSUBSPANA
(3) else let $u_1, \ldots, u_m, c \in \mathbb{Z}^n$ be the output of the procedure (here $c = 0$), set $U \in \mathbb{Z}^{n \times m}$ be the matrix whose i-th column is u_i
(4) Calculate the SNF (K, D, L) of $U|_\ell$. Thus $K \in \mathrm{GL}(\ell, \mathbb{Z}), L \in \mathrm{GL}(m, \mathbb{Z}), D \in \mathbb{Z}^{\ell \times m}$ and so $U|_\ell = KDL$.
(5) If $1\text{-count}(D) \geqslant d$ output 'Yes', otherwise if $1\text{-count}(D) < d$ output 'No'.

Step (1) is polynomial time by Lemma 6.5 and step (2) is polynomial time by Theorem 6.3 and step (3) 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 (2), then there does not exist $x \in \mathbb{Z}^n$ which satisfies $Ax = 0$, so we output 'No' for MATRIXSUBSPANA. Thus, w.l.o.g we may assume there exists a solution to the procedure in Lemma 6.5, which finds U and c such that $c = 0$ and $Ax = 0$ if and only if $x \in \mathrm{span}(U)$. We then can check if there exists $v_1, \ldots, v_d \in \mathrm{span}(U)$ for such that for matrix $V = (v_1 \; \cdots \; v_d)$, we have $\mathrm{span}((V|_\ell)^T) = \mathbb{Z}^d$, and by Lemma 6.6 V exists if and only if there exists $W \in \mathbb{Z}^{\ell \times d}$ such that $\mathrm{span}(W^T) = \mathbb{Z}^d$ and each column of W lies in $\mathrm{span}(U|_\ell)$. Using D of the SNF (K, D, L) calculated in step (4), by Lemma 6.9 and the contrapositive of Corollary 6.12 such a W exists if and only if $1\text{-count}(D) \geqslant d$, thus justifying the output in step (5). $\square$

6.2. Solving MatrixSubspanB.

In this subsection we show that MATRIXSUBSPANB is decidable in polynomial time. Note that our method in this subsection closely follows [3, Proposition 4.2 and Lemma 4.3].

First, we note the following.

Lemma 6.14. *For* $a_1, \ldots, a_s \in \mathbb{Z}$ *and* , $\mathrm{span}(\begin{bmatrix} a_1 & \cdots & a_s \end{bmatrix}) = \mathbb{Z}$ *if and only if* $\gcd(a_1, \ldots, a_s) = 1$.

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

Input: Given $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, $\ell \in \mathbb{Z}$ where $\ell \in [0, n-1]$.

Question: Does there exist an integer n-matrix $\nu = \begin{bmatrix} \nu_1 & \cdots & \nu_n \end{bmatrix}^T \in \mathbb{Z}^n$ such that $A\nu + b = 0$ and $\gcd(\nu_{n-\ell+1}, \ldots, \nu_n) = 1$.

Next we present some basic facts about gcd, generalising [3, Lemma 4.3].

Lemma 6.15. *Let* $n, k, \ell \in \mathbb{N}_+$.

(1) Let $U \in \mathbb{Z}^{\ell \times k}$ with SNF (K, D, L) and $r \in \mathbb{Z}^\ell$. There exists $\mu = (\mu_1 \; \cdots \; \mu_\ell)^T \in \mathrm{span}_r(U) \in \mathbb{Z}^\ell$ such that $\gcd(\mu_1, \ldots, \mu_\ell) = 1$ if and only if there exists $v = (v_1 \; \cdots \; v_\ell) \in \mathrm{span}_{K^{-1}r}(D) \in \mathbb{Z}^\ell$ such that $\gcd(v_1, \ldots, v_\ell) = 1$.
(2) If $s \geqslant 2$, $\mathfrak{d}, b_1, \ldots, b_s \in \mathbb{Z}$ such that $b_i \neq 0$ for at least one $i \in [2, s]$, and $\gcd(\mathfrak{d}, b_1, \ldots, b_s) = 1$, then there exists $x \in \mathbb{Z}$ such that $\gcd(x\mathfrak{d} + b_1, b_2, \ldots, b_s) = 1$.

(3) If $s, \mathfrak{d}_1, \ldots, \mathfrak{d}_n, b_1, \ldots, b_s \in \mathbb{Z}$ and $\mathfrak{d}_i \mid \mathfrak{d}_{i+1}$ for $i \in [1, n-1]$, then there exist $a_1, \ldots, a_s \in \mathbb{Z}$ such that

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

if and only if one the following holds:
   (a) $b_1, \ldots, b_s = 0$ and $\mathfrak{d}_1 \in \{-1, 1\}$
   (b) $\gcd(b_1, \ldots, b_s) = 1$
   (c) $\gcd(b_1, \ldots, b_s) = c > 1$, $\gcd(\mathfrak{d}_1, c) = 1$, and
      (i) $b_i \neq 0$ for some $i \in [2, s]$
      (ii) $s = 1$ and $c \equiv 1 \mod \mathfrak{d}_1$
      (iii) $b_2, \ldots, b_s = 0$ and $c \equiv 1 \mod \mathfrak{d}_1$ or $\mathfrak{d}_2 \neq 0$.

Proof. To prove item (1), assume there exists $\mu = (\mu_1 \cdots \mu_\ell)^T \in \text{span}_r(U)$ with $\gcd(\mu_1, \ldots, \mu_\ell) = 1$. Letting $v = K^{-1}\mu$, we have $v \in \text{span}_{K^{-1}r}(K^{-1}U)$. By Lemma 6.7 $\text{span}(K^{-1}U) = \text{span}(D)$ we have $v = (v_1 \cdots v_\ell)^T \in \text{span}_{K^{-1}r}(D)$. As $v = K^{-1}\mu$ and $K^{-1} \in \text{GL}(\ell, \mathbb{Z})$, there exists a sequence of elementary matrices $E_1 \cdots E_k = K^{-1}$, and multiplication by an elementary matrix does not change the gcd, so $\gcd(K^{-1}\mu) = \gcd(\mu)$, thus $\gcd(v) = \gcd(\mu) = 1$.

Item (2) is [3, Lemma 4.3].

This leaves item (3). Assume one of the conditions (a)–(c) hold. If $b_i = 0$ and $\mathfrak{d}_1 = \pm 1$ set $a_1 = 1$ and $a_j = 0$ for $j \geqslant 2$ and if $\gcd(b_1, \ldots, b_s) = 1$ then set $a_i = 0$. If $\gcd(b_1, \ldots, b_s) = c > 1$, $\gcd(\mathfrak{d}_1, c) = 1$, we have three subcases. If $b_i \neq 0$ for some $i \in [2, s]$, then by item (2) there exists $x \in \mathbb{Z}$ such that $\gcd(x\mathfrak{d}_1 + b_1, b_2, \ldots, b_s) = 1$ so set $a_1 = x$ and $a_2, \ldots, a_s = 0$. 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 $\alpha \in \mathbb{Z}$, so 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 $\alpha b_1 + \mathfrak{d} = 1$, and 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 $\mathfrak{d}_2, b_1 \neq 0$ so by item (2) there exists $x \in Z$ so that $\gcd(x\mathfrak{d}_1 + b_1, \mathfrak{d}_2) = 1$, so 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

$$\gcd(a_1 \mathfrak{d}_1 + b_1, \ldots, a_s \mathfrak{d}_s + b_s) = 1 \tag{6.2}$$

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 have $\gcd(a_1 \mathfrak{d}_1, \ldots, a_s \mathfrak{d}_s) > |\mathfrak{d}_1|$ which contradicts Eq. (6.2). 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. (6.2). 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. (6.2) 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. (6.2) 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). $\qquad \square$

Recall from p.25 that MATRIXSUBSPANB may be stated as follows: given $A \in \mathbb{Z}^{m \times n}$, $b \in \mathbb{Z}^m$, $\ell \in \mathbb{Z}$ where $\ell \in [0, n-1]$, decide if there is an integer n-matrix $\nu = (\nu_1, \ldots, \nu_n)^T \in \mathbb{Z}^n$ such that $A\nu + b = 0$ and $\gcd(\nu_{n-\ell+1}, \ldots, \nu_n) = 1$.

Proposition 6.16. 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 6.5 on input $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$
   (2) if this algorithm returns 'No', return 'No' to MATRIXSUBSPANB

(3) else 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, and set $U \in \mathbb{Z}^{n \times m}$ be the matrix whose i-th column is u_i

(4) compute the SNF (K, D, L) of $U|_\ell \in \mathbb{Z}^{\ell \times m}$. Thus $K \in \mathrm{GL}(\ell, \mathbb{Z})$, $L \in \mathrm{GL}(m, \mathbb{Z})$, $D \in \mathbb{Z}^{\ell \times m}$ with diagonal entries $\mathfrak{d}_i$ with $i \in [1, \ldots, \mathrm{rank}(D)]$ and $U|_\ell = KDL$. Set:
   - $\mathfrak{d}_i = 0$ for $i \in [\mathrm{rank}(D) + 1, \ell]$
   - $c = (c_1 \ \cdots \ c_\ell) = K^{-1}(c_{n-\ell+1}' \ \cdots \ c_n') \in \mathbb{Z}^\ell$.

(5) Return 'Yes' if one the following conditions hold, 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 $f \equiv 1 \mod \mathfrak{d}_1$
       (iii) $c_2, \ldots, c_\ell = 0$ and $f \equiv 1 \mod \mathfrak{d}_1$ or $\mathfrak{d}_2 \neq 0$.

Step (1) is polynomial time by Lemma 6.5, step (4) is polynomial time by Theorem 6.3, and step (5) is polynomial time by Lemma 6.4.

If 'No' is returned in step (2), then there does not exist $x \in \mathbb{Z}^n$ which satisfies $Ax + b = 0$, so we output 'No' for MATRIXSUBSPANB. Thus, w.l.o.g we may assume there exists a solution to the procedure in Lemma 6.5, which finds U and c' such that $Ax + b = 0$ if and only if $x \in \mathrm{span}_{c'}(U)$. Let $r = (c_{n-\ell+1}' \ \cdots \ c_n')^T \in \mathbb{Z}^\ell$, we then can check if there exists $\nu \in \mathrm{span}_{c'}(U)$ such that $\gcd(\nu_1 \ \cdots \ \nu_d) = 1$, and by Lemma 6.6 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 6.15 (Item 1) such a μ exists if and only if there exists $v = (v_1 \ \cdots \ v_\ell)^T \in \mathrm{span}_{K^{-1}b}(D)$ such that $\gcd(v_1, \ldots, v_\ell) = 1$. As $c = K^{-1}r$, all elements in $\mathrm{span}_c(D)$ take the form $a_1 \mathfrak{d}_1 + c_1 + \cdots + a_\ell \mathfrak{d}_\ell + c_\ell$ for $a_1, \ldots, a_\ell \in \mathbb{Z}$, so checking if v exists is equivalent to checking if there exists $a_1, \ldots, a_\ell \in \mathbb{Z}$ such that $\gcd(a_1\mathfrak{d}_1 + c_1, \ldots, a_\ell\mathfrak{d}_\ell + c_\ell) = 1$ which is solved in step (5) by Lemma 6.15 (Item 3). $\qquad\square$

Proof of Theorem D. Propositions 6.13 and 6.16 immediately give Theorem D. $\qquad\square$

7. Proof of Theorem B

We now turn our attention to epimorphism 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 2.1, this establishes that the epimorphism problem onto such a group is NP-complete (Theorem B). This complements the work of Kuperberg and Samperton, who proved an analogous result when the target is a finite simple group (see Subsection 8.2). Recall that for $\mathrm{Epi}(\mathrm{FinPres}, D_{2n})$, 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. Goldmann and Russell prove the following:

Theorem 7.1 ([4, 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.*

Fix

$$\left\langle\, s, t \mid s^2 = t^n = 1, \ sts = t^{-1} \,\right\rangle$$

as 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 automorphism group of D_{2n} is straightforward to compute (see, for example, [12]).

Lemma 7.2. *For $r, \mu \in \mathbb{Z}$ let $\varphi_{r,\mu} \colon D_{2n} \to D_{2n}$ be the map $s \mapsto st^r, t \mapsto t^\mu$. If $n \geqslant 3$, then $\mathrm{Aut}(D_{2n}) = \{\varphi_{r,\mu} \mid r \in [0, n-1], \mu \in [1, n-1], \gcd(\mu, n) = 1\}$.*

The proof of Theorem B is divided into three cases which require slightly different techniques.

7.1. **Odd Case.** For $n > 1$ odd, we will show that deciding whether a system of equations over D_{2n} has a solution can be reduced to $\mathrm{Epi}(\mathrm{FinPres}, D_{2n})$ in polynomial time.

Lemma 7.3. *If $n > 1$ is odd, then*

$$D_{2n} = \left\{\alpha_0 \, (^{\alpha_1} t) \cdots (^{\alpha_n} t) \mid \alpha_i \in \{1, s\}\right\}.$$

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 7.1 and the fact that

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 1. Computing exponents of t in Lemma 7.3

$t^n = 1$, we have $\{\alpha_0 t^{n-2\ell} \mid \alpha_0 \in \{1, s\}, \ell \in [0, n]\} = \{\alpha_0 t^r \mid \alpha_0 \in \{1, s\}, r \in [0, n-1]\}$, which proves the claim. $\qquad\square$

Lemma 7.4. *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 $\ell \in [1, n-1]$. 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 $2(r - \ell)$, and since $r, \ell \in [0, n-1]$ we have $r = \ell$. This implies the center is trivial for $n \geqslant 3$ since $x \in Z(D_{2n})$ implies x commutes with st and st^2. $\qquad\square$

Definition 7.5 (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

$$X_j \mapsto Y_{0,j} \cdot (^{Y_{1,j}} t) \cdot (^{Y_{2,j}} t) \cdots (^{Y_{n,j}} t), \qquad X_j^{-1} \mapsto (^{Y_{n,j}} t)^{-1} \cdots (^{Y_{1,j}} t)^{-1} \cdot Y_{0,j}^{-1}; \qquad j \in [1, k]$$
$$s \mapsto s, t \mapsto t, t^{-1} \mapsto t^{-1}.$$

Lemma 7.6. *Let $n, \mathbb{X}, \mathbb{Y}$ and ONF be as Definition 7.5. Let $(u_i)_{[1,m]}$ 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 7.3, replacing each variable X_j by the word $Y_{0,j} \, (^{Y_{1,j}} t) \cdots (^{Y_{n,j}} t) = \mathsf{ONF}(X_j)$ 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. $\qquad\square$

Next, we describe a way to build a finitely presented group from a system of equations over D_{2n}.

Definition 7.7 (Group presentation for odd dihedral case). Let $n, \mathbb{X}, \mathbb{Y}, \mathsf{ONF}$, and $(u_i)_{[1,m]}$ be as in Lemma 7.6. 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

$$
\lambda \colon \begin{cases} s & \mapsto a \\ t & \mapsto d, \qquad t^{-1} \mapsto d^{-1} \\ Y_{i,j} & \mapsto g_{i,j}, \qquad Y_{i,j}^{-1} \mapsto g_{i,j}^{-1}; \qquad i \in [0,n], j \in [1,k]. \end{cases}
$$

Then $G_o(n, (u_i)_{[1,m]})$ 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 7.8. It is clear that for n a fixed constant, the finite presentation for $G_o(n, (u_i)_{[1,m]})$ can be constructed in linear time in the size $k + \sum_{i=1}^{m} |u_i|$ of the system of equations.

The idea of this construction is to force any epimorphism from $G_o(n, (u_i)_{[1,m]})$ to D_{2n} to send a to $\varphi(s)$, d to $\varphi(t)$, and $g_{i,j}$ to $\{1, \varphi(s)\}$ 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 7.9. *If $\psi \colon G_o(n, (u_i)_{[1,m]}) \to D_{2n}$ is an epimorphism, then there exists $\varphi \in \mathrm{Aut}(D_{2n})$ such that*

$$
\psi \colon \begin{cases} a & \mapsto \varphi(s) \\ d & \mapsto \varphi(t) \\ g_{i,j} & \mapsto \gamma_{i,j} \in \langle \varphi(s) \rangle; \qquad i \in [0,n], j \in [1,k]. \end{cases}
$$

Proof. For readability we denote $G_o(n, (u_i)_{[1,m]})$ 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, which means 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 that $\psi(a) \in \{1, st^r \mid r \in [0, n-1]\}$ which is the set of all elements of order 2 in D_{2n}. If $\psi(a) = 1$, then by the relation $adad$, we have that $\psi(d)^2 = 1$ which is not possible, so $\psi(a) = st^r$ 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 $\psi(a)$ so by Lemma 7.4 $\langle \psi(a), \psi(g_{0,1}), \ldots, \psi(g_{n,k}) \rangle = \langle \psi(a) \rangle$.

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

$$
1 = \psi(adad) = st^r \alpha t^p st^r \alpha t^p = \begin{cases} st^r st^p st^r st^p = t^{-2r+2p} & \alpha = s \\ st^{r+p} st^{r+p} = 1 & \alpha = 1. \end{cases}
$$

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 $D_{2n} \ni t$ we have

$$
t = (t^p)^{i_0}(st^r)(t^p)^{i_1} \ldots (st^r)(t^p)^{i_{2m}} \quad \text{(the number of } s \text{ letters must be even)}
$$

$$
= t^{-pi_0} t^{-r-pi_1} t^{r+pi_2} t^{-r-pi_3} \ldots t^{-r-pi_{2m-1}} t^{r+pi_{2m}}
$$

$$
= t^{pi_0} t^{-pi_1} t^{pi_2} t^{-pi_3} \ldots t^{-pi_{2m-1}} t^{pi_{2m}} = (t^p)^{i_0 - i_1 + \cdots + i_{2m}}
$$

so 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 7.2 there exists $\varphi_{r,p} \in \mathrm{Aut}(D_{2n})$ such that $\varphi_{r,p}(t) = t^p = \psi(d)$ and $\varphi_{r,p}(s) = st^r = \psi(a)$. $\square$

Lemma 7.10. *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 $\psi: G_o(n, (u_i)_{[1,m]}) \to D_{2n}$ if and only if there exists a solution $\sigma: \mathbb{X} \to D_{2n}$ to the system $(u_i)_{[1,m]}$.*

Proof. Assume that there exists an epimorphism $\psi': G_o(n, (u_i)_{[1,m]}) \to D_{2n}$. By Lemma 7.9 there exists $\varphi \in \mathrm{Aut}(D_{2n})$ such that

$$\psi': \begin{cases} a & \mapsto \varphi(s) \\ d & \mapsto \varphi(t) \\ g_{i,j} & \mapsto \gamma'_{i,j} \in \langle \varphi(s) \rangle; \quad i \in [0, n], j \in [1, k] \end{cases}$$

so letting $\psi = \varphi^{-1} \circ \psi'$ we have an epimorphism

$$\psi: \begin{cases} a & \mapsto s \\ d & \mapsto t \\ g_{i,j} & \mapsto \gamma_{i,j} \in \langle s \rangle; \quad i \in [0, n], j \in [1, k]. \end{cases}$$

Define $\sigma: \mathbb{Y} \to \{1, s\}$ by $\sigma(Y_{i,j}) = \gamma_{i,j}, \sigma(Y_{i,j}^{-1}) = \gamma_{i,j}^{-1}$. Note that since $s^2 = 1$, then for all $Y_{i,j} \in \mathbb{Y}$, $\sigma(Y_{i,j}) = \sigma(Y_{i,j}^{-1})$, so w.l.o.g. we may assume $\mathbb{Y} = \{Y_{0,1}, \ldots, Y_{n,k}\}$. For $i \in [1, m]$ let $v_i \in (\{s, t, t^{-1}\} \cup \mathbb{Y}$ be 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

$$\begin{aligned} 1 = \psi(\lambda(\mathsf{ONF}(u_i))) &= \psi(\lambda(v_i(s, t, t^{-1}, Y_{0,1}, \ldots, Y_{n,k}))) \\ &= \psi(v_i(a, d, d^{-1}, g_{0,1}, \ldots, g_{n,k})) \\ &= v_i(s, t, t^{-1}, \gamma_{0,1}, \ldots, \gamma_{n,k}) \\ &= \sigma(v_i(s, t, t^{-1}, Y_{0,1}, \ldots, Y_{n,k})) = \sigma(\mathsf{ONF}(u_i)) \end{aligned}$$

so σ solves $(\mathsf{ONF}(u_i))_{[1,m]}$, and the result follows by Lemma 7.6.

Conversely, assume there exists a solution to $(u_i)_{[1,m]}$, so by Lemma 7.6 there exists a solution $\sigma: \mathbb{Y} \to \{1, s\}$ to $(\mathsf{ONF}(u_i))_{[1,m]}$, so for $i \in [1, m]$, if $\mathsf{ONF}(u_i) = v_i$ we have

$$\sigma(\mathsf{ONF}(u_i)) = \sigma(v_i(s, t, t^{-1}, \mathbb{Y})) = 1. \tag{7.1}$$

Define $\psi: \{a, d, d^{-1}\} \cup \mathcal{G}_{n,k} \cup \mathcal{G}_{n,k}^{-1} \to D_{2n}$ as the set map

$$\psi: \begin{cases} a & \mapsto s \\ d & \mapsto t, & d^{-1} \mapsto t^{-1} \\ g_{i,j} & \mapsto \sigma(Y_{i,j}) & g_{i,j}^{-1} \mapsto \sigma(Y_{i,j})^{-1}; & g_{i,j} \in \mathcal{G}. \end{cases}$$

Since the other relations in $G_o(n, (u_i)_{[1,m]})$ clearly map to 1 in D_{2n}, by Lemma 1.1 ψ induces a homomorphism from $G_o(n, (u_i)_{[1,m]})$ to D_{2n} if and only if $\psi(\lambda(\mathsf{ONF}(u_i))) = 1$ for all $i \in [1, m]$. We have

$$\begin{aligned} \psi(\lambda(\mathsf{ONF}(u_i))) &= \psi(\lambda(v_i(s, t, t^{-1}, \mathbb{Y}))) \\ &= v_i(s, t, t^{-1}, \sigma(\mathbb{Y})) = \sigma(v_i(s, t, t^{-1}, \mathbb{Y})) = 1 \quad \text{by Eq. (7.1)} \end{aligned}$$

so ψ is a homomorphism, which is surjective since $\psi(G_o(n, (u_i)_{[1,m]})) = \langle s, t \rangle = D_{2n}$. $\square$

7.2. Even Case. We now turn to the case where n is even. We begin by observing some preliminary facts.

Lemma 7.11. *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, st^b commute for $0 \leqslant a \leqslant b \leqslant n-1$ 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 gives 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 center), and $[t^r, s] = t^{2r}$ so t^r is in the centre if and only if $r = 0$ or $\frac{n}{2}$.

For item (c), if st^a and st^b commute then

$$1 = [st^a, st^b] = st^a st^b t^{-a} st^{-b} s = t^{-a} t^b t^{-a} t^b = t^{2(b-a)}$$

which means n divides $2(b-a)$, and $a, b \in [0, n-1]$ means $b - a \leqslant n-1$, so $b - a \in \{0, \frac{n}{2}\}$. $\square$

Our strategy requires a different proof for the 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 Epi(FinPres, D_{2n}). We alert the reader to the fact that here we are dealing with dihedral groups of different sizes. Fix

$$D_n = \left\langle s_1, t_1 \mid s_1^2 = t_1^{n/2} = 1, \; s_1 t_1 s_1 = t_1^{-1} \right\rangle$$
$$D_{2n} = \left\langle s_2, t_2 \mid s_2^2 = t_2^{n} \quad = 1, \; s_2 t_2 s_2 = t_2^{-1} \right\rangle$$

as presentations for the groups D_n, D_{2n} respectively.

Lemma 7.12. *Let $n = 4c$ where $c \in \mathbb{N}_+$, and*

$$H = \left\{ \alpha_0 \left(^{\alpha_1} t_2\right) \cdots \left(^{\alpha_{n/2}} t_2\right) \mid \alpha_i \in \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\} \right\}.$$

Then H is a subgroup of D_{2n} that is isomorphic to D_n.

Proof. Since $^{\alpha_i} t_2 = t_2$ for $\alpha_i \in \{1, t_2^{n/2}\}$, and $^{\alpha_i} t_2 = t_2^{-1}$ for $\alpha_i \in \{s_2, s_2 t_2^{n/2}\}$, we have

$$\alpha_0 \cdot \left(^{\alpha_1} t_2\right) \cdots \left(^{\alpha_{n/2}} t_2\right) = \alpha_0 t_2^{(n/2-\ell)-\ell} = \alpha_0 t_2^{n/2 - 2\ell}$$

where $\ell = \left| \{ i \in [1, \frac{n}{2}] \mid \alpha_i \in \{s_2, s_2 t_2^{n/2}\} \} \right|$. Thus

$$H = \left\{ \alpha_0 t_2^{n/2 - 2\ell} \mid \alpha_0 \in \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}, \ell \in [0, \tfrac{n}{2}] \right\}$$
$$= \left\{ \alpha_0 t_2^{2(n/4 - \ell)} \mid \alpha_0 \in \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}, \ell \in [0, \tfrac{n}{2}] \right\}.$$

Since $\frac{n}{2}$ is even, as ℓ ranges over $[0, \frac{n}{2}]$, we have the values in Table 7.2. From these values and

ℓ	0	1	$\cdots$	$\frac{n}{4} - 1$	$\frac{n}{4}$	$\frac{n}{4} + 1$	$\cdots$	$\frac{n}{2} - 1$	$\frac{n}{2}$
$\frac{n}{2} - 2\ell$	$\frac{n}{2}$	$\frac{n}{2} - 2$	$\cdots$	2	0	-2	$\cdots$	$\frac{-n}{2} + 2$	$\frac{-n}{2}$
$(\frac{n}{2} - 2\ell) + n$			$\cdots$			$n - 2$	$\cdots$	$\frac{n}{2} + 2$	$\frac{n}{2}$

TABLE 2. Computing exponents of t_2 in Lemma 7.12

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^{2r} for r ranging over $[0, \frac{n}{2} - 1]$, with all values of r realised in this range. Note that the additional term $t_2^{n/2}$ does not add any new powers of t_2 since $\frac{n}{2}$ is even. Thus

$$H = \left\{ \alpha_0 t_2^{2r} \mid \alpha_0 \in \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}, r \in [0, \tfrac{n}{2} - 1] \right\}$$

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 $s_1 \mapsto s_2, t_1 \mapsto t_2^2$. $\qquad\square$

Definition 7.13 (Even normal form). Let $n, k \in \mathbb{N}_+$ with n even, $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_k, X_k^{-1}\}$ and $\mathbb{Y} = \{Y_{0,1}, Y_{0,1}^{-1}, \ldots, Y_{n/2,k}, Y_{n/2,k}^{-1}\}$. 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

$$X_j \mapsto Y_{0,j} \cdot \left({}^{Y_{1,j}} t_2 \right) \cdots \left({}^{Y_{n/2,j}} t_2 \right), \qquad X_j^{-1} \mapsto \left({}^{Y_{n/2,j}} t_2 \right)^{-1} \cdots \left({}^{Y_{1,j}} t_2 \right)^{-1} \cdot Y_{0,j}^{-1}; \quad j \in [1, k]$$
$$s_1 \mapsto s_2 t_1 \mapsto t_2^2, t_1^{-1} \mapsto t_2^{-2}.$$

Lemma 7.14. *Let $n = 2^b c$ where $c > 1$ is odd and $b > 1$, $\mathbb{X}, \mathbb{Y}, \mathsf{ENF}$ as in Definition 7.13, and $(u_i)_{[1,m]}$ 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 $u_i(s_1, t_1, t_1^{-1}, X_1, X_1^{-1}, \ldots, X_k, X_k^{-1})$. By Lemma 7.12 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 from D_n to D_{2n}. Thus, we can rewrite each u_i as $\mathsf{ENF}(u_i)$ and the result follows. $\qquad\square$

In analogy with Definition 7.7 we construct a finitely presented group G_{4c} as follows.
Notation. For x, y letters, the string $[[\ldots [[x, y], y], \ldots], y]$ 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, which we denote as $[x, {}_n y]$. For example:

$$\begin{aligned} [x, {}_4 y] &= [[[[x, y], y], y], y] \\ &= [[[xyx^{-1}y^{-1}, y], y], y] \\ &= [[(xyx^{-1}y^{-1})y(xyx^{-1}y^{-1})^{-1}y^{-1}, y], y] \quad \text{and so on.} \end{aligned}$$

Definition 7.15 (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 be as in Definition 7.13, $(u_i)_{[1,m]}$ a system of equations in D_n with each equation $u_i \in (\mathbb{X} \cup \{s_1, t_1, t_1^{-1}\})^*$, and $\mathcal{G}_{n/2,k} = \{g_{i,j} \mid i \in [0, \frac{n}{2}], j \in [1, k]\}$ a set of $(\frac{n}{2} + 1)k$ distinct letters. Define $\lambda \colon (\{s_2, t_2^2, t_2^{-2}\} \cup \mathbb{Y})^* \to (\{a, d^2, d^{-2}\} \cup \mathcal{G}_{n/2,k} \cup \mathcal{G}_{n/2,k}^{-1})^*$ to be the monoid homomorphism induced by the bijection

$$\begin{aligned} s_2 &\mapsto a \\ t_2 &\mapsto d, & t_2^{-1} &\mapsto d^{-1} \\ Y_{i,j} &\mapsto g_{i,j}, & Y_{i,j}^{-1} &\mapsto g_{i,j}^{-1}; & i \in [0, n], j \in [1, k]. \end{aligned}$$

Then $G_{4c}(n, (u_i)_{[1,m]})$ 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 7.16. Similarly to G_o, it is clear that for n a fixed constant, the finite presentation for $G_{4c}(n, (u_i)_{[1,m]})$ can be constructed in linear time in the size $k + \sum_{i=1}^m |u_i|$ of the system of equations.

Lemma 7.17. *Let $n = 2^b c$ where $c > 1$ is odd and $b > 1$, and $G = G_{4c}(n, (u_i)_{[1,m]})$ as in Definition 7.15. If $\psi \colon G \to D_{2n}$ 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, 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, and $\mathcal{G} = \mathcal{G}_{n/2,k}$, 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 7.11 (a), $\psi(x) \in \{1, t^{n/2}, st^r\}$ for some $r \in [0, n-1]$. Let $M = \{r \in [0, n-1] \mid \exists x \in \{a\} \cup \mathcal{G}, \psi(x) = st^r\}$. 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 $0 \leqslant a < b \leqslant n-1$. Since all elements in $\{a\} \cup \mathcal{G}$ pairwise commute, by Lemma 7.11 (c) we have $b = a + \frac{n}{2}$.

Next we claim $\psi(d)^2 \neq 1$. For contradiction, assume $\psi \colon G_R \to D_{2n}$ is an epimorphism and $\psi(d)^2 = 1$, so by Lemma 7.11 (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 which contradicts 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

$$1 = \psi(adad) = st^r st^p st^r st^p = st^r st^p t^{-r} st^{-p} s = [st^r, st^p] = [\psi(a), \psi(d)]$$

which shows that $\psi(a)$ and $\psi(d)$ commute. By Lemma 7.11 (c) we have $\psi(d) = st^{r \pm n/2}$, and by the first claim $\psi(x)$ has this form or lies in the center for $x \in \mathcal{G}$, so $\psi(d)$ commutes with $\psi(x)$ for all $x \in \{a\} \cup \mathcal{G}$, so $\psi(G)$ is abelian, contradicting that ψ is surjective.

Otherwise, $\psi(a) \in \{1, t^{n/2}\}$. Suppose that $\psi(x) \in \{1, \frac{n}{2}\}$ for all $x \in \mathcal{G}$. Then $\psi(G)$ is abelian since every element can be expressed in the form $(t^{\frac{n}{2}})^i (\psi(d))^j$. Thus we may assume there is some $x \in \mathcal{G}$ with $\psi(x) = st^\ell$. Then by the relation $[d^c, {}_b x]$, 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

$$1 = \psi([d^c, {}_b x]) = \psi([d, {}_b x]) \quad \text{since } \psi(d)^2 = 1 \text{ and } c \text{ is odd}$$

$$= [st^p, {}_b st^\ell]$$

$$= [\cdots [[[[st^p, st^\ell], st^\ell], st^\ell], st^\ell], \cdots st^\ell] \quad (b \text{ times})$$

$$= [\cdots [[[t^{2(\ell-p)}, st^\ell], st^\ell], st^\ell], \cdots st^\ell] \quad (b-1 \text{ times})$$

$$= [\cdots [[t^{4(\ell-p)}, st^\ell], st^\ell], \cdots st^\ell] \quad (b-2 \text{ times})$$

$$= [\cdots [t^{8(\ell-p)}, st^\ell], \cdots st^\ell] \quad (b-3 \text{ times})$$

$$\vdots$$

$$= [t^{2^{b-1}(\ell-p)}, st^\ell] \quad (b-(b-1) \text{ times})$$

$$= t^{2^b(\ell-p)}.$$

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 $l - p = qc$.

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

$$
\begin{aligned}
st^\ell \cdot st^{\ell+qc} &= t^{qc} \\
(st^\ell)^{-1} \cdot st^{\ell+qc} &= t^{qc} \\
st^\ell \cdot (st^{\ell+qc})^{-1} &= t^{qc} \\
(st^\ell)^{-1} \cdot (st^{\ell+qc})^{-1} &= t^{-qc}
\end{aligned}
$$

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 has an even number of s letters, so the word will be a power of t^c. Since $c > 1$ this is not possible, so ψ is not surjective. (Note that at this step we rely on the hypothesis that $c > 1$ is odd, $ie.$ n is not a power of 2.)

Thus we may assume for the remainder of the proof that $\psi(d)^2 \neq 1$. By Lemma 7.11 (a) we have $\psi(d) = t^p$ for $p \in [0, \frac{n}{2} - 1] \cup [\frac{n}{2} + 1, n - 1]$.

If $\psi(a) \in \{1, t^{n/2}\}$, then by the relation $adad = 1$ in G we have

$$1 = \psi(adad) = \psi(a)\psi(d)\psi(a)\psi(d) = \psi(d)^2$$

which is a contradiction. Thus, $\psi(a) = st^r$ for some $r \in [0, n-1]$. By the first claim we have $\psi(g) \in \{1, t^{n/2}, st^r, st^{r\pm n/2}\}$ for all $g \in \mathcal{G}$.

To show that $\gcd(n, p) = 1$, we first note that

$$
\psi(G) = \left\langle \psi(a), \psi(d), \psi(\mathcal{G}) \right\rangle \subseteq \left\langle st^r, t^{n/2}, st^{r+n/2}, t^p \right\rangle = \left\langle st^r, t^p, t^{n/2} \right\rangle
$$

for $r \in [0, n-1]$ and $p \in [0, \frac{n}{2} - 1] \cup [\frac{n}{2} + 1, n - 1]$.

Since ψ surjects onto D_{2n} by hypothesis, t is spelled by a word $w \in \{st^r, t^{-r}s, t^p, t^{-p}, t^{n/2}\}^*$, where w has even number occurrences of s, and after commuting all $t^{n/2}$ factors to the left and applying $(st^r)(st^r) = 1$, has 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 $\epsilon_j \in \{-1, 1\}$, $k, i_j \in \mathbb{Z}$.

Since $(st^r)t^\eta = t^{-\eta}(st^r)$ and $(st^r)^{-1}t^\eta = t^{-r}st^\eta = t^{-\eta}t^{-r}s = t^{-\eta}(st^r)^{-1}$ for $\eta \in \mathbb{Z}$, moving all factors $(st^r)^{\epsilon_j}$ to the right via these rules we obtain

$$
\begin{aligned}
w &= (t^{n/2})^k (t^p)^{i_0 - i_1 + i_2 - \cdots + i_{2m}} (st^r)^{\epsilon_1 + \cdots + \epsilon_{2m}} \\
&= (t^{n/2})^k (t^p)^y (st^r)^{2z} \\
&= (t^{n/2})^k (t^p)^y \qquad (\text{ since } (st^r)^2 = 1)
\end{aligned}
$$

where $y = i_0 - i_1 + i_2 - \cdots + i_{2m}$ and $z = m - |\{j : \epsilon_j = -1\}|$. Thus $1 = \frac{kn}{2} + py$. (Note at this step we are using the hypothesis $b > 1$, since $b = 1$ would not give us an automorphism.) Writing $n = 2^b c$ with $b > 1$ we obtain

$$1 = \frac{kn}{2} + py = k2^{b-1}c + py$$

from which we can see $\gcd(p, 2) = 1$ and $\gcd(p, c) = 1$, which (inductively) implies $\gcd(p, 2^b c) = 1$.

Thus

$$
\psi \colon \begin{cases}
a & \mapsto s_2 t_2^r = \varphi(s_2) \\
d & \mapsto t_2^p = \varphi(t_2) \\
g_{i,j} & \mapsto \gamma_{i,j} \in \{\varphi(1), \varphi(s_2), \varphi(t_2^{n/2}), \varphi(s_2 t_2^{n/2})\}; \quad i \in [0, n], j \in [1, k]
\end{cases}
$$

where $\varphi \colon s_2 \mapsto s_2 t_2^r, t_2 \mapsto t_2^p$ is an automorphism by Lemma 7.2. $\qquad \square$

Lemma 7.18. *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 $G_{4c}(n, (u_i)_{[1,m]})$ be as in Definitions 7.13 and 7.15. Then there exists an epimorphism $\psi \colon G_{4c}(n, (u_i)_{[1,m]}) \to D_{2n}$ 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 $\psi' \colon G_{4c}(n, (u_i)_{[1,m]}) \to D_{2n}$. By Lemma 7.17 there exists $\varphi \in \mathrm{Aut}(D_{2n})$ such that

$$\psi' \colon \begin{cases} a & \mapsto \varphi(s_2) \\ d & \mapsto \varphi(t_2) \\ g_{i,j} & \mapsto \gamma'_{i,j} \in \{\varphi(1), \varphi(s_2), \varphi(t_2^{n/2}), \varphi(s_2 t_2^{n/2})\}; \quad i \in [0, n], j \in [1, k] \end{cases}$$

so letting $\psi = \varphi^{-1} \circ \psi'$ we have 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 $\sigma(Y_{i,j}) = \gamma_{i,j}, \sigma(Y_{i,j}^{-1}) = \gamma_{i,j}^{-1}$. Note that since $\gamma_{i,j}^2 = 1$ for all $i \in [0, n], j \in [1, k]$, then for all $Y_{i,j} \in \mathbb{Y}$, $\sigma(Y_{i,j}) = \sigma(Y_{i,j}^{-1})$, so w.l.o.g. we may 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_{4c}, $i \in [1, m]$ 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 7.14.

Conversely, assume there exists a solution to $(u_i)_{[1,m]}$. By Lemma 7.14, there exists a solution $\sigma \colon \mathbb{Y} \to \{1, s_2, t_2^{n/2}, s_2 t_2^{n/2}\}$ to $(\mathsf{ENF}(u_i))_{[1,m]}$. Thus, for $i \in [1, m]$, if $\mathsf{ENF}(u_i) = v_i$, we have:

$$\sigma(\mathsf{ENF}(u_i)) = \sigma(v_i(s_2, t_2^2, t_2^{-2}, \mathbb{Y})) = 1. \tag{7.2}$$

Define $\psi \colon \{a, d, d^{-1}\} \cup \mathcal{G}_{n/2,k} \cup \mathcal{G}_{n/2,k}^{-1} \to D_{2n}$ as the set map

$$\psi \colon \begin{cases} a & \mapsto s_2, \\ d & \mapsto t_2, \qquad d^{-1} \mapsto t_2^{-1}, \\ g_{i,j} & \mapsto \sigma(Y_{i,j}), \qquad g_{i,j}^{-1} \mapsto \sigma(Y_{i,j})^{-1}; \qquad g_{i,j} \in \mathcal{G}_{n/2,k}. \end{cases}$$

By construction (Definition 7.15), it is clear that the relations a^2, d^n, $adad$, $[g, a]$, $[g, g']$, and g^2 map to 1 in D_{2n} for all $g, g' \in \mathcal{G}_{n/2,k}$. 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 $[t_2^c, \psi(g)] = 1$ so $[t_2^c, {}_b\, \psi(g)] = 1$. 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 $[t^c, st^r] = t^c st^r t^{-c} t^{-r} s = t^c st^{-c} s = t^{2c}$ we have

$$\begin{aligned} \psi([d^c, {}_b\, g]) &= [t^c, {}_b\, st^r] \quad \text{since } \psi(d)^2 = 1 \text{ and } c \text{ is odd} \\ &= [\cdots [[[[t^c, st^r], st^r], st^r], st^r], \cdots st^r] \quad (b \text{ times}) \\ &= [\cdots [[[t^{2c}, st^r], st^r], st^r], \cdots st^r] \quad (b - 1 \text{ times}) \\ &= [\cdots [[t^{4c}, st^r], st^r], \cdots st^r] \quad (b - 2 \text{ times}) \\ &= [\cdots [t^{8c}, st^r], \cdots st^r] \quad (b - 3 \text{ times}) \\ &\;\;\vdots \\ &= [t^{2^{b-1}c}, st^r] \quad (b - (b - 1) \text{ times}) \end{aligned}$$

$$=t^{2^b c} = 1.$$

(Note that this calculation that shows why we have chosen to write d^c in our nested commutator.) For ψ to induce a homomorphism $G_{4c}(n, (u_i)_{[1,m]})$ to D_{2n}, it remains to check if $\psi(\lambda(\mathsf{ENF}(u_i))) = 1$ for $i \in [1, m]$. We have

$$\psi(\lambda(\mathsf{ENF}(u_i))) = \psi(\lambda(v_i(s_2, t_2^2, t_2^{-2}, \mathbb{Y})))$$
$$= v_i(s_2, t_2^2, t_2^{-2}, \sigma(\mathbb{Y})) = \sigma(v_i(s_2, t_2^2, t_2^{-2}, \mathbb{Y})) = 1 \quad \text{by Eq. (7.2).}$$

Thus by Lemma 1.1, ψ is a homomorphism, which is surjective since $\psi(G_{4c}(n, (u_i)_{[1,m]})) = \langle s_2, t_2 \rangle = D_{2n}$. $\qquad\square$

Theorem 7.19. *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 $\mathrm{Epi}(\mathrm{FinPres}, D_{2n})$ *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 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 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 $G_o(n, (u_i)_{[1,m]})$ as defined in Definition 7.7. This can be achieved in polynomial time by Remark 7.8. By Lemma 7.10, a solution to $(u_i)_{[1,m]}$ exists if and only if there exists an epimorphism from $G_o(n, (u_i)_{[1,m]})$ to D_{2n}.

Let $n = 2^b c$ where $b > 1$ and $c > 1$ is 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 $G_{4c}(n, (u_i)_{[1,m]})$ as defined in Definition 7.15 (in polynomial time by Remark 7.16). By Lemma 7.18, a solution to $(u_i)_{[1,m]}$ exists if and only if there exists an epimorphism from $G_{4c}(n, (u_i)_{[1,m]})$ to D_{2n}.

Since D_{2n} is non-abelian for $n > 1$, the result follows from Theorem 7.1. $\qquad\square$

Remark 7.20. Note that the case $n = 2c$ is not covered by the even case proof since Lemmas 7.12 and 7.17 break down for this case. Rather than trying to modify these, we have a different approach as shown in the next subsection.

7.3. **Direct product of abelian and trivial center.** To deal with the remaining $n = 2c$ case, we proceed as follows.

We first note that for $c > 1$ odd, D_{4c} is isomorphic to $D_{2c} \times C_2$. (One way to show this is via Tietze transformations: starting from $D_{4c} = \langle s, t \mid t^{2c}, s^2, stst \rangle$, add $x = t^c, y = t^2$, then remove $t = xy^{-\lfloor \frac{c}{2} \rfloor}$). By Lemma 7.4, $Z(D_{2c}) = \{1\}$.

Lemma 7.21. *Let G be a finitely presented group, A an abelian group, and B a group with trivial center. There is an epimorphism from $G \times A$ to $B \times A$ if and only if there is 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 $\pi_B((x, y)) = x$ 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 $\psi((1, z)) \in Z(B)$. Thus $\psi((1, z)) = 1$ for all $z \in A$ since B has trivial center. Since ψ is an epimorphism, for each $b \in B$ there exists $(x, y) \in G \times A$ so

that $\psi((x, y)) = b$. Then

$$b = \psi((x, y)) = \psi((x, 1))\psi((1, y)) = \psi((x, 1))$$

since $y \in A$, so ψ restricted to G is an epimorphism.

Conversely if $\tau: G \to B$ is an epimorphism, then the map $\tau': G \times A \to B \times A$ defined by $\tau'((x, y)) = (\tau(x), y)$ is an epimorphism. □

Lemma 7.22 (Direct product with abelian and no center). *Let A be a finitely generated abelian group and B a finite group with the following properties.*

(1) Epi(FinPres, B) *is* NP-*hard*
(2) $Z(B) = \{1\}$.

Then Epi(FinPres, $B \times A$) *is* NP-*complete.*

Proof. Since B is finite, by Theorem 3.7, Epi(FinPres, $B \times A$) is in NP. We show it is NP-hard by showing that Epi(FinPres, B) is polynomial reducible to Epi(FinPres, $B \times A$). Let $\langle P \mid Q \rangle$ be a finite presentation for A.

On input a finite presentation $\mathcal{P} = \langle X \mid R \rangle$ for a group $G \in$ FinPres, construct a presentation $\mathcal{P}'$ for $G \times A$ by writing

$$\langle X \cup P \mid R \cup Q \cup \{[x, y] \mid x \in X, y \in P\} \rangle$$

which can clearly be done in linear time in the size of $\mathcal{P}$. By Lemma 7.21 Epi(FinPres, B) returns 'Yes' on input $\mathcal{P}$ if and only if Epi(FinPres, $B \times A$) returns 'Yes' on input $\mathcal{P}'$. □

Proof of Theorem B. Theorem 7.19 combined with Lemma 2.1 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 7.22 since D_{4c} is isomorphic to $D_{2c} \times C_2$, and $Z(D_{2c}) = \{1\}$. □

Remark 7.23. Note that D_{2n} is nilpotent if and only if n is a power of 2. It is unclear whether Theorem B extends to these groups, or if there is some way to show Epi(FinPres, D_{2^k}) is in P.

8. Proof of Theorem C

Theorem C collects together some known facts and observations to add to the list of cases for which an upper bound on the complexity of the epimorphism problem can be given.

8.1. Epimorphism onto free groups.
Recall the notation for systems of equations from Subsection 1.1. Let $m, n, d \in \mathbb{N}_+$, $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$, F_d be a free group of rank d with identity element $e \in F_d$, and $(u_i)_{[1,m]}$ a system of equations without constants over F_d, so each $u_i = u_i(\mathbb{X}) \in \mathbb{X}^*$. Define the *rank* of a solution $\sigma: \mathbb{X} \to F_d$ to be the rank of the free subgroup $\langle \sigma(X_1), \ldots, \sigma(X_n) \rangle$ of F_d. 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. Define the *rank* of the system without constants $(u_i)_{i \in [1,m]}$ to be the maximum rank over all solutions.

As an example, suppose $u = X^{-1}Y^{-1}XYZ^s$ is a system of one equation over F_d. Recall that $v \in F_d$ is a *primitive element* if it is not equal to a proper power. By [11] (see [8, 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 8.1 (Razborov [9, 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.*

Note that Razborov's algorithm runs via constructing "Makanin-Razborov diagrams", and the complexity to compute these is not known, most likely at least doubly exponential space (see for example [2, page 2]).

Lemma 8.2. Epi(FinPres, FreeGrp) *is decidable.*

Proof. Assume the input is a finite presentation $\langle g_1, \ldots, g_n \mid r_1, \ldots, r_m \rangle$ for a group $G \in$ FinPres, and $d \in \mathbb{N}_+$ specifies a target free group of rank d. Let $\mathcal{G} = \{g_1, g_1^{-1}, \ldots, g_n, g_n^{-1}\}$ and $\mathbb{X} = \{X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}\}$. Perform the following procedure:

(1) Fix a free group $H = \langle a_1, \ldots, a_d \rangle$.
(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 8.1 with input $(\lambda(r_j))_{[1,m]}$ over the group H, to compute the rank $\mathfrak{r} \in [0, n]$ of the system. If $\mathfrak{r} \geqslant d$, return 'Yes', else return 'No'.

The justification for the procedure is as follows. Let $h_1, \ldots, h_n \in H$. By Lemma 1.1, $\{X_i \mapsto h_i, X_i^{-1} \mapsto h_i^{-1} \mid i \in [1, n]\}$ 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 $\mathfrak{r} \geqslant d$ then there is a homomorphism κ from G onto a subgroup K of H such that K is free of rank $\mathfrak{r}$. Then K has some free basis, say $\{y_1, \ldots, y_{\mathfrak{r}}\}$ (which we do not have to compute) and there exists a subgroup

$$K' = \langle y_1, \ldots, y_d \rangle \text{ of } H \text{ and map } \tau \colon K \to K' \text{ defined by } \tau(y_i) = \begin{cases} y_i & i \leqslant d \\ 1 & i > d \end{cases}. \text{ Then } \tau \circ \kappa \text{ is a}$$

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 $\psi \colon G \to H$ is a solution to the system of rank d. $\qquad\square$

Remark 8.3. We were not able to prove the analogue of Theorem 3.7 for targets of the form $N \times Q$ when N is a free group of finite rank. Our attempt to do this explains why Lemma 3.2 is stated for an arbitrary group N, but we were not able to follow the same strategy as in Section 3 from that point.

Open question. Is EQUATIONSSUBSPAN decidable on input a system of equations (without constants) over N when N is a free group of finite rank?

In addition we can ask whether it is possible to give complexity bounds for computing the rank of a system of equations without constants over a free group (cf. Theorem 8.1), for example can this be done in EXPSPACE or PSPACE?

Open problem. Determine bounds for the complexity of computing the rank of a system of equations $(u_i)_{[1,m]}$ without constants over a free group F_d.

8.2. **Epimorphism onto non-abelian finite simple groups.** 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. Let H be a fixed, finite, non-abelian simple group. Kuperberg and Samperton [7, Corollary 1.2] prove the following problem is NP-complete.

Input: $M \in$ Hom and the promise that every non-trivial homomorphism from $\pi_1(M)$ to H is surjective

Question: Is there a non-trivial homomorphism from $\pi_1(M)$ to H?

It follows immediately that Epi(FinPres, H) is NP-hard, via the following reduction. On input 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 for $\pi_1(M)$. Then there is an epimorphism from $\pi_1(M)$ to H if and only if there is a non-trivial homomorphism from $\pi_1(M)$ to H.

This gives Item (2) of Theorem C. Item (3) follows from Lemma 7.22, Item (2) and Theorem 7.19.

8.3. Epimorphism onto abelian groups.

We can sharpen Theorem 3.7 for the case when the target group is abelian (the direct product of a free abelian group with a finite abelian group) to show that $\mathrm{Epi}(\mathrm{FinPres}, \mathrm{Abe})$ is in P. Here we give a brief outline of the proof, see [12] for more details (including the proof for the technical Lemma 8.5).

Notation. For a group G, $G_{ab} = G/[G:G]$ is the *abelianisation* of G. Note that if $\langle\, S \mid R \,\rangle$ is a presentation for G then $\langle\, S \mid R \cup \{[s,t]: s,t \in S\} \,\rangle$ is a presentation for G_{ab}, which can clearly be obtained in time linear in the size of $\langle\, S \mid R \,\rangle$. Recall that C_a denotes the cyclic group of order $a \in \mathbb{N}_+ \cup \{\infty\}$. By the well-known fundamental theorem of finitely generated abelian groups, if G is a finitely generated abelian group then

$$G \cong (C_\infty)^d \times C_{a_1} \times \cdots \times C_{a_k}$$

for some $d, a_1, \ldots, a_k \in \mathbb{N}_+$ where $a_i \mid a_{i+1}$ for $i \in [1, k-1]$. Such a description for a finitely generated abelian group will be called its *standard form.*

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 8.4. *Let $G \in \mathrm{FinPres}$ and $H \in \mathrm{Abe}$. Then there exists an epimorphism $\psi\colon G \to H$ if and only if there exists an epimorphism $\varphi\colon G_{ab} \to H$.*

The following technical lemma that allows us to check if an epimorphism exists between two finitely generated abelian groups given in standard form.

Lemma 8.5. *Let*

$$G \cong (C_\infty)^d \times C_{a_1} \times \cdots \times C_{a_s} \quad \text{and} \quad H \cong C_{c_1} \times \cdots \times C_{c_t}$$

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 $s \geqslant t - d$ and $c_{d+i} \mid a_i$ for $i \in [1, t-d]$.

Using Theorem 6.3 (computing the Smith normal form in P) on input finite presentations for G_1, G_2 we can compute integers $s, t, a_i, c_j \in \mathbb{N}_+$ such that $c_{i+1} \mid c_i$, $a_{i+1} \mid a_i$ and

$$G_1 \cong (C_\infty)^{d_1} \times C_{a_1} \times \cdots \times C_{a_s} \quad \text{and} \quad G_2 \cong (C_\infty)^{d_2} \times C_{c_1} \times \cdots \times C_{c_t}.$$

We require the free abelian rank of G_1 to be at least that of G_2 for an epimorphism to be possible. If so, applying Lemma 8.5 to

$$(C_\infty)^{d_1 - d_2} \times C_{a_1} \times \cdots \times C_{a_s} \quad \text{and} \quad C_{c_1} \times \cdots \times C_{c_t}$$

we can decide $\mathrm{Epi}(\mathrm{Abe}, \mathrm{Abe})$ in P. Putting this all together we obtain

Lemma 8.6. $\mathrm{Epi}(\mathrm{FinPres}, \mathrm{Abe})$ *is in P, where the input for both source and target groups are finite presentations.*

Proof. Let $G \in \mathrm{FinPres}$ and $H \in \mathrm{Abe}$. The following procedure solves our problem.

(1) Compute a presentation for G_{ab}.
(2) If $\mathrm{Epi}(\mathrm{Abe}, \mathrm{Abe})$ on input G_{ab} as the domain group and H as the target group returns 'Yes, return 'Yes'. Else return 'No'.

Step (1) constructs a finite presentation for G_{ab} in polynomial time, and step (2) is in P as described above. $\qquad\square$

Proof of Theorem C. Lemma 8.2 shows that epimorphism with finite rank free group targets is decidable. [7, Corollary 1.2] shows that epimorphism to a non-abelian finite simple group is NP-hard, combining with Lemma 2.1 we have the NP-complete result. Lemma 8.6 shows that epimorphism with abelian targets is in P. □

9. Concluding remarks

We have shown the epimorphism problem from the class of finitely presented groups to three classes of virtually abelian groups, and to a fixed finite non-nilpotent dihedral group, is NP-complete. In addition the problem is NP-complete when the target is a fixed group $B \times A$ where B a finite group with trivial center and Epi(FinPres, B) is NP-hard, and A is an abelian group. These results, together with observations that epimorphism from finitely presented groups to abelian groups is in P, to a fixed finite non-abelian simple group is NP-complete, to free groups is decidable, and from non-abelian nilpotent to non-abelian nilpotent is undecidable, represent the current state of knowledge for the problem.

For fixed finite targets a possible conjecture might be that epimorphism from finitely presented groups to a fixed group that is not nilpotent is NP-complete. A challenge problem is to decide for example whether Epi(FinPres, D_8) is in P or NP-hard.

The motivation for the present paper was to show that the problems considered by Friedl and Löh in [3] have reasonable complexity, and to extend the classes of virtually abelian and other targets for which the (uniform) epimorphism problem is decidable. Even though we have shown epimorphism is less difficult in those cases than Friedl and Löh might have indicated, we appear to be no closer to resolving their conjecture.

Conjecture 9.1 ([3, Conjecture 1.5])**.** *The uniform epimorphism problem onto the class of all finitely generated virtually abelian groups is not decidable.*

Acknowledgements

References

[1] Katalin A. Bencsáth, Marianna C. Bonanome, Margaret H. Dean, and Marcos Zyman. *Tools: Presentations and Their Calculus*, pages 5–7. Springer New York, New York, NY, 2013.

[2] Volker Diekert. Makanin's algorithm for solving word equations with regular constraints. Arbeitspapier, Technischer Bericht / Universität Stuttgart, Fakultät Informatik, Elektrotechnik und Informationstechnik, 1988.

[3] Stefan Friedl and Clara Löh. Epimorphism testing with virtually Abelian targets. *Confluentes Math.*, 13(1):61–78, 2021.

[4] Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. *Information and Computation*, 178(1):253–262, 2002.

[5] D.F. Holt and W. Plesken. *Perfect Groups*. Oxford mathematical monographs. Clarendon Press, 1989.

[6] Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. *SIAM J. Comput.*, 8(4):499–507, 1979.

[7] Greg Kuperberg and Eric Samperton. Computational complexity and 3-manifolds and zombies. *Geom. Topol.*, 22(6):3623–3670, 2018.

[8] Roger C. Lyndon and Paul E. Schupp. *Combinatorial group theory*. Classics in Mathematics. Springer-Verlag, Berlin, 2001. Reprint of the 1977 edition.

[9] A. A. Razborov. Systems of equations in a free group. *Izv. Akad. Nauk SSSR Ser. Mat.*, 48(4):779–832, 1984.

[10] V. N. Remeslennikov. An algorithmic problem for nilpotent groups and rings. *Sibirsk. Mat. Zh.*, 20(5):1077–1081, 1167, 1979.

[11] Marcel-Paul Schützenberger. Sur l'équation $a^{2+n} = b^{2+m}c^{2+p}$ dans un groupe libre. *C. R. Acad. Sci. Paris*, 248:2435–2436, 1959.

[12] Jerry Shen. *On the complexity of epimorphism problems for finitely presented groups*. PhD thesis, University of Technology Sydney, 2025. In preparation.

[13] Charles C. Sims. *Computation with finitely presented groups*, volume 48 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994.

SCHOOL OF MATHEMATICAL AND PHYSICAL SCIENCES, UNIVERSITY OF TECHNOLOGY SYDNEY, ULTIMO NSW 2007, AUSTRALIA
Email address: murray.elder@uts.edu.au

SCHOOL OF MATHEMATICAL AND PHYSICAL SCIENCES, UNIVERSITY OF TECHNOLOGY SYDNEY, ULTIMO NSW 2007, AUSTRALIA
Email address: qing.shen-1@uts.edu.au

INSTITUT FÜR FORMALE METHODEN DER INFORMATIK, UNIVERSITÄT STUTTGART, 70569 STUTTGART, GERMANY
Email address: armin.weiss@fmi.uni-stuttgart.de