CONFLUENTES MATHEMATICI

Stefan FRIEDL and Clara LÖH

Epimorphism testingwith virtually Abelian targets

Tome 13, nº 1 (2021), p. 61–78.
<http://cml.centre-mersenne.org/item/CML_2021__13_1_61_0/>

Confluentes Math.
13, 1 (2021) 61-78

EPIMORPHISM TESTING WITH VIRTUALLY ABELIAN TARGETS

STEFAN FRIEDL AND CLARA LÖH

Abstract. We show that the epimorphism problem is solvable for targets that are virtually cyclic or a product of an Abelian group and a finite group.

1. Introduction

Given two finitely presented groups Γ and Λ, it is natural to wonder if one can determine algorithmically whether there exists a group epimorphism $\Gamma \longrightarrow \Lambda$ or not. For example, the existence of a group epimorphism $\pi_1(M) \longrightarrow \pi_1(N)$ between the fundamental groups of oriented closed connected manifolds M and N is a first, rudimentary, necessary condition for the existence of a continuous map $M \longrightarrow N$ of degree ± 1, see [4, p. 178].

If the domain group Γ is trivial, then the epimorphism problem is equivalent to deciding whether the target Λ is trivial or not. However, it is well known that the triviality problem is undecidable [6]. Therefore, in general, the epimorphism problem is undecidable.

Thus it is reasonable to restrict oneself to suitable classes of groups. In this paper we want to study the following uniform version of the epimorphism problem.

Question 1.1 (uniform epimorphism problem). — *Let C and D be two classes of finitely presented groups. Does there exist an algorithm that solves the* uniform epimorphism problem from C onto D *? More precisely, does there exist an algorithm that takes as an input a finite presentation $\langle S \mid R\rangle$ of a group in C and a finite presentation $\langle S' \mid R'\rangle$ of a group in D and that determines whether there exists an epimorphism $\bigl|\langle S \mid R\rangle\bigr| \longrightarrow \bigl|\langle S' \mid R'\rangle\bigr|$ or not. When C is the class of all finitely presented groups, then we refer to the above as the* uniform epimorphism problem onto D.

Example 1.2. —

- As discussed above, the uniform epimorphism problem is undecidable whenever C contains the trivial group and D equals the class of all finitely presented groups.
- Let $C = D$ be the class of all finitely presented nilpotent groups. Remeslennikov showed that the uniform epimorphism problem from C to D is *not* decidable [7]. In particular the uniform epimorphism problem onto C is undecidable. The proof by Remeslennikov is based on a reduction to the unsolvability of Hilbert's tenth problem.

In contrast note that if D is the class of finite groups or the class of Abelian groups, then the uniform epimorphism problem onto D is actually solvable. Indeed,

2010 *Mathematics Subject Classification:* 20E18, 20F65.
Keywords: residual properties of groups, algorithms on groups.

for finite targets, we can compute the whole set of epimorphisms (Proposition 5.2), for Abelian targets, we can explicitly compute the abelianisation of the domain group and apply the structure theory of finitely generated Abelian groups.

It is natural to ask whether the uniform epimorphism problem is solvable for classes of groups that are "close" to being Abelian or finite. This leads us to the following question.

QUESTION 1.3. — *Is the uniform epimorphism problem onto the class of virtually Abelian groups solvable?*

Our main result gives a partial answer to Question 1.3.

THEOREM 1.4. —

- *The uniform epimorphism problem onto the class of groups that are a direct product of a finitely generated Abelian group with a finite group is solvable* (*see Theorem 5.5 for the precise formulation*).
- *The uniform epimorphism problem onto the class of groups that are virtually cyclic is solvable* (*see Theorem 5.6 for the precise formulation*).

As the epimorphism problem for virtually Abelian targets leads to a similar problem in linear algebra (Section 3.2) as in the above case of nilpotent targets studied by Remeslennikov [7], the following is plausible:

CONJECTURE 1.5. — *The uniform epimorphism problem onto the class of all finitely generated virtually Abelian groups is* not *decidable.*

We also have two questions on the two opposite rays of Bridson's universe of groups.

QUESTION 1.6. —

- *Let D be the class of groups that are isomorphic to subgroups of products of a finitely generated Abelian group and a finite group. Is the uniform epimorphism problem onto D solvable?*
- *Let H be the class of hyperbolic groups. Is the uniform epimorphism problem from H onto H solvable?*

We conclude this introduction with a discussion on the relevance of the epimorphism problem for the isomorphism problem. To do so we introduce the following notation: given a group G and a class of groups C we define $\mathrm{Epi}(G, C)$ to be the class of quotients of G that lie in C. If two groups G and H are isomorphic, then for any C we evidently have $\mathrm{Epi}(G, C) = \mathrm{Epi}(H, C)$.

The set $C = \mathrm{Fin}$ of all isomorphism types of finite groups is well-studied. In fact, we know that for two finitely generated groups G and H we have $\mathrm{Epi}(G, \mathrm{Fin}) = \mathrm{Epi}(G, \mathrm{Fin})$ if and only if the profinite completions of the two groups are isomorphic [8, Corollary 3.2.8].

In practice studying $\mathrm{Epi}(-, \mathrm{Fin})$ can be a very effective way for showing that two groups are not isomorphic. For example this approach gets used in the tabulation of knots.

Nonetheless there are even very basic examples where this approach fails. For example Baumslag [1] gave examples of pairs of non-isomorphic groups G and H which are both virtually-$\mathbb{Z}$, in fact they are both finite cyclic-by-$\mathbb{Z}$, but with

$\mathrm{Epi}(G, \mathrm{Fin}) = \mathrm{Epi}(H, \mathrm{Fin})$. This shows that it is useful to have larger classes of groups with which we can probe G and H. Let Virt-$\mathbb{Z}$ be the class of groups that are virtually $\mathbb{Z}$. It is not difficult to give an algorithm that lists all isomorphism types in Virt-$\mathbb{Z}$. This observation together with Theorem 1.4 (2) implies that there exists an algorithm that can detect the non-equality of $\mathrm{Epi}(G, \text{Virt-}\mathbb{Z})$ and $\mathrm{Epi}(H, \text{Virt-}\mathbb{Z})$ for given finitely presented groups G and H.

A note on algorithms. In this article, we describe algorithms in natural language. On the one hand, these pseudo-algorithms lack some concreteness. On the other hand, these descriptions have the advantage that we do not impose a programming paradigm (such as declarative, imperative, functional, ...) and that we do not clutter the algorithmic ideas with irrelevant technical details.

Moreover, as all of the algorithms that we consider will have ridiculous worst-case complexity anyway, we do not pay any attention on efficiency.

Organisation of this article. After a short explanation of basic notation (Section 2), we begin with characterisations of existence of epimorphisms and translations of these characterisations into linear algebra (Section 3). In Section 4, we explain how to solve the linear algebraic problems in specific cases. Using these methods, we solve the epimorphism problem for targets that are products of Abelian and finite groups as well as for virtually cyclic targets (Theorem 5.5, Theorem 5.6).

2. Preliminaries

Here, we fix basic notation and terminology.

2.1. Generators and relations.

A *group presentation* is a pair $\langle S \mid R\rangle$ consisting of a set S and a subset R of the free group $\mathrm{Free}(S)$, freely generated by S. We will usually view $\mathrm{Free}(S)$ as the set of reduced words in $S \cup S^{-1}$. A group presentation $\langle S \mid R\rangle$ is finite if both S and R are finite. If $\langle S \mid R\rangle$ is a group presentation, then we denote the group described by this presentation by

$$\bigl|\langle S \mid R\rangle\bigr| := \mathrm{Free}(S)/\langle R\rangle^{\triangleleft}_{\mathrm{Free}(S)}.$$

Definition 2.1 (symmetric presentation). — A group presentation $\langle S \mid R\rangle$ is *symmetric* if the following hold:

- Each relation in R is a positive word in S.
- For each $s \in S$ there exists an $s' \in S$ with $ss' \in R$ or $s's \in R$.

Here, a word is *positive* with respect to a generating set if it only consists of positive powers of generators. It should be noted that this notion of symmetry of a presentation is different from the notion of "symmetrized sets of relators" by Lyndon and Schupp.

2.2. Virtually Abelian groups.

A group is *virtually Abelian* if it contains a finite index subgroup that is Abelian.

Proposition 2.2. — *Let Λ be a finitely generated virtually Abelian group. Then there exists a short exact sequence (of groups) of the form*

$$1 \longrightarrow A \longrightarrow \Lambda \longrightarrow F \longrightarrow 1\,,$$

where F is a finite group and $A \cong \mathbb{Z}^d$ for some $d \in \mathbb{N}$. In particular, Λ has a finite presentation and is residually finite.

$$\begin{tikzcd}
1 \arrow[d] & 1 \arrow[d] \\
K \arrow[r, dashed, "\widetilde{\varphi}|_K"] \arrow[d] & A \arrow[d, "i"] \\
\Gamma \arrow[r, dashed, "\widetilde{\varphi}"] \arrow[dr, "\varphi"'] & \Lambda \arrow[d, "\pi"] \\
 & F \arrow[d] \\
 & 1
\end{tikzcd}$$

FIGURE 3.1. Some basic notation (Definition 3.2)

Proof. — Let Λ be a finitely generated virtually Abelian group. We only need to show that Λ contains a finite-index finitely generated free Abelian normal subgroup. By hypothesis, Λ contains a finite-index Abelian normal subgroup B. Since Λ is finitely generated we see that B is also finitely generated. The normal core of a finite index free Abelian subgroup of B now has all the required properties. ☐

In Proposition 5.4, we will explain how a constructive description of virtually Abelian groups can be obtained from any finite presentation.

3. Characterisations of existence of epimorphisms

SETUP 3.1. — Let $\langle S \mid R \rangle$ be a symmetric finite presentation, let $\Gamma := \bigl|\langle S \mid R \rangle\bigr|$ be the corresponding group, and let Λ be a finitely generated virtually Abelian group, fitting into a short exact sequence

$$1 \longrightarrow A \xrightarrow{\ i\ } \Lambda \xrightarrow{\ \pi\ } F \longrightarrow 1\ ,$$

where F is a finite group, $A \cong_{\mathbb{Z}} \mathbb{Z}^d$, and i is the inclusion of a subgroup.

The key idea is to split the epimorphism problem $\Gamma \longrightarrow \Lambda$ into finitely many cases by

- first determining all epimorphisms $\Gamma \longrightarrow F$,
- and then checking for each epimorphism $\varphi\colon \Gamma \longrightarrow F$ whether there exists an epimorphism $\Gamma \longrightarrow \Lambda$ that induces φ.

3.1. **An abstract characterisation.**

DEFINITION 3.2 (lifting/epimorphism set). — In the situation of Setup 3.1, let $\varphi\colon \Gamma \longrightarrow F$ be an epimorphism and let $K := \ker \varphi \subset \Gamma$. Then we write (Figure 3.1)

$$\begin{aligned}
L(\varphi) &:= \bigl\{\widetilde{\varphi} \in \operatorname{Hom}(\Gamma, \Lambda) \bigm| \pi \circ \widetilde{\varphi} = \varphi\bigr\}\\
K(\varphi) &:= \bigl\{\widetilde{\varphi}|_K \bigm| \widetilde{\varphi} \in L(\varphi)\bigr\}\\
E(\varphi) &:= \bigl\{\psi \in K(\varphi) \bigm| \psi(K) = A\bigr\}.
\end{aligned}$$

Proposition 3.3. — *In the situation of Setup 3.1, let $\varphi\colon \Gamma \longrightarrow F$ be an epimorphism. Then there exists an epimorphism $\widetilde{\varphi}\colon \Gamma \longrightarrow \Lambda$ with $\pi \circ \widetilde{\varphi} = \varphi$ if and only if $E(\varphi)$ is non-empty.*

Proof. — We begin with a simple observation: If $\widetilde{\varphi} \in L(\varphi)$ and $K = \ker \varphi$, then

$$\operatorname{im}(\widetilde{\varphi}) \cap A = \operatorname{im}(\widetilde{\varphi}) \cap \ker \pi = \widetilde{\varphi}(K).$$

Hence, if $\widetilde{\varphi} \in L(\varphi)$ is an epimorphism, then $\widetilde{\varphi}(K) = A$.

Conversely, suppose that $A = \widetilde{\varphi}(K)$. If $y \in \Lambda$, then we can write y in the form

$$y = y' \cdot a$$

where $y' \in \operatorname{im} \widetilde{\varphi}$ and $a \in A$ (because $\pi \circ \widetilde{\varphi} = \varphi$ is surjective). Therefore, there exist $x' \in \Gamma$ and $k \in K$ with $y' = \widetilde{\varphi}(x')$ and $a = \widetilde{\varphi}(k)$. In particular,

$$\widetilde{\varphi}(x' \cdot k) = y' \cdot a = y,$$

which shows that $\widetilde{\varphi}(\Gamma) = \Lambda$. $\square$

Corollary 3.4. — *In the situation of Setup 3.1, the following are equivalent:*

(1) *There exists an epimorphism $\Gamma \longrightarrow \Lambda$.*
(2) *There exists an epimorphism $\varphi\colon \Gamma \longrightarrow F$ with $E(\varphi) \neq \emptyset$.*

Proof. — Let $\widetilde{\varphi}\colon \Gamma \longrightarrow \Lambda$ be an epimorphism. Then $\varphi := \pi \circ \widetilde{\varphi}\colon \Gamma \longrightarrow F$ is an epimorphism and thus $E(\varphi) \neq \emptyset$ by Proposition 3.3.

Conversely, if $\varphi\colon \Gamma \longrightarrow F$ satisfies $E(\varphi) \neq \emptyset$, then Proposition 3.3 shows in particular that there exists an epimorphism $\Gamma \longrightarrow \Lambda$. $\square$

3.2. **Translation to linear algebra.** In view of Corollary 3.4, the epimorphism problem for Λ basically reduces to checking whether for a given epimorphism $\varphi\colon \Gamma \longrightarrow F$, the set $E(\varphi)$ is non-empty or not. However, in general, the set $K(\varphi)$ is *not* finite. Therefore, in order to be able to handle $E(\varphi)$ it will be useful to have an efficient description/parametrisation of $K(\varphi)$. We will now give such a description in terms of (integral) linear algebra:

Setup 3.5. — In the situation of Setup 3.1, we add a choice of a set-theoretic section $\sigma\colon F \longrightarrow \Lambda$ to our data.

Definition 3.6. — In the situation of Setup 3.5, let $\varphi\colon \Gamma \longrightarrow F$ be an epimorphism, let $K := \ker \varphi \subset \Gamma$, and let $T \subset \operatorname{Free}(S)$ be a finite set representing a generating set of K.

- A map $f\colon S \longrightarrow A$ is *hom-like* if the map

$$\begin{aligned} \sigma * f\colon S &\longrightarrow \Lambda \\ s &\longmapsto \sigma\big(\varphi(s)\big) \cdot f(s) \end{aligned}$$

  induces a well-defined group homomorphism $\Gamma = \big|\langle S \,|\, R\rangle\big| \longrightarrow \Lambda$. If f is hom-like, we denote this homomorphism by $\psi_f\colon \Gamma \longrightarrow \Lambda$.
- We then set

$$\begin{aligned} \mathbb{L}(\varphi) &:= \big\{ f \in \operatorname{map}(S, A) \;\big|\; f \text{ is hom-like} \big\} \\ \mathbb{K}(\varphi) &:= \big\{ \psi_f|_T \in \operatorname{map}(T, A) \;\big|\; f \in \mathbb{L}(\varphi) \big\} \\ \mathbb{E}(\varphi) &:= \big\{ f \in \mathbb{K}(\varphi) \;\big|\; f(T) \text{ generates } A \big\}. \end{aligned}$$

The notion of being hom-like depends on both φ and σ. A straightforward calculation shows that the notation in Definition 3.6 is just a translation of Definition 3.2 into a more explicit framework:

Remark 3.7. — In the situation of Setup 3.5, let $\varphi\colon \Gamma \longrightarrow F$ be an epimorphism, let $K := \ker\varphi \subset \Gamma$, and let $T \subset \mathrm{Free}(S)$ be a finite set representing a generating set in K. Then the diagram

$$\begin{tikzcd}
L(\varphi) \arrow[r, "\cdot|_S"] \arrow[d, "\cdot|_K"'] & \mathbb{L}(\varphi) \arrow[d, "\psi.|_T"] \\
K(\varphi) \arrow[r, "\cdot|_T"] & \mathbb{K}(\varphi) \\
E(\varphi) \arrow[u, hook] \arrow[r, "\cdot|_T"'] & \mathbb{E}(\varphi) \arrow[u, hook]
\end{tikzcd}$$

is commutative and all three horizontal maps are bijections.

Corollary 3.8. — *In the situation of Setup 3.5, the following are equivalent:*
(1) *There exists an epimorphism* $\Gamma \longrightarrow \Lambda$.
(2) *There exists an epimorphism* $\varphi\colon \Gamma \longrightarrow F$ *with* $\mathbb{E}(\varphi) \neq \emptyset$.

Proof. — We only need to combine Corollary 3.4 with the translation from Remark 3.7. ☐

Hence, the epimorphism problem for Λ reduces to deciding whether, for a given epimorphism $\varphi\colon \Gamma \longrightarrow F$, the set $\mathbb{E}(\varphi)$ is non-empty or not (this will be explained in full detail in the proofs of Theorem 5.5 and Theorem 5.6).

Proposition 3.9. — *In the situation of Setup 3.5, let* $\varphi\colon \Gamma \longrightarrow F$ *be an epimorphism, let* $K := \ker\varphi \subset \Gamma$, *and let* $T \subset \mathrm{Free}(S)$ *be a finite set representing a generating set in* K. *Then*

$$\mathbb{L}(\varphi) \subset \mathrm{map}(S, A)$$
$$\mathbb{K}(\varphi) \subset \mathrm{map}(T, A)$$

are empty or they are affine subspaces of the (finitely generated free) $\mathbb{Z}$*-modules* $\mathrm{map}(S, A)$ *and* $\mathrm{map}(T, A)$, *respectively (with respect to the point-wise module structures).*

Proof. — Because the map $\psi.|_T\colon \mathbb{L}(\varphi) \longrightarrow \mathbb{K}(\varphi)$ is $\mathbb{Z}$-linear and surjective (by construction), it suffices to show that $\mathbb{L}(\varphi)$ is an affine subspace of $\mathrm{map}(S, A)$ or empty. By construction, we have

$$\mathbb{L}(\varphi) = \bigcap_{r \in R} \mathbb{L}(\varphi, r),$$

where

$$\mathbb{L}(\varphi, r) := \bigl\{ f \in \mathrm{map}(S, A) \bigm| \mathrm{Free}(\sigma * f)(r) = e \bigr\}$$

(and $\mathrm{Free}(\sigma * f)\colon \mathrm{Free}(S) \longrightarrow \Lambda$ denotes the unique group homomorphism extending the map $\sigma * f$). Thus, it suffices to show that for each $r \in R$, the set $\mathbb{L}(\varphi, r)$ is an affine subspace of $\mathrm{map}(S, A)$. We will accomplish this by interpreting $\mathbb{L}(\varphi, r)$ as solution space of a suitable (inhomogeneous) $\mathbb{Z}$-linear equation.

Let $r \in R$, say $r = s_1 \dots s_m$ with $s_1, \dots, s_m \in S$. Moreover, let

$$\lambda_j := \sigma\big(\varphi(s_j)\big)$$

for each $j \in \{1, \dots, m\}$; then $\pi(\lambda_1 \cdot \dots \cdot \lambda_m) = \varphi(r) = e$ and thus the product $\lambda := \lambda_1 \cdot \dots \cdot \lambda_m$ lies in A. We now proceed as follows:

Let $f \in \operatorname{map}(S, A)$ and, for $j \in \{1, \dots .m\}$, let

$$x_j := f(s_j).$$

Because A is a normal subgroup of Λ, for each $\lambda \in \Lambda$, the conjugation homomorphism $C_\lambda \colon \Lambda \longrightarrow \Lambda$ by λ restricts to an automorphism of A. We then have

$$\begin{aligned} \operatorname{Free}(\sigma * f)(r) &= \lambda_1 \cdot x_1 \cdot \dots \cdot \lambda_m \cdot x_m \\ &= C_{\lambda_1}(x_1) \cdot C_{\lambda_1 \cdot \lambda_2}(x_2) \cdot \dots \cdot C_{\lambda_1 \cdot \dots \cdot \lambda_m}(x_m) \cdot \lambda_1 \cdot \dots \cdot \lambda_m. \end{aligned}$$

Hence, f lies in $\mathbb{L}(\varphi, r)$ if and only if

$$e = C_{\lambda_1}(x_1) \cdot C_{\lambda_1 \cdot \lambda_2}(x_2) \cdot \dots \cdot C_{\lambda_1 \cdot \dots \cdot \lambda_m}(x_m) \cdot \lambda_1 \cdot \dots \cdot \lambda_m.$$

Because $\lambda = \lambda_1 \cdot \dots \cdot \lambda_m \in A$ and the C_{λ_j} are automorphisms of A, we can reformulate this condition equivalently as the additive linear inhomogeneous equation

$$C_{\lambda_1}(x_1) + C_{\lambda_1 \cdot \lambda_2}(x_2) + \dots + C_{\lambda_1 \cdot \dots \cdot \lambda_m}(x_m) = -\lambda. \tag{3.1}$$

This shows that $\mathbb{L}(\varphi, r)$ is the solution set of an (inhomogeneous) $\mathbb{Z}$-linear equation in the A-valued variables "$f(s)$" with $s \in S$. More precisely, $\mathbb{L}(\varphi, r)$ is the preimage of $-\lambda$ under the $\mathbb{Z}$-linear map

$$\begin{aligned} A^S &\longrightarrow A \\ (y_s)_{s \in S} &\longmapsto \sum_{s \in S} \sum_{j \in \{1, \dots, m\} \text{ with } s_j = s} C_{\lambda_1 \cdot \dots \cdot \lambda_j}(y_s). \end{aligned} \qquad \square$$

Remark 3.10. — In the situation of Proposition 3.9, a finite "generating set" for $\mathbb{K}(\varphi)$ can be computed from the given data, a basis of A, and matrices for the conjugations $C_{\sigma(x)}$ with $x \in F$. We just need to follow the proof of Proposition 3.9:

- Using a basis of A, we can write down the corresponding "dual" bases of $\operatorname{map}(S, A)$ and $\operatorname{map}(T, A)$, respectively.
- For $r \in R$, we check whether $\varphi(r) = e$ or not (using a multiplication table for F).
  - If $\varphi(r) \neq e$, then $\mathbb{L}(\varphi, r) = \emptyset$.
  - If $\varphi(r) = e$, then we can write down the corresponding inhomogeneous $\mathbb{Z}$-linear equation (3.1) for $\mathbb{L}(\varphi, r)$. Here, we use the fact that

    $$C_{\lambda_j} = C_{\sigma(\pi(\lambda_j))}$$

    holds for all $j \in \{1, \dots, m\}$ (because A is Abelian). Using the Smith normal form algorithm [3, Algorithm 2.4.14] we can then determine whether $\mathbb{L}(\varphi, r)$ is empty or not. In the latter case, we can compute a finite set $X \subset \operatorname{map}(S, A)$ and a $b \in \operatorname{map}(S, A)$ with

    $$\mathbb{L}(\varphi, r) = \operatorname{Span}_{\mathbb{Z}} X_r + b_r.$$

- Note that the finite intersection $\mathbb{L}(\varphi) = \bigcap_{r \in R} \mathbb{L}(\varphi, r)$ is just the solution set to an affine linear equation system. Thus once again using the Smith normal form algorithm [3, Algorithm 2.4.14] we can compute the finite intersection $\mathbb{L}(\varphi) =$

$$\begin{tikzcd}
K \arrow[r, two heads, "\pi_K"] \arrow[d] & K_{\mathrm{ab}} \arrow[r, dashed, "f \circ \kappa"] \arrow[d, "\kappa"] & A \arrow[d, "i"] \\
\Gamma \arrow[r, two heads, "\pi_\Gamma"] \arrow[rr, dashed, bend right, "(f \circ \pi_\Gamma, \varphi)"'] & \Gamma_{\mathrm{ab}} \arrow[ur, dashed, "f"'] & A \times F
\end{tikzcd}$$

FIGURE 3.2. Some basic notation in the product case (Definition 3.12)

$\bigcap_{r \in R} \mathbb{L}(\varphi, r)$ in the following sense: We compute whether this intersection is empty or not; in the latter case, we compute a finite set $X \subset \operatorname{map}(S, A)$ and an offset $b \in \operatorname{map}(S, A)$ with

$$\mathbb{L}(\varphi) = \operatorname{Span}_{\mathbb{Z}} X + b.$$

- Because the (surjective) linear map $\psi.|_T \colon \mathbb{L}(\varphi) \longrightarrow \mathbb{K}(\varphi)$ admits an explicit description (e.g., by a matrix), we can also compute a corresponding description for $\mathbb{K}(\varphi)$.

3.3. **Product targets.** When dealing with targets that are a product of a finitely generated free Abelian group and a finite group, the following alternative description will be convenient:

SETUP 3.11. — Let $\langle S \mid R \rangle$ be a symmetric finite presentation, let $\Gamma := \big|\langle S \mid R \rangle\big|$ be the corresponding group, let A be an Abelian group (in the applications, this will be $\mathbb{Z}^d$), let F be a finite group, and let

$$\Lambda := A \times F.$$

We write $i \colon A \longrightarrow \Lambda$ for the inclusion as first factor and $\pi \colon \Lambda \longrightarrow F$ for the projection onto the second factor.

DEFINITION 3.12. — In the situation of Setup 3.11, let $\varphi \colon \Gamma \longrightarrow F$ be an epimorphism, let $K := \ker \varphi \subset \Gamma$, and let $\kappa \colon K_{\mathrm{ab}} \longrightarrow \Gamma_{\mathrm{ab}}$ be the homomorphism on the Abelianisations induced by the inclusion $K \longrightarrow \Gamma$. Then, we write (Figure 3.2)

$$\begin{aligned}
\mathbb{L}_{\mathrm{ab}}(\varphi) &:= \operatorname{Hom}(\Gamma_{\mathrm{ab}}, A) \\
\mathbb{K}_{\mathrm{ab}}(\varphi) &:= \big\{ f \circ \kappa \in \operatorname{Hom}(K_{\mathrm{ab}}, A) \bigm| f \in \mathbb{L}_{\mathrm{ab}}(\varphi) \big\} \\
\mathbb{E}_{\mathrm{ab}}(\varphi) &:= \big\{ f \in \mathbb{K}_{\mathrm{ab}}(\varphi) \bigm| f(K_{\mathrm{ab}}) = A \big\}.
\end{aligned}$$

PROPOSITION 3.13. — *In the situation of Setup 3.11, the following are equivalent:*

(1) *There exists an epimorphism $\Gamma \longrightarrow A \times F$.*
(2) *There exists an epimorphism $\varphi \colon \Gamma \longrightarrow F$ with $\mathbb{E}_{\mathrm{ab}}(\varphi) \neq \emptyset$.*

Proof. — We consider the following commutative diagram:

$$\begin{tikzcd}
L(\varphi) \arrow[d, "\cdot|_K"'] & \mathbb{L}_{\mathrm{ab}}(\varphi) \arrow[l, "\textcircled{1}"'] \arrow[d, "\cdot\circ\kappa"] \\
K(\varphi) & \mathbb{K}_{\mathrm{ab}}(\varphi) \arrow[l, "\textcircled{2}"'] \\
E(\varphi) \arrow[u, hook] & \mathbb{E}_{\mathrm{ab}}(\varphi) \arrow[l, "\textcircled{3}"] \arrow[u, hook]
\end{tikzcd}$$

Let $\pi_\Gamma \colon \Gamma \longrightarrow \Gamma_{\mathrm{ab}}$ and $\pi_K \colon \Gamma \longrightarrow K_{\mathrm{ab}}$ denote the canonical projections. Because the target group splits as a product $A \times F$, homomorphisms to the target split into pairs of homomorphisms to A and F, respectively. Thus, we define

$$\begin{aligned}
\textcircled{1} \colon \mathbb{L}_{\mathrm{ab}}(\varphi) &\longrightarrow L(\varphi) \\
f &\longmapsto (f \circ \pi_\Gamma, \varphi) \\
\textcircled{2} \colon \mathbb{K}_{\mathrm{ab}}(\varphi) &\longrightarrow K(\varphi) \\
f &\longmapsto (f \circ \pi_K, e) \\
\textcircled{3} \colon \mathbb{E}_{\mathrm{ab}}(\varphi) &\longrightarrow E(\varphi) \\
f &\longmapsto (f \circ \pi_K, e).
\end{aligned}$$

Then the above diagram is commutative and the horizontal maps are bijections (by definition of the various homomorphism sets). Therefore, the claim follows from the corresponding statement on the left column (Corollary 3.4). □

4. Solving the problems in linear algebra

In view of Corollary 3.8, Proposition 3.9 and Remark 3.10, we are interested in solving the following problem:

Question 4.1 (column-generation problem). — *Let $d, N \in \mathbb{N}$. Does there exist an algorithm that given a finite subset $X \subset M_{d\times N}(\mathbb{Z})$, and a $b \in M_{d\times N}(\mathbb{Z})$ decides whether there exists an element in $\operatorname{Span}_{\mathbb{Z}} X + b$ whose columns generate $\mathbb{Z}^d$?*

In general, such algorithms do *not* exist [7]. However, as we will see, special cases of the column-generation problem are solvable.

4.1. **The one-dimensional case.**

For the treatment of virtually cyclic target groups, we will use the following solution of the one-dimensional column-generation problem:

Proposition 4.2. — *Let $N \in \mathbb{N}$. Then there exists an algorithm that given a finite subset $X \subset \mathbb{Z}^N$ and $b \in \mathbb{Z}^N$ decides whether there exists an element in $\operatorname{Span}_{\mathbb{Z}} X + b$ whose entries generate $\mathbb{Z}$.*

Proof. — Let $X \subset \mathbb{Z}^N$ and let $b \in \mathbb{Z}^N$. In view of the Smith normal form algorithm [3, Algorithm 2.4.14], we may assume without loss of generality that

$$X = \{\alpha_1 \cdot e_1, \ldots, \alpha_N \cdot e_N\},$$

where $(e_1, \ldots, e_N)$ is the standard basis of $\mathbb{Z}^N$ and $\alpha_1, \ldots, \alpha_N \in \mathbb{Z}$ satisfy

$$\alpha_1 \mid \alpha_2, \quad \alpha_2 \mid \alpha_3, \quad \ldots, \quad \alpha_{N-1} \mid \alpha_N$$

(note that these coefficients also can be zero). Moreover, we write $A := \operatorname{Span}_{\mathbb{Z}} X + b$ and we denote the coefficients of b by $b_1, \dots, b_N$.

The original decision problem is then equivalent to deciding whether there exist $x_1, \dots, x_N \in \mathbb{Z}$ with

$$\gcd(\alpha_1 \cdot x_1 + b_1, \dots, \alpha_N \cdot x_N + b_N) = 1.$$

This problem can be solved as follows:

- If $\gcd(b_1, \dots, b_N) = 1$, then the answer is *yes* (we can take $x_1 = \dots = x_N = 0$).
- If $b = 0$, then:
  - If $\alpha_1 = \pm 1$, then the answer is *yes* (we can take $x_1 = 1$, $x_2 = \dots = x_N = 0$).
  - If $\alpha_1 = 0$, then $\alpha_2 = \dots = \alpha_N = 0$ and so $A = \{0\} + 0 = \{0\}$. Hence, the answer is *no*.
  - If $\alpha_1 \notin \{-1, 0, 1\}$, then $\gcd(\alpha_1, \dots, \alpha_N) > 1$, and so the answer is *no*.
- If $b \neq 0$ and $c := \gcd(b_1, \dots, b_N) > 1$, then:
  - If $\gcd(\alpha_1, c) > 1$, then the answer is *no* because then we have also $\gcd(\alpha_1, \dots, \alpha_N, c) > 1$ and so $\gcd(\alpha_1 \cdot x_1 + b_1, \dots, \alpha_N \cdot x_N + b_N) > 1$ for all $x_1, \dots, x_N \in \mathbb{Z}$.
  - If $\gcd(\alpha_1, c) = 1$, then:
    * If there exists a $j \in \{2, \dots, N\}$ with $b_j \neq 0$, then the answer is *yes*: By Lemma 4.3 below, there exists an $x \in \mathbb{Z}$ such that

      $$\gcd(x \cdot \alpha_1 + b_1, b_2, \dots, b_N) = 1.$$

      Hence, we can take $x_1 = x, x_2 = \dots = x_N = 0$.
    * If $b_j = 0$ for all $j \in \{2, \dots, N\}$, then:
      - If $N = 1$ or $\alpha_2 = 0$ (whence $\alpha_2 = \dots = \alpha_N = 0$), then the answer is *yes* if and only if c is congruent to 1 modulo α_1.
      - If $\alpha_2 \neq 0$, then the answer is *yes*: We can apply Lemma 4.3 below to α_1, b_1, α_2 to find an $x \in \mathbb{Z}$ with

        $$\gcd(x \cdot \alpha_1 + b_1, \alpha_2) = 1.$$

        Hence, we can take $x_1 = x$, $x_2 = 1$, $x_3 = \dots = x_N = 0$. □

Lemma 4.3. — *Let $N \in \mathbb{N}_{\geqslant 2}$, let $\alpha_1, b_1, \dots, b_N \in \mathbb{Z}$ such that there exists a $j \in \{2, \dots, N\}$ with $b_j \neq 0$ and*

$$\gcd(\alpha_1, b_1, \dots, b_N) = 1.$$

Then there exists an $x \in \mathbb{Z}$ with

$$\gcd(x \cdot \alpha_1 + b_1, b_2, \dots, b_N) = 1.$$

Proof. — *Assume* for a contradiction that for all $x \in \mathbb{Z}$ we have

$$c_x := \gcd(x \cdot \alpha_1 + b_1, b_2, \dots, b_N) > 1. \tag{4.1}$$

Let $P \subset \mathbb{N}$ be the set of primes that divide $\gcd(b_2, \dots, b_N)$ (because $b_j \neq 0$, this set is finite). Let $p \in P$. Then we claim that there exists a $d_p \in \mathbb{Z}$ with

$$D_p := \{x \in \mathbb{Z} \mid p \text{ divides } c_x\} \subset d_p + p \cdot \mathbb{Z}.$$

Let us prove this claim: Let $x, y \in D_p$. It then suffices to show that p divides $x - y$ (as then all elements of D_p share the same remainder modulo p). On the one hand, we have $p \mid x \cdot \alpha_1 + b_1$ and $p \mid y \cdot \alpha_1 + b_1$, and so

$$p \bigm| (x - y) \cdot \alpha_1.$$

On the other hand, p does *not* divide α_1: Because of $p \mid c_x$, we have that $p \mid \gcd(b_2, \dots, b_N)$. If $p \mid \alpha_1$, then $p \mid b_1$ (because $p \mid x \cdot \alpha_1 + b_1$) and so $p \mid \gcd(\alpha_1, b_1, \dots, b_N)$, which contradicts the assumptions in the proposition. therefore, p does not divide α_1.

Because p is prime, it follows that $p \mid (x - y)$. This proves the claim.

By assumption (4.1), the construction of the sets D_p, and the fact that each c_x has prime factors in P, we have

$$\mathbb{Z} = \bigcup_{p \in P} D_p \subset \bigcup_{p \in P} (d_p + p \cdot \mathbb{Z}).$$

Because P is finite, the Chinese remainder theorem yields an element $z \in \mathbb{Z}$ such that for all $p \in P$ we have

$$z \not\equiv d_p \mod p.$$

But this contradicts $\mathbb{Z} = \bigcup_{p \in P} D_p$. Hence, we can conclude that there must be an $x \in \mathbb{Z}$ with $c_x = 1$. □

4.2. **The symmetric homogeneous case.** Let us now turn to the situation of target groups that decompose as a product $A \times F$ of a finitely generated free Abelian group A and a finite group F. In this case, in the situation of Proposition 3.9, the subset $\mathbb{K}(\varphi) \subset \operatorname{map}(T, A)$ is linear subspace (and not only an affine subspace) and the equation (3.1) is invariant under automorphisms of A (because all the conjugations $C_{\dots}$ are just the identity map). Therefore, we end up with a very special version of the column-generation problem (which turns out to be solvable).

However, instead of using the notation of the column-generation problem (which is rather confusing in this case), we prefer to use an alternative description of $\mathbb{K}(\varphi)$ and $\mathbb{E}(\varphi)$, which is more convenient (see Proposition 3.13). Proposition 4.4 will then enter in the proof of Theorem 5.5.

Every finitely generated $\mathbb{Z}$-module is finitely presented (because $\mathbb{Z}$ is Noetherian) and can thus be described by a matrix over $\mathbb{Z}$. If $m, n \in \mathbb{N}$ and $A \in M_{n \times m}(\mathbb{Z})$, then we write

$$M(A) := \mathbb{Z}^n / \{A \cdot x \mid x \in \mathbb{Z}^m\}$$

for the finitely generated $\mathbb{Z}$-module presented by A.

Proposition 4.4. — *There exists an algorithm that, given the input*

- *matrices* $A_1 \in M_{n_1 \times m_1}(\mathbb{Z})$ *and* $A_2 \in M_{n_2 \times m_2}(\mathbb{Z})$,
- *a homomorphism* $\kappa \colon M(A_1) \longrightarrow M(A_2)$ *(given as an* $n_2 \times n_1$*-matrix),*
- *a* $d \in \mathbb{Z}$,

decides whether there exists an epimorphism $\psi\colon M(A_1) \longrightarrow \mathbb{Z}^d$ *such that there is a homomorphism* $\widetilde{\psi}\colon M(A_2) \longrightarrow \mathbb{Z}^d$ *with* $\widetilde{\psi} \circ \kappa = \psi$*.*

$$\begin{tikzcd} M(A_1) \arrow[r, two heads, "\psi"] \arrow[d, "\kappa"'] & \mathbb{Z}^d \\ M(A_2) \arrow[ur, dashed, "\widetilde{\psi}"'] & \end{tikzcd}$$

Proof. — Using the Smith normal form of A_1 and A_2, we can compute the maximal free quotients of $M(A_1)$ and $M(A_2)$ and the corresponding contribution of κ. Because the target group $\mathbb{Z}^d$ is free Abelian, we can therefore assume without loss of generality that $M(A_1)$ and $M(A_2)$ are free. Moreover, the image of κ can be computed and so we may assume that κ is the inclusion of a submodule (of which we know a basis in Smith normal form).

Hence, we reduced the original problem to the following decision problem: Given the input

- $d, n \in \mathbb{N}$,
- $\alpha_1, \dots, \alpha_n \in \mathbb{Z}$ with $\alpha_1 \mid \alpha_2, \dots, \alpha_{n-1} \mid \alpha_n$,

decide whether there exists an epimorphism $\psi\colon N \longrightarrow \mathbb{Z}^d$ that admits an extension to a homomorphism $\mathbb{Z}^n \longrightarrow \mathbb{Z}^d$, where

$$N := \operatorname{Span}_{\mathbb{Z}}\{\alpha_1 \cdot e_1, \dots, \alpha_n \cdot e_n\} \subset \mathbb{Z}^n$$

This problem can be solved as follows: Let $r \in \{0, \dots, n\}$ be the minimal index for which $\alpha_{r+1} \notin \{1, -1\}$ (where we set $r := n$ if $\alpha_n \in \{1, -1\}$). We then distinguish the following cases:

- If $r \geqslant d$, then the answer is *yes*: clearly, the projection
$$\begin{aligned} \psi\colon \mathbb{Z}^n &\longrightarrow \mathbb{Z}^d \\ x &\longmapsto (x_1, \dots, x_d) \end{aligned}$$
onto the first d coordinates restricts to an epimorphism $N \longrightarrow \mathbb{Z}^d$.
- If $r < d$, then the answer is *no*:
  - If $n < d$ or $\alpha_{r+1} = 0$, then the rank of N is smaller than d (and so there does not exist any epimorphism $N \longrightarrow \mathbb{Z}^d$).
  - If $n \geqslant d$ and $\alpha_{r+1} \neq 0$, then: Let $\widetilde{\psi}\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^d$ be a homomorphism and let $\psi := \widetilde{\psi}|_N$. We will now show that ψ is *not* surjective:
  Let $N' := \psi(N)$ and let p be a prime factor of α_{r+1}. Then $N = \mathbb{Z}^r \oplus p \cdot R$ for some submodule $R \subset \mathbb{Z}^{n-r}$ and hence
  $$N' \otimes_{\mathbb{Z}} \mathbb{Z}/p = \big(\psi(\mathbb{Z}^r) + p \cdot \psi(R)\big) \otimes_{\mathbb{Z}} \mathbb{Z}/p = \psi(\mathbb{Z}^r) \otimes_{\mathbb{Z}} \mathbb{Z}/p$$
  has $\mathbb{Z}/p$-dimension at most r, which in turn is smaller than d. In particular, ψ cannot be surjective. □

5. Solvability

Using the tools of Section 3 and Section 4, we will now establish solvability of the epimorphism problem for targets that are products of Abelian groups with finite groups or targets that are virtually cyclic (Theorem 5.5 and Theorem 5.6).

5.1. **Preparation.** For the sake of completeness, we recall some basics from algorithmic group theory.

Proposition 5.1. — *There exists an algorithm that, given the input*

- *a finite presentation* $\langle S \mid R \rangle$,

determines a symmetric finite presentation $\langle S' \mid R' \rangle$ *with* $S \subset S'$ *such that the inclusion* $S \longrightarrow S'$ *induces an isomorphism* $\big|\langle S \mid R \rangle\big| \longrightarrow \big|\langle S' \mid R' \rangle\big|$.

Proof. — For instance, we can take

$$\begin{aligned} S' &:= S \times \{-1, 1\} \\ R' &:= \big\{(s,1)(s,-1) \bigm| s \in S\big\} \\ &\quad \cup \big\{(s_1,\varepsilon_1)\cdots(s_m,\varepsilon_m) \bigm| m \in \mathbb{N},\ s_1,\dots,s_m \in S,\ \varepsilon_1,\dots,\varepsilon_m \in \{-1,1\}, \\ &\qquad\qquad s_1^{\varepsilon_1}\cdots s_m^{\varepsilon_m} \in R\big\}. \end{aligned}$$

Strictly speaking, in this construction, S is not a subset of S', but this can be fixed by renaming. □

Proposition 5.2. — *There exists an algorithm that, given the input*

- *a finite presentation* $\langle S \mid R \rangle$,
- *a finite group* F (*as set of elements and its multiplication table*),

determines the set of all epimorphisms $\big|\langle S \mid R \rangle\big| \longrightarrow F$.

Proof. — Because S is a generating set of $\Gamma := \big|\langle S \mid R \rangle\big|$, group homomorphisms $\Gamma \longrightarrow F$ can be represented by maps $S \longrightarrow F$. We will compute the set of all epimorphisms $\Gamma \longrightarrow F$ in the sense that we compute the subset of $\operatorname{map}(S,F)$ consisting of all maps corresponding to epimorphisms $\Gamma \longrightarrow F$.

Let $n := |S|$ and let $S = \{s_1, \dots, s_n\}$.

- Then we can compute the finite set $\operatorname{map}(S,F)$.
- For each $f \in \operatorname{map}(S,F)$, we can check whether for each $r \in R$, we have $\operatorname{Free}(f)(r) = e$ in F (using the multiplication table in F). Hence, we can compute the finite set

  $$H := \big\{f \in \operatorname{map}(S,F) \bigm| \forall_{r \in R} \quad \operatorname{Free}(f) = e \text{ in } F\big\},$$

  which corresponds to the set of all homomorphisms $\Gamma \longrightarrow F$ (via the universal property of generators and relations).
- We then compute the set of all generating sets of F as follows: For each subset $T \subset F$, the set

  $$G(T) := \big\{t_1 \cdot \dots \cdot t_n \bigm| n \in \{0, \dots, |F|\},\ t_1, \dots, t_n \in T \cup T^{-1}\big\} \subset F$$

  equals the subgroup of F generated by T (by the pigeon-hole principle, longer words in $T \cup T^{-1}$ cannot contribute new elements).

  Therefore, we can compute the set of all generating sets of F as the (finite) set

  $$G := \{T \subset F \mid G(T) = F\}.$$
- Hence, we can compute

  $$E := \big\{f \in H \bigm| f(S) \in G\big\},$$

  which corresponds to the set of all epimorphisms $\Gamma \longrightarrow F$. □

Proposition 5.3. — *There exists an algorithm that, given the input*

- *a symmetric finite presentation* $\langle S \mid R \rangle$,
- *a finite group* F (*as set of elements and its multiplication table*),
- *an epimorphism* $\varphi\colon \bigl|\langle S \mid R \rangle\bigr| \longrightarrow F$ (*given by the images on* S),

determines a symmetric finite presentation of $\ker\varphi$ (*where the generators are specified as words in* S).

Proof. — The given data allows to find a map $\sigma\colon F \longrightarrow \operatorname{Free}(S)$ with

$$\varphi \circ \pi \circ \sigma = \mathrm{id}_F,$$

where $\pi\colon \operatorname{Free}(S) \longrightarrow \bigl|\langle S \mid R \rangle\bigr|$ denotes the canonical projection (by enumerating all elements in $\operatorname{Free}(S)$ and computing their images in F via $\varphi \circ \pi$, until a preimage is found for every element in F); without loss of generality, we may assume that $\sigma(e) = \varepsilon$. In other words, σ specifies a coset representative system for $\ker\varphi$ in $\bigl|\langle S \mid R \rangle\bigr|$ (expressed in terms of words over S). We write

$$c := \sigma \circ \varphi \circ \pi\colon\ \operatorname{Free}(S) \longrightarrow \operatorname{Free}(S)$$

for the map that determines the coset representative of an element selected by σ. Then the words

$$\bigl\{\sigma(f) \cdot s(c(\sigma(f) \cdot s))^{-1} \bigm| s \in S,\ f \in F\bigr\}$$

describe a generating set of $\ker\varphi$ [5, Theorem 2.7]. The Reidemeister rewriting process associated with respect to this generating set and the map c then computes a finite presentation of $\ker\varphi$ [5, Corollary 2.7.2, Theorem 2.8]. Finally, we symmetrise this finite presentation via Proposition 5.1. □

For virtually Abelian targets that do not decompose as a product of a free Abelian group and a finite group, we first want to clarify what it means that a virtually Abelian group is given as "input". Naively, we could just take a finite presentation $\langle S \mid R \rangle$ of which we know for some external reason that the group $\bigl|\langle S \mid R \rangle\bigr|$ is virtually Abelian. A more constructive point of view would require to include a reason why and how the given group is virtually Abelian, i.e., that we are given a constructive description of this group as extension of a finitely generated free Abelian group by a finite group. In fact, every naive description can be turned algorithmically into a constructive description. We will explain this now in detail:

Proposition 5.4. — *There exists an algorithm that, given the input*

- *a finite presentation* $\langle S \mid R \rangle$ *of a virtually Abelian group*

determines

- *a finite group* F (*as set of elements and its multiplication table*),
- *a* $d \in \mathbb{N}$,
- *a group homomorphism* $C\colon F \longrightarrow \operatorname{Aut}(\mathbb{Z}^d)$,
- *a cocycle* $c \in \mathrm{C}^2(F; \mathbb{Z}^d)$ (*with respect to the action* C)

such that $\bigl|\langle S \mid R \rangle\bigr|$ *is isomorphic to the extension group of* $\mathbb{Z}^d$ *by* F *that corresponds to the cocycle* c.

Before giving the proof, we briefly review the cocycle notation: Let F be a group, let A be an Abelian group, and let $C\colon F \longrightarrow \operatorname{Aut}(A)$ be an F-action on A. Then $\mathrm{C}_2(G)$, the bar resolution of G in degree 2 is the free $\mathbb{Z}F$-module, freely generated by the pairs $([g_1|g_2])_{g_1,g_2 \in F}$. Then a *cocycle* $c \in \mathrm{C}^2(F;A)$ is a $\mathbb{Z}F$-linear map $\mathrm{C}_2(G) \longrightarrow A$ that satisfies the cocycle condition

$$0 = C(g_1)\big(c[g_2|g_3]\big) - c[g_1 \cdot g_2|g_3] + c[g_1|g_2 \cdot g_3] - c[g_1|g_2]$$

for all $g_1, g_2, g_3 \in F$.

Now let us recall the following explicit description of the extension group Λ of $\mathbb{Z}^d$ by F corresponding to c [2, Chapter IV.3]: As underlying set, we take the Cartesian product $A \times F$ and as multiplication, we use

$$\begin{aligned} (A \times F) \times (A \times F) &\longrightarrow (A \times F) \\ \big((x,y),(x',y')\big) &\longmapsto \big(x + C(y)(x') + c(1 \cdot [y|y']), y \cdot y'\big); \end{aligned}$$

the neutral element of Λ is (e', e_F), where $e' = -c(1 \cdot [e_F|e_F])$. Then Λ fits into the extension

$$1 \longrightarrow A \xrightarrow{\ i\ } \Lambda \xrightarrow{\ \pi\ } F \longrightarrow 1$$

where

$$\begin{aligned} i \colon A &\longrightarrow A \times F \\ x &\longmapsto (x + e', e_F) \\ \pi \colon \Lambda &\longrightarrow F \\ (x,y) &\longrightarrow y. \end{aligned}$$

A set-theoretic section of π is, for instance,

$$\begin{aligned} \sigma \colon F &\longrightarrow \Lambda \\ y &\longmapsto (0,y). \end{aligned}$$

Proof of Proposition 5.4. — Let $\Gamma := \big|\langle S \mid R \rangle\big|$. We enumerate all (multiplication tables of isomorphism types of) finite groups (e.g., as subgroups of finite permutation groups). For every finite group F, we then perform the following steps:

- We compute the (finite) set of all epimorphisms $\Gamma \longrightarrow F$ (using Proposition 5.2).
- For each epimorphism $f \colon \Gamma \longrightarrow F$, we compute a finite presentation $\langle T \mid Q \rangle$ of $\ker f$ (Proposition 5.3), where the elements of T are specified as words in the given generating set S of Γ.
- We then check whether all elements in T commute with each other. This is possible for the following reason: As finitely generated virtually Abelian group, Γ is residually finite and therefore the uniform solution of the word problem for residually finite groups [6, Theorem 5.2] provides us with an explicit algorithm to solve the word problem for Γ in the presentation $\langle S \mid R \rangle$.
- If not all elements in T commute with each other, then $\ker f$ is not Abelian and we discard f and proceed with the next epimorphism/finite group.
- If all elements in T commute with each other, then $\ker f$ is Abelian. From the presentation $\langle T \mid Q \rangle$, we can compute (via the Smith normal form algorithm) whether $\ker f$ is free Abelian or not.
  - If $\ker f$ is not free Abelian, then we discard f and proceed with the next epimorphism/finite group.
  - If $\ker f$ is free Abelian, then we proceed as follows:

  * We set $A := \ker f$ and we determine a basis B of A (via the standard algorithm). This also provides us with a transformation that allows to rewrite elements in T in this basis.
  * We then compute the F-conjugation action $F\colon \operatorname{Aut}(A)$ with respect to this basis: We search for f-lifts of each element in F and then compute for each of these lifts x and each member b of B the conjugation $x{\cdot}c{\cdot}x^{-1}$ in Γ. The result will first be a word in $S \cup S^{-1}$. We then rewrite this word in terms of T (via the Reidemeister rewriting process; proof of Proposition 5.3), and then in terms of B.
  * Finally, we compute the cocycle $c \in \mathrm{C}^2(F; A)$ of the extension

$$1 \longrightarrow A = \ker f \longrightarrow \Gamma \xrightarrow{\;f\;} F \longrightarrow 1$$

    through the well-known explicit formula [2, Chapter IV.3].

Because $\bigl|\langle S \mid R\rangle\bigr|$ is known to be virtually Abelian, Proposition 2.2 guarantees that this algorithm terminates. □

5.2. **Product targets.**

THEOREM 5.5. — *There exists an algorithm that, given the input*

- *a finite presentation* $\langle S \mid R\rangle$,
- *a finite group* F (*as set of elements and its multiplication table*),
- *a* $d \in \mathbb{N}$,

decides whether there exists an epimorphism $\bigl|\langle S \mid R\rangle\bigr| \longrightarrow \mathbb{Z}^d \times F$ *or not.*

Proof. — We write $\Gamma := \bigl|\langle S \mid R\rangle\bigr|$. In view of Proposition 3.13, it suffices to check for each epimorphism $\varphi\colon \Gamma \longrightarrow F$, whether $\mathbb{E}_{\mathrm{ab}}(\varphi) = \emptyset$ or not.

- By Proposition 5.1, we may assume without loss of generality that $\langle S \mid R\rangle$ is a symmetric finite presentation.
- We compute the set E of all epimorphisms $\Gamma \longrightarrow F$ (as a subset of $\operatorname{map}(S, F)$; Proposition 5.2).
- We determine a finite presentation of Γ_{ab}, namely

$$\langle S \mid R \cup \{sts^{-1}t^{-1} \mid s, t \in S\}\rangle.$$

  For each $\varphi \in E$, we determine finite presentations of $K := \ker\varphi$ (Proposition 5.3) and then also of K_{ab}. This allows us to find integral matrices A_1 and A_2 with canonical isomorphisms $K_{\mathrm{ab}} \cong_{\mathbb{Z}} M(A_1)$ and $\Gamma_{\mathrm{ab}} \cong_{\mathbb{Z}} M(A_2)$ as well as a matrix description of the corresponding homomorphism $M(A_1) \longrightarrow M(A_2)$ induced by the inclusion $K \longrightarrow \Gamma$.
- We then compute (using these finite presentations in matrix form and Proposition 4.4) the subset

$$\widetilde{E} := \{\varphi \in E \bigm| \mathbb{E}_{\mathrm{ab}}(\varphi) \neq \emptyset\}$$

- – If $\widetilde{E} \neq \emptyset$, then the answer is *yes*, there exists an epimorphism $\Gamma \longrightarrow F$.
  – If $\widetilde{E} = \emptyset$, the answer is *no*.

Correctness of this algorithm is guaranteed by Proposition 3.13. □

5.3. **Virtually cyclic targets.**

Theorem 5.6. — *There exists an algorithm that, given the input*

- *a finite presentation* $\langle S \mid R\rangle$,
- *a finite presentation* $\langle S' \mid R'\rangle$ *of a group* Λ *that is virtually* $\mathbb{Z}$,

decides whether there exists an epimorphism $\bigl|\langle S \mid R\rangle\bigr| \longrightarrow \Lambda$ *or not.*

Proof of Theorem 5.6. — We write $\Gamma := \bigl|\langle S \mid R\rangle\bigr|$. In view of Corollary 3.8, it suffices to check for each epimorphism $\varphi\colon \Gamma \longrightarrow F$, whether $\mathbb{E}(\varphi) = \emptyset$ or not.

- By Proposition 5.1, we may assume without loss of generality that $\langle S \mid R\rangle$ is a symmetric finite presentation.
- Using the algorithm of Proposition 5.4, we transform the presentation $\langle S' \mid R'\rangle$ into
  - a finite group F (as set of elements and its multiplication table),
  - a group homomorphism $C\colon F \longrightarrow \operatorname{Aut}(\mathbb{Z})$,
  - a cocycle $c \in \mathrm{C}^2(F;\mathbb{Z})$ (with respect to the action C),

  such that Λ is isomorphic to the extension of $\mathbb{Z}$ by F corresponding to the cocycle c.
- We compute the set E of all epimorphism $\Gamma \longrightarrow F$ (as a subset of $\operatorname{map}(S, F)$; Proposition 5.2).
- We then compute (using the algorithm outlined in Remark 3.10, and Proposition 4.2) the subset

$$\widetilde{E} := \bigl\{\varphi \in E \bigm| \mathbb{E}(\varphi) \neq \emptyset\bigr\}.$$

  - If $\widetilde{E} \neq \emptyset$, then the answer is *yes*, there exists an epimorphism $\Gamma \longrightarrow F$.
  - If $\widetilde{E} = \emptyset$, the answer is *no*.

Correctness of this algorithm is guaranteed by Corollary 3.8. □

Acknowledgements

We wish to thank Nicolaus Heuer, Christoforos Neofytidis, José Pedro Quintanilha and Alan Reid for helpful comments and conversations. We would like to thank the anonymous referee for spotting a mistake in one of the cases of the proof of Proposition 4.2.

This work was supported by the CRC 1085 *Higher Invariants* (Universität Regensburg, funded by the DFG).

References

[1] G. Baumslag. Residually finite groups with the same finite images, *Compos. Math.* 29, 249-252, 1974.

[2] K. S. Brown. *Cohomology of Groups*, volume 87 of *Graduate Texts in Mathematics*, Springer, 1982.

[3] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*, Springer, 1993.

[4] C. Löh. *Geometric group theory. An introduction*, Universitext, Springer, 2017.

[5] W. Magnus, A. Karrass, D. Solitar. *Combinatorial Group Theory. Presentations of Groups in Terms of Generators and Relations*, second revised edition, Dover, 1976.

[6] C. F. Miller III. *Decision problems for groups-survey and reflections*, Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989), 1–59, Math. Sci. Res. Inst. Publ., 23, Springer, 1992.

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

[8] L. Ribes and P. Zalesskii. *Profinite groups*, Second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics 40. Springer-Verlag, Berlin, 2010.

Manuscript received October 22, 2020,
revised March 15, 2021,
accepted March 20, 2021.

Stefan FRIEDL & Clara LÖH
Fakultät für Mathematik, Universität Regensburg, 93040 Regensburg, Germany
stefan.friedl@mathematik.uni-r.de
http://www.mathematik.uni-r.de/friedl
clara.loeh@mathematik.uni-r.de
http://www.mathematik.uni-r.de/loeh