EFFECTIVE EQUATION SOLVING, CONSTRAINTS AND GROWTH IN VIRTUALLY ABELIAN GROUPS

LAURA CIOBANU, ALEX EVETTS, ALEX LEVINE

ABSTRACT. In this paper we study the satisfiability and solutions of group equations when combinatorial, algebraic and language-theoretic constraints are imposed on the solutions. We show that the solutions to equations with length, lexicographic order, abelianisation or context-free constraints added, can be effectively produced in finitely generated virtually abelian groups. Crucially, we translate each of the constraints above into a rational set in an effective way, and so reduce each problem to solving equations with rational constraints, which is decidable and well understood in virtually abelian groups.

A byproduct of our results is that the growth series of a virtually abelian group, with respect to any generating set and any weight, is effectively computable. This series is known to be rational by work of Benson, but his approach is not constructive.

1. INTRODUCTION

One of the most famous and longstanding open questions in theoretical computer science is whether one can solve equations with length constraints in free monoids. The elucidation of this problem has deep implications: if undecidable, it would offer a new solution to Hilbert's 10th problem about the satisfiability of polynomial equations with integer coefficients. The resolution of this problem also has important applications in the context of string solvers (SMT) for software engineering and security analysis [2]. Solving equations with length and other related constraints in any structures 'close' to free monoids, in the realm of monoids or groups, will shed light on this outstanding open problem. In this paper we bring the first positive results in the area, the decidability of solving equations with length constraints in virtually abelian groups, as well as further types of constraints.

Our paper combines group theory, theoretical computer science and combinatorics to study group equations, where constraints are imposed on the solutions (see Sections 2.4, 2.5). There is a successful line of research that considers rational constraints ([13, 14, 9, 32]) when solving equations in groups, that is, when the solutions are required to belong to specified rational sets (Definition 2.4) but little is known for non-rational constraints. We consider this latter direction in the paper in the context of virtually abelian groups. We study constraints that in general groups are non-rational (such as context-free, length or abelianisation constraints, see Definitions 2.10, 2.11), that turn out, somewhat surprisingly, to be rational in virtually abelian groups. Since solving equations with rational constraints in virtually abelian groups is decidable ([32, 13]), all types of equation solving problems in this paper are decidable. However,

this alone is not enough to give decidability; the explicit construction of rational sets starting from a priori non-rational specifications is also necessary. We provide such algorithms that produce rational sets from the given constraints. We do not, however, claim any complexity results or practical efficiency of our algorithms.

The paper is inspired by work in theoretical computer science, where equations with (non-rational) language theoretic, length and abelianisation constraints in free monoids have been studied intensively for decades ([18, 1, 7, 16, 24]). As already mentioned, deciding algorithmically whether a free monoid equation has solutions satisfying linear length constraints is a major open question, with both theoretical implications (if undecidable, it would offer a new solution to Hilbert's 10th problem about the satisfiability of polynomial equations with integer coefficients) and practical ones, in the context of string solvers for security analysis [2]. For much of the last century, SAT solvers were the canonical tools to deal with the golden standard of NP-complete problems. In an SAT solver the computer program looks for a solution (i.e. values of 0 and 1 to substitute in for the variables) to a Boolean logic formula. Moving a step higher, both in complexity and applicability, are the SMT solvers, which have boomed over the last 10 years. There, one is given a first-order formula in a wider context, such as real numbers, integers, data structures, and most relevant for our paper, strings over finite alphabets. The question is then whether there is a solution for a first-order formula that is not just in the realm of Boolean formulas, but significantly more complex: the name 'satisfiability modulo theories' (SMT) represents the fact that the solvers work 'modulo' a certain theory (in a universe more complex than the Boolean one) in first-order logic with equality. In algebraic terms, this is essentially equivalent to solving equations in free monoids and related structures (as many of the constraints lead naturally to commutativity or other relations between the alphabet letters), since every string can be seen as an element over the generators of a finitely generated monoid or group.

SMT solvers have a dramatic impact on software engineering and security of Web applications: the widespread interest in cybersecurity has given strong impulse to string constraint solvers because bad string manipulations can have negative effects for Web applications developed in languages like PHP or JavaScript. The performance improvements that constraint solvers have achieved over the last 5 years have been going hand in hand with progress made by computer science theorists on tackling decades-old open questions relating to complexity and decidability of word equations in free monoids. However, many of the theoretical questions, which are still open and highly relevant to understanding the boundaries of what can be done in the solvers, need an influx of ideas from algebra and mathematics more generally: solving equations in groups while keeping the constraints that have been at the core of applications can inform the monoid equations results and feed into the circle of theory and applications complementing each other.

In the context of non-abelian free groups and free monoids (as well as hyperbolic, right-angled Artin groups etc.), length, abelianisation and context-free constraints are not rational, and the results tend to be negative: our results for virtually abelian groups contrast those of the first author and Garreta. They showed in [11] that the Diophantine Problem, that is, the question of satisfiability of equations in a group (see Section 2.4), with abelianisation constraints (called 'abelian predicates' in that paper) for non-abelian right-angled Artin groups, or for hyperbolic groups with abelianisation rank ≥ 2, is undecidable.

It is fairly immediate to see that in the case of abelian groups, imposing abelian or length constraints is equivalent to adding additional equations to the original system, so this is simply an instance of the Diophantine Problem in abelian groups. Imposing lexicographic order constraints on solutions to abelian group equations amounts to checking for membership in easily computable sets. However, moving from abelian to virtually abelian, to establish the rationality of the language-theoretic or algebraic constraints, and especially the explicit description of those constraints as rational sets, becomes a lot more involved. Our main result is as follows.

Theorem 1.1. *In any finitely generated virtually abelian group, it is effectively decidable whether a finite system of equations with the following kinds of constraints has solutions:*

- *(i) linear length constraints (with respect to <u>any</u> weighted word metric),*
- *(ii) abelianisation constraints,*
- *(iii) context-free constraints,*
- *(iv) lexicographic order constraints.*

Theorem 1.1 is a consequence of two facts: (1) each of the above constraints is a rational set (Theorem 1.2), and (2) the problem of satisfiability of finite systems of equations with rational constraints is decidable and the solutions can be effectively produced [22, 32, 13].

Theorem 1.2. *In any finitely generated virtually abelian group, there is an effective way to construct a rational set from a*

- *(i) linear length constraint (with respect to <u>any</u> weighted word metric) (Theorem 5.2),*
- *(ii) abelianisation constraint (Theorem 6.5),*
- *(iii) context-free constraint (Theorem 7.5),*
- *(iv) lexicographic order constraint (Theorem 8.5).*

Theorem B of [32] states that the solution sets to finite systems of equations with rational constraints can be represented by EDT0L languages (with respect to a natural normal form), and that these EDT0L languages can be explicitly constructed. We refer the reader to the survey [12] for background on EDT0L languages and equations in groups, and do not define or discuss EDT0L languages here, since these are not needed in the rest of the paper. Corollary 6.18 of [10] implies that the set of solutions to such a system can also be expressed as an EDT0L language with respect to a geodesic normal form. Thus we obtain the following.

Corollary 1.3. *The set of solutions to a finite system of equations with the kinds of constraints listed in Theorem 1.1 may be expressed as an EDT0L language in (at least) two different ways: with respect to a natural normal form, and with respect to a geodesic normal form.*

Finally, a consequence of our work is Proposition 1.4.

Proposition 1.4. *(see Corollary 4.13) The weighted growth series (with respect to <u>any</u> finite generating set) of a finitely generated virtually abelian group G can be computed explicitly.*

The fact that this growth series is a rational function for any generating set was proved by Benson [4], but his proof does not include an algorithm to calculate the series. The fact that we insist on establishing results for *any generating set* of a virtually abelian group is particularly important here: we use Bensons' ideas as well as further results about semilinear sets to make the computations explicit and valid for all generating sets.

2. Preliminaries

2.1. **Describing virtually abelian groups.** It is a standard fact that we may assume that any finitely generated virtually abelian group is a finite extension of a finitely generated free abelian group. Throughout the section we let G be a finitely generated virtually abelian group with free abelian normal subgroup A of finite index, and use the short exact sequence

$$(1) \qquad\qquad 1 \to A \to G \to \Delta \to 1$$

for some finite group Δ.

In any decision problem that can be asked about a group, one must first decide what information about the group is 'known'. This is frequently a presentation, but can take other forms. In our case, we describe G using a free abelian basis B for A and a (finite, right) transversal, which together define a finite generating set. In addition to this, we need to know how to multiply generators. In fact, all of this information may be obtained from a finite presentation of a virtually abelian group, as shown by Friedl and Löh [23].

Before we can formally define this information, we must first define a normal form for a virtually abelian group. We start by recalling the definition of a normal form.

Definition 2.1. Let G be a group and Σ be a generating set. A *normal form* μ for G is a function $\mu \colon G \to \Sigma^*$ that maps every element g to a word $\mu(g)$ that represents g.

Note that our definition implies that each element has a unique representative. We will frequently abuse this definition, and refer to a normal form μ to mean the image $\mu(G)$.

We now define the standard normal form we will be using for virtually abelian groups.

Definition 2.2. Let G be a finitely generated virtually abelian group. Fix a finite-index free abelian normal subgroup A, a free abelian basis B for A, and a total order $\leq$ on B; that is, write $B = \{b_1, b_2, \ldots, b_n\}$. Let T be a finite transversal of A (we choose a right transversal below, but it is not necessary to adhere to right or left since the subgroup is normal). Note that $B \cup T$ generates G, and every element of G can be represented uniquely in the form

$$(b_1^* \cup (b_1^{-1})^*) \cdots (b_n^* \cup (b_n^{-1})^*)T.$$

The *subgroup-tranversal normal form* for G, with respect to $(B, \leq, T)$, denoted $\eta_{B,\leq,T}$ is the function that maps an element G to its unique representative word in the above set. If B, $\leq$ and T are implicit, we will frequently denote this using η.

We are now in a position where we can formally define the information we will be using to construct these algorithms. Note that by [23, Proposition 5.4], the following information may be obtained from a finite presentation, but the definition collects key points that we will refer back to.

Definition 2.3. Let G be a finitely generated virtually abelian group. A *virtually abelian group description* for G comprises the following:

(1) A (finite) free abelian basis B for a finite-index free abelian normal subgroup A of G, with a total order associated with it;
(2) A finite transversal T for A in G;
(3) A presentation of the finite quotient $\Delta = G/A$;

(4) The function $f\colon (B\cup T)^{\pm} \times (B\cup T)^{\pm} \to (B^{\pm})^*T$ that maps a pair (a_1, a_2) to $\eta(a_1a_2)$. That is, f 'collects' the multiplication of the generators.

2.2. Rational and context-free sets in groups.

Let Σ be a finite alphabet and let $S = \Sigma^{\pm 1}$. Suppose G is a group generated by S, and let $\pi\colon S^* \to G$ be the natural projection from the free monoid S^* generated by S to G, taking a word over the generators to the element it represents in the group.

A *language* is any subset of S^* and is called *regular* if it is recognised by a finite state automaton, as is standard ([30]). A *context-free* language is recognised by a pushdown automaton or context-free grammar. The convention we employ here is that all context-free languages are given by context-free grammars in Chomsky normal forms (see [30, Section 2.6.13]).

We next define sets of elements in a group that are images or preimages of regular or context-free languages over the generators of the group.

Definition 2.4.

(1) A subset L of G is *recognisable* if the full preimage $\pi^{-1}(L)$ is a regular subset of S^*.
(2) A subset L of G is *rational* if L is the image $\pi(R)$ of a regular subset R of S^*.
(3) A subset L of G is *recognisably context-free* if $\pi^{-1}(L)$ is a context-free subset of S^*.
(4) A subset L of G is *context-free* if L is the image $\pi(C)$ of a context-free subset $C \subset S^*$.

It follows immediately from the definition that recognisable subsets of G are rational. Similarly, if a set is of type (3) then it is of type (4). The type (4) sets above are sometimes called *algebraic* in the literature ([5, 8]), but we avoid this terminology because it can be confused with 'algebraic sets' in the sense of 'solutions sets to equations'.

Definition 2.5. A rational set $L \subseteq G$ is said to be *effectively constructible* from some input I if there exists an algorithm that, on input of I, produces a regular subset $R \subseteq S^*$ such that $\pi(R) = L$.

Note that if we are given rational sets L and L' in some group, and corresponding regular languages R and R' over the generators of G, the concatenation LL' and the union $L \cup L'$ are effectively constructible rational sets. If, moreover, we are given an automorphism $f\colon G \to G$, defined by its action on the generators, the image $f(L)$ is an effectively constructible rational set [30].

2.3. Semilinear sets.

Definition 2.6. Let G be a group or monoid. A subset of G is *linear* if it has the form $aB^* = \{ab : b \in B^*\}$ for some $a \in G$ and finite $B \subset G$. Any finite union of linear sets is called *semilinear*.

Semilinear sets are most frequently studied in commutative monoids $\mathbb{N}^k$ and $\mathbb{Z}^k$ and there we can write the monoid operation additively, so that a linear set has the form $a + B^* = \{a + b : b \in B^*\}$. We record here a strengthened version of a classical result of Parikh that we will need in Section 7. Let $\Sigma = \{a_1, \dots a_k\}$ and let $\mathsf{ab} : \Sigma^* \mapsto \mathbb{N}^{|\Sigma|}$ be the *abelianisation* or *Parikh map* for free monoids:

$$\mathsf{ab} : \Sigma^* \mapsto \mathbb{N}^{|\Sigma|}$$

that records the occurrences of each letter a_i in a word. That is, $\mathsf{ab}(w) = (|w|_{a_1}, \ldots, |w|_{a_k})$, where $|w|_{a_i}$ denotes the number of occurrences of letter a_i in w.

Theorem 2.7 ([20], Theorem 1.1). *Let L be a context-free language over Σ. Then $\mathsf{ab}(L)$ is a semilinear subset of $\mathbb{N}^{|\Sigma|}$, and there exists a regular language R over Σ such that $\mathsf{ab}(L) = \mathsf{ab}(R)$.*

Moreover, given a context-free grammar G with n variables, one can effectively construct a finite state automaton M with $O(4^n)$ states such that the languages $L(G)$ and $L(M)$ have the same Parikh image, that is, $\mathsf{ab}(L(G)) = \mathsf{ab}(L(M))$.

To prove the decidability results of Section 5, we are interested in showing that certain semilinear sets can be algorithmically calculated. To make this precise, we make the following definition. In our case, the specified input will always be a virtually abelian group description along with some form of constraint.

Definition 2.8. Let $X \subset \mathbb{N}^k$ (respectively $X \subset \mathbb{Z}^k$), be a subset which we know to be semilinear. We say that X is *effectively constructible* if, given a specified input, we can find elements $a_1, \ldots, a_d$ and finite subsets $B_1, \ldots, B_d$ of $\mathbb{N}^k$ (respectively $\mathbb{Z}^k$) so that $X = \bigcup_{i=1}^{d} (a_i + B_i^*)$.

2.4. **The Diophantine problem ($\mathcal{DP}$) in groups.** Let $\mathbf{x} = \{X_1, \ldots, X_m\}$ be a set of variables, where $m \geq 1$. For a group G, a *finite system of equations* in G over the variables $\mathbf{x}$ is a finite subset $\mathcal{E}$ of the free product $G * F(\mathbf{x})$, where $F(\mathbf{x})$ is the free group on $\mathbf{x}$. If $\mathcal{E} = \{w_1, \ldots, w_n\}$, then a *solution* to the system $w_1 = \cdots = w_n = 1$ is a homomorphism $\phi \colon G * F(\mathbf{x}) \to G$, such that $\phi(w_1) = \cdots = \phi(w_n) = 1_G$ and $\phi(g) = g$ for all $g \in G$. If $\mathcal{E}$ has a solution, then it is *satisfiable*.

Example 2.9. *Consider the system $\mathcal{E} = \{w_1, w_2\} \subset F(a, b) * F(X_1, X_2)$ over the free group $F(a, b)$, where $w_1 = X_1^2(abab)^{-1}$, $w_2 = X_2 X_1 X_2^{-1} X_1^{-1}$; we set $w_1 = w_2 = 1$, which can be written as $X_1^2 = abab, X_2 X_1 = X_2 X_1$. The solutions are $\phi(X_1) = ab, \phi(X_2) = (ab)^k$, $k \in \mathbb{Z}$.*

For a group G, we say that systems of equations over G are *decidable* over G if there is an algorithm to determine whether any given system is satisfiable. The question of decidability of (systems of) equations is called the *Diophantine Problem* for G, and denoted $\mathcal{DP}(G)$.

2.5. **The Diophantine Problem with constraints.** If we ask not only whether a system of equations has solutions, but whether it has solutions that belong to certain specified sets, then we call those sets *constraints* and consider the Diophantine Problem with various kinds of constraints. We start first with language-theoretic constraints:

Definition 2.10. Let $\mathcal{E}$ be a system of equations on variables $\mathbf{x} = \{X_1, \ldots, X_k\}$ in a group G. The *Diophantine Problem with rational or recognisable or context-free constraints* (of type (3) or (4)) asks about the existence of solutions to $\mathcal{E}$, with some of the variables restricted to taking values in specified rational, recognisable or context-free sets, respectively.

We next attach three types of constraints that have an algebraic or combinatorial nature, rather than a language theoretic one, to the Diophantine Problem. These constraints are typically not rational in arbitrary groups, although will turn out to be rational in virtually abelian groups.

Recall that G is finitely generated by S and so every element $g \in G$ has a length $|g|_S$, which is the length of a shortest word w representing g in G. The length of a solution to $\mathcal{E}$ with respect to S refers to the length(s) of the group element(s) corresponding to the solution.

For any group G, let $\mathsf{ab}: G \to G^{\mathsf{ab}}$ be the natural abelianisation map to $G^{\mathsf{ab}} = G/G'$, that is, the quotient of G by its commutator subgroup.

Finally, we may fix an ordering on the generating set of G and consider the lexicographic or shortlex order for the group based on this. Or more specifically, we may fix an ordering on the free abelian basis of A, and fix an ordering on T to obtain a lexicographic ordering $\leq_{\mathrm{lex}}$ on the normal form words. By ordering the normal form words using shortlex instead, we obtain another ordering $\leq_{\mathrm{shortlex}}$ (see Definition 8.1).

Definition 2.11.

(1) We let $\mathcal{DP}(G, \mathrm{L})$ denote the $\mathcal{DP}$ with *linear length constraints*. A set of linear length constraints is a system Θ of linear integer equations and inequalities where the unknowns correspond to the lengths of solutions (with respect to $|.|_S$) to each variable $X_i \in \mathbf{x}$ (see also Definition 5.1). Then $\mathcal{DP}(G, \mathrm{L})$ asks whether solutions to $\mathcal{E}$ exist for which the lengths satisfy the system Θ.

(2) We write $\mathcal{DP}(G, \mathsf{ab})$ for the $\mathcal{DP}$ where an abelian predicate is added, or equivalently, *abelianisation constraints* are imposed. A set of abelianisation constraints is a system Θ of equations in the group G^{ab}, and $\mathcal{DP}(G, \mathsf{ab})$ asks whether a solution to $\mathcal{E}$ exists such that the abelianisation of the solution satisfies the system Θ in G^{ab}.

(3) We write $\mathcal{DP}(G, <)$ for the $\mathcal{DP}$ where an order predicate is added. A set $\mathcal{O}$ of order constraints consists of several order relations imposed on the solutions, and $\mathcal{DP}(G, <)$ asks whether a solution to $\mathcal{E}$ exists that satisfies the constraints in $\mathcal{O}$.

Example 2.12. *Consider the virtually abelian group $G = \langle a, b : bab^{-1} = a^{-1} \rangle$. This is the Klein bottle group, or alternatively the Baumslag-Solitar group $BS(1, -1)$, and is virtually $\mathbb{Z}^2$, with abelianisation $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and length function $|.| = |.|_{\{a,b\}}$. We study the equation $XaY^2bY^{-1} = 1$ over variables X, Y in G.*

(1) *An instance of $\mathcal{DP}(G, \mathrm{L})$ is: decide whether there are any solutions (x, y) such that $|x| = |y| + 2$; the answer is yes, since $(x, y) = (b^{-1}a^{-1}, 1)$ is a solution with $|x| = |y| + 2$.*

(2) *An instance of $\mathcal{DP}(G, \mathsf{ab})$ is: decide whether there are any solutions (x, y) such that $\mathsf{ab}(x) = \mathsf{ab}(y)$ (we use additive notation for $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})$); the answer is no, since $\mathsf{ab}(xay^2by^{-1}) = \mathsf{ab}(x) + \mathsf{ab}(y) + (1, \bar{1}) = (0, \bar{0})$ together with $\mathsf{ab}(x) = \mathsf{ab}(y)$ lead to $2\mathsf{ab}(y) = (-1, \bar{1})$, which is not possible in $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

(3) *Fix the order $a < a^{-1} < b < b^{-1}$ and let $\leq_{lex}$ represent the induced lexicographic order on all elements of G, i.e. pairs of elements $(g, h) \in G \times G$ such that $g \leq_{lex} h$ if g is lexicographically smaller than h.*

   An instance of $\mathcal{DP}(G, \leq_{lex})$ is: decide whether there are any solutions (x, y) such that $x \leq_{lex} y$; the answer is 'yes' since $x = a^{-1}, y = b^{-1}$ is a solution with $x \leq_{lex} y$.

3. Semilinear sets: effective construction in free abelian groups

In this section we collect some useful results on effective construction of semilinear sets. Here, we deal exclusively with semilinear subsets of the group $\mathbb{Z}^k$ and therefore write the group operation additively, so that a linear set has the form $a + B^* = \{a + b : b \in B^*\}$.

Remark 3.1. *By definition, if we are given semilinear expressions for sets X and Y in any group or monoid, then $X \cup Y$ is a semilinear set, and we can effectively construct a semilinear expression for it: simply the union of the constituent linear sets of X and Y.*

The analogous statements for intersection and complement require proof. In Theorem III of [19], Eilenberg and Schützenberger prove that intersections and complements of semilinear subsets of any commutative monoid are semilinear, but they do not show effectiveness of their construction. The effectiveness statement does follow, however, from [25], [26], or [17], appearing explicitly in [37].

Theorem 3.2. *Let X and Y be semilinear subsets of $\mathbb{Z}^k$. Then $X \cap Y$ and $X \setminus Y$ are semilinear, and effectively constructible from X and Y.*

Definition 3.3. An *integer affine map* $\phi \colon \mathbb{Z}^k \to \mathbb{Z}^l$ is a function given by an $l \times k$ matrix M and a constant $c \in \mathbb{Z}^l$, so that $\phi(x) = Mx + c$ for all $x \in \mathbb{Z}^k$. Note that this is a group homomorphism composed with a translation.

It is straightforward to obtain the following Corollary of 3.2.

Corollary 3.4. *Let $\phi \colon \mathbb{Z}^k \to \mathbb{Z}^l$ be an integer affine map. If $X \subset \mathbb{Z}^k$ is semilinear then its image $\phi(X) \subset \mathbb{Z}^l$ is semilinear and effectively constructible. If $Y \subset \mathbb{Z}^l$ is semilinear then its preimage $\phi^{-1}(Y) \subset \mathbb{Z}^k$ is semilinear and effectively constructible.*

So-called *polyhedral sets* are subsets of $\mathbb{Z}^k$ defined by affine hyperplanes. They were introduced by Benson in [4] to study the growth series of virtually abelian groups and have since proved to be an invaluable tool for other applications to growth and equations in these groups (e.g. [22]). It is not hard to see that polyhedral sets coincide with semilinear subsets (and hence with rational subsets) of $\mathbb{Z}^k$.

Definition 3.5. Let $k \in \mathbb{N}$, and let $\cdot$ denote the Euclidean scalar product.

  (i) Any subset of $\mathbb{Z}^k$ of the form
   (1) $\{z \in \mathbb{Z}^k : u \cdot z = a\}$,
   (2) $\{z \in \mathbb{Z}^k : u \cdot z \equiv a \mod b\}$, or
   (3) $\{z \in \mathbb{Z}^k : u \cdot z > a\}$
   for $u \in \mathbb{Z}^k$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, is an *elementary region*, of type (1), (2), and (3) respectively;
  (ii) any finite intersection of elementary sets will be called a *basic polyhedral set*;
  (iii) any finite union of basic polyhedral sets will be called a *polyhedral set*.

Proposition 3.6. [10, Proposition 3.11] *A subset of $\mathbb{Z}^k$ is polyhedral if and only if it is semilinear.*

Finally, we note that Theorem 3.2 allows us to effectively pass from a polyhedral description of a set to a semilinear description.

Corollary 3.7. *Given an expression for a polyhedral set (as a finite union of finite intersections of elementary sets), we can effectively construct a semilinear expression for the same set.*

4. Computing geodesics in virtually abelian groups

The set of all geodesics in a virtually abelian group has been analysed from the point of view of language theory and growth by several authors [35, 36], with the results often using particular generating sets. Most recently, geodesics were studied with respect to all generating sets in [6]. Here we consider a subset of the entire set of geodesics, that is, we describe how to compute a *geodesic normal form*, that is, one geodesic word per group element, for a finitely

generated virtually abelian group with respect to *any* choice of (weighted) generating set. We formally define the notion of weight below.

Definition 4.1. Let G be a group with finite generating set Σ which has a weight function $\omega \colon \Sigma \to \mathbb{N} \setminus \{0\}$. This weight function extends to elements $g \in G$ in the natural way:

$$\omega(g) = \min \left\{ \sum_{i=1}^{k} \omega(\sigma_i) : \sigma = \sigma_1 \cdots \sigma_k =_G g, \sigma_i \in \Sigma \right\}.$$

A word that has minimal weight amongst all representatives of the same group element will be called *geodesic*.

In [4], Benson proved that every virtually abelian group admits a geodesic normal form (with respect to any weighted generating set) that can be described using polyhedral sets, which are semilinear by Proposition 3.6. In this section, we show that the semilinear sets in question are effectively constructible. As a consequence we see, in Corollary 4.13, that the growth series of the group can be effectively calculated.

Theorem 4.2. *Let G be a finitely generated virtually abelian group, with a description as in Definition 2.3. Let Σ be any finite generating set for G, with elements of Σ given in subgroup-transversal normal form, equipped with a weight function ω.*

Then there exists a geodesic normal form $\mathcal{U} \subset \Sigma^*$ with a finite partition into subsets U, each equipped with an injective map $\phi \colon U \to \mathbb{N}^m$ (for some m depending on U) such that each image $\phi(U)$ is semilinear and effectively constructible (from the group description). Furthermore, the weights of the elements $u \in U$ can be easily calculated from their images $\phi(u)$.

In Section 5 we will see that Theorem 4.2 allows us to solve equations with length constraints. To prove Theorem 4.2, we follow the ideas of [4] and set-up of [21, 10] to construct the geodesics, but ensure that each step is effective.

Definition 4.3. Let G be virtually abelian with description as in Definition 2.3, and write $\mathbb{Z}^n$ for the normal free abelian subgroup of finite index. Define the *extended generating set*

$$S = \{s_1 s_2 \cdots s_k : s_i \in \Sigma, \ 1 \le k \le [G : \mathbb{Z}^n]\},$$

where the weight of an element of S is $\omega(s) = \sum_i \omega(s_i)$, and extend this to a weight on the group as in (4.1). Observe that the weight with respect to S is equal to the weight with respect to Σ. We work with S from now on. Words in S^* that have minimal weight amongst all words that represent the same group element will be called *geodesic*.

Definition 4.4 (Patterns and patterned words)**.** Let G be as in the statement of Theorem 4.2, with $\mathbb{Z}^n$ and S as in Definition 4.3.

(1) Define $X = S \cap \mathbb{Z}^n = \{x_1, \ldots, x_r\}$ and $Y = S \setminus X = \{y_1, \ldots, y_s\}$ (membership of $\mathbb{Z}^n$ can be determined by repeated applications of the function f of Definition 2.3). Let $P = \{\pi \in Y^* : |\pi|_S \le [G : \mathbb{Z}^n]\}$ be a finite set that we call the set of *patterns*.
(2) For each pattern $\pi = \pi_1 \pi_2 \cdots \pi_k \in P$, define the set of *patterned words*

$$W^{\pi} = \left\{ x_1^{w_1} \cdots x_r^{w_r} \pi_1 x_1^{w_{r+1}} \cdots x_r^{w_{2r}} \pi_2 \cdots \pi_k x_1^{w_{kr+1}} \cdots x_r^{w_{kr+r}} : w_i \in \mathbb{N} \right\} \subset S^*.$$

(3) For each W^π, define the bijection $\phi_\pi \colon W^\pi \to \mathbb{N}^{kr+r}$ which records the powers of the generators from X:

$$\phi_\pi \colon x_1^{w_1} \cdots x_r^{w_r} \pi_1 x_1^{w_{r+1}} \cdots x_r^{w_{2r}} \pi_2 \cdots \pi_k x_1^{w_{kr+1}} \cdots x_r^{w_{kr+r}} \mapsto \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_{kr+r} \end{pmatrix} \in \mathbb{N}^{kr+r}.$$

For brevity, write $m(\pi) = kr + r$.

The following lemma ensures that our set of patterns P is sufficient to provide geodesics for every element of G.

Lemma 4.5 (Proposition 11.3 of [4]). *For each element $g \in G$, there exists some $\pi \in P$ such that W^π contains a geodesic representative for g.*

We now construct matrices, vectors, and integer affine maps that will allow us to move between patterned words and their corresponding subgroup-transversal normal forms.

Definition 4.6 (Structure constants). Form the $n \times r$ matrix

$$Z = \begin{pmatrix} | & | & & | \\ x_1 & x_2 & \cdots & x_r \\ | & | & & | \end{pmatrix}$$

whose columns are the elements of X (expressed as column vectors in $\mathbb{Z}^n$). For $y_k \in Y$ and a standard basis vector $e_i \in \mathbb{Z}^n$, normality gives $y_k e_i y_k^{-1} \in \mathbb{Z}^n$. Use the function f of Definition 2.3 to calculate each conjugate in terms of standard basis vectors. For each $y_k \in Y$, form the $n \times n$ matrix

$$\Gamma_k = \begin{pmatrix} | & | & & | \\ y_k e_1 y_k^{-1} & y_k e_2 y_k^{-1} & \cdots & y_k e_n y_k^{-1} \\ | & | & & | \end{pmatrix}.$$

For each $\pi = y_{i_1} y_{i_2} \cdots y_{i_k} \in P$, construct the $n \times m(\pi)$ matrix

$$(Z \mid \Gamma_{i_1} Z \mid \cdots \mid \Gamma_{i_1} \Gamma_{i_2} \cdots \Gamma_{i_k} Z)$$

and write A_i^π for its ith row, so that we define n vectors in $\mathbb{Z}^{m(\pi)}$, for each pattern.

Each element of G can be written uniquely as an element of the product $\mathbb{Z}^n \cdot T$, where T is the transversal coming from the description of G. For a fixed pattern π, normality of $\mathbb{Z}^n$ implies that every word in W^π represents an element of the coset $\mathbb{Z}^n \pi$. Write $t_\pi \in T$ for the corresponding representative (which can be calculated from the description of G), and define $B_1^\pi, \ldots, B_n^\pi \in \mathbb{Z}$ so that the word π represents the group element $(B_1^\pi, \ldots, B_n^\pi)^\intercal t_\pi$. Thus for $w \in W^\pi$, we have

$$w =_G \left\{ \begin{pmatrix} A_1^\pi \cdot \phi_\pi(w) \\ \vdots \\ A_n^\pi \cdot \phi_\pi(w) \end{pmatrix} + \begin{pmatrix} B_1^\pi \\ \vdots \\ B_n^\pi \end{pmatrix} \right\} t_\pi,$$

which is in subgroup transversal normal form.

Furthermore, let $A_{n+1}^\pi \in \mathbb{N}^{m(\pi)}$ record the weights of the x_is, repeating the sequence $k + 1$ times,

$$A_{n+1}^\pi = (\omega(x_1), \ldots, \omega(x_r), \omega(x_1), \ldots, \omega(x_r), \ldots, \omega(x_1), \ldots, \omega(x_r)),$$

and write $B^\pi_{n+1} = \omega(\pi)$. So we have $\omega(w) = A^\pi_{n+1} \cdot \phi_\pi(w) + B^\pi_{n+1}$ for $w \in W^\pi$. Define integer affine maps $\mathcal{E}^\pi \colon \phi_\pi(W^\pi) \to \mathbb{Z}^{n+1}$ via

$$
\mathcal{E}^\pi \colon x \mapsto \begin{pmatrix} A^\pi_1 \cdot x + B^\pi_1 \\ \vdots \\ A^\pi_{n+1} \cdot x + B^\pi_{n+1} \end{pmatrix}.
$$

Definition 4.7 (Ordering). We define an order on each W^π which is compatible with the weight, as follows. Extend the set $\{A^\pi_1, \ldots, A^\pi_{n+1}\}$ by choosing standard basis vectors $A^\pi_{n+2}, \ldots, A^\pi_K$ so that $\{A^\pi_1, \ldots, A^\pi_K\}$ has $\mathbb{R}$-rank equal to $m(\pi)$.

Then define an order on W^π as: $v \leq_\pi w$ if and only if either $v = w$ or there exists $k \in [1, K]$ such that $A^\pi_i \cdot \phi_\pi(v) = A^\pi_i \cdot \phi_\pi(w)$ for $i < k$ and $A^\pi_k \cdot \phi_\pi(v) < A^\pi_k \cdot \phi_\pi(w)$. If restricted to any subset of W^π representing a single group element, this is a total order, and indeed a well-order (the proof is straightforward and can be found in [4]).

Now we reduce the set W^π of all π-patterned words to a set V^π of only those words which are minimal-weight element representatives (amongst W^π).

Definition 4.8. Define

$$
V^\pi = \{v \in W^\pi : \text{if } w \in W^\pi \text{ and } v =_G w \text{ then } v \leq_\pi w\}.
$$

Lemma 4.10 demonstrates that we can construct each V^π as a semilinear set. The proof is a modification of that of Proposition 6.2 of [4] to make it constructive (see also Proposition 4.7 of [21]). We will need the following straightforward corollary of Theorem 3.2. A subset U of $\mathbb{Z}^k$ will be called *monotone* if, for each $i \in \{1, \ldots k\}$, the ith coordinates of every element of U have the same sign, or are zero.

Corollary 4.9. *Let $S \subseteq \mathbb{Z}^k$ be semilinear. Then we may decompose S as a finite disjoint union of (effectively constructible) monotone semilinear sets.*

Lemma 4.10. *Let $V^\pi = \{v \in W^\pi : \text{if } w \in W^\pi \text{ and } v =_G w \text{ then } v \leq_\pi w\}$ be as above and ϕ_π as in Def. 4.4 (3). Then $\phi_\pi(V^\pi) \subset \mathbb{N}^{m(\pi)}$ is an effectively constructible semilinear set.*

Proof. Let $m(\pi)$ be as in Definition 4.4 (3), and K as in Definition 4.7. Define

$$
\mathcal{T}^\pi = \bigcup_{i=1}^{K-n} \left(\left(\bigcap_{j=1}^{n+i-1} \{\tau \in \mathbb{Z}^{m(\pi)} : A^\pi_j \cdot \tau = 0\} \right) \cap \{\tau \in \mathbb{Z}^{m(\pi)} : A^\pi_{n+i} \cdot \tau > 0\} \right).
$$

It is straightforward to show that for $v, w \in W^\pi$, v and w represent the same group element with $w \leq_\pi v$ if and only if there exists $\tau \in \mathcal{T}^\pi$ with $\phi_\pi(v) = \phi_\pi(w) + \tau$ (see Section 6 of [4]). The set $\mathcal{T}^\pi$ is clearly polyhedral and so, by Corollary 3.7, we can construct a semilinear expression for it, say $\mathcal{T}^\pi = \bigcup_{i=1}^r (a_i + B^*_i)$, for some $a_i \in \mathbb{Z}^{m(\pi)}$, and finite sets $B_i \subset \mathbb{Z}^{m(\pi)}$. Note also that by Corollary 4.9 we may assume that for each i, each element of B_i is in the same orthant as a_i. We claim that $\phi_\pi(V^\pi) = \mathbb{N}^{m(\pi)} \setminus \bigcup_{i=1}^r (a_i + \mathbb{N}^{m(\pi)})$. By Theorem 3.2 we can then express this complement as a semilinear set, finishing the proof.

To see the claim, first suppose that $v \in V^\pi$, but also $\phi_\pi(v) \in a_i + \mathbb{N}^{m(\pi)}$ for some i. So $\phi_\pi(v) = a_i + \phi_\pi(w)$ for some $w \in \mathbb{N}^{m(\pi)}$, and therefore v and w represent the same group element with $w \leq_\pi v$, but this contradicts the assumption that $v \in V^\pi$.

Conversely, suppose we have $v \in W^\pi$ with $\phi_\pi(v) \in \mathbb{N}^{m(\pi)} \setminus \bigcup_{i=1}^r (a_i + \mathbb{N}^{m(\pi)})$ but $v \notin V^\pi$. So there exists $\tau \in \mathcal{T}^\pi$, $v_0 \in V^\pi$, with $\phi_\pi(v) = \phi_\pi(v_0) + \tau$ (and v, v_0 representing the same group element). We have $\tau = a_i + b$ for some i and some $b \in B_i^*$, and so $\phi_\pi(v) = a_i + b + \phi_\pi(v_0)$. We claim that $\phi_\pi(v) - a_i \in \mathbb{N}^{m(\pi)}$, so that $\phi(v) \in a_i + \mathbb{N}^{m(\pi)}$, which is a contradiction. Since a_i and b are in the same orthant, we have $e_j \cdot a_i \leq e_j \cdot (a_i + b)$ for each standard basis vector e_j. In the case $e_j \cdot a_i \geq 0$ we therefore have $e_j \cdot a_i \leq e_j \cdot (a_i + b)$, and so $e_j \cdot (\phi_\pi(v) - a_i) \geq e_j \cdot (\phi_\pi(v) - a_i - b) = e_j \cdot \phi_\pi(v_0) \geq 0$ (since $v_0 \in V^\pi$). In the case $e_j \cdot a_i < 0$ we have $e_j \cdot (\phi_\pi(v) - a_i) \geq -e_j \cdot a_i \geq 0$. So we have $\phi_\pi(v) - a_i \in \mathbb{N}^{m(\pi)}$ as claimed. $\qquad\square$

We have now constructed everything we require to prove the main theorem of this section.

Proof of Theorem 4.2. The sets V^τ have been constructed so as to provide us with a geodesic representative for every group element (Lemma 4.5 ensures that our finite set of patterns is sufficient). However, there may be group elements represented by words with more than one pattern, which will be represented in more than one of the sets V^τ. In order to pass to a set of *unique* geodesics, and hence a normal form, we need to remove such overlaps. Let $\mathbf{1}_i$ denote the $(2n+2)$-dimensional vector whose ith entry is 1 with zeroes elsewhere. Define polyhedral sets

$$\Theta = \bigcap_{i=1}^n \left\{ \theta \in \mathbb{Z}^{2n+2} : \theta \cdot (\mathbf{1}_i - \mathbf{1}_{i+n+1}) = 0 \right\} \cap \left\{ \theta \in \mathbb{Z}^{2n+2} : \theta \cdot (\mathbf{1}_{n+1} - \mathbf{1}_{2n+2}) > 0 \right\},$$

$$\Theta_* = \bigcap_{i=1}^n \left\{ \theta \in \mathbb{Z}^{2n+2} : \theta \cdot (\mathbf{1}_i - \mathbf{1}_{i+n+1}) = 0 \right\} \cap \left\{ \theta \in \mathbb{Z}^{2n+2} : \theta \cdot (\mathbf{1}_{n+1} - \mathbf{1}_{2n+2}) = 0 \right\}.$$

By Corollary 3.7 we can rewrite Θ and Θ_* as semilinear subsets of $\mathbb{Z}^{2n+2}$. Write $p \colon \mathbb{Z}^{2n+2} \to \mathbb{Z}^{n+1}$ for projection onto the first $n+1$ coordinates (which is an integer affine map). Now define

$$R^{\pi,\mu} = (\mathcal{E}^\pi)^{-1} \circ p\left[(\mathcal{E}^\pi \circ \phi_\pi(V^\pi) \times \mathcal{E}^\mu \circ \phi_\mu(V^\mu)) \cap \Theta \right],$$

$$R_*^{\pi,\mu} = (\mathcal{E}^\pi)^{-1} \circ p\left[(\mathcal{E}^\pi \circ \phi_\pi(V^\pi) \times \mathcal{E}^\mu \circ \phi_\mu(V^\mu)) \cap \Theta_* \right]$$

for each $\pi, \mu \in P$. By Theorem 3.2 and Corollary 3.4, each of these can be explicitly expressed as semilinear sets. Fix an arbitrary total order on the set of patterns $P = \{\pi_1, \pi_2, \ldots, \pi_{|P|}\}$. For each pattern, define

$$Q^{\pi_k} = \phi_{\pi_k}(V^{\pi_k}) \setminus \left(\bigcup_{i \neq k} R^{\pi_k, \pi_i} \cup \bigcup_{j < k} R_*^{\pi_k, \pi_j} \right).$$

Theorem 3.2 implies that each Q^{π_k} is an effectively constructible semilinear set. Finally, define the set of geodesics $U^{\pi_k} = \phi_{\pi_k}^{-1}(Q^{\pi_k})$. By construction, the sets U^τ provide a complete set of unique geodesics for the elements of G. See also Section 12 of [4], or the proof of Theorem 4.2 of [21]. Furthermore, the weight of $u \in U^\tau$ is related to that of its image by $\omega(u) = A_{n+1}^\pi \cdot \phi_\pi(u) + B_{n+1}^\pi$ (recalling Definition 4.6). This proves the theorem. $\qquad\square$

4.1. **Growth Series.** This section discusses a corollary of Theorem 4.2 that does not relate to solving equations. We have the following slight generalisation of the standard definition of growth.

Definition 4.11. Let G be a group with finite weighted generating set S. The (spherical) weighted growth function is given by $\sigma_{G,S}(n) = \#\{g \in G : \omega(g) = n\}$, where $\omega(g)$ denotes the weight of g with respect to S. The weighted growth series of G is then the generating function

$$\sum_{n=0}^{\infty} \sigma_{G,S}(n) z^n \in \mathbb{Z}[[z]].$$

Definition 4.12. The set of $\mathbb{N}$-*rational functions* is the smallest set of functions $f(z)$ containing all polynomials in z and closed under multiplication, addition, and quasi-inverse (that is, if $f(z)$ is in the set with $f(0) = 0$, then its quasi-inverse $\frac{1}{1-f(z)}$ is in the set).

The main result of [4] is that the weighted growth series of a virtually abelian group is an $\mathbb{N}$-rational function, but the proof is non-constructive. Explicitly constructing the semilinear sets describing the geodesics allows us to calculate the growth series. More precisely, we have the following corollary of Theorem 4.2.

Corollary 4.13. *The ($\mathbb{N}$-rational) weighted growth series of a finitely generated virtually abelian group can be explicitly computed with respect to* <u>any</u> *generating set.*

To establish Corollary 4.13, we need the following lemma that follows from the proof of [19, Theorem IV].

Lemma 4.14. *(see* [19, Theorem IV]*) If $X \subset \mathbb{N}^k$ is semilinear, it can be expressed as a disjoint union of finitely many linear sets $X = \bigcup_{i=1}^{r}(a_i + B_i^*)$ such that each B_i consists of linearly independent elements. Furthermore, a_i and B_i can be effectively computed from the original semilinear expression for X.*

Lemma 4.14 allows us to make the following proposition, appearing in [10], effective. See also [15] for more work on the growth series of semilinear sets.

Proposition 4.15. *If $X \subset \mathbb{N}^k$ is semilinear, its growth series (with respect to a weighted ℓ_1-norm) is $\mathbb{N}$-rational and can be explicitly computed.*

Proof. Lemma 4.14 implies that X can be effectively expressed as the disjoint union of finitely many linear sets of the form $a_i + B_i^*$, where each B_i is a linearly independent set. Such a linear set has growth series

$$z^{\omega(a_i)} \prod_{b \in B_i} \frac{1}{1 - z^{\omega(b)}}.$$

The growth series of X is then the sum of rational sets of the given form. $\square$

Finally, we can add together the rational growth series from each disjoint piece of $\mathcal{U}$ to obtain the growth series of the whole.

Proof of Corollary 4.13. The growth series of the group is equal to the growth series of the set of geodesics $\mathcal{U}$. We have

$$\sum_n \sigma_{\mathcal{U}}(n) z^n = \sum_\pi \sum_n \sigma_{U^\pi}(n) z^n = \sum_\pi z^{\omega(\pi)} \sum_n \sigma_{\phi_\pi(U^\pi)}(n) z^n$$

so it suffices to calculate the growth series of each semilinear set $\phi_\pi(U^\pi)$. This can be done effectively by Proposition 4.15. $\square$

In future work we intend to extend the results of this section to other growth series associated to the group, as studied in [21] and [10].

5. Length constraints in virtually abelian groups

In this section we show that tuples of elements in a virtually abelian group G whose word lengths satisfy systems of linear (in)equalities form rational subsets of G. Moreover, these rational sets can be described explicitly in terms of effectively constructible semilinear subsets of $\mathbb{Z}^n$ (which is, as usual, the finite index normal free abelian subgroup of G).

Definition 5.1. Let G be a finitely generated group, with finite generating set S. For any positive integer k, a *length constraint* on G^k will be a subset of G^k in one of the following forms

$$\left\{ (g_1, \ldots, g_k) \in G^k : \sum_{i=1}^k \alpha_i |g_i|_S = \beta \right\},$$

$$\left\{ (g_1, \ldots, g_k) \in G^k : \sum_{i=1}^k \alpha_i |g_i|_S \leq \beta \right\},$$

where $\alpha_i, \beta \in \mathbb{Z}$, and $|g|_S$ denotes word length of $g \in G$ with respect to S.

The following Theorem asserts that we can explicitly compute a rational expression for any length constraint, using the sets of geodesics U^π, constructed in Section 4.

Theorem 5.2. *Any length constraint (as in Definition 5.1) in a virtually abelian group, with respect to any generating set, can be effectively expressed as a semilinear, and hence rational, subset.*

Proof. As usual, let G be a finitely generated virtually abelian group described as in Definition 2.3, and recall the geodesic normal form $\mathcal{U} = \bigcup U^\pi$ constructed above. Throughout this proof we will use the notation of Section 4.

Suppose we have a length constraint $L \subset G^k$ of the first form in the definition. The same argument will work for the second form. We may obtain a complete set of unique geodesics for L by decomposing it according to which pattern the element geodesics fall into. That is, if an element $g \in G$ has its unique geodesic representative $u \in S^*$ in the set U^{π_k} (where $1 \leq k \leq |P|$ as in Definition 4.4), then we work with $\omega(u)$ and the corresponding quantities related to the pattern π_k. Considering k-tuples of geodesics, we have

$$\bigcup_{(\pi_1, \ldots, \pi_k) \in P^k} \left\{ (u_1, \ldots, u_k) : u_i \in U^{\pi_i}, \ \sum_{i=1}^k \alpha_i \omega(u_i) = \beta \right\}$$

$$= \bigcup_{(\pi_1, \ldots, \pi_k) \in P^k} \left\{ (u_1, \ldots, u_k) : u_i \in U^{\pi_i}, \ \sum_{i=1}^k \alpha_i (A^{\pi_i}_{n+1} \cdot \phi_{\pi_i}(u_i) + B^{\pi_i}_{n+1}) = \beta \right\},$$

where we use the vectors A^π_{n+1} and integers B^π_{n+1} of Definition 4.6 to construct the weight of the words u_i. The summation condition can be rewritten as the identity

$$\left(\alpha_1 A^{\pi_1}_{n+1}, \cdots \alpha_k A^{\pi_k}_{n+1} \right) \cdot \left(\phi_{\pi_1}(u_1), \cdots, \phi_{\pi_k}(u_k) \right) = \beta - \sum_{i=1}^k \alpha_i B^{\pi_i}_{n+1},$$

where we have concatenated vectors on the left hand side, resulting in the scalar product of two vectors in $\mathbb{Z}^{\sum_i m(\pi_i)}$. Thus the following expression defines the set of k-tuples of vectors corresponding to unique geodesic representatives for group elements satisfying the length constraint:

$$M_{(\pi_1,\ldots,\pi_k)} = \left\{ x \in \mathbb{Z}^{\sum_i m(\pi_i)} : \left(\alpha_1 A_{n+1}^{\pi_1}, \cdots \alpha_k A_{n+1}^{\pi_k} \right) \cdot x = \beta - \sum_{i=1}^{k} \alpha_i B_{n+1}^{\pi_i} \right\} \cap \phi_{\pi_1}(U^{\pi_1}) \times \cdots \times \phi_{\pi_k}(U^{\pi_k}).$$

By Theorem 4.2, and Corollary 3.7, we can explicitly construct this semilinar subset, for each of finitely many k-tuples in P^k.

Write $p^{\pi_j} \colon \mathbb{Z}^{\sum_i m(\pi_i)} \to \mathbb{Z}^{m(\pi_j)}$ for the projection onto just the components corresponding to π_j. Recall the integer affine maps $\mathcal{E}^{\pi} \colon \phi_\pi(W^\pi) \to \mathbb{Z}^{n+1}$, and define $\tilde{\mathcal{E}}^{\pi} \colon \phi_\pi(W^\pi) \to \mathbb{Z}^n$ to be the projection onto the first n coordinates, so that $\tilde{\mathcal{E}}^{\pi} \circ \phi_\pi(w) \cdot t_\pi =_G w$ for any $w \in W^\pi$. We then have

$$L = \left(\tilde{\mathcal{E}}^{\pi_1} \circ \phi_{\pi_1} \circ p^{\pi_1}(M_{(\pi_1,\ldots,\pi_k)}) \right) t_{\pi_1} \times \cdots \times \left(\tilde{\mathcal{E}}^{\pi_k} \circ \phi_{\pi_k} \circ p^{\pi_k}(M_{(\pi_1,\ldots,\pi_k)}) \right) t_{\pi_k}$$

$$= \left(\tilde{\mathcal{E}}^{\pi_1} \circ \phi_{\pi_1} \circ p^{\pi_1}(M_{(\pi_1,\ldots,\pi_k)}) \times \cdots \times \tilde{\mathcal{E}}^{\pi_k} \circ \phi_{\pi_k} \circ p^{\pi_k}(M_{(\pi_1,\ldots,\pi_k)}) \right) \cdot t_{\pi_1} \cdots t_{\pi_k}.$$

Since each factor $\tilde{\mathcal{E}}^{\pi_i} \circ \phi_{\pi_i} \circ p^{\pi_i}(M_{(\pi_1,\ldots,\pi_k)})$ is semilinear, the cartesian product is also semilinear, and hence so too is L itself. Furthermore, we have an explicit semilinear expression for L, which is of course a rational expression, as required. $\qquad \square$

6. ABELIANISATION CONSTRAINTS

We start with the following fact about abelianisation constraints (in any group) which allows us to reduce the question to checking membership in cosets of the commutator subgroup.

Lemma 6.1. *Let G be a group and $\mathcal{E}$ be a system of equations in G with abelianisation constraints. Then there exists a system of equations $\bar{\mathcal{E}}$ in G with the same set of solutions as $\mathcal{E}$ which has no abelianisation constraints, but instead the constraints:*

$$X_i \in [G, G]h_i,$$

where each X_i is a variable and each $h_i \in G$.

Proof. Let Θ denote the system of equations in G^{ab} that are the abelianisation constraints in $\mathcal{E}$. For each equation in Θ we have two cases: the equation has one variable, occurring only once, or the equation has at least two variables, or more than one occurrence of the same variable. In the first case, the equation is immediately equivalent to $X^{\mathsf{ab}} = g^{\mathsf{ab}}$ for some $g \in G$. This is equivalent to $X \in [G, G]g$. Thus we can start defining $\bar{\mathcal{E}}$ to have the same equations and abelianisation constraints as $\mathcal{E}$, except with the constraints $X \in [G, G]g$ replacing the single-variable, single occurrence abelianisation constraints.

For the remaining abelianisation constraints that have two or more occurrences of variables, note that (after grouping variables) they are equations of the form $(X_1^{\mathsf{ab}})^{i_1} \cdots (X_k^{\mathsf{ab}})^{i_k} = h^{\mathsf{ab}}$ within G^{ab}, where $X_1, \ldots, X_k$ are variables and $h \in G$. We can therefore define a new variable Y in G for each such equation as $Y = X_1^{i_1} \cdots X_k^{i_k}$. Then this abelianisation constraint is equivalent to $Y^{\mathsf{ab}} = h^{\mathsf{ab}}$ within G^{ab}, which is the same as $Y \in [G, G]h$. Thus we can replace

FIGURE 1. Exact diagram from virtually abelian group

each such abelianisation constraint in $\mathcal{E}$ with a new variable, an additional equation, and a constraint of the form $Y \in [G,G]h$ to define $\bar{\mathcal{E}}$, which has the desired form. □

In light of the above lemma, to understand solutions to systems of equations with abelianisation constraints, we need to understand the cosets of the commutator subgroup. In the case of virtually abelian groups, we show that these are in fact rational sets, and provide an algorithm for effectively computing a rational expression for a coset from the virtually abelian group description and any coset representative.

Since subgroups of finitely generated virtually abelian groups are finitely generated virtually abelian, we have the following result.

Lemma 6.2. *Let G be a finitely generated virtually abelian group, with a finite-index normal free abelian subgroup of index k. Then $[G,G]$ is finitely generated virtually abelian, and admits a free abelian normal subgroup of index at most k.*

Now we construct a diagram of maps which we will use to compute the rank of the commutator subgroup of $[G,G]$ from the rank of G. We show below, in a 'Snake Lemma' type result, that the diagram exists and is exact.

Lemma 6.3. *Let G be a virtually abelian group with a finite-index free abelian normal subgroup A, and let Δ be the quotient of G by A. Then there exist homomorphisms ϕ, ψ, θ such that the diagram in Figure 6.3 is exact. The remaining homomorphisms are the natural inclusions and projections.*

Proof. (ϕ): Let $p \colon G \to \Delta$ be the natural projection. We start by defining $\phi \colon [G,G] \to [\Delta,\Delta]$ as $\phi([g_1,h_1]\cdots[g_k,h_k]) = [p(g_1),p(h_1)]\cdots[p(g_k),p(h_k)]$; that is, ϕ is the restriction of p to $[G,G]$. As the restriction of an epimorphism, ϕ is also an epimorphism, and since $\ker p = A$, it follows that $\ker \phi = A \cap [G,G]$.

(ψ): Let $\psi \colon A/(A \cap [G,G]) \to G/[G,G]$ be defined by $(A \cap [G,G])g \mapsto [G,G]g$. We first show that ψ is well-defined. Let $(A \cap [G,G])g = (A \cap [G,G])h \in A/A \cap [G,G]$. Then $gh^{-1} \in A \cap [G,G]$, and so $[G,G]g = [G,G]h$, and ψ is well-defined.

To see that ψ is injective, let $(A\cap[G,G])g \in \ker\psi$. Then $[G,G]g = [G,G]$, and so $g \in [G,G]$. Since $g \in A$, we have that $g \in A \cap [G,G]$, and so $(A \cap [G,G])g = A \cap [G,G]$.

(θ): Let $\theta\colon G/[G,G] \to \Delta/[\Delta,\Delta]$ be defined by $[G,G]g \to [\Delta,\Delta]p(g)$. To see that θ is well-defined, note that if $[G,G]g = [G,G]h \in G/[G,G]$, then $gh^{-1} \in [G,G]$, and so $p(g)(p(h))^{-1} \in [\Delta,\Delta]$ and $[\Delta,\Delta]p(g) = [\Delta,\Delta]p(h)$. Since p is surjective, we have that θ is. As p is a homomorphism, θ is.

To see that $\ker\theta = \operatorname{im}\psi$, first note that $\operatorname{im}\psi = \{[G,G]g : g \in A\}$. It is clear that if $g \in A$, then $g \in \ker p$, and so $[G,G]p(g) = [G,G]$. Thus $\operatorname{im}\psi \subseteq \ker\theta$. Now let $[G,G]g \in \ker\theta$. Then $[\Delta,\Delta]p(g) = [\Delta,\Delta]$ and so $p(g) \in [\Delta,\Delta]$. Since $p(g) \in [\Delta,\Delta] \subseteq \Delta$, $g \in A$, and so $[G,G]g \in \operatorname{im}\psi$. $\qquad\square$

Using the exact diagram, we can compute the rank of the commutator subgroup of a virtually abelian group, which in turn allows us to find a finite generating set for the commutator subgroup. An immediate corollary of this is that the commutator subgroup is a rational set, and so every coset of it is.

Proposition 6.4. *There is an algorithm that takes as input a finitely generated virtually abelian group description (as in Definition 2.3), and outputs a finite generating set for the commutator subgroup.*

Proof. Let G be a finitely generated virtually abelian group, and let A be a finite-index normal free abelian subgroup of G, and T be a right transversal for A in G. Consider the diagram shown in Figure 6.3. First note that we can construct a presentation for G using the transversal and free abelian generators. Using this presentation, we can compute a presentation for the abelianisation $G/[G,G]$, by adding the commutator relation for each pair of generators. Using the fact that $G/[G,G]$ is abelian, we can standardise this presentation by grouping occurences of each generator within each non-commutator relation. By removing redundent relations, we can count the number of torsion-free generators to compute the torsion-free rank m of $G/[G,G]$. Let n be the free abelian rank of A. Since $\Delta/[\Delta,\ \Delta]$ is finite, we can use standard linear algebra to deduce that the torsion-free rank of $A/(A\cap[G,G])$ must also be m, and then to conclude that the free abelian rank of $A \cap [G,G]$ must be $n - m$.

We now compute a free abelian basis for $A \cap [G,G]$ by initially setting our basis set to be $B = \emptyset$, and then iterating through elements of A, represented (uniquely) by shortlex-minimal geodesic words in their shortlex order and adding an element to B whenever it both lies in $[G,G]$ and is linearly independent from all the elements of B. We terminate this once we have $n - m$ such elements. We will then have a set of minimal elements of A that lie in $A \cap [G,G]$ and are all linearly independent, and thus this must be a basis for $A \cap [G,G]$. We now have a (finite) generating set B for $A \cap [G,G]$.

We now simply need to compute a (right) transversal for $A \cap [G,G]$ in $[G,G]$. Note that this will be finite, as $[\Delta,\Delta]$ is. Since Δ is finite, we can compute the right Cayley graph from the products of elements of T (which we know). To choose a transversal for $A \cap [G,G]$, we simply need to trace one path in the Cayley graph of $[\Delta,\Delta]$ from $1_{[\Delta,\Delta]}$ to every state, and take our transversal U to be to be the set of the natural lift of each word traced. We have now computed $U \cup B$, which is a finite generating set for $[G,G]$. $\qquad\square$

Now that we know that the commutator subgroup is rational, it follows that all its cosets are rational, and so abelianisation constraints (when converted into the form of Lemma 6.1) are instances of rational constraints.

Theorem 6.5. *If G is a finitely generated virtually abelian group with a finite generating set Σ, then every abelianisation constraint is a rational subset of G.*

Moreover, a rational expression for an abelianisation constraint can be computed from any coset representative h of the abelianisation constraint.

Proof. To effectively compute a rational expression for $[G, G]h$, we simply need to compute a monoid generating set for $[G, G]$, which can be done using the finite generating set from Proposition 6.4 and closing it under inverses (if necessary). □

7. Context-free sets in virtually abelian groups

In this section we consider context-free sets (see Definition 2.4(3) and (4)) in virtually abelian groups. In some of the literature [28, 8] our 'recognisably context-free sets' are called simply 'context-free', while our 'context-free sets' are called 'algebraic'. However, we avoid the terminology 'algebraic', as this can be confused with 'algebraic set' in the sense of 'solution set to an equation' in a group. Since, using our terminology, a recognisably context-free set is context-free, all results here will hold for recognisably context-free sets automatically because we prove them for context-free sets, and we do not refer to them additionally.

It is known that context-free sets are in fact rational in virtually abelian groups ([28, 8]). This can be seen in two steps. First, context-free sets in finitely generated free abelian groups coincide with rational sets via semilinear sets, by Parikh's theorem (see for example [30], Theorem 2.6.23). Then every context-free set C in a virtually abelian group G is the finite union of context-free sets in the cosets of a free abelian finite index subgroup (see for example [8, Prop. 3.11]); since the latter are rational by Parikh's result, the set C in G is rational. We make all this effective in Theorem 7.5.

Since context-free sets are rational in virtually abelian groups, the Diophantine Problem with (recognisably) context-free constraints reduces (again) to a known decidable problem: the Diophantine Problem with rational constraints in virtually abelian groups [32]. We'd like to contrast this to the Diophantine Problem with context-free constraints in other classes of groups, where imposing such constraints leads immediately to undecidability; this is because the context-free subset membership problem on its own is undecidable. For example, the context-free set membership problem is undecidable in groups containing a free non-abelian subgroup. This follows from the result below, linking membership in context-free sets to membership in rational sets of direct products, together with the fact that membership in finitely generated, and thus rational, subgroups of $F_2 \times F_2$ is undecidable by Mihailova [34].

Theorem 7.1. [31, Corollary 6.3] *The context-free membership problem is decidable in a group G if and only if the rational subset membership is decidable in $G \times F_2$, where F_2 is the free group on two generators.*

The convention we employ here is that all context-free languages are given by context-free grammars in Chomsky normal forms (see, for example, [30, Section 2.6.13]). In the proof of

Theorem 7.5 we will need to translate certain languages and preserve their complexity, and we achieve this using transducers, which we review below following [31].

Definition 7.2. Let Σ and Ω be two finite alphabets. A finite automaton over $\Sigma^* \times \Omega^*$ is called a *finite transducer* from Σ^* to Ω^*. A subset recognised by a finite transducer, that is, a rational set of $\Sigma^* \times \Omega^*$, is a *finite transduction*. If $\rho \subseteq \Sigma^* \times \Omega^*$ is a transduction and $L \subseteq \Sigma^*$, then the *image of L under ρ* is the language

$$\rho(L) = \{v \in \Omega^* : (u, v) \in \rho \text{ for some } u \in L\} \subseteq \Omega^*.$$

One can think of a transducer as a finite state automaton where the labels on the edges are pairs of words from $\Sigma^* \times \Omega^*$ instead of single letters as in a standard automaton. Then a path's label in the transducer can be seen as the graph of a function mapping words in Σ^* to words in Ω^*.

Proposition 7.3. [5, Ch.III, Corollary 4.2] *Each rational transduction preserves rational and context-free languages. That is, if L is a language over a finite alphabet Σ, then for each rational transduction ρ, $\rho(L)$ is rational if L is rational, and $\rho(L)$ is context-free if L is context-free.*

Lemma 7.4. [31, Lemma 3.3] *Let G be a finitely generated group with a finite-index free normal subgroup A, and let X and Y be finite generating sets of G and A, respectively.*

1. *Then there is an explicit, computable, rational transduction $\sigma \subseteq Y^* \times X^*$ such that $W_X(h) = \sigma(W_Y(h))$, for every $h \in A$, where $W_Y(h)$ and $W_X(h)$ are the sets of all words that represent element h in A over Y and X, respectively.*
2. *Furthermore, $\sigma^{-1} : X^* \to Y^*$ is a partial function such that, for $w \in X^*$, $\sigma^{-1}(w)$ is defined if and only if w represents an element of A, in which case $\sigma^{-1}(w)$ is an element of Y^* representing the same element of A as w.*

The transducer σ in Lemma 7.4 is based on the Schreier coset graph of G/A. The vertices correspond to the finitely many cosets At_i of A in G with t_i in the transversal T, and A is both initial and final state. Edges have the form (At_i, At_ix), for $x \in X$, with labels $(w_{t_i,x}, x)$, where $w_{t_i,x} \in Y^*$ is a word representing the unique element $g \in A$ such that $t_ix = gt_j$ and $At_ix = At_j$ (see the proof of [31, Lemma 3.3] and [33, Section 5] for further details).

Theorem 7.5. *Any context-free set C in a finitely generated virtually abelian group G is rational and, moreover, a rational expression for C can be effectively computed.*

Proof. Let G be a finitely generated virtually abelian group with a finite-index free abelian normal subgroup A, and a finite transversal T, as in Definition 2.3. Since A is a subgroup of finite index it is a recognisable set, as are all cosets At with $t \in T$. Let X and Y be finite generating sets of G and A, respectively. Moreover, let A_X be the preimage of A in X^*, that is, $A_X = \pi^{-1}(A)$. The set A_X is regular, and a finite state automaton M_{A_X} over the alphabet X can be effectively computed to produce A_X: we can construct the automaton for $\pi^{-1}(A)$ since we know a presentation for the quotient $\Delta = G/A$ (Definition 2.3(3)) with respect to the generating set $\bar{X} = \{\bar{x} = xA : x \in X\}$; then $\pi^{-1}(A)$ is just the word problem of Δ with respect to $\bar{X}$, and the words representing the identity in Δ can be read off the finite Cayley graph of Δ. In fact, the automaton M_{A_X} can be taken to be $Cay(\Delta, \bar{X})$ and (re)using x for every generator $\bar{x}$.

Let C be a context-free set in G over X. We write $C = \bigcup_{t \in T}(C \cap At)$, and it suffices to show that each $C \cap At$ is effectively rational over X. In fact, $C \cap At$ is effectively rational if and only if $(C \cap At)t^{-1} = Ct^{-1} \cap A$ is. So it suffices to prove the result for $Ct \cap A$, $t \in T$. The set Ct is context-free as the translate of C; that is, there is a context-free set $C_t \subset X^*$ explicitly given by a grammar Γ_{C_t} in Chomsky normal form such that $\pi(C_t) = Ct$.

We claim that $Ct \cap A$ is effectively rational over Y, the generating set of A. To show this, let $L_{X,t} = C_t \cap A_X$; this is a context-free language over X that can be effectively computed from M_{A_X} and Γ_{C_t}, and such that $\pi(L_{X,t}) = Ct \cap A$. By Lemma 7.4 there is an explicit, computable, rational transduction $\sigma \subseteq Y^* \times X^*$ such that $A_X = \sigma(A_Y)$, where A_Y is the language of all words over Y that represent elements in A. That is, $\sigma^{-1} : X^* \to Y^*$ is a partial function such that, for $w \in X^*$, $\sigma^{-1}(w)$ is defined if and only if w represents an element of A, in which case $\sigma^{-1}(w)$ is an element of Y^* representing the same element of A as w. Moreover, $\sigma^{-1}(L_{X,t})$ produces a language, say $L_{Y,t}$, of words over Y consisting of words that represent exactly the elements in $Ct \cap A$. Since being context-free is preserved by preimages of rational transductions, $L_{Y,t}$ is context-free and a grammar for it can be effectively computed since the rational transduction σ is explicit.

Now $L_{Y,t}$ is context-free and $\pi(L_{Y,t})$ and $\mathsf{ab}(L_{Y,t})$ represent the same subset of elements of A, namely $Ct \cap A$. By the strengthened version of Parikh's result (Theorem 2.7), $\mathsf{ab}(L_{Y,t})$ is a (computably) semilinear set over Y, and a finite state automaton M_{L_t} for a regular language R_t over Y with the same Parikh image is computable, therefore $Ct \cap A$ is effectively rational since it can be obtained from M_{L_t}. This proves the claim that $Ct \cap A$ is effectively rational over Y. Finally, we can apply the transduction σ to $R_t \subset Y^*$ and get $Ct \cap A$ effectively rational over X, which proves therefore the theorem. $\square$

8. Order Constraints

In this section we look at lexicographic order of solutions to equations, when these are written in the standard normal form. We then also consider shortlex order, using the length arguments from Section 5. The lexicographic and shortlex order constraints compare normal form words, as defined below.

Definition 8.1. Let G be a virtually abelian group given as in Definition 2.3. Fixing a finite-index free abelian normal subgroup A and a (finite) right transversal T, we obtain the subgroup transversal normal form η. For a fixed ordering on the free abelian basis of A, and a fixed ordering on T, we obtain a lexicographic ordering $\leq_{\mathrm{lex}}$ on the normal form words. By ordering the normal form words using shortlex instead, we obtain another ordering $\leq_{\mathrm{shortlex}}$.

Note that both of these are dependent on the choice of normal subgroup and transversal used to define η, and the orderings on the free abelian basis and transversal, and thus there will be multiple lexicographic and shortlex orderings on a given virtually abelian group.

Remark 8.2. *Lexicographic or shortlex are total orders on the elements of a virtually abelian group, but are not left (or right) invariant orders, i.e. they are not invariant under left (or right) multiplication. For the virtually abelian groups with infinitely many left orders there exist left-invariant orders for which comparing two elements is undecidable [3], so using left-invariant orders is not a feasible constraint when considering the Diophantine Problem.*

Before we can prove the main result of this section, we must show that we can effectively construct intersections of rational subsets of virtually abelian groups. We need the following result of Grunschlag.

Lemma 8.3. [27, Corollary 2.3.8] *Let G be a group with finite generating set S and H a finite index subgroup of G with right transversal T. For each rational subset $U \subset G$ such that $U \subset Ht$ for some $t \in T$, there exists an effectively constructible rational subset $V \subset H$ such that $U = Vt$.*

In [10], rational subsets of virtually abelian groups are characterised as certain kinds of semilinear subsets, which implies that their intersections are also rational. The following lemma makes this effective.

Lemma 8.4. *Let G be a finitely generated virtually abelian group. Given finitely many rational subsets of G, their intersection is an effectively constructible semilinear set.*

Proof. Let S be a finite generated set for G and let A denote a free abelian normal subgroup of G of finite index and T a choice of right transversal. Since A has finite index in G, any coset At is *recognisable.* In other words, the full preimage of At in S^* is a regular language (see [29, Proposition 6.3]).

Suppose that U is a rational subset of G with $R \subset S^*$ a regular language whose image is U. Then intersecting R with the full preimage of any coset At gives a new regular language R' whose image is $U \cap tA$. Since intersections of regular languages can be found algorithmically [30], each intersection $U \cap At$ is an effectively constructible rational set. Now since $U \cap At \subset At$, Lemma 8.3 implies that we can find a rational subset $V_t \subset A$ such that $U \cap At = V_t t$, for each $t \in T$ (and so $U = \bigcup V_t t$).

In [19, Section 2] it is shown that in any commutative monoid, rational sets and semilinear sets coincide and, moreover, given a rational expression for a set, a semilinear expression can be found. Thus, we can effectively express each rational subset $V_t \subset A$ as a semilinear subset of A, so that

$$U = \bigcup_{t \in T} \bigcup_{i=1}^{k_t} (a_{t,i} + B_{t,i}^*)t$$

for some $a_{t,i} \in A$ and finite $B_{t,i} \subset A$ (where we write the group operation in A additively). Now, since intersection distributes over union (and in light of Remark 3.1), the intersection of two (and hence finitely many) rational sets $U, U' \subset G$ is an effectively constructible semilinear (and hence rational) set as long as the intersection of any two linear sets of the form $(a_{t,i} + B_{t,i}^*)t$ is an effectively constructible semilinear set. Consider two such sets $(a + B^*)t$ and $(c + D^*)s$, for $t, s \in T$, $a, c \in A$, and finite $C, D \subset A$. We have

$$(a + B^*)t \cap (c + D^*)s = \begin{cases} \emptyset & t \neq s \\ ((a + B^*)t \cap (c + D^*)) & t = s \end{cases}.$$

By Theorem 3.2, the intersection $(a + B^*) \cap (c + D^*)$ is semilinear and effectively constructible and hence so is its translate by t, finishing the proof. □

We now show that lexicographic order constraints are equivalent to a collection of rational constraints. Note that two lexicographically comparable words in the subgroup transversal normal form share a common prefix.

Theorem 8.5. *Let G be a finitely generated virtually abelian group. Fix a finite-index free abelian subgroup A, a free abelian basis $B = \{a_1, \ldots, a_n\}$ with $a_1 < a_1^{-1} \ldots < a_n < a_n^{-1}$ for A, and a (finite) right transversal T also equipped with an order $\leq$.*

Then verifying a lexicographic order constraint $X \leq_{\mathrm{lex}} Y$ is equivalent to checking membership of each of X, Y and $X^{-1}Y$ in a certain effectively constructible rational set.

Proof. We write all group elements in (subgroup transversal) normal form $a_1^{i_1} \cdots a_n^{i_n} s$, where $a_i \in B$ and $s \in T$, and note that $a_1^{i_1} \cdots a_n^{i_n} s \leq_{\mathrm{lex}} a_1^{j_1} \cdots a_n^{j_n} t$ implies one of: (1) $i_1 = j_1, \ldots, i_n = j_n$ and $s \leq t$, or (2) there exists $p \in \{1, \ldots, n\}$ such that $i_1 = j_1, \ldots, i_{p-1} = j_{p-1}$ and $i_p < j_p$.

Case 1: there exists $p \in \{1, \ldots, n\}$ such that $i_1 = j_1, \ldots, i_{p-1} = j_{p-1}$ and $i_p < j_p$. This case is a finite disjunction across $p \in \{1, \ldots n\}$ of the case where for this fixed p, $i_1 = j_1, \ldots, i_{p-1} = j_{p-1}$ and $i_p < j_p$. Thus it suffices to show each of these cases reduces to checking membership in effectively constructible rational sets. So fix such a $p \in \{1, \ldots, n\}$.

We first show that checking $i_q = j_q$ for all $q < p$ can be done by checking membership of $(a_1^{i_1} \cdots a_n^{i_n} s)^{-1}(a_1^{j_1} \cdots a_n^{j_n} t)$ in a rational set. Let $\phi_s, \phi_t \in \mathrm{Aut}(A)$ be the automorphisms induced by conjugation by s and t, respectively. We will show that verifying that $i_q = j_q$ for all $q < p$ is equivalent to checking membership in the set $\phi_s^{-1}(\pi((a_p^{\pm})^* \cdots (a_n^{\pm})^*)))\pi(s^{-1}t)$. If $i_q = j_q$ for all $q < p$, then

$$(a_1^{i_1} \cdots a_n^{i_n} s)^{-1}(a_1^{j_1} \cdots a_n^{j_n} t) = s^{-1} a_1^{j_1 - i_1} \cdots a_n^{j_n - i_n} t$$
$$= s^{-1} a_p^{j_p - i_p} \cdots a_n^{j_n - i_n} t$$
$$= \phi_s^{-1}(a_p^{j_p - i_p} \cdots a_n^{j_n - i_n}) s^{-1} t \in \phi_s^{-1}(\pi((a_p^{\pm})^* \cdots (a_n^{\pm})^*)))\pi(s^{-1}t).$$

Conversely, suppose $(a_1^{i_1} \cdots a_n^{i_n} s)^{-1}(a_1^{j_1} \cdots a_n^{j_n} t) \in \phi_s^{-1}(\pi((a_p^{\pm})^* \cdots (a_n^{\pm})^*)))\pi(s^{-1}t)$. Then

$$(a_1^{i_1} \cdots a_n^{i_n} s)^{-1}(a_1^{j_1} \cdots a_n^{j_n} t) = s^{-1} a_1^{j_1 - i_1} \cdots a_n^{j_n - i_n} t$$
$$= \phi_s^{-1}(a_1^{j_1 - i_1} \cdots a_n^{j_n - i_n}) s^{-1} t$$

This lies in $\phi_s^{-1}(\pi((a_p^{\pm})^* \cdots (a_n^{\pm})^*)))\pi(s^{-1}t)$ if and only if $j_1 - i_1 = \cdots = j_{p-1} - i_{p-1} = 0$, as required.

If $x, y \in G$ are arbitrary elements, then x and y are of the above form; that is $x = a_1^{i_1} \cdots a_n^{i_n} s$ and $y = a_1^{j_1} \cdots a_n^{j_n} t$ for some $i_1, \ldots, i_n, j_1, \ldots, j_n \in \mathbb{Z}$ and $s, t \in T$ with $i_q = j_q$ for all $q < p$. We have that $i_q = j_q$ for all $q < p$ if and only if xy^{-1} lies in the set $\phi_s^{-1}(\pi((a_p^{\pm})^* \cdots (a_n^{\pm})^*)))\pi(s^{-1}t)$. However, as this set's definition depends on s and t, this set depends on x and y. So what we must do is union across all possibilities of $s^{-1}t$, which will be $T^{-1}T$. Thus x and y satisfy the property that $i_q = j_q$ for all $q < p$ if and only if $xy^{-1} \in \phi_s^{-1}(\pi((a_p^{\pm})^* \cdots (a_n^{\pm})^*)))T^{-1}T$.

Note that $\phi_s^{-1}(\pi((a_p^{\pm})^* \cdots (a_n^{\pm})^*)))T^{-1}T$ is rational as the image of a rational set under an automorphism is effectively rational, and the concatenation of rational sets is rational (see Section 2.2).

It remains to show that $i_p < j_p$ can be determined by checking membership in an effectively constructible rational set. Let k be the exponent of a_p within $\phi_s(s^{-1}t)$. We will show that $i_p < j_p$ if and only if $(a_1^{i_1} \cdots a_n^{i_n} s)^{-1}(a_1^{j_1} \cdots a_n^{j_n} t) \in$

$\phi_s^{-1}(\pi(a_1^\pm)^* \cdots (a_{p-1}^\pm)^*(a_p^{k+1}a_p^*)(a_{p+1}^\pm)^* \cdots (a_n^\pm)^*)T$. We have

$$(a_1^{i_1} \cdots a_n^{i_n} s)^{-1}(a_1^{j_1} \cdots a_n^{j_n} t) = \phi_s^{-1}(a_1^{j_1-i_1} \cdots a_n^{j_n-i_n})s^{-1}t$$
$$= \phi_s^{-1}(a_1^{j_1-i_1} \cdots a_n^{j_n-i_n}\phi_s(s^{-1}t)).$$

Thus the exponent of a_p in the expression for $a_1^{j_1-i_1} \cdots a_n^{j_n-i_n}\phi_s(s^{-1}t)$ will equal $j_p - i_p + k$, and so $i_p < j_p$ if and only if this exponent is strictly greater than k and so checking $i_p < j_p$ is equivalent to checking membership in $\phi_s^{-1}(\pi(a_1^\pm)^* \cdots (a_{p-1}^\pm)^*(a_p^{k+1}a_p^*)(a_{p+1}^\pm)^* \cdots (a_n^\pm)^*)T$, which is rational as the automorphic image of a rational set. We have thus shown that $x \leq_{\text{lex}} y$ and we are in this case (Case 1) if and only if $xy^{-1} \in \phi_s^{-1}(\pi((a_p^\pm)^* \cdots (a_n^\pm)^*)))T^{-1}T$ and $xy^{-1} \in \phi_s^{-1}(\pi(a_1^\pm)^* \cdots (a_{p-1}^\pm)^*(a_p^{k+1}a_p^*)(a_{p+1}^\pm)^* \cdots (a_n^\pm)^*)T$, and so checking we lie in this case and that $x \leq_{\text{lex}} y$ is equivalent to verifying membership of xy^{-1} in a finite intersection of effectively constructible rational sets. By Lemma 8.4, this is equivalent to verifying membership in a single effectively constructible rational set.

Case 2: $i_1 = j_1, \ldots, i_n = j_n$ and $s \leq_{\text{lex}} t$.
We can use the argument from the first part of Case 1 to check that $i_1 = j_1, \ldots, i_n = j_n$, by just taking q to be $n+1$.

Note that for each $r \in T$, the coset Ar is rational and explicitly computable: it is the projection of the language $(a_1^\pm)^* \cdots (a_n^\pm)^*r$. As T is finite, checking $g \leq_{\text{lex}} h$ in this case reduces to checking if $g \in Ar$ and $h \in Ar'$ for any (of the finitely many) $(r, r') \in T \times T$, with $r \leq_{\text{lex}} r'$. $\square$

Since one element is shortlex smaller than another if and only if it is length smaller, or length equal and lexicographically smaller, shortlex constraints reduce to checking length constraints and lexicographic constraints, both of which are equivalent to checking effectively constructible rational sets.

Corollary 8.6. *Let G be a finitely generated virtually abelian group. Fix a finite-index free abelian subgroup A, a free abelian basis B for A and a (finite) right transversal T. Then verifying any shortlex order constraint $X \leq_{shortlex} Y$ is equivalent to checking membership of each of X, Y and $X^{-1}Y$ in a certain effectively constructible rational set.*

Proof. We have that X is shortlex less than or equal to Y if and only if $|X| < |Y|$, or $|X| = |Y|$ and $X \leq_{\text{lex}} Y$. We can check both $|X| < |Y|$ and $|X| = |Y|$ using Theorem 5.2 (with each element of the generating set $B \cup T$ weighted with a 1), and we can check if $X \leq_{\text{lex}} Y$ using Theorem 8.5. We can put together two conditions, such as $|X| = |Y|$ and $X \leq_{\text{lex}} Y$, by checking membership in all the rational sets corresponding to these constraints produced effectively in Theorems 5.2 and 8.5, and using Lemma 8.4 to resolve any intersections. $\square$

Appendix A. Proofs for Section 3

Proof of Corollary 3.4. By Remark 3.1, we may assume that X is linear, say $X = a + B^*$. We have $\phi \colon x \mapsto Mx + c$ for some $l \times k$ integer matrix M and constant $c \in \mathbb{Z}^l$. The image of X is then

$$\phi(X) = \{\phi(a+b) : b \in B^*\} = \phi(a) + \{Mb : b \in B^*\} = \phi(a) + \{Mb : b \in B\}^*,$$

which is a linear set.

Let $\theta \colon \mathbb{Z}^k \to \mathbb{Z}^{k+l}$ be the integer affine map defined by $x \mapsto (x, \phi(x))$, whose image $\theta(\mathbb{Z}^k)$ is semilinear and effectively constructible by the previous paragraph. Since Y is semilinear in $\mathbb{Z}^l$, we can construct $\mathbb{Z}^k \times Y$ as a semilinear subset of $\mathbb{Z}^{k+l}$. By Theorem 3.2, $\theta(\mathbb{Z}^k) \cap (\mathbb{Z}^k \times Y)$ is semilinear and effectively constructible. If we let $p \colon \mathbb{Z}^{k+l} \to \mathbb{Z}^k$ be the integer affine map defined by projecting to the first k coordinates, we have

$$\phi^{-1}(Y) = p\left(\theta(\mathbb{Z}^k) \cap (\mathbb{Z}^k \times Y)\right)$$

and again this image is semilinear and effectively constructible. $\square$

Proof of Corollary 3.7. The proof of Proposition 3.11 of [10] shows that any elementary set can be expressed as a semilinear set. Polyhedral sets are finite unions of finite intersections of elementary sets so the result follows from Remark 3.1 and Theorem 3.2. $\square$

To prove Corollary 4.9 we need the following.

Lemma A.1. *For each $k \geq 1$, $\mathbb{Z}^k$ can be partitioned into 2^k (effectively constructible) monotone linear subsets.*

Proof. Write $e_1, \ldots e_k$ for the standard generators of $\mathbb{Z}^k$. The proof is by induction on k. For $k = 1$ we have the partition $\mathbb{Z} = \{e_1\}^* \cup (e_1^{-1} + \{e_1^{-1}\}^*)$. Now assume that we have a disjoint union $\mathbb{Z}^{k-1} = \bigcup_{i=1}^{2^{k-1}} (b_i + C_i^*)$ where each $b_1 + C_i^*$ is a monotone linear set. For each i, define $U_i^+ = b_i + C_i^* + \{e_k\}^* = b_i + (C_i \cup \{e_k\})^*$ and $U_i^- = b_i + C_i^* + e_k^{-1} + \{e_k^{-1}\}^* = b_i + e_k^{-1} + (C_i \cup \{e_k^{-1}\})^*$. By construction, each of these new sets is monotone and linear, and they are all disjoint. Furthermore, we have $\mathbb{Z}^k = \bigcup_{i=1}^{2^{k-1}} (U_i^+ \cup U_i^-)$, which is a disjoint union of 2^k monotone linear sets. $\square$

Proof of Corollary 4.9. Let $\bigcup_{i=1}^{2^k} Q_i$ denote any partition of $\mathbb{Z}^k$ into 2^k monotone linear sets. Lemma A.1 ensures that such a partition exists and is effectively constructible. Let $S_i = S \cap Q_i$ for each i. Each S_i is monotone by construction and semilinear and effectively constructible by Theorem 3.2. Their union is disjoint and equal to S. $\square$

References

[1] Parosh Aziz Abdulla, Mohamed Faouzi Atig, Yu-Fang Chen, Lukáš Holík, Ahmed Rezine, Philipp Rümmer, and Jari Stenman. String constraints for verification. In Armin Biere and Roderick Bloem, editors, *Computer Aided Verification*, pages 150–166, Cham, 2014. Springer International Publishing.

[2] Roberto Amadini. A survey on string constraint solving. *ACM Comput. Surv.*, 55(1), nov 2021.

[3] Yago Antolín, Cristóbal Rivas, and Hang Lu Su. Regular left-orders on groups. *J. Comb. Algebra*, 6(3-4):265–314, 2022.

[4] M. Benson. Growth series of finite extensions of $\mathbf{Z}^n$ are rational. *Invent. Math.*, 73(2):251–269, 1983.

[5] Jean Berstel. *Transductions and context-free languages.* B. G. Teubner, Stuttgart, 1979.

[6] A. Bishop. Geodesic growth in virtually abelian groups. *J. Algebra*, 573:760–786, 2021.

[7] J. Richard Büchi and Steven Senger. Definability in the existential theory of concatenation and undecidable extensions of this theory. *Zeitschrift fur mathematische Logik und Grundlagen der Mathematik*, 34(4):337–342, 1988.

[8] A. Carvahlo. Algebraic and context-free subsets of subgroups. 2022. https://arxiv.org/abs/2210.10001.

[9] L. Ciobanu and M. Elder. The complexity of solution sets to equations in hyperbolic groups. *Israel J. Math.*, 245(2):869–920, 2021.

[10] L. Ciobanu and A. Evetts. Rational sets in virtually abelian groups: languages and growth. *L'Enseignement mathématique*, 2023. https://arxiv.org/abs/2205.05621.

[11] L. Ciobanu and A. Garrett. Group equations with abelian predicates. *Int. Math. Res. Notices*, 2023+. https://arxiv.org/abs/2204.13946.

[12] L. Ciobanu and A. Levine. Languages, groups and equations. 2023. https://arxiv.org/abs/2303.07825.

[13] F. Dahmani. Existential questions in (relatively) hyperbolic groups. *Israel J. Math.*, 173:91–124, 2009.

[14] François Dahmani and Vincent Guirardel. Foliations for solving equations in groups: free, virtually free, and hyperbolic groups. *J. Topol.*, 3(2):343–404, 2010.

[15] Flavio D'Alessandro, Benedetto Intrigila, and Stefano Varricchio. Quasi-polynomials, linear Diophantine equations and semi-linear sets. *Theoret. Comput. Sci.*, 416:1–16, 2012.

[16] Joel D Day, Vijay Ganesh, Paul He, Florin Manea, and Dirk Nowotka. The satisfiability of word equations: Decidable and undecidable theories. In *International Conference on Reachability Problems*, pages 15–29. Springer, 2018.

[17] Volker Diekert. Commutative monoids have complete presentations by free (noncommutative) monoids. *Theoret. Comput. Sci.*, 46(2-3):319–327, 1986.

[18] V. G. Durnev. Equations on free semigroups and groups. *Mat. Zametki*, 16:717–724, 1974.

[19] S. Eilenberg and M. P. Schützenberger. Rational sets in commutative monoids. *J. Algebra*, 13:173–191, 1969.

[20] Javier Esparza, Pierre Ganty, Stefan Kiefer, and Michael Luttenberger. Parikh's theorem: a simple and direct automaton construction. *Inform. Process. Lett.*, 111(12):614–619, 2011.

[21] A. Evetts. Rational growth in virtually abelian groups. *Illinois J. Math.*, 63(4):513–549, 2019.

[22] A. Evetts and A. Levine. Equations in virtually abelian groups: Languages and growth. *Internat. J. Algebra Comput.*, 32(3):411–442, 2022.

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

[24] Albert Garreta and Robert Gray. On equations and first-order theory of one-relator monoids. *Inform. and Comput.*, 281, December 2021.

[25] Seymour Ginsburg and Edwin H. Spanier. Bounded ALGOL-like languages. *Trans. Amer. Math. Soc.*, 113:333–368, 1964.

[26] Jan Grabowski. An algorithm to identify slices, with applications to vector replacement systems. In *Fundamentals of computation theory (Szeged, 1981)*, volume 117 of *Lecture Notes in Comput. Sci.*, pages 425–432. Springer, Berlin-New York, 1981.

[27] Z. Grunschlag. *Algorithms in geometric group theory*. PhD thesis, University of California, Berkeley, 1999.

[28] Thomas Herbst. On a subclass of context-free groups. *RAIRO Inform. Théor. Appl.*, 25(3):255–272, 1991.

[29] Thomas Herbst and Richard M. Thomas. Group presentations, formal languages and characterizations of one-counter groups. *Theoret. Comput. Sci.*, 112(2):187–213, 1993.

[30] D. F. Holt, S. Rees, and C. E. Röver. *Groups, languages and automata*, volume 88 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2017.

[31] Mark Kambites, Pedro V. Silva, and Benjamin Steinberg. On the rational subset problem for groups. *J. Algebra*, 309(2):622–639, 2007.

[32] Alex Levine. EDT0L solutions to equations in group extensions. *J. Algebra*, 619:860–899, 2023.

[33] Markus Lohrey. The rational subset membership problem for groups: a survey. In *Groups St Andrews 2013*, volume 422 of *London Math. Soc. Lecture Note Ser.*, pages 368–389. Cambridge Univ. Press, Cambridge, 2015.

[34] K. A. Mihaĭlova. The occurrence problem for direct products of groups. *Mat. Sb. (N.S.)*, 70 (112):241–251, 1966.

[35] W. D. Neumann and M. Shapiro. Automatic structures, rational growth, and geometrically finite hyperbolic groups. *Invent. Math.*, 120(2):259–287, 1995.

[36] W. D. Neumann and M. Shapiro. Regular geodesic normal forms in virtually abelian groups. *Bull. Austral. Math. Soc.*, 55(3):517–519, 1997.

[37] Pedro V. Silva. Recognizable subsets of a group: finite extensions and the abelian case. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, (77):195–215, 2002.

MAXWELL INSTITUTE OF MATHEMATICAL SCIENCES, AND DEPARTMENT OF MATHEMATICS, HERIOT-WATT UNIVERSITY, EDINBURGH EH14 4AS, UK

Email address: `l.ciobanu@hw.ac.uk`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MANCHESTER M13 9PL, UK AND THE HEILBRONN INSTITUTE FOR MATHEMATICAL RESEARCH, BRISTOL, UK

Email address: `alex.evetts@manchester.ac.uk`

SCHOOL OF ENGINEERING, MATHEMATICS AND PHYSICS, UNIVERSITY OF EAST ANGLIA, NORWICH NR4 7TJ, UK

Email address: `a.levine@uea.ac.uk`