Group equations with abelian predicates

Author(s)

Abstract

In this paper we begin the systematic study of group equations with abelian predicates in the main classes of groups where solving equations is possible. We extend the line of work on word equations with length constraints, and more generally, on extensions of the existential theory of semigroups, to the world of groups.

We use interpretability by equations to establish model-theoretic and algebraic conditions which are sufficient to get undecidability. We apply our results to (non-abelian) partially commutative or right-angled Artin groups (RAAGs), and show that the problem of solving equations with abelian predicates is undecidable for these. By contrast, we prove that in groups with finite abelianization, the problem can be reduced to solving equations with recognisable constraints, and so this is decidable in right-angled Coxeter groups, or more generally, graph products of finite groups, as well as hyperbolic groups with finite abelianization.

2012 ACM Subject Classification Theory of computation → Logic:Equational logic and rewriting; Mathematics of computing → Combinatorics on words

Keywords and phrases Word equations, Diophantine Problem, constraints, definability, interpretability, hyperbolic groups, partially commutative groups.

Digital Object Identifier 10.4230/LIPIcs...

Category Track B: Automata, Logic, Semantics, and Theory of Programming

1 Introduction

The study of equations in algebraic structures such as semigroups, groups or rings is a fundamental topic in mathematics and theoretical computer science that finds itself at the frontier between decidable and undecidable. In this paper we draw inspiration from the extensive work on word equations with various length constraints [1, 4, 7, 10, 13] and consider equations in groups with similar (non-rational) constraints. Deciding algorithmically whether a word equation has solutions satisfying certain linear length constraints is a major open question, and it has deep implications, both theoretical (if undecidable, it would offer a new solution to Hilbert's 10th problem about the satisfiability of polynomial equations with integer coefficients) and practical, in the context of string solvers for security analysis. We refer the reader to the surveys [3, 9] for an overview of the area from several viewpoints, of both theoretical and applied nature.

We find similarities to word equations with length constraints, but also new territory, when entering the world of groups. The question of decidability of (systems of) equations is widely known as the *Diophantine Problem*, and we denote it by $\mathcal{DP}$, or by $\mathcal{DP}(G)$ when it refers to a (semi)group G (see Section 2.1). We extend the $\mathcal{DP}$ by requiring that the solution sets satisfy certain (non-rational) constraints, and study this augmented problem in some of the most important classes of infinite groups for which the $\mathcal{DP}$ is known to be decidable, such as partially commutative groups (the group counterparts of trace monoids) and more generally, graph products of groups, as well as hyperbolic groups. Our motivation is twofold: first, explore extensions of the $\mathcal{DP}$ that have not been systematically studied for groups before, and second, develop algebraic and model-theoretic tools that can complement the combinatorial techniques used for solving word equations.

Among several types of length constraints (see Section 2.2), we focus on abelian predicates (such as AbelianEq in [7]), which we also call *abelianization constraints*, and denote by ab;

these require that the 'abelian form' of the solutions, where any two symbols commute, satisfies a given set of equations as well (equivalently, the constraints can be viewed as equations in the abelianization of G). We denote this problem by $\mathcal{DP}(G, \mathsf{ab})$, and note that this can be seen as introducing an abelian predicate or relation to the existential theory of G. Our main results are:

▶ **Theorem A.** *(Theorem 38) Let G be a partially commutative group (or right-angled Artin group) that is not abelian. Then $\mathcal{DP}(G, \mathsf{ab})$ is undecidable.*

▶ **Theorem B.** *(Theorems 19, 20, 22) Let G be a group where the $\mathcal{DP}$ with recognisable constraints is decidable. Then $\mathcal{DP}(G, \mathsf{ab})$ is decidable. In particular, this holds if:*
1. *G is a hyperbolic group with finite abelianization.*
2. *G be a graph product of finite groups, such as a right-angled Coxeter group.*

A key contribution of the paper is the interleaving of algebra and model theory, and the tools we are introducing and using; these tools have the potential to lead to results for further classes of groups and possibly semigroups, and more diverse length constraints. In fact, in upcoming work we use the tools developed here in order to extend the Item 1. in Theorem B to hyperbolic groups with infinite abelianization. The main tool used to prove undecidability results in this paper is *interpretability* using disjunctions of equations (i.e. positive existential formulas), or *PE-interpretability*, which allows us to translate one structure into another and to reduce the Diophantine Problem from one structure to the other (Section 2.3). The main reductions are to the Diophantine Problem in the ring of integers, which is a classical undecidable problem (Hilbert's 10th problem). We give a technical result in Section 5 which enables us to encode the Diophantine Problem over the integers into the Diophantine Problem with abelianization constraints in a group, assuming the group satisfies certain model-theoretic properties. This technical result (Lemma 26) is then applied to partially commutative groups, and in work in progress also to hyperbolic groups with large abelianization or more general graph products.

Our starting point is Büchi and Senger's well-known paper [4], where they show that (positive) integer addition and multiplication can be encoded into word equations in the free semigroup Σ^* on a finite alphabet Σ, when requiring that the solutions satisfy an abelian predicate; by the undecidability of Hilbert's 10th problem, such enhanced word equations are also undecidable. In order to encode the multiplication in the ring $(\mathbb{Z}, \oplus, \odot)$ within a group or semigroup, they need two 'independent' elements, which can be taken to be two of the free generators if the (semi)group is free. In non-free groups we require the existence of two elements that play a similar role; however, it is not enough to pick two generators, these elements also need to satisfy additional properties with respect to the abelianization. Finding such a pair of elements, which we call *abelian-primitive*, is difficult or impossible for arbitrary groups, but in this paper we show that they can be found in partially commutative groups. A large part of the paper is concerned with defining, studying and finding abelian-primitive generators, which are not well-defined in general.

The outline of the article is as follows. In Section 2 we introduce free and partially commutative groups, which are the main objects of the paper, together with notions of length and exponent-sum functions associated to a generator in a group. We also introduce the abelianization of a group, which is essentially the commutative version of the group. We then describe equations in groups and introduce the Diophantine Problem together with several variants, where the solutions have to satisfy not just a system of equations in a chosen group, but also certain constrains, such as rational, recognisable, or a set of equations in the abelianization (Section 2.2). We introduce *definability* by equations, or *PE-definability*,

and *interpretability* using equations, or *PE-interpretability*, in Section 2.3. This allows us to translate one structure into another and to reduce the $\mathcal{DP}$ from one structure to the other (Proposition 14). In Section 3 we give results for free groups and semigroups following Büchi and Senger; although these results might be known to the experts and get generalised in later sections, it is useful to see the basic idea in action for free groups.

Section 4 provides an interesting contrast to the rest of the paper, in that we obtain positive results for $\mathcal{DP}(G, \mathsf{ab})$ for cases when G has finite abelianization. In this case the $\mathcal{DP}(G, \mathsf{ab})$ can be reduced to the $\mathcal{DP}(G)$ with recognisable constraints, and we showcase groups for which these problems are decidable. Section 5 provides the technical tools (Lemma 26) required to encode the Diophantine Problem over the integers into a group Diophantine Problem with abelianization constraints, if the group satisfies certain model-theoretic properties. We use this technical section to establish the most involved result of the paper (Theorem 38) in Section 6, namely, that the $\mathcal{DP}$ with abelianization constraints is undecidable in (non-abelian) partially commutative groups. In the final section we outline several of the many possible directions of future research that naturally stem from this paper.

2 Preliminaries

Let Σ be a finite set, and let $||w||$ denote the word length of any $w \in \Sigma^*$. For any $a \in \Sigma$, let $||w||_a$ count the number of occurrences of a in w; for example, $||abab^2||_a = 2$.

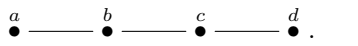
Free groups. Define Σ^{-1} as the set of formal inverses of elements in Σ and denote the free group with generating set Σ by $F(\Sigma)$; $F(\Sigma)$ can be viewed as the set of all *freely reduced words* over $\Sigma^{\pm 1} = \Sigma \cup \Sigma^{-1}$, that is, words not containing xx^{-1} as subwords, $x \in \Sigma^{\pm 1}$, together with the operations of concatenation and free reduction (that is, the removal of any xx^{-1} that might occur when concatenating two words, where $(x^{-1})^{-1}$ for any $x \in \Sigma^{\pm 1}$.

Partially commutative groups (RAAGs). A group G generated by the finite set Σ, subject to a set of relations $R \subset F(\Sigma) \times F(\Sigma)$, is denoted as $G = \langle \Sigma \mid R \rangle$ and can be viewed as $F(\Sigma)$ modulo the relations in R: two elements are equal in G if there is a way of writing them as words which can be transformed into each other via the relations in R, together with deleting or inserting xx^{-1}, $x \in \Sigma^{\pm}$. For example, the free abelian group $(\mathbb{Z}^2, +)$ can be given by generators $\Sigma = \{a, b\}$ that satisfy the relation (ab, ba), which we write as $ab = ba$. One may replace $ab = ba$ by $aba^{-1}b^{-1} = 1$, and use the commutator notation $[a, b] = 1$.

A class of groups that lie between the free (non-abelian) and the free abelian groups, in terms of their presentations, are the *partially commutative groups*. They are the group theoretic counterpart to partially commutative monoids, or trace monoids. In geometric group theory these are called *right-angled Artin groups* (RAAGs), and we will use this short-hand notation to save space. The most common way of describing a RAAG is via a finite undirected graph Γ with no auto-adjacent vertices (i.e. no loops at any vertex) and no multiple edges between two vertices, and letting the vertices of Γ be the generators of the RAAG $G\Gamma$ based on Γ. The relations between generators correspond to the edges: for every edge (u, v) in Γ we introduce the commuting relation $uv = vu$.

We note that we will often write G instead of $G\Gamma$ when the graph Γ is unambiguous.

▶ **Example 1.** Let Γ be the graph below with vertices $\{a, b, c, d\}$ and 3 edges. The RAAG $G = G\Gamma$ based on Γ has the presentation $\langle a, b, c, d \mid [a, b] = [b, c] = [c, d] = 1 \rangle$; that is, G has generators $\{a, b, c, d\}$ which satisfy the relations $ab = ba$, $bc = cb$, and $cd = dc$.



Abelianization. For any group G, let $\mathsf{ab} : G \to G^{\mathsf{ab}}$ be the natural abelianization map. That is, G^{ab} is the group with the presentation of G, plus the additional relations that any two generators commute. In algebraic terms, $G^{\mathsf{ab}} = G/G'$, that is, the quotient of G by its commutator subgroup; G^{ab} is a commutative group which will decompose into an infinite part of the form $\mathbb{Z}^m$, for some $m \geqslant 1$, and a finite abelian group H. The integer m is called *the free rank* of G^{ab}. So for example, the abelianization of $F(a,b)$ is the free abelian group $(\mathbb{Z}^2, +)$ and is of free rank 2; this is because $F(a,b)$ has generators $\{a,b\}$ and no relations, and the abelianization has the same generators, but now they commute. The analogous map $\mathsf{ab} : \Sigma^* \mapsto \mathbb{N}^{|\Sigma|}$ for free monoids is called the *Parikh map* in language theory.

Length and exponent-sum. Every element g in a group G generated by Σ has a length $|g|_\Sigma$, which is the word length $||.||$ of a shortest word w representing g in G. For example, the length of aba^{-1} in $\mathbb{Z}^2$ is $|aba^{-1}|_\Sigma = ||b|| = 1$.

For any generator x of $F(\Sigma)$, the map $|.|_x : F(\Sigma) \to \mathbb{Z}$ represents the *exponent-sum* of x in a word w; that is, $|w|_x = ||w||_x - ||w||_{x^{-1}}$, so for example $|xyx^{-1}y^2|_x = 0$. One can define the exponent-sum of a generator x in an element g for certain (but not all) groups beyond free groups, and then we use the same notation $|g|_x$, as we explain next. The length and the image under abelianization are well-defined for any element in any finitely generated group. However, the situation regarding the exponent-sum (of a generator) is more complicated. For example, if H is a group and $x \in H$ a generator of order 5, then one may claim the exponent-sum of x in the element x^3 to be 3; but $x^3 = x^{-2}$ in H, and in x^{-2} the exponent-sum of x appears to be -2.

We give below sufficient conditions for the exponent-sum function to be well-defined. Among other requirements, we need the groups to be infinite and have infinite abelianization, and moreover, the generators for which we consider the exponent-sums to have infinite order not just in the group, but also in the abelianization.

▶ **Definition 2.** *Let G be a group generated by a set S, and let $\mathsf{ab} : G \to G^{\mathsf{ab}}$ be the natural abelianization map. Suppose G^{ab} has free rank $\geqslant 1$, that is, G^{ab} is infinite.*

A subgroup $K \leqslant G^{ab}$ is a $\mathbb{Z}$-factor if K is isomorphic to $\mathbb{Z}$ and $G^{ab} = K \times H$ for some $H \leqslant G^{ab}$. If $s \in S$ is such that $\mathsf{ab}(s)$ generates a $\mathbb{Z}$-factor in G^{ab}, we say that s is abelian-primitive.

Note that any abelian-primitive element s has infinite order.

▶ **Example 3.** Any generator of a free group is abelian-primitive. More generally, any group element corresponding to a vertex in the graph defining a RAAG is abelian-primitive.

We extend the definition of exponent-sum from free groups to any group G containing abelian-primitive elements. Let π be the natural projection $\pi : F(S) \to G$, $s \in S$ be abelian-primitive, and $\mathsf{abs}(x)$ be the absolute value of $x \in \mathbb{Z}$ (we use abs to avoid confusion with the notation for length). For $g \in G$ we let the *exponent-sum* of s in g be

$$|g|_s := |w_g|_s, \text{ where } w_g \in F_S \text{ is such that}$$
$$\mathsf{abs}(|w_g|_s) \text{ is minimal among } w \in F(S) \text{ such that } \pi(w) = g.$$

The next lemma shows that the exponent-sum function is well-defined.

▶ **Lemma 4.** *Let G be generated by S, and suppose $w_g, w'_g \in F(S)$ are such that $w_g \neq w'_g$, $\pi(w_g) = \pi(w'_g) = g$, $\mathsf{abs}(|w_g|_s) = \mathsf{abs}(|w_{g'}|_s)$ is minimal, and s is abelian-primitive.*

Then $|w_g|_s = |w_{g'}|_s$.

Proof. Suppose $|w_g|_s \neq |w_{g'}|_s$. Then $|w_g|_s = -|w_{g'}|_s \neq 0$. From the equality $\mathsf{ab}(\pi(w_g)) = \mathsf{ab}(\pi(w_{g'}))$, solving for $\mathsf{ab}(s)$ in G^{ab}, one obtains $(\mathsf{ab}(s))^t \in H$ for some subgroup H such that $G^{\mathsf{ab}} = \langle \mathsf{ab}(s) \rangle \times H$, contradicting the fact that s is abelian-primitive. ◀

The above definition of $|g|_s$, altough a generalisation of the exponent-sum in a free monoid or group, may seem rather unnatural due to the presence of the absolute value function. Next we provide an equivalent, but more natural definition. All arguments in this paper use this equivalent formulation for the notion of being abelian-primitive.

▶ **Lemma 5.** *Let $G = \langle S \rangle$ be a group generated by a set S, and let $s \in S$ be abelian-primitive, so that $G^{ab} \cong \langle \mathsf{ab}(s) \rangle \times H \cong \mathbb{Z} \times H$. Then for each $g \in G$ there exists a unique $t_g \in \mathbb{Z}$ and a unique $c_g \in G$ such that $g = s^{t_g} c_g$, $\mathsf{ab}(c_g) \in H$, and $t_g = |g|_s$.*

That is, for all $g \in G$, the exponent-sum $|g|_s$ of s in g is precisely the exponent of $\mathsf{ab}(s)$ in the natural projection of g onto the abelianization $G^{ab} = \langle \mathsf{ab}(s) \rangle \times H$.

The following lemma follows immediately from Lemma 5 and will be used extensively, often without precise reference. It allows us to compute $|g|_s$ by expressing g as a product of generators and their inverses, and then summing over the exponent-sums of s in such a product. The resulting value is independent of the chosen product for g.

▶ **Lemma 6** ($|\cdot|_s$ is a homomorphism)**.** *Let $G = \langle S \rangle$ be a group, and let $s \in S$ be abelian-primitive. Then $|\cdot|_s$ defines a group homomorphism $|\cdot|_s : G \to \mathbb{Z}$, that is*

$$|gh|_s = |g|_s + |h|_s \tag{1}$$

for all $g, h \in G$.

2.1 The Diophantine problem in groups and semigroups

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

▶ **Example 7.** 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 $\mathcal{DP}(G)$.

2.2 The Diophantine Problem with constraints

Let Σ be a finite alphabet and let $S = \Sigma^{\pm 1}$. Suppose G is a group generated by S, and let $\pi : S^* \to G$ 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 over S is *regular* if it is recognised by a finite state automaton, as is standard.

▶ **Definition 8.**

(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 $\pi(L')$ of a regular subset L' of S^*.*

It follows immediately from the definition that recognisable subsets of G are rational.

Let $\mathcal{E}$ be a system of equations on variables $\mathcal{X} = \{X_1, \ldots, X_k\}$ in a (semi)group G.

The *Diophantine Problem with rational or recognisable constraints* asks about the existence of solutions to $\mathcal{E}$, with some of the variables restricted to taking values in specified rational or recognisable sets.

We next attach three types of non-rational constraints to the Diophantine problem:

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 where the unknowns correspond to the lengths of solutions to each variable $X_i \in \mathcal{X}$. Then $\mathcal{DP}(G, \mathrm{L})$ asks whether solutions to $\mathcal{E}$ exist for which the lengths satisfy the system Θ.
2. Suppose the generators of G can be enumerated as $S = \{g_i \mid 1 \leqslant i \leqslant m\}$, with each g_i being abelian-primitive, and write $|.|_i$ for $|.|_{g_i}$.
   We let $\mathcal{DP}(G, \{|.|_i\}_i)$ denote the $\mathcal{DP}$ with *linear exponent-sum constraints*. A set of exponent-sum constraints is a system Θ of linear Diophantine equations where the unknowns correspond to the exponent-sums of generators in the solutions to each variable $X_i \in \mathcal{X}$. Then $\mathcal{DP}(G, \{|.|_i\}_i)$ asks whether a solution to $\mathcal{E}$ exists satisfying the system Θ. This definition can be extended to the case where only a strict subset of S are abelian-primitive by using unknowns in Θ that only correspond to abelian-primitive generators.
3. We write $\mathcal{DP}(G, \mathsf{ab})$ for the $\mathcal{DP}$ where an abelian predicate is added, or equivalently, *abelianization constraints* are imposed. A set of abelianization 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 abelianization of the solution satisfies the system Θ in G^{ab}.

▶ **Example 9.** Consider the equation $XaY^2bY^{-1} = 1$ over variables X, Y in the free group on two generators $F(a, b)$ with length function $|.| = |.|_{\{a,b\}}$ and abelianization $(\mathbb{Z}^2, +)$.

1. An instance of $\mathcal{DP}(F(a, b), \mathrm{L})$ 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 $\mathcal{DP}(F(a, b), \{|.|_a, |.|_b\})$ is: decide whether there are any solutions (x, y) such that $|x|_a = 2|y|_a + |y|_b$ and $|x|_b = 3|y|_b$; the answer is 'no' by solving a basic linear system over the integers with variables $|x|_a, |x|_b, |y|_a, |y|_b$ and we leave this as an exercise.
3. An instance of $\mathcal{DP}(F(a, b), \mathsf{ab})$ is: decide whether there are any solutions (x, y) such that $\mathsf{ab}(x) = 3\mathsf{ab}(y)$ (we use additive notation for $\mathbb{Z}^2$); the answer is no, since $\mathsf{ab}(xax^2by^{-1}) = \mathsf{ab}(x) + \mathsf{ab}(y) + (1, 1) = (0, 0)$ together with $\mathsf{ab}(x) = 3\mathsf{ab}(y)$ lead to $4\mathsf{ab}(y) = (-1, -1)$, which is not possible in $\mathbb{Z}^2$.

Next we provide a brief formal and unifying description of the notions of "constraints" and "relations". A relation r in a group G can be specified as a subset of $S_r \subseteq G^{n_r}$. Then, a tuple $(g_1, \ldots, g_r)$ satisfies the relation r if and only if $(g_1, \ldots, g_r) \in S_r$. In general, one can consider a set of relations $\mathcal{R}$ in a group G, and study the so-called *Diophantine Problem in G with $\mathcal{R}$-constraints*, denoted $\mathcal{D}(G, \mathcal{R})$. The instances to this problem are *systems of equations with constraints in* $(G, \mathcal{R})$, that is, systems of equations in G on variables $\mathbf{x}$ together with finitely many formal expressions of the form $r(w_1(\mathbf{x}), \ldots, w_{n_r}(\mathbf{x}))$, where $r \in \mathcal{R}$, n_r is the arity of r, and the $w_i(\mathbf{x})$ are words on $\mathbf{x}$ and possibly constant elements from G. A solution to such an instance is a solution to the system of equations such that all expressions $r(w_1(\mathbf{x}), \ldots, w_{n_r}(\mathbf{x}))$ are true (i.e. the corresponding tuples of elements belong to S_r) after replacing each variable by its corresponding value. For example, the three problems $\mathcal{DP}(G, L), \mathcal{DP}(G, \{|\cdot|_i\}_i)$ and $\mathcal{DP}(G, \mathsf{ab})$ can be formulated in this manner; for $\mathcal{DP}(G, \mathsf{ab})$ we think of ab as the relation determined by the set $S_{\mathsf{ab}} = \{(g, h) \in G^2 \mid \mathsf{ab}(g) = \mathsf{ab}(h)\}$.

The following will be used later in the paper.

▶ **Lemma 10.** *Let G_1 and G_2 be two groups, and suppose that $\mathcal{DP}(G_1, \mathsf{ab})$ is undecidable. Then $\mathcal{DP}(G_1 \times G_2, \mathsf{ab})$ is also undecidable.*

2.3 Interpretability

Here we define *interpretability by positive existential formulas* (PE-interpretability). This is a partial order between algebraic structures which implies reducibility of the Diophantine Problem from one structure to the other. A *positive existential formula* in a language L is a first-order formula which can be written using only existential quantifiers, disjunctions, conjunctions, equality, and the symbols from L (possibly with an extended set of constants). It is well known that such a formula is logically equivalent to a disjunction of systems of equations. This explains the terminology used in Definition 11. This equivalence will be used extensively throughout the paper without further referring to it, and we will sometimes identify the concepts "positive existential formula" with "disjunction of systems of equations".

We restrict ourselves to groups and rings, although all definitions can be generalised to arbitrary algebraic structures, and make the convention that all logical formulas are allowed to use any number of constants from the group or ring considered.

Given a group G, we will denote its operation by $\cdot_G$, and its identity element by 1_G. We will use non-cursive boldface letters to denote tuples of elements: e.g. $\mathbf{a} = (a_1, \dots, a_n)$.

▶ **Definition 11.** *Let G be a group and let $\mathcal{R}$ be a set of relations in G. A set $D \subset G \times \overset{m}{\dots} \times G = G^m$ is called* definable by positive existential formulas *in $(G, \mathcal{R})$, or* PE-definable *in $(G, \mathcal{R})$, if there exist finitely many (finite) systems of equations with constraints in $(G, \mathcal{R})$, $\mathcal{E}_{D,1}, \dots, \mathcal{E}_{D,r}$ on variables $(x_1, \dots, x_m, y_1, \dots, y_k) = (\mathbf{x}, \mathbf{y})$ and some constants from G, such that for any tuple $\mathbf{a} \in G^m$, one has that $\mathbf{a} \in D$ if and only if there exists $i \in \{1, \dots, r\}$ such that the system of equations with constraints $\mathcal{E}_{D,i}(\mathbf{a}, \mathbf{y})$ on variables $\mathbf{y}$ has a solution in G. In this case $\mathcal{E}_{D,i}$ is said to* PE-define *D in G.*

If $\mathcal{R} = \emptyset$ then we simply speak of PE-definability in G.

▶ **Example 12.** A typical PE-definable set in a monoid or a group G is the centraliser of an element g, that is, the set $C_G(g) = \{h \in G \mid gh = hg\}$; an element $x \in G$ belongs to $C_G(g)$ if and only if x is a solution to the equation $xg = gx$.

Another classical example is the centre $Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$ of a group G generated by a finite set $\{g_1, \dots, g_n\}$. Indeed, an element $x \in Z(G)$ if and only if x satisfies the system of equations $[x, g_1] = 1, \dots, [x, g_n] = 1$.

The use of disjunctions of systems allows to work comfortably with unions of PE-definable sets: if S_1 and S_2 are PE-defined in G and Φ_1, Φ_2 are two disjunctions of systems of equations PE-defining these sets, then $\Phi_1 \vee \Phi_2$ is again PE-formula, and it PE-defines $S_1 \cup S_2$.

▶ **Definition 13.** *Let G and H be groups and let $\mathcal{R}_G$ and $\mathcal{R}_H$ be sets of relations in G and H, respectively. We say that $(H, \mathcal{R}_H)$ is* PE-interpretable *in $(G, \mathcal{R}_G)$ if there exists $n \in \mathbb{N}$, a subset $D \subseteq G^n$ and an onto map (called the* interpreting *map) $\phi : D \twoheadrightarrow H$, such that:*

1. *D is PE-definable in $(G, \mathcal{R})$.*
2. *The preimage under ϕ of the operation $\cdot_H$, i.e. the set $\{(\phi^{-1}(x_1), \phi^{-1}(x_2), \phi^{-1}(x_3)) \in H^3 \mid x_1 \cdot_H x_2 = x_3\}$, is PE-definable in $(G, \mathcal{R})$.*
3. *The preimage under ϕ of the graph of the equality relation in H, namely the set $\{(\phi^{-1}(x_1), \phi^{-1}(x_2)) \in H^2 \mid x_1 = x_2\})$, is PE-definable in $(G, \mathcal{R})$.*
4. *For each relation $r \in \mathcal{R}_H$ with arity t_r, the preimage under ϕ of the graph of r namely the set $\{\boldsymbol{w} = (\phi^{-1}(x_1), \dots, \phi^{-1}(x_{t_r})) \in H^{t_r} \mid \boldsymbol{w}$ satisfies $r\})$, is PE-definable in $(G, \mathcal{R}_G)$.*

In this paper all PE-interpretations will have the identity map as the interpreting map.

One can establish the analogous notion of a ring R which is PE-interpretable in $(G, \mathcal{R})$. *The definition in this case is analogous, requiring the preimages of the graphs of the ring sum, multiplication, and the equality relation, to be PE-definable in $(G, \mathcal{R})$.*

If $\mathcal{R}_G = \emptyset$ then we simply speak of PE-interpretability in G.

▶ **Proposition 14.** *(Reduction of Diophantine problems) Let G be a group, let $\mathcal{R}$ be a set of relations in G, let M be either a ring or a group, and let $\mathcal{R}_M$ be a set of relations in M. If $(M, \mathcal{R}_M)$ is PE-interpretable in $(G, \mathcal{R}_G)$, then $\mathcal{DP}(\mathcal{M}, \mathcal{R}_M)$ is reducible to $\mathcal{DP}(G, \mathcal{R}_G)$. Consequently, if $\mathcal{DP}(\mathcal{M}, \mathcal{R}_M)$ is undecidable, then $\mathcal{DP}(G, \mathcal{R}_G)$ is undecidable as well.*

Proposition 14 is well-known if one replaces disjunctions of equations by first-order formulas, and the problems $\mathcal{DP}(M, \mathcal{R}_M)$ and $\mathcal{D}(G, \mathcal{R})$ by the elementary theory of M enriched with the relations $\mathcal{R}_M$ and G enriched with the relations $\mathcal{R}_G$ (see Theorem 5.3.2 of [12] and its consequences). Our result can be proved following Theorem 5.3.2 of [12] step-by-step, replacing first-order formulas by finite disjunctions of equations, and elementary theories by Diophantine problems.

3 Results for free groups and free monoids

The results in this section will be generalised later in the paper and might be known to the experts, but the simpler arguments for free groups are worth including here. We use the ideas in [4] to encode addition and multiplication in $\mathbb{Z}$ into the $\mathcal{DP}(F(\Sigma), \mathsf{ab})$, and by the undecidability of Hilbert's 10th, get the same result for free groups.

▶ **Theorem 15** ([4], Cor. 4)**.** *The Diophantine problems $\mathcal{DP}(\Sigma^*, \mathsf{ab})$ and $\mathcal{DP}(\Sigma^*, \{||.||_i\}_i)$ are undecidable.*

Lemma 16 shows that there are connections between the Diophantine Problems with different kinds of constraints, when working with free monoids or free groups. These connections can be established by interpretability.

▶ **Lemma 16.** *Let $\Sigma = \{g_i \mid 1 \leqslant i \leqslant m\}$ be the set of generators of Σ^* or $F(\Sigma)$.*
(1) The $\mathcal{DP}(F(\Sigma), \{|.|_i\}_i)$ is decidable if and only if the $\mathcal{DP}(F(\Sigma), \mathsf{ab})$ is decidable.
(2) Similarly, $\mathcal{DP}(\Sigma^*, \{|.|_i\}_i)$ is decidable if and only if $\mathcal{DP}(\Sigma^*, \mathsf{ab})$ is decidable, and the decidability of these problems implies the decidability of $\mathcal{DP}(\Sigma^*, \mathrm{L})$.

▶ **Theorem 17.** *The $\mathcal{DP}(F(\Sigma), \mathsf{ab})$ and $\mathcal{DP}(F(\Sigma), \{|.|_i\}_i)$ are undecidable if $|\Sigma| \geqslant 2$.*

Proof. By Lemma 16, it suffices to prove that $\mathcal{DP}(F(\Sigma), \{|.|_i\}_i)$ is undecidable. To prove this we interpret the ring $(\mathbb{Z}, \oplus, \odot) \cong (\{g^t \mid t \in \mathbb{Z}\}, \oplus, \odot)$ in $\mathcal{DP}(F(\Sigma), \{|.|_i\}_i)$, where we define $g^{t_1} \oplus g^{t_2} =_{def} g^{t_1+t_2}$ and $g^{t_1} \odot g^{t_2} =_{def} g^{t_1 t_2}$, and g is a generator of $F(\Sigma)$. Here the interpreting map Φ is the identity map id on $\{g^t \mid t \in \mathbb{Z}\}$.

First, observe that the set $\{g^t \mid t \in \mathbb{Z}\}$ is defined by the equation $[x, g] = 1$ and the operation $\oplus$ coincides with the group multiplication in $F(\Sigma)$. Of course, the equality relation on $\{g^t \mid t \in \mathbb{Z}\}$ is also trivially PE-definable. Hence the abelian group $(\{g^t \mid t \in \mathbb{Z}\}, \oplus)$ is PE-interpretable in $F(\Sigma)$. We now PE-interpret $\odot$ in $(F(\Sigma), \{|.|_{g_i}\})$. Let $h \neq g$ be another generator. We claim that three elements $a_1, a_2, a_3 \in \{g^t \mid t \in \mathbb{Z}\}$ satisfy $a_1 \odot a_2 = a_3$ if and only if there exist $b, c \in F(\Sigma)$ such that

$$[b, h] = 1 \wedge [c, gb] = 1 \wedge |a_1|_g = |b|_h \wedge |a_2|_g = |c|_g \wedge |a_3|_g = |c|_h. \tag{2}$$

Indeed, write $a_i = g^{t_i}$ for some integers t_i $(i = 1, 2, 3)$. We prove first the converse. Let b, c be elements satisfying the above equations with exponent-sum constraints. Then $b = h^{t_1}$ and $c = (gh^{t_1})^{t_2}$, and the last equality implies that $t_3 = |(gh^{t_1})^{t_2}|_h = t_1 t_2$. Hence $a_1 \odot a_2 = a_3$.

For the direct implication, suppose $a_1 \odot a_2 = a_3$, so $t_3 = t_1 t_2$, and take $b = h^{t_1}, c = (gb)^{t_2}$. Then b, c satisfy (2). ◀

4 Groups with finite abelianization

Let $G^{\mathsf{ab}} = G/G'$ be the abelianization of G. In this section we show that solving the $\mathcal{DP}(G, \mathsf{ab})$ can be reduced, when G^{ab} is finite, to solving the Diophantine Problem in G with recognisable constraints (see Definition 8). We then apply this to important classes of groups where $\mathcal{DP}$ with recognisable constraints is known to be decidable, such as hyperbolic groups with finite abelianization and graph products of finite groups.

▶ Remark 18. By [11, Proposition 6.3] a subset of a group G is recognisable if and only if it is a union of cosets of a subgroup of finite index in G, and hence a union of cosets of a normal subgroup of finite index (the core of a finite index subgroup will be both normal in G and of finite index in G); recognisability is independent of the choice of generating set for G.

▶ **Proposition 19.** *Let G be a group with finite abelianization. Then $\mathcal{DP}(G, \mathsf{ab})$ is reducible to the Diophantine Problem in G with recognisable constraints.*

Proof. Let $\mathsf{ab} : G \to G^{\mathsf{ab}}$ be the natural abelian projection to $G^{\mathsf{ab}} = G/G'$, which is the finite abelianization of G; this implies that G' has finite index, and so any coset of G' is recognisable by Remark 18. Let $\mathcal{E}$ be a system of equations on variables $\mathcal{X} = \{X_1, \ldots, X_k\}$ in G with abelian constraints $\mathcal{A}$ consisting of a system of equations over $\mathcal{X}$ in G^{ab}.

We claim that any equation in $\mathcal{A}$ can be seen as a recognisable constraint imposed on $\mathcal{E}$. Because of the commutativity of G^{ab}, any equation in $\mathcal{A}$ can be rewritten as $W(\mathcal{X}) = \alpha$, where $W(\mathcal{X})$ is a constant-free word on the variables $\mathcal{X}$ and $\alpha \in G^{\mathsf{ab}}$. We introduce a new variable Z for each such $W(\mathcal{X})$, and set $Z = \alpha$ (which implies $W(\mathcal{X}) = Z$), so that we can more easily apply constraints to Z instead of $W(\mathcal{X})$ below; let $\mathcal{X}'$ be the expanded set of variables for $\mathcal{E}'$, which includes the new Z variables, and consists of $\mathcal{E}$ together with the newly introduced equations $Z = \alpha$. Then $W(\mathcal{X}) = \alpha$ holds in G^{ab} if and only if $Z \in \mathsf{ab}^{-1}(\alpha)$. This is equivalent to $Z \in \alpha G'$, that is, Z belongs to a coset of the commutator subgroup G'. Since G^{ab} is finite, G' has finite index, and so any coset of G' is recognisable; thus all equations in $\mathcal{A}$ can be seen as recognisable constrains imposed on the set of variables $\mathcal{X}'$ (more precisely, $\mathcal{X}' \setminus \mathcal{X}$). ◀

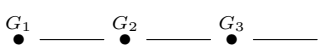
Hyperbolic groups have been studied extensively in geometric group theory, and the Diophantine Problem is known to be decidable by work of Rips & Sela [14] and Dahmani & Guirardel [6]. We do not give the definitions and background on hyperbolic groups here due to lack of space, and also since they are not the focus of the paper, but refer the reader to [2].

▶ **Theorem 20.** *Let G be a hyperbolic group with finite abelianization. Then $\mathcal{DP}(G, \mathsf{ab})$ is decidable.*

Graph products of groups are another widely studied class of groups, and the graph product construction generalises both direct and free products. As in the case of RAAGs, we start with a finite undirected graph Γ with no loops at any vertex and no multiple edges between two vertices. We associate a group to each vertex of Γ, and let the graph product $\mathcal{G}\Gamma$ be the group whose generator set is the union of the vertex group generators, and the relations consist of the relations in the vertex groups together with commuting relations between the generators of any vertex groups connected by an edge in Γ. RAAGs are simply graph products where each vertex group is equal to $\mathbb{Z}$.

▶ **Example 21.** Let Γ be the graph below with vertex groups G_1, G_2, G_3, G_4, where G_i is the cyclic group of order $2i$ generated by x_i. The graph product $\mathcal{G}\Gamma$ based on Γ has the presentation $\langle x_1, x_2, x_3, x_4 \mid [x_1, x_2] = [x_2, x_3] = [x_3, x_4] = 1, x_1^2 = x_2^4 = x_3^6 = x_4^8 = 1\rangle$; the

abelianization of $\mathcal{G}\Gamma$ is the direct product $C_2 \times C_4 \times C_6 \times C_8$ of finite cyclic groups of orders $2, 4, 6, 8$, respectively.



▶ **Theorem 22.** *Let G be a graph product of finite groups. Then $\mathcal{DP}(G, \mathsf{ab})$ is decidable.*

Proof. Equations with recognisable constraints in graph products of finite groups are decidable by Diekert and Lohrey's work [8], and since a graph product of finite groups has finite abelianization, the theorem follows from Proposition 19. ◀

The following is a consequence of Theorem 22, since right-angled Coxeter groups are graph products where each vertex group is equal to the cyclic group of order two C_2.

▶ **Corollary 23.** *Let G be a right-angled Coxeter group. Then $\mathcal{DP}(G, \mathsf{ab})$ is decidable.*

5 Interpreting the ring $\mathbb{Z}$ via the Diophantine Problem with abelian constraints

In this section we present a general technical result (Lemma 26) that will allow us to obtain undecidability of the $\mathcal{DP}(G, \mathsf{ab})$ for all non-abelian RAAGs. This lemma can be seen as a generalisation of Theorem 17 for free groups. Currently Lemma 26 is only applied to RAAGs, but we are presenting it in a more general form here in order to make it applicable to other groups in future work.

▶ **Definition 24.** *Let G be a group generated by a finite set S.*

(1) If $X \subseteq S$ is a subset of abelian-primitive elements, we let $R_X = R_X(\cdot, \cdot)$ be the binary relation defined as: $g, h \in G$ satisfy R_X if and only if $|g|_x = |h|_x$ for all $x \in X$.

(2) For any abelian-primitive $s, t \in S$ let $R_{s,t} = R_{s,t}(\cdot, \cdot)$ be the binary relation in G defined as: given $g, h \in G$, $R_{s,t}(g, h)$ is true if and only if $|g|_s = |h|_t$.

(3) If $X \subseteq S$ is a subset of abelian-primitive elements, we let $R_{diag,X}$ be the unary relation satisfied by elements $g \in G$ such that $|g|_v = |g|_u$ for any two $v, u \in X$.

We will simply write R_s if $X = \{s\}$ in (1).

We begin with the following basic observation.

▶ **Lemma 25.** *Let G be a group generated by a set S, let $\{s_1, \dots, s_t\} \subseteq S$ be a set of abelian-primitive generators, and let*

$$K_{s_1,\dots,s_t} := \{g \in G \mid |g|_{s_i} = 0 \ \forall i = 1, \dots, t\}.$$

Then $K_{s_1,\dots,s_t}$ is a normal subgroup of G, and for each $g \in G$ there exists $k_g \in K_{s_1,\dots,s_t}$ such that $g = k_g \Pi_{i=1}^{t} s_i^{|g|_{s_i}}$.

Proof. The normality of $K_{s_1,\dots,s_t}$ follows from the fact that $|\cdot|_{s_i}$ is a homomorphism (Lemma 6). The last part of the lemma follows by standard arguments once we note that $G' \leqslant K_{s_1,\dots,s_t}$, which makes $G/K_{s_1,\dots,s_t}$ abelian. ◀

In what follows we say that an n-ary relation R in G is *PE-definable in G* if the set

$$\{(g_1, \dots, g_n) \in G^n \mid (g_1, \dots, g_n) \text{ satisfies } R\}$$

is PE-definable in G.

The following lemma is an abstraction of the arguments used in the proof of Theorem 17 about the undecidability of $\mathcal{DP}(F(S), \mathsf{ab})$. The most technical point is given by Item (2). The reader may note from the proof of Theorem 17 that Item (2) holds for $(F(S), \mathsf{ab})$

▶ **Lemma 26** (General technical lemma). *Let G be a group generated by a set S. Let $s_1, s_2 \in S$ be abelian-primitive elements with $s_1 \neq s_2$. Suppose that*

(1) The relations R_{s_1}, R_{s_2}, and R_{s_1,s_2} are PE-definable in (G, ab), and

(2) There exists a disjunction $\bigvee_{i=1}^{m} \Sigma_i(z, x, y_1, \dots, y_n)$ of systems Σ_i of equations on variables $z, x, y_1, \dots, y_n$, such that for each $g \in K_{s_1}$ there exists $h_g \in G$ such that:

(i) the disjunction of systems $\bigvee_{i=1}^{m} \Sigma_i(g, x, y_1, \dots, y_n)$ PE-defines in (G, ab) the set

$$h_g^{-1}\{(s_1 s_2^{|g|_{s_2}})^t \mid t \in \mathbb{Z}\}K_{s_1,s_2}h_g \subseteq G,$$

or equivalently:

(ii) a tuple $(x', y_1', \dots, y_n')$ is a solution to some of the systems of equations $\Sigma_i(g, x, y_1, \dots, y_n)$ $(i = 1, \dots, m)$ if and only if

$$x' \in h_g^{-1}\{(s_1 s_2^{|g|_{s_2}})^t \mid t \in \mathbb{Z}\}K_{s_1,s_2}h_g.$$

Then the problem $\mathcal{DP}(G, \mathsf{ab})$ is undecidable.

6 Partially commutative groups (RAAGs)

We now show that the Diophantine Problem with abelianization constraints is undecidable for partially commutative groups (or RAAGs) that are not abelian. The idea of the proof is, like in the free group case, to find two sufficiently independent elements which can be manipulated so that we can encode the ring $(\mathbb{Z}, \oplus, \odot)$ in a RAAG. Finding two such elements is more difficult than for free groups: we first need to find two sets of vertices/generators, which we call *weak modules*, and then obtain the two abelian-primitive elements by multiplying together all the elements in each weak module, respectively.

6.1 Preliminaries on RAAGs

Let Γ be a finite, undirected graph with no auto-adjacent vertices, and let $G\Gamma$ be the partially commutative group or RAAG induced by Γ (we refer to [5] for a thorough introduction to RAAGs). We identify the vertices of Γ with the corresponding generators of $G\Gamma$. Given a vertex $v \in V\Gamma$ we let $link(v)$ be the set of vertices adjacent to v, and we let $star(v) = \{v\} \cup link(v)$. This notation is extended to sets of vertices: if $S \subseteq V\Gamma$, then $link(S) = \bigcap_{v \in S} link(v)$ and $star(S) = \{S\} \cup link(S)$. A *clique* is a set of vertices S such that each vertex in S is adjacent to all other vertices in S. Given an element $g \in G\Gamma$, we let $supp(g)$, the *support* of g be the set of vertices v such that $g = g_1 v g_2$ for some $g_1, g_2 \in G\Gamma$ and $g_1 v g_2$ is a geodesic, that is, cannot be shortened by any group relations or free cancellations. This set is well-defined. We define $link(g)$ and $star(g)$ as $link(supp(g))$ and $star(supp(g))$.

Given $v, u \in V\Gamma$ we write $v \leqslant u$ if and only if $star(v) \subseteq star(u)$. This constitutes a partial order on $V\Gamma$ which has been frequently used in the study of RAAGs.

A pair of (not necessarily distinct) vertices $v, u \in V\Gamma$ is a *weak pair* if both v and u are minimal with respect to $\leqslant$, and $star(v) = star(u)$. Let S be a non-empty set of minimal vertices in Γ such that any two vertices in S form a weak pair, and such that S is maximal (with respect to set inclusion) among all sets of vertices with these properties. Then we will say that S is a *weak module*. We note that for any weak module S and $v \in S$, we have $S \subseteq star(v) = star(S)$. It follows that S is a clique. The following remark can be derived from the definition of weak module and the properties above.

▶ Remark 27. If S and T are two distinct weak modules of Γ, then $S \cap T = \emptyset$. Moreover, for any distinct $v \in S$ and $u \in T$, we have $star(u) \cap star(v) = star(S) \cap star(T) = \emptyset$.

▶ **Example 28.** In the graph below $star(a) \subset star(b)$ and $star(d) \subset star(c)$, so $a \leqslant b$, $d \leqslant c$, the vertices a and d are minimal, and each is a weak module consisting of a single vertex.

▶ Remark 29. Having weak modules with more than one vertex significantly increases the complexity of the arguments. The reader may assume that every weak module consists of a single minimal vertex, as in the example above.

The following describes centralisers in RAAGs (see Example 12), first for vertices and then for general elements.

▶ **Proposition 30** ([15]). *Let $G = G\Gamma$ be a RAAG and let v be a vertex of Γ. Then $C_G(v)$ is the subgroup of G generated by $star(v)$. More precisely, $C_G(v) = \langle v \rangle \times \langle link(v) \rangle$.*

A *cyclically reduced* element in a RAAG corresponds to a word w that cannot be made shorter when cyclically permuting the letters of w and then applying free cancellations and the group commuting relations. In [15] it is proved that for any cyclically reduced element g in G there exist unique elements $u_1, \dots, u_m$, which we call *blocks*, and integers $n_1, \dots, n_m$ such that $[u_i, u_j] = 1$ for all i, j and $g = u_1^{n_1} \cdots u_m^{n_m}$. The latter expression is called the *block-decomposition* of g.

▶ **Theorem 31** ([15]). *Let $G = G\Gamma$ be a RAAG and let $g \in G$. Let $h \in G$ be such that g^h is cyclically reduced, and let $b_1, \dots, b_\ell \in G$ be elements such that the block decomposition of g^h is $b_1^{t_1} \dots b_\ell^{t_\ell}$. Then $C_G(g) = \left(\Pi_{i=1}^{\ell} \langle b_i^{t_i} \rangle \times \langle link(b_1, \dots, b_\ell) \rangle\right)^{h^{-1}}$.*

We will use the following observation implicitly:

▶ Remark 32. Let Γ be a graph, and v be a vertex of Γ. Then v is abelian-primitive in $G\Gamma$.

6.2 Main result for partially commutative groups (or RAAGs)

We next turn to our main result about RAAGs, namely Theorem 38, which states that $\mathcal{DP}(G\Gamma, \mathsf{ab})$ is undecidable in any nonabelian RAAG $G\Gamma$.

Outline of the main proof. The proof of Theorem 38 is an involved reprisal of the proof of undecidability of $\mathcal{DP}(F(\Sigma), \mathsf{ab})$, and we emphasise the parallels between the two proofs in the next paragraphs. Our proof strategy is as follows.

Recall that if $S \subseteq G$ is a subset of abelian-primitive elements of G, we let R_S be the binary relation defined in G by: $g, h \in G$ satisfy R_S if and only if $|g|_s = |h|_s$ for all $s \in S$ (see Definition 24). The key lemma of this section is Lemma 33. This states that if S is a weak module, then R_S is PE-definable in G. This is similar to the starting point for the proof of undecidability of $\mathcal{DP}(F(\Sigma), \mathsf{ab})$, where we are able to PE-define R_S in $F(\Sigma)$ by means of centralisers. In the RAAG case, however, we are forced to deal with a whole weak minimal module S, rather than a single generator s. The proof, in fact, is much simpler if we assume that $G\Gamma$ has at least two distinct weak modules consisting each of a single vertex.

Next, we show that we can assume that $G\Gamma$ has at least two distinct weak modules S, T. This is similar to the presence of at least two generators s, t in the free group case: there we crucially use the exponents of the elements in the subgroups $\langle s \rangle, \langle t \rangle$ as proxies for the set $\mathbb{Z}$. This cannot be replicated in a RAAG simply with S and T since the latter are sets of vertices. For this reason we take the "diagonal generators of S and T", namely $h_1 = \prod_{v \in S} v$ and $h_2 = \prod_{u \in T} u$.

In free groups we are able to PE-define the sets $\langle s\rangle, \langle t\rangle$ via the centralisers of s and t and thus have "access" to the exponents of s and t, which serve as our $\mathbb{Z}$. In a RAAG the centraliser of h_1 (similarly for h_2) is more complicated: it has the form $\langle S\rangle \times \langle link(S)\rangle$, with $\langle S\rangle \cong \mathbb{Z}^{|S|}$. Each one of these two factors presents a problem which has no parallel with the proof in free groups. The second factor is dealt with, roughly, by using the technical lemma Lemma 26. The main idea is that the elements from $\langle link(S)\rangle$ never use any vertex from S or T, and thus they become eventually irrelevant in our arguments. Regarding the first factor $\langle S\rangle$, to be able to read off the exponents of h_i within it, $i = 1, 2$, we introduce the subgroup $G_{diag,S,T}$ defined as the set of elements g of $G\Gamma$ that satisfy $R_{diag,S}$ and $R_{diag,T}$, where g satisfies $R_{diag,S}$ if and only if $|g|_s = |g|_{s'}$ for all $s, s' \in S$. In such a subgroup the centraliser of h_i is $\langle h_i\rangle \times \langle link(S)\rangle$.

We finally show that $(G_{diag,S,T}, \mathsf{ab})$ is PE-interpretable in (G, ab); thus it suffices to prove that $\mathcal{DP}(G_{diag,S,T}, \mathsf{ab})$ is undecidable. At this point we have two abelian-primitive elements h_1, h_2 whose centralisers are almost as nicely behaved as in a free group, and the proof can be finished by applying the technical Lemma 26, where its second condition is seen to be met in $G_{diag,S,T}$ by inspecting the centralisers $C_{G_{diag,S,T}}(h_1 g)$, with g ranging among all $g \in G_{diag,S_1,S_2}$ satisfying $|g|_{h_1} = 0$.

This concludes our intuitive explanation of the proof of Theorem 38. To prove this result formally will require the following several lemmas.

▶ **Lemma 33.** *Let $G = G\Gamma$, and let S be a weak module of Γ. Then the relation R_S is PE-definable in (G, ab).*

Proof. Let R'_S refer to the unary relation satisfied by $g \in G$ if and only if $|g|_s = 0$ for all $s \in S$. Since $|\cdot|_s$ is additive, $|k|_s = |h|_s$ for $k, h \in G$ if and only if $|kh^{-1}|_s = 0$, so it suffices to prove that R'_S is PE-definable in (G, ab).

First we claim that there exist vertices $u_1, \ldots, u_n \in V\Gamma$ such that

$$V\Gamma \setminus S = \bigcup_{i=1}^{n} star(u_i).$$

Indeed, consider the set of vertices $V\Gamma \setminus star(S)$. For any $w \in V\Gamma \setminus star(S)$ we have that $star(w) \cap S = \emptyset$. Hence

$$\bigcup_{u \in V\Gamma \setminus star(S)} star(u) \subseteq V\Gamma \setminus S.$$

Observe that $V\Gamma \subseteq \cup_{u \in V\Gamma \setminus star(S)} star(u)$: if $w \in V\Gamma$ does not belong to $star(S)$ then there is nothing to argue. If it does, then it belongs to $link(S) = star(S) \setminus S$. Next we show that $star(w) \not\subseteq star(S)$. Once this is shown, we obtain that $w \in link(w')$ for any $w' \in star(w) \setminus star(S)$, and so $w \in \cup_{u \in V\Gamma \setminus star(S)} star(u)$, completing the proof of the first claim of the lemma, indeed we take $\{u_1, \ldots, u_n\} = V\Gamma \setminus star(S)$.

Tho prove that $star(w) \not\subseteq star(S)$, note that $star(w)$ cannot be properly contained in $star(S)$, since this would contradict the minimality of any of the vertices in S. Hence either $star(w) \not\subseteq star(S)$ or $star(w) = star(S)$. In the latter case, w is a minimal vertex since $star(w) = star(S) = star(v)$ for any $v \in S$, and hence w is adjacent to each vertex in S. This would contradict the fact that S is a weak module, and so we must have $star(w) \not\subseteq star(S)$, as required.

Our second claim is that an element $x \in G$ satisfies R'_S if and only if there exists $y \in \Pi_{i=1}^{n} C_G(u_i)$ such that $\mathsf{ab}(x) = \mathsf{ab}(y)$, where the u_i's are the vertices from the first claim of the lemma. Indeed, due to the first claim and by Proposition 30 about centralisers in RAAGs, any element from $\Pi_{i=1}^{n} C_G(u_i) = \Pi_{i=1}^{n} \langle star(u_i)\rangle$ satisfies R'_S .Conversely, if an

element x belongs to $\langle V\Gamma \setminus S\rangle$, then $x = z_1 \dots z_{k_x}$ where $z_i \in V\Gamma \setminus S$ for all $i = 1, \dots, k_x$, and again due to the first claim of the lemma and Proposition 30, we have that for each z_i there exists u_{j_i} such that $z_i \in C_G(u_{j_i}) = \langle star(u_{j_i})\rangle$. Hence $x \in \Pi_{i=1}^{k_x} C_G(u_{j_i})$, and so $\mathsf{ab}(x) \in \Pi_{i=1}^{n} \mathsf{ab}(C_G(u_i))$. It follows that $\mathsf{ab}(x) = \mathsf{ab}(y_1) \dots \mathsf{ab}(y_n)$ for some $y_i \in C_G(u_i)$ such that $\mathsf{ab}(y_i) \in \mathsf{ab}(C_G(u_i))$ $(i = 1, \dots, n)$. Then it suffices to take $y = y_1 \dots, y_n$.

The lemma now follows immediately from the second claim and the fact that in any group the centraliser of an element is PE-definable. ◀

It will be important that $G\Gamma$ does not decompose as a non-trivial direct product. In this case the set of minimal vertices of Γ satisfies certain favorable properties, as shown next.

▶ **Lemma 34.** *Let Γ be a graph and suppose that Γ has only one weak module M. Then $G\Gamma = \langle M\rangle \times \langle V\Gamma \setminus M\rangle$.*

In particular, if $G\Gamma$ does not decompose as a nontrivial direct product, then Γ has at least two distinct weak modules with empty intersection.

Proof. Observe that if u is an arbitrary vertex of Γ, then there exists a minimal vertex $v \in M$ such that $star(v) = star(M) \subseteq star(u)$ since $\leqslant$ is a partial order in $V\Gamma$. Since $M \subseteq star(M)$ we have $M \subseteq star(u)$, so u is adjacent to every vertex in M. The lemma follows. ◀

▶ **Lemma 35.** *Let S and T be two distinct weak modules of Γ. Let $S_0 \subseteq S$ and $T_0 \subseteq T$ be two non-empty subsets of S and T, and let $g = \prod_{v\in S_0} v$, $h = \prod_{u\in T_0} u$. Then $C_{G\Gamma}(gh) = \langle gh\rangle$.*

Proof. The element gh is cyclically reduced, and its block decomposition consists of a single block $b_1 = gh$, due to Remark 27 there is no way to partition the support of gh, namely $S_0 \cup T_0$, into two nonempty distinct subsets of vertices A, B, such that each vertex in A commutes with B and vice-versa. Hence by Theorem 31, we have $C_{G\Gamma}(gh) = \langle gh\rangle \times \langle link(gh)\rangle$. By Remark 27 we obtain $link(gh) = \emptyset$, and the lemma follows. ◀

Let S be a weak module of Γ. We let $R_{diag,S}$ be the unary relation satisfied by elements $g \in G\Gamma$ such that $|g|_v = |g|_u$ for any two $v, u \in S$. Note that if S has only one vertex then all $g \in G\Gamma$ satisfy this relation.

▶ **Lemma 36.** *Let Γ be a graph such that $G\Gamma$ does not decompose as a non-trivial direct product. Let S be a weak module of Γ. Then the relation $R_{diag,S}$ is PE-definable in $G\Gamma$.*

Proof. By Lemma 34, there exists a non-empty weak module T different from S. Let $w = \prod_{v\in S} v$ and let $u \in T$. Then $C(wu) = \langle wu\rangle = \{(wu)^t \mid t \in \mathbb{Z}\}$ by Lemma 35. Notice that all elements in $\langle wu\rangle$ satisfy $R_{diag,S}$. It follos that an element $g \in G\Gamma$ satisfies $R_{diag,S}$ if and only if there exists $h \in C(wu)$ such that $|g|_s = |h|_s$ for all $s \in S$, i.e. if g, h satisfy the relation R_S. Since we proved that R_S is PE-definable in $G\Gamma$, we conclude that also $R_{diag,S}$ is PE-definable in $G\Gamma$. ◀

Given some distinct weak modules $S_1, \dots, S_t$ of Γ, we let $G_{diag,S_1,\dots,S_t}$ be the subset of $G = G\Gamma$ formed by those elements of G satisfying all the unary relations $R_{diag,S_1}, \dots, R_{diag,S_t}$:

$$G_{diag,S_1,\dots,S_t} = \{g \in G \mid R_{diag,S_i}(g) \text{ holds for all } i = 1, \dots, t\}.$$

Recall R_S, R_{s_1,s_2} and $R_{diag,S}$ from Definition 24.

▶ **Lemma 37.** *Let Γ be a graph such that G does not decompose as a non-trivial direct product, and let S_1, S_2 be two distinct weak modules of Γ. Then*

1. *G_{diag,S_1,S_2} is a PE-definable subgroup of G,*

2. *the elements* $h_1 = \prod_{w \in S_1} w$ *and* $h_2 = \prod_{w \in S_2} w$ *are abelian-primitive in* G_{diag,S_1,S_2}*, and*
3. *the relations* $R_{h_1}, R_{h_2}, R_{h_1,h_2}$ *are PE-definable in* G_{diag,S_1,S_2}*.*

Combining all the lemmas in this section leads to the main result for RAAGs (see the outline of the proof at the beginning of this section):

▶ **Theorem 38.** *Let* $G = G\Gamma$ *be a RAAG such that* G *is not a free abelian group. Then* $\mathcal{DP}(G, \mathsf{ab})$ *is undecidable.*

7 Conclusions and future work

Motivated by the the vast literature on word equations with length constraints in the context of free semigroups, in this paper we started a systematic study of the Diophantine Problem with length constraints in groups, focusing on the constraints that require the solutions to satisfy a system of equations in the abelianization of the group; this is akin to imposing Parikh - type constraints or adding abelian predicates to the existential theory of semigroups.

There are clear parallels between the decidability results for semigroups versus groups. For example, the proofs that the Diophantine Problem with abelianization constraints $(\mathcal{DP}, \mathsf{ab})$ is undecidable follow a similar pattern for free semigroups and groups. In both cases we follow the strategy of Büchi and Senger [4] to encode the ring of integers into $(\mathcal{DP}, \mathsf{ab})$. However, we phrase this into the more elegant, abstract and general language of interpretability, which allows us to deal with classes of groups beyond the free ones. The framework of interpretability and further tools from model theory have a lot of potential and can lead to further applications. To this effect, we see several directions of future work:

1. While using interpretability via equations to encode the ring of integers into the algebraic structures we consider, it became clear that the algebraic properties of semigroups often require a different approach compared to groups. A prime example is that while we were able to show that $(\mathcal{DP}, \mathsf{ab})$ is undecidable for partially commutative groups (or RAAGs), the same approach was not immediately applicable to partially commutative semigroups, or trace monoids. The main reason for this is the reliance of our arguments on the normality of certain subgroups, a concept not available in a monoid. We intend to study $(\mathcal{DP}, \mathsf{ab})$ for trace monoids next.

2. Trace monoids and partially commutative groups are examples of graph products of monoids and groups, respectively. We plan on more generally studying graph products of monoids and groups, and expect that at least in the group case our 'General technical lemma' (Lemma 26) will apply.

3. Another direction of future work is understanding $(\mathcal{DP}, \mathsf{ab})$ for more of the groups where $\mathcal{DP}$ is known to be decidable. Preliminary work shows that $(\mathcal{DP}, \mathsf{ab})$ is undecidable for hyperbolic groups with 'large' abelianization, that is, abelianization of free rank $\geqslant 2$. However, it is not clear what happens if the abelianization of a hyperbolic group has free rank exactly 1. We showed in this paper that if the abelianization is finite, then $(\mathcal{DP}, \mathsf{ab})$ is decidable, so the rank 1 case lies between decidability and undecidability.

There are other intriguing groups where the abelianization has free rank $= 1$, such as the Baumslag–Solitar groups $BS(1, n)$, or the braid group on three strands $\langle a, b \mid aba = bab \rangle$. In all these cases $\mathcal{DP}$ is decidable, but $(\mathcal{DP}, \mathsf{ab})$ unclear.

4. Finally, we plan on looking at other length constraints, that is, studying $\mathcal{DP}(G, \mathrm{L})$ and $\mathcal{DP}(G, \{|.|_i\}_i)$ for appropriate classes of groups (see Section 2.2), and establishing equivalences between these and $\mathcal{DP}(G, \mathsf{ab})$ in the spirit of Lemma 16.

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 J. M. Alonso, T. Brady, D. Cooper, V. Ferlini, M. Lustig, M. Mihalik, M. Shapiro, and H. Short. Notes on word hyperbolic groups. In *Group theory from a geometrical viewpoint (Trieste, 1990)*, pages 3–63. World Sci. Publ., River Edge, NJ, 1991.

3 Roberto Amadini. A survey on string constraint solving. *ACM Comput. Surv.*, 55(1), nov 2021. URL: https://doi.org/10.1145/3484198, doi:10.1145/3484198.

4 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. doi:10.1002/malq.19880340410.

5 Ruth Charney. An introduction to right-angled artin groups. *Geometriae Dedicata*, 125, 11 2006. doi:10.1007/s10711-007-9148-6.

6 François Dahmani and Vincent Guirardel. Foliations for solving equations in groups: free, virtually free, and hyperbolic groups. *J. Topol.*, 3(2):343–404, 2010. doi:10.1112/jtopol/jtq010.

7 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.

8 Volker Diekert and Markus Lohrey. Word equations over graph products, 2008. URL: https://doi.org/10.1142/S0218196708004548, doi:10.1142/S0218196720500198.

9 Vijay Ganesh, Mia Minnes, Armando Solar-Lezama, and Martin Rinard. Word equations with length constraints: What's decidable? volume 7857, pages 209–226, 11 2012. doi:10.1007/978-3-642-39611-3_21.

10 Albert Garreta and Robert Gray. On equations and first-order theory of one-relator monoids. *Information and Computation*, 281, December 2021. doi:10.1016/j.ic.2021.104745.

11 Thomas Herbst and Richard M. Thomas. Group presentations, formal languages and characterizations of one-counter groups. *Theoret. Comput. Sci.*, 112(2):187–213, 1993. URL: https://doi.org/10.1016/0304-3975(93)90018-O, doi:10.1016/0304-3975(93)90018-O.

12 W. Hodges. *Model theory*, volume 42 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1993. URL: http://dx.doi.org/10.1017/CBO9780511551574, doi:10.1017/CBO9780511551574.

13 Rupak Majumdar and Anthony W Lin. Quadratic word equations with length constraints, counter systems, and presburger arithmetic with divisibility. *Logical Methods in Computer Science*, 17, 2021.

14 E. Rips and Z. Sela. Canonical representatives and equations in hyperbolic groups. *Invent. Math.*, 120(3):489–512, 1995. doi:10.1007/BF01241140.

15 Herman Servatius. Automorphisms of graph groups. *Journal of Algebra*, 126:34–60, 1989.

Appendix

Proof of Lemma 5. Let $\pi : F(S) \to G$ be the natural projection of the free group $F(S)$ onto G. Throughout the proof, an element $s \in S$ "seen in" G will be denoted $\pi(s)$.

Let $\mathsf{ab}' : F(S) \to \mathbb{Z}^{|S|}$ be the natural projection of $F(S)$ onto its abelianization, and similarly let $\mathsf{ab} : G \to G/G'$. Additionally, let $\pi' : \mathbb{Z}^{|S|} \to G/G'$ be an homomorphism such that $\pi' \circ ab' = ab \circ \pi$ (where composition is applied from right to left). We claim that π' sends the subgroup $\langle \mathsf{ab}'(s) \rangle$ isomorphically onto $\langle \mathsf{ab}(\pi(s)) \rangle$. To prove the claim, note that the homomorphism $\pi'|_{\langle \mathsf{ab}'(s) \rangle}$ is onto. It suffices to prove that it is one-to-one. But this is clear because if $\mathsf{ab}'(s)^i$ belongs to the kernel of this homomorphism, then $\pi(s)^i$ belongs to

the kernel of ab, which forces $i = 0$ since $\mathsf{ab}(\pi(s))$ has infinite order in G/G' because s is abelian-primitive. The claim is proved.

Now let $g \in G$. Let $w_g \in F(S)$ be such that $|w_g|_s = |g|_s$. It is clear from the definition of abelian-primitive elements that there exist unique $t_g \in \mathbb{Z}$ and $c_g \in G'$ such that $g = \pi(s)^{t_g} c_g$, with $\mathsf{ab}(c_g) \in H$, where $H \leqslant G/G'$ is such that $G/G' = \langle \mathsf{ab}(\pi(s)) \rangle \times H$.

We want to see that $t_g = |w_g|_s$. Indeed, it follows from the claim above and the definition of t_g that the exponent sum of $\mathsf{ab}'(s)$ in the element $\mathsf{ab}'(w_g) \in \mathsf{ab}'(F(S))$ is precisely t_g, which can only occur if $|w_g|_s = t_g$. ◀

Proof of Lemma 10. Let $G = G_1 \times G_2$. Let π_1 and π_2 be the natural projections of G onto G_1 and G_2. Let $w(x_1, \ldots, x_n) = 1$ be an equation in G. Then $g_1, \ldots, g_n \in G$ forms a solution to such an equation if and only if $w(\pi_i(g_1), \ldots, \pi_i(g_n)) = 1_{G_i}$ for both $i = 1, 2$. Since $G/G' \cong G_1/G_1' \times G_2/G_2'$, an analogous statement holds for any equation in the abelianization G/G'. The lemma follows immediately from these observations. ◀

Proof of Proposition 14. It is a direct consequence of the following lemma, which, roughly, states that when one structure M_1 is PE-interpretable in another M_2, then one can "rewrite" any disjunctions of systems of equations with relations (or constraints) in M_1 as an equivalent disjunction of systems of equations with relations in M_2. As with Proposition 14, this is a variation of well-known results from model theory, and the proof presented here simply follows step-by-step the proofs of such well-known results, see Theorem 5.3.2 in [12]. The lemma below is stated for groups enriched with the relation ab. It can be easily adapted to the case that we are PE-interpreting a ring R into a group enriched with the relation ab.

▶ **Lemma 39.** *Let (G, ab) and (H, ab) be two groups enriched with the relation ab. Let ϕ be an e-interpreting map of (H, ab) in (G, ab), with $\phi : X \subset G^n \to H$ (see Definition 13). Let $\sigma(\curvearrowleft) = \sigma(x_1, \ldots, x_n)$ be an arbitrary disjunction of systems of equations with abelianization constraints in H. Then there exists a disjunction of systems of equations $\Sigma_\sigma(\curvearrowright)$ in G with abelianization constraints, such that a tuple $(b_1, \ldots, b_n) \in G^n$ is a solution to $\Sigma_\sigma(y_1, \ldots, y_n)$ if and only if $(b_1, \ldots, b_n) \in X$ and $\phi((b_1, \ldots, b_n)$ is a solution to σ.*

We now proceed to prove this lemma. We can assume without loss of generality, and we do so, that σ consists of a single system of equations with abelianization constraints.

We claim that, by introducing new variables and new equations, we can rewrite σ so that σ consists of equations $\sigma_1, \ldots, \sigma_m$ with the following property: For all $i = 1, \ldots, m$, σ_i is either of the form $z = xy$, $x = y$, $x = h$, or $\mathsf{ab}(x) = \mathsf{ab}(y)$ for some variables x, y, z and constant element $h \in H$. The lemma follows from the claim, since by the definition of e-interpretability, the present lemma is true for each of σ_i, $i = 1, \ldots, m$. Hence, it suffices to take Σ_σ to be $\Sigma_{\sigma_1} \wedge \cdots \wedge \Sigma_{\sigma_n}$.

We now prove the claim. We proceed by induction on the syntactic length (i.e. the number of symbols) $|\sigma|$ of σ, the base cases being clear. It suffices to prove the claim in the case that σ consists on a single equation or relation, since once this case is proved, if there are more than one equations or relations, we can apply this case separately for each equation or relation.

First of all, since we are working over groups (or rings), we can assume that σ has either the form $w(x_1, \ldots, x_n) = 1$ or $\mathsf{ab}(w(x_1, \ldots, x_n)) = 1$ for some word w with constants and variables $x_1, \ldots, x_n$. Suppose first that σ is of the form $w(x_1, \ldots, x_n) = 1$, and that it is not of one of the desired short forms. We shall omit the references to the variables $x_1, \ldots, x_n$ to make the presentation more readable. Let t_1, t_2 be the first two symbols of w, and let w' be a word such that $w = t_1 t_2 w'$. We can rewrite σ into the equivalent system of equations

$t_1t_2y = 1 \wedge y^{-1}w' = 1$, where y is a new variable. The syntactic length of each one of these equations is strictly less than $|\sigma|$, and then we can proceed by induction. If σ has the form $\mathsf{ab}(w) = 1$, we can proceed similarly by rewriting it the system of constraints $\mathsf{ab}(t_1t_2y) = 1 \wedge \mathsf{ab}(y^{-1}w') = 1$. Each one of the relations in the conjunction has syntactic length smaller than $|\sigma|$, and again we can proceed by induction. This proves the claim. ◀

Proof of Lemma 16. (1) It is clear that the decidability of $\mathrm{DP}(F(\Sigma), \{|.|_i\})$ implies the decidability of $\mathrm{DP}(F(\Sigma), \mathsf{ab})$. Conversely, we prove that each $|.|_i$ can be interpreted by a system of equations in $(F(\Sigma), ab)$. Indeed, two elements x, y satisfy $|x|_i = |y|_i$ if and only if there exist elements $x', y' \in \langle g_1\rangle \cdots \langle g_{i-1}\rangle \cdot \langle g_{i+1}\rangle \cdots \langle g_n\rangle$ and $w \in \langle g_i\rangle$ such that $ab(x) = ab(wx') \wedge ab(y) = ab(wy')$. Since the centraliser of any generator g_k in a free group is $\langle g_k\rangle$ (infinite cyclic and generated by g_k), we can express the above equivalently as: $|x|_i = |y|_i$ if and only if there exist $z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n, u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n, w, x', y'$ such that

$$\bigwedge_{j\neq i}[z_j, g_j] = 1 \ \wedge \ \bigwedge_{j\neq i}[u_j, g_j] = 1 \ \wedge \ [w, g_i] = 1 \ \wedge \tag{3}$$

$$x' = \prod_{j\neq i} z_i \ \wedge \ y' = \prod_{j\neq i} u_i \ \wedge \ ab(x) = ab(wx') \ \wedge \ ab(y) = ab(wy'). \tag{4}$$

Hence $|\cdot|_i$ is e-interpretable in $(F(\Sigma), ab)$ for all $i = 1, \ldots, n$. It follows that $DP(F(\Sigma), \{|.|_i\}_i)$ is reducible to $DP(F(\Sigma), ab)$.

(2) For free monoids this is proved in [4]. ◀

For the following proof we will need to recall an important concept from [6].

▶ **Definition.**

(1) A regular subset L' of S^* is quasi-isometrically embedded *(q.i. embedded) in G if there exist $\lambda \geqslant 1$ and $\mu \geqslant 0$ such that, for any $w \in L'$, $|\pi(w)|_G \geqslant \frac{1}{\lambda}|w| - \mu$.*

(2) A rational subset L of G is quasi-isometrically embeddable *(q.i. embeddable) in G if there exists a quasi-isometrically embedded regular subset L' of S^* such that $\pi(L') = L$.*

Proof of Theorem 20. The Diophantine Problem with quasi-isometrically embeddable rational constraints is decidable in hyperbolic groups by [6].

Let S be a finite generating set for G. We will show that a recognisable set $L \subset G$ can be made to quasi-isometrically embed: let $QGeo(G, \mu, \lambda)$ be the set of (λ, μ)-quasi-geodedics over S, which is known to be regular, and consider the set $P = \pi^{-1}(L) \cap QGeo(G, \mu, \lambda)$. Then P is a regular set, as the intersection of two regular sets, and $\pi(P) = L$. Since the abelianization G^{ab} of G is finite, the theorem follows from Proposition 19 and [6]. ◀

Proof of Lemma 26. We will PE-interpret the ring $(\mathbb{Z}, +, \cdot)$ in (G, ab). As interpretation map we use $|\cdot|_{s_1} : G \to \mathbb{Z}$. The preimage under this map of the equality relation in $\mathbb{Z}$, i.e. of the set

$$\{(g, h) \in G \times G \mid |g|_{s_1} = |h|_{s_1}\},$$

is PE-definable in (G, ab), because the relation R_{s_1} is by (1).

We now PE-define in G the preimage by $|\cdot|_{s_1}$ of integer addition, namely the set

$$S_+ = \{(g_1, g_2, g_3) \in G^3 \mid \quad |g_1|_{s_1} + |g_2|_{s_1} = |g_3|_{s_1}\}.$$

We claim that a tuple $(g_1, g_2, g_3) \in G^3$ belongs to S_+ if and only if $g_3K_{s_1} = g_1g_2K_{s_1}$. Indeed, if $g_3K_{s_1} = g_1g_2K_{s_1}$, then $g_3 = g_1g_2k$ for some $k \in K_{s_1}$, so $|g_3|_{s_1} = |g_1g_2k|_{s_1} = |g_1|_{s_1} + |g_2|_{s_1}$, where for the second equality we used Lemma 6. Conversely, if $|g_1|_{s_1} + |g_2|_{s_1} = |g_3|_{s_1}$ then

$|g_1|_{s_1} + |g_2|_{s_2} = |g_1 g_2|_{s_1} = |g_3|_{s_1}$, hence $|g_1 g_2 g_3^{-1}|_{s_1} = 0$ and so $g_1 g_2 g_3^{-1} \in K_{s_1}$, and the claim follows. By the claim, we have $S_+ = \{(g_1, g_2, g_3) \in G^3 \mid g_1 g_2 g_3^{-1} \in K_{s_1}\}$. It now follows from the fact that K_{s_1} is PE-definable in G that S_+ is also PE-definable K_{s_1} in G.

We next PE-define in (G, ab) the preimage under $|\cdot|_{s_1}$ of integer multiplication, i.e. of the set

$$S_\odot = \{(g_1, g_2, g_3) \in G^3 \mid \quad |g_1|_{s_1} \cdot |g_2|_{s_1} = |g_3|_{s_1}\}.$$

We claim that three elements $a_i \in G, i = 1, 2, 3$, belong to $S_\odot$ if and only if there exist $b, c \in G$ such that

$$\left(G \vDash \exists y_1 \ldots \exists y_n, \bigvee_{i=1}^{m} \Sigma_i(b, c, y_1, \ldots, y_n) \right) \wedge \tag{5}$$

$$\wedge \left(|a_1|_{s_1} = |b|_{s_2}\right) \wedge \left(|b|_{s_1} = 0\right) \wedge \left(|a_2|_{s_1} = |c|_{s_1}\right) \wedge \left(|a_3|_{s_1} = |c|_{s_2}\right). \tag{6}$$

If we let $t_i := |a_i|_{s_1}$, where t_i $(i = 1, 2, 3)$ are integers, note that by the definition of $S_\odot$ we have $a_1, a_2, a_3 \in S_\odot$ if and only if $t_3 = t_1 t_2$.

We first prove the converse of the claim. Let b, c be elements satisfying (5) and (6). Then $|b|_{s_2} = t_1$ and $|b|_{s_1} = 0$. Due to the assumption (2) in the lemma, we have

$$c = h_g^{-1}(s_1 s_2^{|b|_{s_2}})^t h_g = h_g^{-1}(s_1 s_2^{t_1})^t h_g$$

for some $t \in \mathbb{Z}$ since c is part of a solution to some of the Σ_i systems. Conjugation does not alter the value of the map $|\cdot|_{s_1}$, so from the additivity of $|\cdot|_{s_1}$ (Lemma 6) we get that $|c|_{s_1} = t$, and from $|c|_{s_1} = |a_2|_{s_1} = t_2$ we have $t = t_2$. Moreover, again by additivity of $|\cdot|_{s_2}$, we obtain $|c|_{s_2} = t_1 t = t_1 t_2$. The equality $|c|_{s_2} = |a_3|_{s_1} = t_3$ in (6) now implies that $t_3 = t_1 t_2$, as required.

To prove the direct implication of the claim, suppose $a_1, a_2, a_3 \in S_\odot$, so $t_3 = t_1 t_2$. Take $b = s_2^{t_1}, c = h_g^{-1}(s_1 b)^{t_2} h_g$. It is straightforward to verify that these elements satisfy the conditions from (6). To check that b, c satisfy (5), we must show that there exist $y_1, \ldots, y_n \in G$ that form a solution to one of the systems of equations $\Sigma_i(b, c, y_1, \ldots, y_n)$ $(i = 1, \ldots, m)$. By assumption, a tuple $(x', y_1', \ldots, y_n')$ is a solution to some of the systems $\Sigma_i(b, x, y_1, \ldots, y_n)$ $(i = 1, \ldots, m)$ if and only if there exists $h \in G$ such that

$$x' \in h_g^{-1}\{(s_1 s_2^{|g|_{s_2}})^t \mid t \in \mathbb{Z}\} h_g.$$

We will argue that for any tuple of elements $(y_1, \ldots, y_n) \in G$ we have that $y_1, \ldots, y_n$ is a solution to one of the systems $\Sigma_i(b, c, y_1, \ldots, y_n)$ $(i = 1, \ldots, m)$. Indeed, we have

$$c = h_g^{-1}(s_1 s_2^{|b|_{s_2}})^{t_2} h_g \in h_g^{-1}\{(s_1 s_2^{|b|_{s_2}})^t \mid t \in \mathbb{Z}\} h_g,$$

hence $(c, y_1, \cdots, y_n)$ is a solution to some of the systems $\Sigma_i(b, x, y_1, \ldots, y_n)$ $(i = 1, \ldots, m)$ for any tuple of elements $y_1, \ldots, y_n$ This completes the proof of the claim.

The proof of the lemma now follows from the fact that all conditions appearing in (5) are PE-definable in (G, ab) by the assumptions (1) in the statement of the lemma. ◀

Proof of Lemma 37. **1.** That G_d is a subgroup follows from the additivity of the maps $|\cdot|_s$ (Lemma 6), and that G_{diag,S_1,S_2} is PE-definable in G follows from Lemma 36.

2. Next we show that $h_i = \prod_{w \in S_i} w$ is abelian primitive in G_{diag,S_1,S_2} for both $i = 1, 2$. Let π be the natural projection of G onto its abelianization. We first note that any element g of G_{diag,S_1,S_2} can be written uniquely in the following form:

$$g = h_1^{n_1(g)} h_2^{n_2(g)} \left(\prod_{v \in V\Gamma \setminus (S_1 \cup S_2)} v^{n_v(g)} \right) c$$

for some $n_1(g), n_2(g), n_v(g) \in \mathbb{Z}$ and some $c \in G'$ (this can be seen by projecting g onto $\pi(G)$, arranging the generators, and then, informally speaking, "pushing" the element back to $G\Gamma$).

Let π_{diag,S_1,S_2} the projection of G_{diag,S_1,S_2} onto its abelianization. We claim that

$$\langle \pi_{diag,S_1,S_2}(h_1)\rangle \cap \langle \pi_{diag,S_1,S_2}(\{h_2\} \cup V\Gamma \setminus (S_1 \cup S_2))\rangle = 1.$$

Note that once this claim is proved we will have shown that h_1 is abelian-primitive. The argument for h_2 is analogous.

To prove the claim, we note from the observation above that

$$\langle \pi(h_1)\rangle \cap \langle \pi(\{h_2\} \cup V\Gamma \setminus (S_1 \cup S_2))\rangle = 1.,$$

that is

$$\langle h_1\rangle G' \cap \langle(\{h_2\} \cup V\Gamma \setminus (S_1 \cup S_2))\rangle G' = G'.$$

Intersecting on both sides with G'_{diag,S_1,S_2} we have that this equality sill holds if we replace G' by $G' \cap G'_{diag,S_1,S_2}$. Since $G' \cap G'_{diag,S_1,S_2} = G'_{diag,S_1,S_2}$, the claim follows.

3. That R_{h_i} $(i = 1, 2)$ is PE-definable in G_{diag,S_1,S_2} follows from Lemma 33: indeed, a pair of elements $g, h \in G_{diag,S_1,S_2}$ satisfies R_{h_i} if and only if they satisfy R_S, which is PE-definable in G by Lemma 33. Since G_{diag,S_1,S_2} is PE-definable in G we have that R_S is also PE-definable in G_{diag,S_1,S_2}.

   To PE-define the relation R_{h_1,h_2} in G_{diag,S_1,S_2}, observe that two elements $x, y \in G_{diag,S_1,S_2}$ satisfy this relation if and only if there exists an element $z \in \langle h_1h_2\rangle$ such that the pair x, z satisfies R_{h_1} and the pair y, z satisfies R_{h_2} (this is because $|z|_{h_1} = |z|_{h_2}$ for all $z \in \langle h_1h_2\rangle$). Next we claim that

$$\langle h_1h_2\rangle = C_{G_{diag,S_1,S_2}}(h_1h_2).$$

   Indeed, h_1h_2 is cyclically reduced, and because any vertex in S_1 is not adjacent to any vertex in S_2, the block decomposition of h_1h_2 consists in one block. Then the claim follows from Theorem 31.

   From the claim above we obtain that $\langle h_1h_2\rangle$ is PE-definable in G_{diag,S_1,S_2}. Because of this and the fact that R_{h_1} and R_{h_2} are PE-definable in G_{diag,S_1,S_2}, we obtain that R_{h_1,h_2} is also PE-definable in G_{diag,S_1,S_2}, as required.

◀

Proof of Theorem 38. We proceed by induction on the number n of vertices of Γ. The base case $n = 2$ only allows for G to be a free group, and by Theorem 17 $\mathcal{DP}(G, \mathsf{ab})$ is undecidable in this case. Assume $n > 2$. If G does not decompose as a nontrivial direct product, then Γ has two distinct weak modules S_1, S_2 by Lemma 34. Moreover, by Lemma 37 (1), G_{diag,S_1,S_2} is PE-definable in G.

We will apply Lemma 26 to the subgroup G_{diag,S_1,S_2} and the abelian-primitive elements h_1, h_2, where $h_1 = \prod_{w\in S_1} w$, $h_2 = \prod_{w\in S_2} w$. Once we know that $\mathcal{DP}(G_{diag,S_1,S_2}, \mathsf{ab})$ is undecidable, it will follow immediately that $\mathcal{DP}(G, \mathsf{ab})$ is also undecidable by Proposition 14. Condition (1) of Lemma 26 is satisfied because by Lemma 37(3), we know that the relations R_{h_1}, R_{h_2}, and R_{h_1,h_2} are PE-definable in G_{diag,S_1,S_2}.

We next establish that condition (2) of Lemma 26 is satisfied. To ease the notation we will denote G_{diag,S_1,S_2} simply as G_d throughout the rest of the proof. Let $K_{h_i} \leqslant G_d$ be the subgroup consisting of those $g \in G_{diag,S_1,S_2}$ such that $|g|_{h_i} = 0$ $(i = 1, 2)$, and let $K_{h_1,h_2} = K_{h_1} \cap K_{h_2}$. Observe that these subgroups are all PE-definable in G_d because the relations R_{h_i} are PE-definable in G $(i = 1, 2)$ and G_{diag,S_1,S_2} is PE-definable in G.

In order to apply Lemma 26 to G_d it remains to see that there exists a disjunction of systems of equations $\bigvee_{i=1}^{m} \Sigma_i(z, x, y_1, \dots, y_n)$ on variables $z, x, y_1, \dots, y_n$, such that for all $b \in K_{h_1}$ there exists $h_b \in G_d$ such that $\bigvee_{i=1}^{m} \Sigma_i(b, x, y_1, \dots, y_n)$ PE-defines the set $h_g^{-1}\{(h_1 h_2^{|b|_{h_2}})^t \mid t \in \mathbb{Z}\}K_{h_1,h_2}h_g$ in G_d. To prove this, we will essentially show that

$$C_{G_d}(h_1 b)K_{h_1,h_2} = h_b^{-1}\{(h_1 h_2^{|b|_{h_2}})^t \mid t \in \mathbb{Z}\}K_{h_1,h_2}h_b, \tag{7}$$

for a certain h_b. That is, modulo K_{h_1,h_2}, the centraliser of $h_1 b$ is a conjugate of the set $\{(h_1 h_2^{|b|_{h_2}})^t \mid t \in \mathbb{Z}\}$.

Let $b \in K_{h_1}$, and let $h_b \in G_d$ be such that $h_b^{-1}(h_1 b)h_b = (h_1 b)^{h_b}$ is cyclically reduced. Let $b_1^{n_1} \dots b_r^{n_r}$ be the block decomposition of $(h_1 b)^{h_b}$. By Theorem 31

$$C_{G_d}(h_1 b) = C_G(h_1 b) \cap G_d = (C_G(b_1^{n_1} \dots b_r^{n_r}))^{h_b^{-1}} \cap G_d =$$
$$= \left(\prod_{i=1}^{r} \langle b_i^{n_i}\rangle_G \times \langle link(b_1 \dots b_r)\rangle_G\right)^{h_b^{-1}} \cap G_d,$$

where by $\langle\cdot\rangle_G$ we mean generation in the group G (as opposed to G_d)

Since $b \in K_{h_1} \leqslant G_d$, no vertex from S_1 belongs to the support of b, and so $|(h_1 b)^{h_b}|_{h_1} = 1$. Moreover, by definition of module, any vertex $u \in V\Gamma$ is adjacent to a vertex $v \in S_1$ if and only if u is adjacent to all vertices of S_1. This has the following implications: if the support of $(h_1 b)^{h_b}$ contains a vertex not in S_1 and not adjacent to any vertex u in S_1, then all vertices from S_1 appear in the same block together with the vertex u, say b_1. In particular, if some vertices of S_2 belong to $supp((h_1 b)^{h_b})$, then they appear only in the block b_1. If, on the contrary, all vertices not in S_1 in the support of $h_1 b^{h_b}$ commute with some vertex of S_1, then the support of $(h_1 b)^{h_b}$ forms a clique in Γ and $S_2 \cap supp((h_1 b)^{h_b}) = \emptyset$.

In the first case we can write $b_1 = h_1 h_2^{|b_1|_{h_2}} k$ for some $k \in K_{h_1,h_2}$ (this is because $G' \leqslant K_{h_1,h_2}$, so we can project b_1 onto the abelianization, order the h_1, h_2's towards the left, and "pull" the resulting expression back into G_d by adding a commutator element which belongs to K_{h_1,h_2}). This way $(h_1 b)^{h_b} = (h_1 h_2^{|b_1|_{h_2}} k)^{n_1} b_2^{n_2} \cdots b_r^{n_r}$. Note that $n_1 = 1$ because $|h_1 b|_{h_1} = 1$. Since all vertices from S_2 must appear in the first block, we have $b_2^{n_2} \cdots b_r^{n_r} \in K_{h_1,h_2}$. From this we it follows that $C_G(h_1 b^{h_b}) \cap G_d = C_G(h_1 b)^{h_b} \cap G_d = C_G(h_1 b)^{h_b}$. Temporarily letting $L = \langle link(b_1 \dots b_r)\rangle_G$ we obtain

$$\begin{aligned}
C_{G_d}(h_1 b)K_{h_1,h_2} &= (C_{G_d}(b_1^{n_1} \dots b_r^{n_r})K_{h_1,h_2})^{h_b^{-1}} \\
&= \left(\left(\prod_{i=1}^{r} \langle b_i^{n_i}\rangle_G \times L \bigcap G_d\right) K_{h_1,h_2}\right)^{h_b^{-1}} \\
&= \left(\prod_{i=1}^{r} \langle b_i^{n_i}\rangle_G K_{h_1,h_2} \times L K_{h_1,h_2}\right)^{h_b^{-1}} \\
&= (\langle b_1\rangle K_{h_1,h_2})^{h_b^{-1}} \\
&= \left(\langle h_1 h_2^{|b_1|_{h_2}} k\rangle K_{h_1,h_2}\right)^{h_b^{-1}} = \left(\langle h_1 h_2^{|b_1|_{h_2}}\rangle K_{h_1,h_2}\right)^{h_b^{-1}}.
\end{aligned}$$

In the second case we have that each vertex in the support of $(h_1 b_1)^{h_b}$ is its own block. In this case, denoting $U = supp((h_1 b_1)^{h_b}) \setminus (S_1 \cup S_2)$,

$$C_{G_d}(h_1 b)K_{h_1,h_2} = \left(\prod_{v \in S_1} \langle v\rangle_G K_{h_1,h_2} \times \prod_{u \in U} \langle u\rangle_G K_{h_1,h_2}\right) \cap G_d = \langle h_1\rangle_G,$$

where the second equality is due to the intersection with G_d.

Finally, observe that $|b_1|_{h_2} = |b|_{h_2}$, which proves (7). Thus it suffices to take the disjunction of systems of equations given by the expression

$$x = x_1 x_2 \wedge [x_1, h_1 b] = 1 \wedge x_2 \in K_{h_1,h_2},$$

where $x_2 \in K_{h_1,h_2}$ is shorthand notation for the disjunction of systems of equations that PE-define K_{h_1,h_2} in G_d.

Hence Lemma 26 applies and we obtain that $\mathcal{DP}(G_{diag,S_1,S_2}, \mathsf{ab})$ is undecidable. Thus $\mathcal{DP}(G, \mathsf{ab})$ undecidable in the case that Γ has more than two vertices and G does not decompose as a nontrivial direct product. In the case where G decomposes as a non-trivial direct product, we have $G = G\Gamma \cong G\Delta_1 \times G\Delta_2$ for some graphs Δ_1, Δ_2, each with strictly less vertices than Γ. Since G is assumed to not be free abelian, either $G\Delta_1$ or $G\Delta_2$ is also not free abelian, and now we can use the induction hypothesis to obtain that $\mathcal{DP}(G\Delta_1, \mathsf{ab})$ or $\mathcal{DP}(G\Delta_2, \mathsf{ab})$ is undecidable. This implies that $\mathcal{DP}(G, \mathsf{ab})$ is undecidable by Lemma 10. ◀