KNAPSACK PROBLEMS IN GROUPS

ALEXEI MYASNIKOV, ANDREY NIKOLAEV, AND ALEXANDER USHAKOV

ABSTRACT. We generalize the classical knapsack and subset sum problems to arbitrary groups and study the computational complexity of these new problems. We show that these problems, as well as the bounded submonoid membership problem, are **P**-time decidable in hyperbolic groups and give various examples of finitely presented groups where the subset sum problem is **NP**-complete.

1. INTRODUCTION

1.1. **Motivation.** This is the first in a series of papers on non-commutative discrete (combinatorial) optimization. In this series we propose to study complexity of the classical discrete optimization (DO) problems in their most general form — in non-commutative groups. For example, DO problems concerning integers (subset sum, knapsack problem, etc.) make perfect sense when the group of additive integers is replaced by an arbitrary (non-commutative) group G. The classical lattice problems are about subgroups (integer lattices) of the additive groups $\mathbb{Z}^n$ or $\mathbb{Q}^n$, their non-commutative versions deal with arbitrary finitely generated subgroups of a group G. The travelling salesman problem or the Steiner tree problem make sense for arbitrary finite subsets of vertices in a given Cayley graph of a non-commutative infinite group (with the natural graph metric). The Post correspondence problem carries over in a straightforward fashion from a free monoid to an arbitrary group. This list of examples can be easily extended, but the point here is that many classical DO problems have natural and interesting non-commutative versions.

The purpose of this research is threefold. First, this extends the area of DO to a new and mostly unknown territory, shedding some light on the nature of the problems and facilitating a deeper understanding of them. In particular, we want to clarify the "algebraic meaning" of these problems in the non-commutative situation. Second, these are algorithmic problems which are very interesting from the computational algebra viewpoint. They unify various techniques in group theory which seem to be far apart now. On the practical level, non-commutative DO problems occur in many everyday computations in algebra, so it is crucial to study their computational complexity and improve the algorithms. Third, we aim to develop a robust collection of basic algebraic problems which would serve as building blocks for complexity theory in non-commutative algebra. Recall, that the success of the classical complexity theory in the area of **NP** computation is, mostly, due

to a vast collection of discrete optimization problems which are known to be in **P** or **NP**-complete. It took many years, starting from the pioneering works of Cook, Levin and Karp in the 1970's, to gradually accumulate this very concrete knowledge. Nowadays, it is usually a matter of technique to reduce a new algorithmic problem to some known discrete optimization problem. This makes the theory of **NP**-complete DO problems, indeed, very robust. In the computational non-commutative algebra the data base of the known **NP**-complete problems is rather small, and complexity of some very basic problems is unknown. Our goal is to start building such a collection in non-commutative algebra.

1.2. **Stating the problems.** In this paper we focus mostly on subset sum, knapsack, and submonoid membership problems and their variations (described below) in a given group G generated by a finite or countably infinite set $X \subseteq G$. We refer to all such problems as *knapsack-type* problems in groups.

Elements in G are given as words over the alphabet $X \cup X^{-1}$. We begin with three principal decision problems.

The subset sum problem SSP(G, X): Given $g_1, \ldots, g_k, g \in G$ decide if

$$(1.1) \qquad\qquad g = g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

Remark 1.1. The formal description of **SSP**(G, X) and other algorithmic problems introduced below depends on the given finite (or sometimes countable) generating set X of the group G. We go into detail regarding formal set-up and, in particular, dependence of these problems on the generating set X in Section 2. For now we mention that as we show in Subsection 2.3 (Lemma 2.5), if X and Y are two *finite* generating sets for a group G and Π is any of the algorithmic problems introduced in this section, then $\Pi(G, X)$ is in **P** if and only if $\Pi(G, Y)$ is in **P**. However, if at least one of the sets X and Y is infinite, the same is false in general (see Example 2.2). Also note that while the complexity of $\Pi(G, X)$ depends on the choice of a generating set, the *answer* to the problem in each particular instance does not. With that in mind, we often write $\Pi(G)$ if a finite generating set is implied, or if the generating set is fixed explicitly. We also often write Π instead of $\Pi(G)$ when we talk about the problem in general, or when the group G is clear from the context.

The knapsack problem KP(G, X): Given $g_1, \ldots, g_k, g \in G$ decide if

$$(1.2) \qquad\qquad g =_G g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k}$$

for some non-negative integers $\varepsilon_1, \ldots, \varepsilon_k$.

There is also a variation of this problem, termed *integer knapsack problem* (**IKP**), when the coefficients ε_i are arbitrary integers. However, it is easy to see that **IKP** is **P**-time reducible to **KP** for any group G (see Section 2).

The third problem is equivalent to **KP** in the classical (abelian) case, but in general it is a completely different problem that is of prime interest in algebra:

Submonoid membership problem SMP(G, X): Given elements $g_1, \ldots, g_k, g \in G$ decide if g belongs to the submonoid generated by $g_1, \ldots, g_k$ in G, i.e., if the following equality holds for some $g_{i_1}, \ldots, g_{i_s} \in \{g_1, \ldots, g_k\}, s \in \mathbb{N}$:

$$(1.3) \qquad\qquad g = g_{i_1}, \ldots, g_{i_s}.$$

The restriction of **SMP** to the case when the set of generators $\{g_1, \ldots, g_n\}$ is closed under inversion (so the submonoid is actually a subgroup of G) is a well-known problem in group theory, called the *generalized word problem* (**GWP**) or the *uniform subgroup membership problem* in G. There is a huge bibliography on this subject, we mention some related results in Section 1.4.

As usual in complexity theory, it makes sense to consider the *bounded* versions of **KP** and **SMP**, at least they are always decidable in groups where the word problem is decidable. In this case the problem is to verify if the corresponding equalities (1.2) and (1.3) hold for a given g provided that the number of factors in these equalities is bounded by a natural number m which is given in the unary form, i.e., as the word 1^m. In particular, the bounded knapsack problem (**BKP**) for a group G asks to decide, when given $g_1, \ldots, g_k, g \in G$ and $1^m \in \mathbb{N}$, if the equality (1.2) holds for some $\varepsilon_i \in \{0, 1, \ldots, m\}$. This problem is **P**-time equivalent to **SSP** in G (see Section 2.3), so it suffices for our purposes to consider only **SSP** in groups. On the other hand, the bounded **SMP** in G is very interesting in its own right.

Bounded submonoid membership problem BSMP(G, X): Given $g_1, \ldots g_k$, $g \in G$ and $1^m \in \mathbb{N}$ (in unary) decide if g is equal in G to a product of the form $g = g_{i_1} \cdots g_{i_s}$, where $g_{i_1}, \ldots, g_{i_s} \in \{g_1, \ldots, g_k\}$ and $s \leq m$.

There are also interesting and important *search* variations of the decision problems above, when the task is to find an actual solution to equations (1.1), (1.2), or (1.3), provided that some solution exists (see Section 2 for more details on this). In most cases we solve both the decision and search variations of the problems above simultaneously, while establishing the time complexity upper bounds for the algorithms. However, as in the classical case, perhaps the most interesting variations of the search problems are their *optimization* versions. It seems these problems were never formally stated before for groups, so we discuss them in a bit more detail here, leaving a more thorough discussion for Section 2.

The subset sum optimization problem SSOP(G, X): Given an instance $g_1, \ldots, g_k, g \in G$ of **SSP**(G) find a solution, if it exists, $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ subject to the optimization condition that the sum $\sum_i \varepsilon_i$ is minimal. Otherwise, output *No solutions*.

The knapsack optimization problem KOP(G, X): Solve the equation (1.2) with the minimum possible number of factors.

In fact, in Section 2 we also discuss other variations of **KOP** in groups, which are even more direct generalizations of the classical **KOP**. In this case when given $g_1, \ldots, g_k, g \in G$ one has to find $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{N}$ for which the product $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ is as close to g (in the metric of the Cayley graph of G) as possible.

The submonoid membership optimization problem SMOP(G, X): Given $g_1, \ldots, g_k, g \in G$, express (if possible) g as a product

(1.4) $$g =_G g_{i_1} \ldots g_{i_m}$$

with the minimum number of factors m.

The submonoid membership optimization problem plays an important part in geometric group theory. Indeed, in geometric language it asks to find a geodesic of a given element in a group (relative to a fixed finite generating set) or the distortion of

a given element in a given finitely generated subgroup — both are crucial geometric tasks.

Sometimes (like in hyperbolic groups) the time complexity of the search **SMP** is not bounded from above by any computable function, in this case it makes sense to consider the optimization version of the bounded **SMP**, called **BSMOP**, in which one has to solve **BSMP**(G) with the minimal possible number of factors.

In the context of the algorithmic problems introduced in this section, the typical groups we are interested in are free, hyperbolic, abelian, nilpotent, or metabelian. In all these groups, and this is important, the word problem is decidable in **P**-time. We might also be interested in constructing some exotic examples of groups where the problems mentioned above have unexpected complexity.

1.3. **What is new?** The general group-theoretic view on subset sum and knapsack problems provides several insights. It is well known that the classical **SSP** is pseudo-polynomial, i.e., it is in **P** when the integers are given in unary form, and it is **NP**-complete if the integers are given in binary. In the group-theoretic framework the classical case occurs when the group G is the additive group of integers $\mathbb{Z}$. In this case the complexity of **SSP**$(\mathbb{Z})$ depends on whether the set X of generators of $\mathbb{Z}$ is finite or infinite. Indeed, if $X = \{1\}$ then we get **SSP** in $\mathbb{Z}$ in the unary form, so in this case it is in **P** (likewise for any other finite generating set). However, if $X = \{2^n \mid n \in \mathbb{N}\}$ then **SSP**$(\mathbb{Z})$ is **P**-time equivalent to the classical **SSP** in the binary form, so **SSP**$(\mathbb{Z})$ relative to this X is **NP**-complete (see Example 2.2 for details). To our surprise the situation is quite different (and much more complex) in non-commutative groups. In the non-commutative setting inputs are usually given as words in a fixed generating set of the group G, i.e., in the *unary form* (so the size of the word $x^{2^{10}}$ is 2^{10}). It turns out that in the unary form **SSP**(G) is **NP**-complete even in some very simple non-abelian groups, such as the metabelian Baumslag–Solitar groups $B(1,p)$, $p \geq 2$, or the wreath product $\mathbb{Z} \wr \mathbb{Z}$. Furthermore, the reasons why **SSP**(G) is hard for such groups G are absolutely different. Indeed, **SSP** is hard for $G = B(1,p)$ because $B(1,p)$ contains exponentially distorted infinite cyclic subgroups $\mathbb{Z}$; while **SSP** is hard for $\mathbb{Z} \wr \mathbb{Z}$ since this group (also being finitely generated) contains an infinite direct sum $\mathbb{Z}^\omega$. On the other hand, **SSP**(G) and **KP**(G) in the decision, search, or optimization variations are in **P** for hyperbolic groups G (relative to arbitrary finite generating sets). Observe, that hyperbolic groups may contain highly (say exponentially) distorted finitely generated subgroups, though such subgroups are not abelian. In this case the main reason why **SSP**(G) and **KP**(G) are easy lies in the geometry of hyperbolic groups, which is asymptotically "tree-like". Another unexpected result which comes from the polynomial time solution of **KP** in hyperbolic groups is that there is a hyperbolic group G with a finitely generated subgroup H such that the bounded membership subgroup problem for H is in **P**, but the standard subgroup membership problem for H is undecidable. This is the first result of this sort in groups. Further yet, there are **P**-time algorithms solving **SSP** and **SMP** (and all their variations) in finitely generated nilpotent groups, though in this case the algorithms explore the polynomial growth of such groups, not their geometry. It remains to be seen if there is a unifying viewpoint on why **SSP**, **KP**, or **SMP** could be hard in a finitely generated group with polynomial time decidable word problem. However, it is already clear that the nature of the complexity of these problems is much deeper than it reveals itself in the commutative case.

1.4. **Results.** The subset sum problem is one of the few very basic **NP**-complete problems, so it was studied intensely (see [21]). Beyond the general interest **SSP** attracted a lot of attention when Merkle and Hellmann designed a new public key cryptosystem [26] based on the difficulty of some variation of **SSP**. The system was broken by Shamir in [48], but the interest persists and the ideas survive in numerous new cryptosystems and their variations (see [37]). Generalizations of knapsack-type cryptosystems to non-commutative groups seem quite promising from the viewpoint of post-quantum cryptography, but even the basic facts on complexity of **SSP** and **KP** in groups are lacking.

In Section 4 we show that $\mathbf{SSP}(G)$ is **NP**-complete in many well-known groups which otherwise are usually viewed as computationally tame, e.g., free metabelian groups of finite rank $r \geq 2$, the wreath product $\mathbb{Z} \wr \mathbb{Z}$, or, more generally, wreath products of any two finitely generated infinite abelian groups. These groups are finitely generated, but not finitely presented. Even more surprisingly, $\mathbf{SSP}(G)$ is **NP**-complete in each of the Baumslag–Solitar metabelian groups $B(1, p), p \geq 2$, as well as in the metabelian group

$$GB = \langle a, s, t \mid [a, a^t] = 1, \ [s, t] = 1, \ a^s = aa^t \rangle,$$

introduced by Baumslag in [3]. Notice, that these groups are finitely presented and have very simple algebraic structure. Furthermore, it is not hard to see that $\mathbf{SSP}(G)$ is **NP**-hard if it is **NP**-hard in some finitely generated subgroup of G. In particular, every group containing subgroups isomorphic to any of the groups mentioned above has **NP**-hard **SSP**. Baumslag [4] and Remeslennikov [43] showed that every finitely generated metabelian group embeds as a subgroup into a finitely presented metabelian group. This gives a method to construct various finitely presented groups with **NP**-complete **SSP**. On the other hand, Theorem 3.3 shows that $\mathbf{SSP}(G)$ is in **P** for every finitely generated nilpotent group G. The proof is short, but it is based on a rather deep fact that such groups have polynomial growth. One of the main results of the paper is Theorem 5.9 which states that $\mathbf{SSP}(G)$, as well as its search variation, is in **P** for any hyperbolic group G. As we mentioned above this also gives a **P**-time solution to the bounded knapsack problem in hyperbolic groups. In Sections 5.4 and 6.3 we give polynomial time solutions to the various subset sum optimization problems in hyperbolic groups, notably **SSOP**1 and **SSOP**2 (see Section 2.2 for definitions).

The knapsack problems in groups, especially in their search variations, are related to the algorithmic aspects of the *big powers method*, which appeared long before any complexity considerations (see, for example, [2]). Recently, the method shaped up as a basic tool in the study of equations in free or hyperbolic groups [10, 23, 24, 39], algebraic geometry over groups [5], completions and group actions [6, 28, 29], and became a routine in the theory of hyperbolic groups (in the form of various lemmas on quasigeodesics). We prove (Theorem 6.1) that $\mathbf{KP}(G)$ together with its search variation are in **P** for any hyperbolic group G. To show this we reduce $\mathbf{KP}(G)$ in **P**-time to $\mathbf{BKP}(G)$ in a hyperbolic group G. More precisely, we obtain the following result (Theorem 6.7), which is of independent interest. For any hyperbolic group G there is a polynomial $p(x)$ such that if an equation $g = g^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ has a solution $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{N}$, then this equation has a solution with ε_i bounded by $p(n)$, where $n = |g_1| + \ldots + |g_k| + |g|$ (and it can be found in **P**-time). On the other hand, decidability of quadratic equations in free groups is **NP**-complete [22]. We also show that all the optimization versions ($\mathbf{KOP}, \mathbf{KOP}1, \mathbf{KOP}2$) of the knapsack

problem in hyperbolic groups are in **P**. To solve knapsack problems in hyperbolic groups we developed a new graph technique, which we believe is of independent interest. Namely, given an instance of a problem we construct a finite labelled graph (whose size is polynomial in the size of the instance), such that one can see, just by looking at the graph, whether or not a solution to the given instance exists in the group, and if so then find it.

We would like to mention one more result (Theorem 5.12) here which came as a surprise to us, it states that **BSMP**(G) is **P**-time decidable for every hyperbolic group G. There are hyperbolic groups where the subgroup membership problem is undecidable even for a fixed finitely generated subgroup; see [44]. It seems this is the first natural example of an undecidable algorithmic problem in groups, whose bounded version is in **P**. It would be interesting to exploit this direction a bit further. The famous Mikhailova's construction [34] shows that the generalized word problem (**GWP**) is undecidable in the direct product $F \times F$ of a free non-abelian group F with itself. We prove in Section 7 (Theorem 7.4) that there is a finitely generated subgroup H in $F_2 \times F_2$ such that the **BSMP** for this fixed subgroup H in $F_2 \times F_2$ is **NP**-complete. It follows that **BSMP**(G) is **NP**-hard for any group G containing $F_2 \times F_2$ as a subgroup. Notice, that Venkatesan and Rajagopalan proved in [52] that in the multiplicative monoid $\mathrm{Mat}(n, \mathbb{Z})$ of all $n \times n$ integer matrices with $n \geq 20$ the **BSMP** is average-case **NP**-complete. One of the reasons of this is that $\mathrm{Mat}(20, \mathbb{Z})$ contains a subgroup $F_2 \times F_2$.

In another direction observe that fully residually free (or limit) groups, as well as finitely generated groups acting freely on $\mathbb{Z}^n$-trees, have decidable **GWP** [30, 35, 36], though the time complexity of the decision algorithms is unknown. It would be remarkable if **BSMP** for such groups was in **P**. Notice, that Schupp gave a remarkable construction to solve **GWP** in **P**-time in orientable surface groups, as well as in some Coxeter groups [47].

We note in passing that the subgroup and submonoid membership problems in a given group could be quite different. For example, Romanovskii proved in [45] that **GWP** is decidable in every finitely generated metabelian group, but recent examples by Lohrey and Steinberg show that in a free metabelian non-abelian group there is a finitely generated submonoid with undecidable membership problem [25]. It would be very interesting to see what is the time complexity of the **BSMP** in free metabelian or free solvable groups. Notice that Umirbaev showed in [50] that **GWP** in free solvable groups of class ≥ 3 is undecidable.

2. General properties

2.1. **Problem set-up.** Since the knapsack-type problems were not previously studied in a non-commutative setting it is worthwhile to say a few words on how we present the data, models of computations, size functions, etc. (we refer to the book [32] for more details). Our model of computation is RAM (random access machines).

To make the statements of the problems (from Section 1.2) a bit more precise consider the following. If a generating set $X = \{x_1, \ldots, x_n\}$ of a group G is finite, then the *size* of the word $g = x_1 \ldots x_k$ is its length $|g| = k$ and the size of the tuple $g_1, \ldots, g_k, g$ from G is the total sum of the lengths $|g_1| + \ldots + |g_k| + |g|$.

If the generating set X of G is infinite, then the size of a letter $x \in X$ is not necessarily equal to 1, it depends on how we represent elements of X. In what

follows we always assume that there is an efficient injective function $\nu : X \rightarrow \{0,1\}^*$ which encodes the elements in X such that for every $u \in \{0,1\}^*$ one can algorithmically recognize if $u \in \nu(X)$, or not. In this case for $x \in X$ define

$$\text{size}(x) = |\nu(x)|$$

and for a word $w = x_1 \ldots x_n$ with $x_i \in X$ define

$$\text{size}(w) = \text{size}(x_1) + \ldots + \text{size}(x_n).$$

Similar to the above the size of a tuple $(g_1, \ldots, g_k, g)$ is

$$\text{size}(g_1, \ldots, g_k, g) = \text{size}(g_1) + \ldots + \text{size}(g_k) + \text{size}(g).$$

One can go a bit further and identify elements $x \in X$ with their images $\nu(x) \in \{0,1\}^*$, and words $w = x_1 \ldots x_n \in X^*$ with the words $\nu(x_1) \ldots \nu(x_n) \in \{0,1\}^*$. This gives a homomorphism of monoids $\nu^* : X^* \rightarrow \{0,1\}^*$. If, in addition, ν is such that for any $x, y \in X$ the word $\nu(x)$ is not a prefix of $\nu(y)$ (this is easy to arrange), then:

- ν^* is injective,
- $\nu^*(X^*)$ and $\nu^*(X)$ are algorithmically recognizable in $\{0,1\}^*$,
- and for every word $v \in \nu^*(X^*)$ one can find the word $w \in X^*$ such that $\nu^*(w) = v$.

From now on we always assume that a generating set comes equipped with a function ν, termed *encoding*, satisfying all the properties mentioned above. In fact, almost always all of our generating sets X are finite, and on those rare occasions when X is infinite we describe ν precisely.

In general, we view decision problems as pairs (I, D), where I is the space of instances of the problem equipped with a function size : $I \rightarrow \mathbb{N}$ and a set $D \subseteq I$ of affirmative (positive) instances of the problem. Of course, the set I should be constructible and size function should be computable. In all our examples the set I consists either of tuples of words $(g_1, \ldots, g_k, g)$ in the alphabet Σ_X for some (perhaps, infinite) set of generators X of a group G, or, in the case of **BKP** or **BSMP**, tuples of the type $(g_1, \ldots, g_k, g, 1^m)$ where 1^m is a natural number m given in unary. The problem (I, D) is decidable if there is an algorithm $\mathcal{A}$ that for any $x \in I$ decides whether x is in D or not ($\mathcal{A}$ answers "Yes" or "No"). The problem is in class **P** if there is a decision algorithm $\mathcal{A}$ with polynomial time function with respect to the size of the instances in I, i.e., there is a polynomial $p(n)$ such that for any $x \in I$ the algorithm $\mathcal{A}$ starts on x, halts in at most $p(\text{size}(x))$ steps, and gives a correct answer "Yes" or "No". Similarly, we define problems in linear or quadratic time, and non-deterministic polynomial time **NP**.

Recall that a decision problem (I_1, D_1) is **P**-*time reducible* to a problem (I_2, D_2) if there is a **P**-time computable function $f : I_1 \rightarrow I_2$ such that for any $u \in I_1$ one has $u \in D_1 \iff f(u) \in D_2$. Such reductions are usually called either *many-to-one* **P**-time reductions or Karp reductions. Since we do not use any other reductions we omit "many-to-one" from the name and call them **P**-time reductions. Similarly, one can introduce linear or quadratic time reductions, etc. We say that two problems are **P**-time equivalent if each of them **P**-time reduces to the other.

Now we define an optimization problem as a tuple $(I, J, F, \mu, \text{extr})$, where I is the set of instances, J is a set of solutions, $F : I \rightarrow P(J)$ is a function that to each instance $u \in I$ associates a subset $F(u) \subseteq J$ of all feasible solutions for an instance u, $\mu(u, v)$ is a non-negative real function that for $u \in I, v \in F(u)$ measures the cost of

a solution v for an instance u, extr is either min or max. This optimization problem, given $u \in I$, asks to find $v \in F(u)$ such that $\mu(u,v) = \text{extr}\{\mu(u,v') \mid v' \in F(u)\}$. Given two optimization problems $P_i = (I_i, J_i, F_i, \mu_i, \text{extr}_i)$, $i = 1, 2$, we say that P_1 is **P**-*time reducible* to P_2 if there are **P**-time computable functions $f : I_1 \to I_2$, $f_u : F_1(u) \to F_2(f(u)), u \in I_1$, such that $v \in F_1(u) \iff f_u(v) \in F_2(f(u))$ and $\mu_1(u,v) = \text{extr}_1\{\mu_1(u,v') \mid v' \in F_1(u)\} \iff \mu_2(f(u), f_u(v)) = \text{extr}_2\{\mu_2(f(u), v') \mid v' \in F_2(f(u))\}$. In our consequent considerations, the functions f_u are apparent from the set up and we do not mention them in our arguments. We say that two optimization problem are **P**-time equivalent if each of them **P**-time reduces to the other.

2.2. **More on the formulation of the problems.** In this section we continue the discussion from the introduction on different variations of the problems **SSP**, **KP**, **SMP** in groups.

There are two ways to state search variations of the problems: the first one, as described in the introduction, considers only feasible instances of the problem, i.e., we assume that a solution to the instance exists; the second one is stronger, in this case it is required to solve the decision problem and simultaneously find a solution (if it exists) for a given instance. The former requires only a partial algorithm, while the latter asks for a total one. The weaker version of the problems **SSP**(G), **KP**(G), **SMP**(G) is always decidable in groups G with decidable word problems, while the stronger one might be undecidable (for instance, **SMP** in hyperbolic groups). In this paper we consider the stronger version of the search problems.

We mentioned in the introduction that the knapsack optimization problem (**KOP**) may have different formulations in the non-commutative groups. Now we explain what we meant.

Recall first, that perhaps the most typical version of the classical **KOP** asks, when given positive integers $a_1, \ldots, a_k, a$ to find $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{N}$ such that the sum $\varepsilon_1 a_1 + \ldots + \varepsilon_k a_k$ is less or equal to a but maximal possible under this restriction. One can generalize this to non-commutative groups as follows.

KOP$1(G, X)$**:** Given $g_1, \ldots, g_k, g \in G$ find $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{N} \cup \{0\}$ with the least possible distance between g and $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in the Cayley graph $Cay(G, X)$.

This formulation allows solutions with the "total weight" higher than the capacity of the knapsack. To define precisely when a given solution fits in geometrically in the knapsack we need the following. For elements $g, h, u \in G$ we say that u *belongs to the segment* $[g, h]$ if there is a geodesic path in $Cay(G, X)$ from g to h that contains u. Now we can formulate the problem.

KOP$2(G, X)$**:** Given $g_1, \ldots, g_k, g \in G$ find $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{N} \cup \{0\}$ such that $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ belongs to the segment $[1, g]$ and the distance between g and $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in the Cayley graph $Cay(G, X)$ is the least possible.

We formulate similar generalizations for the subset sum problem.

SSOP$1(G, X)$**:** Given $g_1, \ldots, g_k, g \in G$ find $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ such that the distance between g and $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in the Cayley graph $Cay(G, X)$ is the least possible.

SSOP$2(G, X)$**:** Given $g_1, \ldots, g_k, g \in G$ find $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ such that the $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ belongs to the segment $[1, g]$ and the distance between g and $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in the Cayley graph $Cay(G, X)$ is the least possible.

One can also consider optimization problems relative to a given non-trivial "weight" function $c : G \to \mathbb{R}$. For example, instead of optimizing $m \to \min$ in (1.4), one can ask to optimize $\sum c(g_{i_j}) \to \min$. Notice that the optimization problems above correspond to the case when the weight function c is a constant function $c = 1$ on G.

Remark 2.1. Note that, unlike in the case of the decision, search and optimization problems introduced in Section 1.2, the answer to a problem $\Sigma \in \{\mathbf{KOP}1, \mathbf{KOP}2, \mathbf{SSOP}1, \mathbf{SSOP}2\}$ depends on the choice of a generating set (cf. Remark 1.1). In view of this, we never omit the generating set X from the notation $\Sigma(G, X)$, unless we are talking about the problem in general.

2.3. **Examples and basic facts.** The classical **SSP** is the following algorithmic question. Given $a_1, \ldots, a_k \in \mathbb{Z}$ and $M \in \mathbb{Z}$ decide if

$$M = \varepsilon_1 a_1 + \ldots + \varepsilon_k a_k$$

for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$. It is well known (see [16, 41, 42]) that if the numbers in **SSP** are given in binary, then the problem is **NP**-complete, but if they are given in unary, then the problem is in **P**. The examples below show how these two variations of **SSP** appear naturally in the group theory context.

Example 2.2. Three variations of the subset sum problem for $\mathbb{Z}$:
- **SSP**$(\mathbb{Z}, \{1\})$ is linear-time equivalent to the classical **SSP** in which numbers are given in unary. In particular, **SSP**$(\mathbb{Z}, \{1\})$ is in **P**.
- For $n \in \mathbb{N} \cup \{0\}$ put $x_n = 2^n$. The set $X = \{x_n \mid n \in \mathbb{N} \cup \{0\}\}$ obviously generates $\mathbb{Z}$. Fix an encoding $\nu : X^{\pm 1} \to \{0, 1\}^*$ for $X^{\pm 1}$ defined by

$$\begin{cases} x_i & \overset{\nu}{\mapsto} & 0101(00)^i 11, \\ -x_i & \overset{\nu}{\mapsto} & 0100(00)^i 11. \end{cases}$$

  Then **SSP**$(\mathbb{Z}, X)$ is **P**-time equivalent to its classical version where the numbers are given in binary form. In particular, **SSP**$(\mathbb{Z}, X)$ is **NP**-complete.
- Let $X = \{2^n \mid n \in \mathbb{N} \cup \{0\}\}$ and the number 2^n is represented by the word $01(00)^{2^n} 11$ (unary representation). Then **SSP**$(\mathbb{Z}, X)$ is in **P**.
- One can easily define **SSP** and **KP** in arbitrary algebras A over a field. These problems are equivalent to **SSP** and **KP** in the additive group A^+ of A. $\qquad \square$

The first example is of no surprise, of course, since, by definition, we treat words representing elements of the group as in unary. The second one shows that there might be a huge difference in complexity of **SSP**(G, X) for finite and infinite generating sets X. The third one indicates that if X is infinite then it really matters how we represent the elements of X.

Definition 2.3. Let G and H be groups generated by countable sets X and Y with encodings ν and μ, respectively. A homomorphism $\varphi : G \to H$ is called **P**-time computable relative to $(X, \nu), (Y, \mu)$ if there exists an algorithm that given a word $\nu(u) \in \nu(\Sigma_X^*)$ computes in polynomial time (in the size of the word $\nu(u)$) a word $\mu(v) \in \mu(\Sigma_Y^*)$ representing the element $v = \varphi(u) \in H$.

Example 2.4. Let G_i be a group generated by a set X_i with encoding ν_i, $i = 1, 2$. If X_1 is finite then any homomorphism $\varphi : G_1 \to G_2$ is **P**-time computable relative to $(X_1, \nu_1), (X_2, \nu_2)$.

To formulate the following results put

$$\mathcal{DP} \;\; = \;\; \{\mathbf{SSP}, \mathbf{KP}, \mathbf{SMP}, \mathbf{BKP}, \mathbf{BSMP}\},$$
$$\mathcal{P} \;\; = \;\; \mathcal{DP} \;\cup\; \{\mathbf{SSOP}, \mathbf{KOP}, \mathbf{SMOP}, \mathbf{BSMOP}\}.$$

Lemma 2.5. *Let G_i be a group generated by a set X_i with an encoding ν_i, $i = 1, 2$. If $\phi : G_1 \to G_2$ is a $\mathbf{P}$-time computable embedding relative to $(X_1, \nu_1), (X_2, \nu_2)$, then $\mathbf{\Pi}(G_1, X_1)$ is $\mathbf{P}$-time reducible to $\mathbf{\Pi}(G_2, X_2)$ for any problem $\mathbf{\Pi} \in \mathcal{P}$.*

Proof. Straightforward. ☐

In view of Example 2.4 we have the following result.

Proposition 2.6. *If X and Y are finite generating sets for a group G, then $\mathbf{\Pi}(G, X)$ is $\mathbf{P}$-time equivalent to $\mathbf{\Pi}(G, Y)$ for any problem $\mathbf{\Pi} \in \mathcal{P}$.*

Proposition 2.7. *Let G be a group and X a generating set for G. Then the word problem ($\mathbf{WP}$) for G is $\mathbf{P}$-time reducible to $\mathbf{\Pi}(G, X)$ for any problem $\mathbf{\Pi} \in \mathcal{P}$.*

Proof. Let $w = w(X)$. Then $w = 1$ in G if and only if $1^\varepsilon = w$ in G for some $\varepsilon \in \{0, 1\}$, i.e., if and only if the instance $1, w$ of $\mathbf{SSP}(G)$ is positive. Likewise for other problems from $\mathcal{P}$. ☐

Corollary 2.8. *Let G be a group with a generating set X. Then:*
1) *$\mathbf{SSP}(G, X)$ (or $\mathbf{BKP}(G, X)$, or $\mathbf{BSMP}(G, X)$) is decidable if and only if the word problem for G is decidable.*
2) *If the word problem for G is $\mathbf{NP}$-hard, then $\mathbf{\Pi}(G, X)$ is $\mathbf{NP}$-hard for any $\mathbf{\Pi} \in \mathcal{DP}$.*

This corollary shows that from $\mathbf{SSP}$ viewpoint groups with polynomial time decidable word problems are the most interesting.

The following result shows how the decision version of $\mathbf{SSP}(G)$ gives a search algorithm to find an actual sequence of ε_i's that is a particular solution for a given instance of $\mathbf{SSP}(G)$.

Proposition 2.9. *For any group G the search $\mathbf{SSP}(G)$ is $\mathbf{P}$-time Turing reducible to the decision $\mathbf{SSP}(G)$. In particular, if $\mathbf{SSP}(G)$ is in $\mathbf{P}$, then search $\mathbf{SSP}(G)$ is also in $\mathbf{P}$.*

Proof. The argument is rather known, so we just give a quick outline to show that it works in the non-commutative case too. Let $w_1, \ldots, w_k, w$ be a given instance of $\mathbf{SSP}(G)$ that has a solution in G. To find a solution $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ for this instance consider the following algorithm.

- Solve the decision problem for $(w_2, \ldots, w_k), w$ in G. If the answer is positive, then put $\varepsilon_1 = 0$. Otherwise put $\varepsilon_1 = 1$ and replace w with $w_1^{-1} w$.
- Continue inductively and find the whole sequence $\varepsilon_1, \ldots, \varepsilon_k$. ☐

Proposition 2.10. *For any group G the following hold:*
1) *$\mathbf{BKP}(G)$ is $\mathbf{P}$-time reducible to $\mathbf{SSP}(G)$;*
2) *$\mathbf{BSMP}(G)$, as well as its optimization variation, is $\mathbf{P}$-time reducible to $\mathbf{SSOP}(G)$.*

Proof. Given an instance $1^m, w_1, \ldots, w_k, w$ of $\mathbf{BKP}(G)$ we consider a sequence

$$(2.1) \qquad w_1, \ldots, w_1, w_2, \ldots, w_2, \ldots, w_k, \ldots, w_k, w \in G,$$

where each segment $w_i, \ldots, w_i$ has precisely m words w_i. Obviously, the initial instance of $\mathbf{BKP}(G)$ has a solution in G if and only if $\mathbf{SSP}(G)$ has a solution in G for the sequence (2.1). This establishes a $\mathbf{P}$-time reduction of $\mathbf{BKP}(G)$ to $\mathbf{SSP}(G)$.

To reduce $\mathbf{BSMP}(G)$ to $\mathbf{SSOP}(G)$ for a given instance $1^m, w_1, \ldots, w_k, w$ of $\mathbf{BSMP}(G)$ consider a sequence

$$(2.2) \qquad w_1, \ldots, w_k, w_1, \ldots, w_k, \ldots, w_1, \ldots, w_k, w \in G,$$

where each segment $w_1, \ldots, w_k$ occurs precisely m times. Obviously, any solution of $\mathbf{BSMP}$ for a given instance gives a solution of $\mathbf{SSP}(G)$ for the sequence (2.2) and vice versa. Hence, solving $\mathbf{SSOP}(G)$ for the sequence (2.2) also solves $\mathbf{BSMP}(G)$ and $\mathbf{BSMOP}(G)$ for the initial instance. This gives a polynomial time reduction of $\mathbf{BSMP}(G)$ and $\mathbf{BSMOP}(G)$ to $\mathbf{SSOP}(G)$. $\qquad\square$

Finally, note that replacing $w_1, \ldots, w_k$ with $w_1, w_1^{-1}, \ldots, w_k, w_k^{-1}$ gives a polynomial time reduction of $\mathbf{IKP}(G)$ to $\mathbf{KP}(G)$.

3. Nilpotent groups

In this section we study the knapsack-type problems in nilpotent groups.

Let G be a group generated by a finite set X. We assume that X is closed under inversion in G, so $X^{-1} = X$. For $n \in \mathbb{N}$ we denote by $B_n(X)$ the ball of radius n in the Cayley graph $Cay(G, X)$ of G relative to X. We view $B_n(X)$ as a finite directed X-labelled graph, which is the subgraph of $Cay(G, X)$ induced by all vertices at distance at most n from the based vertex 1.

The following result is known as folklore.

Proposition 3.1. *Let G be a virtually nilpotent group generated by a finite set X. Then there is a $\mathbf{P}$-time algorithm that for a given $n \in \mathbb{N}$ outputs the graph $B_n(X)$.*

Proof. Denote by V_n the set of vertices of $B_n(X)$. Clearly, $V_0 = \{1\}$, and

$$(3.1) \qquad V_n = V_{n-1} \cup_{y \in X} V_{n-1} y.$$

By a theorem of Wolf [53] the growth of G is polynomial, i.e., $|V_i| \leq p(i)$ for some polynomial $p(n)$. It follows from (3.1) that it takes at most $|X|$ steps (one for each $y \in X$) to construct $B_n(X)$ if given $B_{n-1}(X)$, where each step requires taking an arbitrary vertex $v \in B_{n-1}(X) - B_{n-2}(X)$ (given by some word in X), multiply it by the given $y \in X$, and check if the new word vy is equal or not to any of the previously constructed vertices. Recall that finitely generated virtually nilpotent groups are linear, therefore their word problems are decidable in polynomial time (in fact, real time [20]). This shows that $B_n(X)$ can be constructed in a time polynomial in n for a given fixed G and X. $\qquad\square$

Remark 3.2. The argument above and Theorem 3.3 below are based on the fact that finitely generated virtually nilpotent groups have polynomial growth. By Gromov's theorem [18] the converse is also true, i.e., polynomial growth implies virtual nilpotence, so the argument cannot be applied to other classes of groups.

Theorem 3.3. *Let G be a finitely generated virtually nilpotent group. Then $\mathbf{SSP}(G)$ and $\mathbf{BSMP}(G)$, as well as their search and optimization variations, are in $\mathbf{P}$.*

Proof. Consider an arbitrary instance $g_1, \ldots, g_k, g$ of $\mathbf{SSP}(G)$. For every $i = 0, \ldots, k$ define a set

$$P_i = \{g_1^{\varepsilon_1} \ldots g_i^{\varepsilon_i} \mid \varepsilon_1, \ldots, \varepsilon_i \in \{0, 1\}\}.$$

Clearly, the given instance is positive if and only if $g \in P_k$. The set P_i can be constructed recursively using the formula:

(3.2) $$P_i = P_{i-1} \cup P_{i-1} \cdot g_i.$$

Observe that all elements of P_k lie in the ball $B_m(X)$, where $m = |g_1| + \ldots + |g_k|$. Using formula (3.2) one can in polynomial time identify all vertices in $B_m(X)$ that belong to P_k (an argument similar to the one in Proposition 3.1 works here as well). During the identification process one can also in polynomial time for each vertex $v \in P_k$ associate a tuple $(\varepsilon_1, \ldots, \varepsilon_k)$, where $\varepsilon_i \in \{0, 1\}$, such that $v = g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in G and with minimal possible total sum $\varepsilon_1 + \ldots + \varepsilon_k$. To do this one needs only to keep the best current tuple during the identification process for each already identified vertex in P_k. Now if the element g is given as a word w in X, one can trace w off in the graph $B_m(X)$ and check if this word defines an element from P_k or not. If it does, one can get an optimal solution from the tuple associated with the vertex in P_k defined by w. This solves $\mathbf{SSP}$ and $\mathbf{SSOP}$ in G in polynomial time. By Proposition 2.10 this implies that $\mathbf{BSMP}(G)$ and $\mathbf{BSMOP}(G)$ are in $\mathbf{P}$ as well.   □

4. Groups with hard $\mathbf{SSP}$

In this section we give many examples of various finitely generated and finitely presented groups G with $\mathbf{NP}$-hard $\mathbf{SSP}(G)$. We start with an infinitely generated group $\mathbb{Z}^{\omega}$, a direct sum of countably many copies of the infinite cyclic group $\mathbb{Z}$. We view elements of $\mathbb{Z}^{\omega}$ as sequences $\mathbb{N} \to \mathbb{Z}$ with finite support. For $i \in \mathbb{N}$ by $\mathbf{e}_i$ we denote a sequence such that $\mathbf{e}_i(j) = \delta_{i,j}$, where $\delta_{i,j}$ is the Kronecker delta function. The set $E = \{\mathbf{e}_i\}_{i \in \mathbb{N}}$ is a basis for $\mathbb{Z}^{\omega}$. We fix an encoding $\nu : E^{\pm 1} \to \{0, 1\}^*$ for the generating set E defined by

$$\left\{ \begin{array}{rcl} \mathbf{e}_i & \stackrel{\nu}{\mapsto} & 0101(00)^i 11, \\ -\mathbf{e}_i & \stackrel{\nu}{\mapsto} & 0100(00)^i 11. \end{array} \right.$$

Proposition 4.1. $\mathbf{SSP}(\mathbb{Z}^{\omega}, E)$ *is* $\mathbf{NP}$-*complete.*

Proof. Below we reduce a problem known to be $\mathbf{NP}$-complete, namely a zero-one equation problem, to $\mathbf{SSP}(\mathbb{Z}^{\omega}, E)$. Recall that a vector $v \in \mathbb{Z}^n$ is called a *zero-one* vector if each entry in v is either 0 or 1. Similarly, a square matrix $A \in \mathrm{Mat}(n, \mathbb{Z})$ is called a *zero-one* matrix if each entry in A is either 0 or 1. Denote by 1_n the vector $(1, \ldots, 1) \in \mathbb{Z}^n$. The following problem is $\mathbf{NP}$-complete (see [14]).

Zero-one equation problem (ZOE): Given a zero-one matrix $A \in \mathrm{Mat}(n, \mathbb{Z})$ decide if there exists a zero-one vector $\overline{x} \in \mathbb{Z}^n$ satisfying $A \cdot \overline{x} = 1_n$, or not.

$\mathbf{ZOE}$ can be reduced to $\mathbf{SSP}(\mathbb{Z}^{\omega}, E)$ as follows. Given zero-one $n \times n$ matrix $A = (a_{ij})$ compute elements

$$g_i = \sum_{j=1}^{n} a_{ij} \mathbf{e}_j \in \mathbb{Z}^{\omega} \quad (\text{for } i = 1, \ldots, n)$$

and put $g = \mathbf{e}_1 + \ldots + \mathbf{e}_n$. Clearly, the tuple $g_1, \ldots, g_n, g$ is **P**-time computable and A is a positive instance of **ZOE** if and only if $g_1, \ldots, g_n, g$ is a positive instance of $\mathbf{SSP}(\mathbb{Z}^\omega, E)$. This establishes a **P**-time reduction of **ZOE** to $\mathbf{SSP}(\mathbb{Z}^\omega, \{\mathbf{e}_i\})$, as claimed.   □

The next proposition is obvious.

Proposition 4.2. *Let G be a group generated by a set X. If $\varphi : \mathbb{Z}^\omega \to G$ is a **P**-time computable embedding relative to the generating sets E and X, then $\mathbf{SSP}(G)$ is **NP**-hard. If, in addition, the word problem for G is decidable in polynomial time, then $\mathbf{SSP}(G)$ is **NP**-complete.*   □

This result gives a wide class of groups G with **NP**-hard or **NP**-complete $\mathbf{SSP}(G)$.

Proposition 4.3. *The following groups have **NP**-complete $\mathbf{SSP}$:*
  (a) *Free metabelian non-abelian groups of finite rank.*
  (b) *Wreath product $\mathbb{Z} \wr \mathbb{Z}$.*
  (c) *Wreath product of two finitely generated infinite abelian groups.*

Proof. Let M_n be a free metabelian group with basis $X = \{x_1, \ldots, x_n\}$, where $n \geq 2$. It is not hard to see that the elements

$$e_i = x_1^{-i}[x_2, x_1]x_1^i \quad \text{(for } i \in \mathbb{N})$$

freely generate a free abelian group $\mathbb{Z}^\omega$ (see, for example, the description of normal forms of elements of M_n in [9]). This gives a **P**-time computable embedding of $\mathbb{Z}^\omega$ into M_n relative to the generating sets E and X. It is known that the word problem in finitely generated metabelian groups is in **P** (see, for example, [31]). Hence, by Proposition 4.2, $\mathbf{SSP}(M_n)$ is **NP**-complete and (a) holds.

The wreath product of two infinite cyclic groups generated by a and t, respectively, is a finitely generated infinitely presented group

$$G = \langle a, t \mid [a, t^{-i}at^i] = 1, \text{ (for } i \in \mathbb{N}) \rangle.$$

The set $\{t^{-i}at^i \mid i \in \mathbb{N}\}$ freely generates a subgroup isomorphic to $\mathbb{Z}^\omega$. In fact, the map $\mathbf{e}_i \to t^{-i}at^i$ defines a **P**-time computable embedding of $\mathbb{Z}^\omega$ into G relative to the generating sets E and $\{a, t\}$. Proposition 4.2 finishes the proof of (b).

Finally, consider arbitrary infinite finitely generated abelian groups A and B. Then $A \simeq A_1 \times \mathbb{Z}$ and $B = B_1 \times \mathbb{Z}$ and $\mathbb{Z} \wr \mathbb{Z}$ can be **P**-time embedded into $A \wr B$. The result now follows from (b).   □

Thompson's group F has a finite presentation

$$\langle a, b \mid [ab^{-1}, a^{-1}ba] = 1, \ [ab^{-1}, a^{-2}ba^2] = 1 \rangle.$$

It is a remarkable group due to a collection of very unusual properties that made it a counterexample to many general conjectures in group theory (see [11]).

Proposition 4.4. *The subset sum problem for the Thompson's group F is **NP**-complete.*

Proof. According to [13] the wreath product $\mathbb{Z} \wr \mathbb{Z}$ can be embedded into F with no distortion. The word problem for F is decidable in polynomial time [11, 49]. Now the result follows from Propositions 4.2 and 4.3.   □

In [3] Baumslag gave an example of a finitely presented metabelian group

$$(4.1) \qquad GB = \langle a, s, t \mid [a, a^t] = 1, \ [s, t] = 1, \ a^s = aa^t \rangle.$$

Proposition 4.5. $\mathbf{SSP}(GB)$ *is* $\mathbf{NP}$*-complete.*

Proof. As shown in [3] the subgroup $\langle a, t \rangle$ of the group GB is isomorphic to $\mathbb{Z} \wr \mathbb{Z}$. Hence, $\mathbb{Z} \wr \mathbb{Z}$ embeds into GB and since $\mathbb{Z} \wr \mathbb{Z}$ is finitely generated this embedding is $\mathbf{P}$-time computable. The word problem for GB is in $\mathbf{P}$ because GB is a finitely presented metabelian group. Thus, by Propositions 4.3 and 4.2, $\mathbf{SSP}(GB)$ is $\mathbf{NP}$-complete. $\qquad \square$

There are many examples of finitely presented metabelian groups with $\mathbf{NP}$-complete subset sum problem. Indeed, Baumslag [4] and Remeslennikov [43] proved that every finitely generated metabelian group G embeds into a finitely presented metabelian group G^*. Since G is finitely generated this embedding is $\mathbf{P}$-time computable with respect to the given finite generating sets. Therefore, if G contains $\mathbf{P}$-time computably embedded subgroup $\mathbb{Z}^\omega$ so does G^*.

Now we describe another type of example of finitely presented groups G with $\mathbf{NP}$-complete $\mathbf{SSP}(G)$. Consider the well-known Baumslag–Solitar metabelian group

$$BS(m, n) = \langle a, t \mid t^{-1} a^m t = a^n \rangle.$$

Theorem 4.6. $\mathbf{SSP}(BS(1, 2))$ *is* $\mathbf{NP}$*-complete.*

Proof. We showed in Example 2.2 that $\mathbf{SSP}(\mathbb{Z}, X)$ is $\mathbf{NP}$-complete for a generating set $X = \{x_n = 2^n \mid n \in \mathbb{N} \cup \{0\}\}$. The map

$$x_n \to t^{-n} a t^n$$

is obviously $\mathbf{P}$-time computable and defines an embedding $\phi : \mathbb{Z} \to BS(1, 2)$ because $t^{-n} a t^n = a^{2^n}$. Hence, $\mathbf{SSP}(\mathbb{Z}, X)$ $\mathbf{P}$-time reduces to $\mathbf{SSP}(BS(1, 2))$. Thus, $\mathbf{SSP}(BS(1, 2))$ is $\mathbf{NP}$-complete. $\qquad \square$

In fact, it is easy to prove that $\mathbf{SSP}(BS(m, n))$ is $\mathbf{NP}$-complete whenever $|m| \neq |n|$ and $m, n \neq 0$. It is less obvious that $\mathbf{SSP}(BS(n, \pm n))$ is in $\mathbf{P}$. We briefly outline the algorithm here. Here we use graphs defined in the next section (see Figure 1) in which edges are allowed to be labeled with arbitrary powers of a. Start with the graph $\Gamma(w_1, \dots, w_k, w)$. Repeatedly apply Britton's lemma to the graph:

- for any path $s_1 \overset{t^{\pm 1}}{\to} s_2 \overset{a^{cm}}{\to} s_3 \overset{t^{\mp 1}}{\to} s_4$ add the edge $s_1 \overset{a^{cm}}{\to} s_4$ in the case of $BS(n, n)$, or the edge $s_1 \overset{a^{-cm}}{\to} s_4$ in the case of $BS(n, -n)$ (where $c \in \mathbb{Z}$), and
- for any path $s_1 \overset{a^s}{\to} s_2 \overset{a^t}{\to} s_3$ add the edge $s_1 \overset{a^{s+t}}{\to} s_3$.

The procedure terminates in polynomial time because powers m are bounded by the length of the input. The answer is "Yes" if there exists an ε-edge from α to ω.

Corollary 4.7. *If a group G contains a subgroup isomorphic to $B(m, n)$ with $|m| \neq |n|$ and $m, n \neq 0$, then $\mathbf{SSP}(G)$ is $\mathbf{NP}$-hard.* $\qquad \square$

5. $\mathbf{SSP}$ IN HYPERBOLIC GROUPS

In this section we prove that the subset sum problem is $\mathbf{P}$-time decidable for every hyperbolic group. We refer to [1, 19] for introduction to hyperbolic groups.

The proofs in this section are based on some results from [15, 33, 51] (see also the book [32]).

Let $G = \langle X \mid R \rangle$ be a finitely presented group. A word $w = w(X)$ is called trivial, or a relator, or null-homotopic in G if $w =_G \varepsilon$. A *van Kampen diagram* over the presentation $\langle X \mid R \rangle$ is a planar finite cell complex D given with a specific embedding $D \subseteq \mathbb{R}^2$ satisfying the following conditions.

- D is connected and simply connected.
- Each edge is labeled with a letter $x \in X$.
- Some vertex $v \in \partial D$ is specified as a base-vertex.
- Each cell is labeled with a word from R.

Theorem 5.1 (van Kampen lemma). *A word $w = w(X)$ represents the identity of G if and only if there exists a van Kampen diagram with the boundary label w.*

For a diagram D one can define a *dual graph $Dual(D) = (V, E)$*, where the vertex set V is the set of all cells of D (including the outer cell) and the edge set E is the set of all pairs of cells (c_1, c_2) in D sharing at least one vertex. The maximal distance in $Dual(D)$ from the outer cell to another cell is called the *depth* of D, denoted by $\delta(D)$. By the depth $\delta(w)$ of a trivial in G word w, we understand the minimal depth of a van Kampen diagram with the boundary label w (see [15, 32, 33]).

Proposition 5.2 ([15]). *Let G be a hyperbolic group given by a finite presentation $G = \langle X \mid R \rangle$. Then for any word $w = w(X)$ with $w =_G 1$ one has $\delta(w) = O(\log_2 |w|)$.*

5.1. **Finite state automata over hyperbolic groups.** Our polynomial time solution for the subset sum problem for hyperbolic groups uses finite state automata and two operations, called *R-completion* and *folding*, described below.

Notation. For a finite automaton Γ over the alphabet X we denote by $L(\Gamma)$ the set of all words accepted by Γ. By $|\Gamma|$ we denote the number of states in Γ. In general, for a set $S \subset X^*$ by $\overline{S}$ we denote the image of S in $G = \langle X \mid R \rangle$ under the standard epimorphism $X^* \to G$.

5.1.1. *R-completion.* Recall that a group presentation $\langle X \mid R \rangle$ is called *symmetrized* if $R = R^{-1}$ and R is closed under taking cyclic permutations of its elements. Given a symmetrized presentation $\langle X \mid R \rangle$ and an automaton Γ over $\Sigma_X = X \cup X^{-1} \cup \{\varepsilon\}$ one can construct a new automaton $\mathcal{C}(\Gamma)$ obtained from Γ by adding a loop labeled by r for every $r \in R$ at every state $v \in \Gamma$. By *R-completion* of Γ we understand the graph $\mathcal{C}^k(\Gamma)$ for some $k \in \mathbb{N}$. We want to point out that, unlike in [33], we do not perform Stallings foldings after adding relator-loops. Instead, we perform a special transformation of the automaton described in Section 5.1.2.

Proposition 5.3 (Properties of $\mathcal{C}(\Gamma)$). *For every $\langle X \mid R \rangle$ and Γ the following holds:*
  (a) *Γ is a subgraph of $\mathcal{C}(\Gamma)$.*
  (b) *$\overline{L(\Gamma)} = \overline{L(\mathcal{C}(\Gamma))}$.*
  (c) *$|\mathcal{C}(\Gamma)| \leq |\Gamma| \cdot \|R\|$, where $\|R\| = \sum_{r \in R} |r|$.*

Proof. Follows from the construction of $\mathcal{C}(\Gamma)$. $\qquad\qquad\square$

5.1.2. *Non-Stallings folding.* Given an automaton Γ over a group alphabet Σ_X one can construct a new automaton $\mathcal{F}(\Gamma)$ obtained from Γ by a sequence of steps, at each step adding new edges as described below. For every pair of consecutive edges

of the form shown in the left column of the table below we add the edge from the right column of the table (in the same row), provided this edge is not yet in the graph.

$s_1 \xrightarrow{x} s_2 \xrightarrow{x^{-1}} s_3$	$s_1 \xrightarrow{\varepsilon} s_3$
$s_1 \xrightarrow{x} s_2 \xrightarrow{\varepsilon} s_3$	$s_1 \xrightarrow{x} s_3$
$s_1 \xrightarrow{\varepsilon} s_2 \xrightarrow{x} s_3$	$s_1 \xrightarrow{x} s_3$
$s_1 \xrightarrow{\varepsilon} s_2 \xrightarrow{\varepsilon} s_3$	$s_1 \xrightarrow{\varepsilon} s_3.$

Clearly, the procedure eventually stops, because the number of vertices does not increase and the alphabet X is finite.

Proposition 5.4. $\overline{L(\Gamma)} = \overline{L(\mathcal{F}(\Gamma))}$ *for any finite automaton Γ over the alphabet Σ_X.*

Proof. The language as a set of reduced words does not change.   □

Lemma 5.5. *Let $\langle X \mid R \rangle$ be a finite presentation of a hyperbolic group. Let Γ be an acyclic automaton over Σ_X with at most l non-trivially labeled edges. Then $1 \in \overline{L(\Gamma)}$ if and only if there exists $u \in L(\mathcal{C}^{O(\log l)}(\Gamma))$ satisfying $u =_{F(X)} \varepsilon$.*

Proof. If $1 \in \overline{L(\Gamma)}$, then there exists $v \in L(\Gamma)$ such that $v =_G 1$. The length of v is bounded by l. By Proposition 5.2 the depth of v is bounded by $O(\log |v|)$. Let D be a diagram with perimeter label v of depth $O(\log |v|)$.

Next, we mimic the proof of [32, Proposition 16.3.14]. Cut D to obtain a new "forest" diagram E of the height l with a perimeter label vu, where $u =_{F(X)} \varepsilon$. See [32, Figure 16.2]. The diagram E embeds into $\mathcal{C}^{O(\log l)}(\Gamma)$ and the initial segment v of the perimeter label of E is mapped onto the corresponding word in Γ. This way we obtain a path from α to ω labeled with u, as claimed.

The other direction of the statement follows from Proposition 5.3.   □

Proposition 5.6. *Let $\langle X \mid R \rangle$ be a finite presentation of a hyperbolic group. Let Γ be an acyclic automaton over Σ_X with at most l non-trivially labeled edges. Then $1 \in \overline{L(\Gamma)}$ if and only if $\mathcal{F}(\mathcal{C}^{O(\log l)}(\Gamma))$ contains an edge $\alpha \xrightarrow{\varepsilon} \omega$.*

Proof. Follows from Lemma 5.5, the definition of $\mathcal{F}$, and Proposition 5.4.   □

5.2. **The algorithm.** For a sequence of words $w_1, \ldots, w_k, w$, construct an automaton $\Gamma = \Gamma(w_1, \ldots, w_k, w)$ as in Figure 1. Edges labeled with w_i's on the picture are sequences of edges labeled with the letters involved in w_i's. The initial state is the leftmost state α and the final state is the rightmost state ω. It is easy to see that $|L(\Gamma)| \leq 2^n$ and the length of every $u \in L(\Gamma)$ is bounded by $|w| + \sum |w_i|$. The lemma below is obvious.

Lemma 5.7. *Let $\Gamma = \Gamma(w_1, \ldots, w_k, w)$. An instance $w_1, \ldots, w_k, w$ of $\mathbf{SSP}(G)$ is positive if and only if $1 \in \overline{L(\Gamma)}$.*   □

FIGURE 1. The graph $\Gamma(w_1, \ldots, w_k, w)$.

Theorem 5.8. *Let G be a hyperbolic group given by a finite presentation $\langle X \mid R \rangle$ and $w_1, \ldots, w_k, w \in F(X)$. Then $w =_G w_1^{\varepsilon_1} \ldots w_k^{\varepsilon_k}$ for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ if and only if the graph $\mathcal{F}(\mathcal{C}^{O(\log(|w| + \sum |w_i|))}(\Gamma))$ contains the edge $\alpha \xrightarrow{\varepsilon} \omega$.*

Proof. Follows immediately from the Lemma 5.7 above and Proposition 5.6 with $l = |w| + \sum |w_i|$. $\qquad\square$

As a corollary we get the following principal result.

Theorem 5.9. $\mathbf{SSP}(G) \in \mathbf{P}$ *for any hyperbolic group G.*

Corollary 5.10. *The search variation of $\mathbf{SSP}(G)$ is $\mathbf{P}$-time solvable for any hyperbolic group G.*

Proof. Follows from Proposition 2.9. $\qquad\square$

Another corollary concerns with the bounded knapsack problem.

Corollary 5.11. $\mathbf{BKP}(G) \in \mathbf{P}$ *for any hyperbolic group G.*

Proof. Follows from Proposition 2.10 $\qquad\square$

5.3. **The bounded submonoid membership problem.** In this section we consider the bounded submonoid problem (**BSMP**) in hyperbolic groups.

Theorem 5.12. *Let G be a hyperbolic group. Then $\mathbf{BSMP}(G) \in \mathbf{P}$.*

Proof. The proof uses the technique introduced in Section 5.1. Let w_i be a word representing the element g_i, $i = 1, \ldots, k$, and w a word representing h. We construct a finite graph Γ similar to the one considered in Section 5.2 as shown in Figure 2.
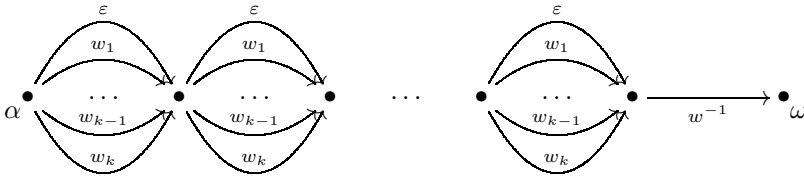

FIGURE 2. Graph Γ.

By Proposition 5.6, $g_1, \ldots, g_k, h, 1^m$ is a positive instance of $\mathbf{BSMP}(G)$ if and only if the graph $F(\mathcal{C}^{O(\log(|w| + m \sum |w_i|))}(\Gamma))$ contains the edge $\alpha \xrightarrow{\varepsilon} \omega$. Hence the result. $\qquad\square$

5.4. **Optimization problems.** In this section we solve in polynomial time several optimization problems in hyperbolic groups.

Theorem 5.13. *Let G be a hyperbolic group. Then the subset sum optimization problem in G is in $\mathbf{P}$.*

Proof. Let $w_1, \ldots, w_k, w$ be a given instance of $\mathbf{SSOP}(G)$. We may assume that $w_i \neq \varepsilon$. Our algorithm is very similar to the algorithm described in Section 5.2, one needs only to use one extra decoration of the graph $\Gamma = \Gamma(w_1, \ldots, w_k, w)$ from Figure 1 (and all of its completions and foldings). We equip the graph Γ with a function $\gamma : E(\Gamma) \to \mathbb{N} \cup \{0\}$, termed the *price function*. This function γ is equal
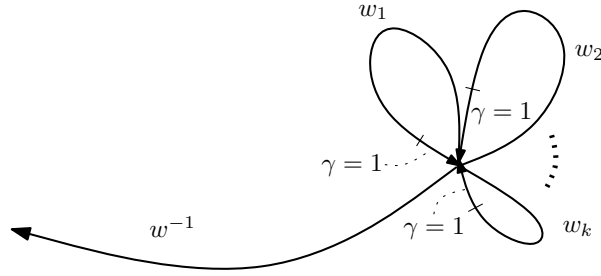
FIGURE 3. Graph Γ, Theorem 5.15.

to zero on all edges except for the last edge in each word w_i, where it is equal to 1. The price of a path $p = e_1, \ldots, e_m$ in Γ from a vertex α to a vertex β is defined by

$$\gamma(p) = \sum \gamma(e_i).$$

Now we describe how γ changes under completions and foldings. In the completion process, as described in Section 5.1.1, one adds loops labelled with relations $r \in R$ and assigns zero price ($\gamma = 0$) to every new edge. Under the folding process every new edge gets the price value that is equal to the sum of the prices of the folded edges. When folding two edges e_1 and e_2, the folding algorithm adds a new edge e only if such an edge does not already exist in the graph. If such e is there already we replace its γ value $\gamma(e)$ with the minimum of $\gamma(e)$ and $\gamma(e_1) + \gamma(e_2)$.

Now we construct the graph $\Delta = \mathcal{F}(\mathcal{C}^{O(\log(|w| + \sum |w_i|))}(\Gamma))$ together with the price function γ, it takes only polynomial time in the size of the instance $w_1, \ldots, w_k$, w. By Theorem 5.8, $\mathbf{SSP}(G)$ has an affirmative solution if and only if the graph Δ contains the edge $\alpha \xrightarrow{\varepsilon} \omega$. Furthermore, it is not hard to see that the price of this edge is the minimal number of w_i's required in the expression (1.4). Now, it is straightforward to find the actual optimal solution from the graph Δ. $\qquad \square$

Corollary 5.14. *Let G be a hyperbolic group. Then the bounded submonoid optimization problem is in* $\mathbf{P}$.

Proof. Follows from the theorem above and Proposition 2.10. $\qquad \square$

We would like to point out that the usual unbounded subgroup membership problem is undecidable in some hyperbolic groups (Rips [44]), hence the search subgroup membership problem in a given hyperbolic group, though decidable, cannot have any computable upper bound on its time complexity. Nevertheless, in some special cases one can solve the unbounded optimization problem in polynomial time, e.g., in free groups.

Theorem 5.15. *The submonoid membership optimization problem in a free group is polynomial time solvable.*

Proof. We construct first a directed graph Γ for $\{w_1, \ldots, w_k\}$ with the tail labelled with w^{-1} as in Figure 3. Then we apply Stallings foldings, decorated with a price function as in the proof of Theorem 5.13. A few details are in order here. The values of the price function are stored in binary. It is easy to see that the bit-length of the values of γ in the folded graph is bounded by $|X| \cdot (|w| + \sum |w_i|)$. Hence, all computations can be done in polynomial time. $\qquad \square$
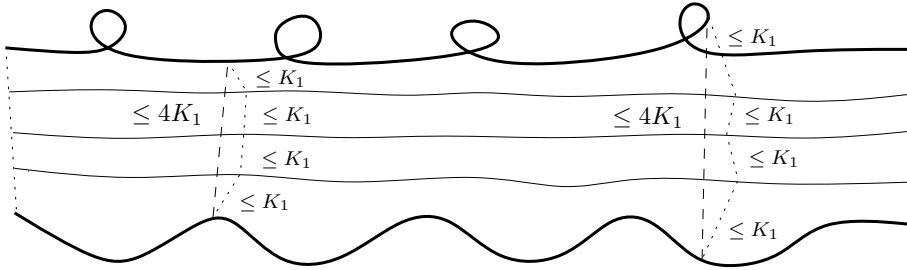
FIGURE 4. Lemma 6.3, $H = 4$.

We give polynomial time solutions to more optimization problems in hyperbolic groups in Section 6.3.

6. KNAPSACK PROBLEM IN HYPERBOLIC GROUPS

In this section we study the knapsack problem $\mathbf{KP}(G)$ in hyperbolic groups G relative to finite generating sets. The main goal is to prove the following theorem.

Theorem 6.1. *Let G be a hyperbolic group generated by finite set X. Then $\mathbf{KP}(G, X) \in \mathbf{P}$. Moreover, there exists a $\mathbf{P}$-time algorithm which for any positive instance $g_1, \ldots, g_k, g \in G$ of $\mathbf{KP}(G)$ computes a sequence of non-negative integers $\varepsilon_1, \ldots, \varepsilon_k$ such that $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k} = g$ in G.*

To prove this theorem we need some results in hyperbolic groups.

6.1. **Auxiliary results in hyperbolic groups.** In our notation we follow the paper [27], where one can also find all the needed notions and definitions.

Lemma 6.2. *Let $\mathcal{H}$ be a δ-hyperbolic geodesic metric space. Let p, q be two (λ, ε)-quasigeodesic paths in $\mathcal{H}$ joining points P_1, P_2 and Q_1, Q_2, respectively. Suppose $H \geq 0$ is such that $|P_1 Q_1| \leq H$ and $|P_2 Q_2| \leq H$. Then there exists $K = K(\delta, \lambda, \varepsilon, H) \geq 0$ such that p, q asynchronously K-fellow travel.*

Proof. This is well known. For example, see [27]. □

Lemma 6.3. *Let $\mathcal{H}$ be a δ-hyperbolic geodesic metric space. Let p, q be two (λ, ε)-quasigeodesic paths in $\mathcal{H}$ joining points P_1, P_2 and Q_1, Q_2, respectively. Suppose $H \geq 1$ is such that $|P_1 Q_1| \leq H$ and $|P_2 Q_2| \leq H$. Then there exists $K_1 = K(\delta, \lambda, \varepsilon) \geq 0$ such that p, q asynchronously $K_1 H$-fellow travel.*

Proof. Let K_1 be the constant $K_1 = K(\delta, \lambda, \varepsilon, 1)$ provided by Lemma 6.2. Then triangle inequality gives a linear in H bound $K \leq K_1 H$ on the constant of fellow travel, as shown in Figure 4. □

It is well known that (quasi-)geodesic polygons in a hyperbolic space are "thin". In the following lemma we give a logarithmic bound on "thickness" of a quasi-geodesic m-gon.

Lemma 6.4. *Let $p_1 p_2 \ldots p_m$ be a (λ, ε)-quasigeodesic m-gon in a δ-hyperbolic space. Then there is a constant $H = H(\delta, \lambda, \varepsilon)$ such that each side p_i, $1 \leq i \leq m$, belongs to the closed $(H + H \ln m)$-neighborhood of the union of other sides $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_m$.*

Proof. First we prove the lemma in the case $m = 2^l$. Drawing a diagonal in a quadrangle, we obtain a constant H_1 such that every side of a (λ, ε)-quasigeodesic quadrangle belongs to the closed H_1-neighborhood of the union of other three sides. (Note that H_1 also delivers the same statement for triangles.) Since $H_1 \leq H_1 + H_1 \ln 4$, this provides the base case $l = 2$.

Suppose the statement is proven for $m = 2^l$ with $H = 3H_1$. Prove that $H = 3H_1$ also suffices in the case $m = 2^{l+1}$.

Indeed, let $p_1, \ldots, p_m$ be an m-gon. For each $1 \leq i \leq m-1$, let p_i have endpoints P_i and P_{i+1}, and p_m have endpoints P_m and P_1. Draw geodesic diagonals $q_1, \ldots, q_{2^l}$ so that q_i, $1 \leq i \leq 2^l - 1$, joins points P_{2i-1}, P_{2i+1}, and q_{2^l} joins P_{m-1}, P_1. (See Figure 5.)
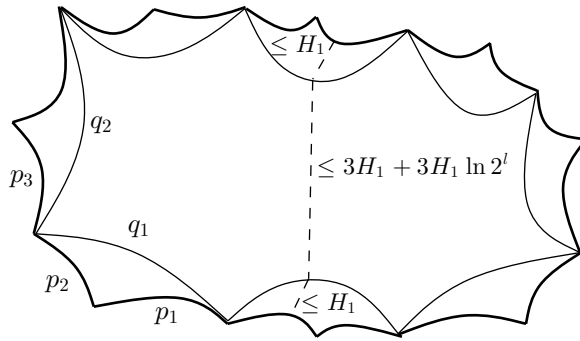

FIGURE 5. Drawing diagonals in a 2^{3+1}-gon.

Since (2^l)-gon $q_1 \ldots q_{2^l}$ belongs to the closed H_1-neighborhood of $p_1 \ldots p_m$, by triangle inequality, every side of $p_1 \ldots p_m$ is contained in the $(H_1 + H_1 + (3H_1 + 3H_1 \ln 2^l))$-neighborhood of the union of other sides. Since

$$H_1 + H_1 + 3H_1 + 3H_1 \ln 2^l \leq 3H_1 + 3H_1 \ln 2^{l+1},$$

the case $m = 2^{l+1}$ is obtained.

Finally, for arbitrary m, considering an m-gon as a degenerate 2^l-gon, where $2^{l-1} < m \leq 2^l$, we obtain that $H = 6H_1$ proves the statement of the lemma.   □

Let $\langle X \mid R \rangle$ be a finite presentation of a hyperbolic group G. We say that an element $g \in G$ is *cyclically reduced* if it has minimal geodesic length among all elements in the conjugacy class g^G. We say that a geodesic word w in the alphabet X is *cyclically reduced* if the corresponding group element $g = \overline{w}$ is cyclically reduced. We say that two elements $g, h \in G$ are *commensurable* if their powers are conjugated, i.e., there exist $m, n \in \mathbb{Z}$, not both zero, $c \in G$ such that $c^{-1}g^m c = h^n$.

Lemma 6.5. *For any finite presentation $\langle X \mid R \rangle$ of a hyperbolic group G, there exist constants λ, ε with the following property. For any cyclically reduced word w, for any $n \in \mathbb{Z}$, the word w^n is (λ, ε)-quasigeodesic.*

Proof. See Lemma 27 of [40].   □

Lemma 6.6. *Suppose $\langle X \mid R \rangle$ is a presentation of a group G. Let w_1 and v_1 be words in the alphabet X such that the corresponding elements $g_1 = \overline{w_1}$, $f_1 = \overline{v_1}$ of*
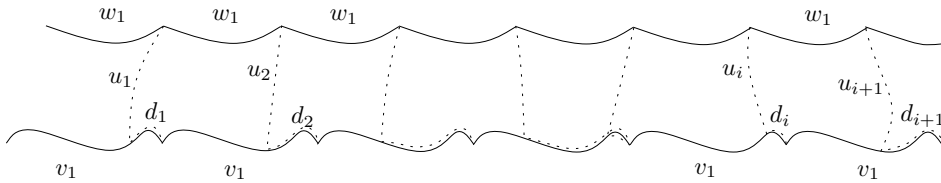
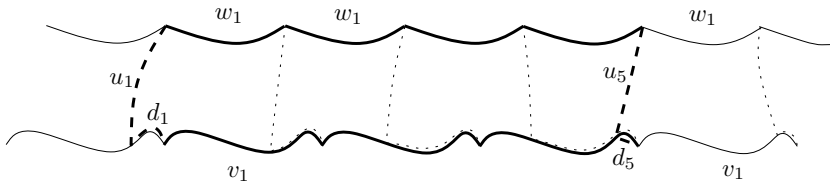FIGURE 6. Paths labeled $u_i d_i$ connect endpoints of copies of w_1 and v_1.

FIGURE 7. If $u_1 d_1 = u_5 d_5$, then $g_1^4 = \overline{u_1 d_1} f_1^3 \overline{u_1 d_1}^{-1}$.

G have infinite order. Suppose w and v are infinite paths in the Cayley graph of $\langle X \mid R \rangle$ labeled by w_1^∞ and v_1^∞.

Then there exists a constant $L = L(|X|)$ with the following property. If a segment of w, containing at least $|v_1| L^K$ copies of w_1, asynchronously K-fellow travels with a segment of v, then g_1 and f_1 are commensurable.

Proof. Note that in such a case, the endpoint of each copy of w_1 is connected by a path labeled by a word u_i of length at most K with a point on v. Therefore, the endpoint of each copy of w_1 is connected by a path labeled $u_i d_i$ with an endpoint of a copy of v_1, where d_i is a terminal subword of v_1 (see Figure 6). Since there are at most $|v_1| \cdot (2|X|)^K$ words of the form $u_i d_i$, taking $L > 2|X|$ guarantees that words $u_i d_i$ repeat, yielding that in G one has

$$(6.1) \qquad g_1^{k_1} = \overline{u_i d_i} f_1^{k_2} \overline{u_i d_i}^{-1},$$

i.e., that g_1, f_1 are commensurable (for example, see Figure 7). $\square$

6.2. **Reduction of KP to BKP.** Let G be a hyperbolic group. The following result, which is of independent interest, **P**-time reduces $\mathbf{KP}(G)$ to $\mathbf{BKP}(G)$. This proves Theorem 6.1 because $\mathbf{BKP}(G)$ is **P**-time decidable by Corollary 5.11.

Theorem 6.7. *Let G be a hyperbolic group. Then there is a polynomial $p(x)$ such that if for $g_1, \ldots, g_k, g \in G$ there exist integers $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{Z}$ such that*

$$g = g_1^{\varepsilon_1} \cdots g_k^{\varepsilon_k},$$

then there exist such integers $\varepsilon_1, \ldots, \varepsilon_k \in \mathbb{Z}$ with

$$\max\{|\varepsilon_1|, \ldots, |\varepsilon_k|\} \leq p(|g_1| + \ldots |g_k| + |g|).$$

Proof. Let E be the maximum order of torsion elements in G (it is well-defined since a hyperbolic group has a finite number of conjugacy classes of finite subgroups, see [7] or [8]), or $E = 1$ if G is torsion-free. For every torsion element g_i, $1 \leq i \leq k$, we may assume that $|\varepsilon_i| < E$. Suppose now that among $g_1, \ldots, g_k$ there is at least one element of infinite order.

Fix a presentation $\langle X \mid R \rangle$ of G and denote $|g_1|_X + \ldots + |g_k|_X + |g|_X = n$ (here $|\cdot|_X$ denotes the geodesic length with respect to X).

Let $g_{i_1}, \ldots, g_{i_m}$ be the entirety of elements of infinite order among $g_1, \ldots, g_k$. For each infinite order g_{i_j}, $1 \leq j \leq m$, let h_j, c_j be such that $g_{i_j} = c_j^{-1} h_j c_j$ and h_j cyclically reduced. Note that $|h_j|_X, |c_j|_X \leq |g_{i_j}|_X \leq n$. Given a product $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$, denote blocks of powers of finite order elements as follows:

$$c_j g_{i_j+1}^{\varepsilon_{i_j+1}} \ldots g_{i_{j+1}-1}^{\varepsilon_{i_{j+1}-1}} c_{j+1}^{-1} = b_{j+1} \qquad \text{for} \quad 1 \leq j \leq m-1,$$

$$b_1 = g_1^{\varepsilon_1} \ldots g_{i_1-1}^{\varepsilon_{i_1-1}} c_1^{-1}, \qquad b_{m+1} = c_m g_{i_m+1}^{\varepsilon_{i_m+1}} \ldots g_k^{\varepsilon_k}.$$

For convenience put $\varepsilon_{i_j} = \alpha_j$ so that

$$g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k} = b_1 h_1^{\alpha_1} b_2 \ldots b_m h_m^{\alpha_m} b_{m+1}.$$

Note that $|b_i| \leq n \cdot n^E + 2n \leq 3n^{E+1}$.

Consider and $(2m+2)$-gon with sides $q_1 p_1 q_2 \ldots p_m q_{m+1} r$ where:

- q_i, $1 \leq i \leq m+1$, is labeled by a geodesic word representing b_i,
- p_i, $1 \leq i \leq m$, is labeled by a (λ, ε)-quasigeodesic word representing $h_i^{\alpha_i}$ (according to Lemma 6.5),
- r is labeled by a geodesic word representing g.

We will show that given a sufficiently large polynomial bound on M, if at least one $|\alpha_j| > M$, then some powers $|\alpha_i| > M$ can be reduced while preserving the equality $g = b_1 h_1^{\alpha_1} b_2 \ldots b_m h_m^{\alpha_m} b_{m+1}$.

Assume some $|\alpha_j| \geq M$, with M to be chosen later. By Lemma 6.4, the side p_j of the polygon belongs to a closed $(H + H \ln(2m+2))$-neighborhood of the union of the other sides, where H only depends on X, R, λ and ε. By Lemma 6.5, λ and ε, in turn, only depend on X, R.

If two points $p_j(t_1), p_j(t_2), t_1 < t_2$ are $(H + H \ln(2m+2))$-close to a side q (where q is one of sides p_i, q_i, r), then by Lemma 6.3 the subpath $p_j(t), t_1 \leq t \leq t_2$ asynchronously $K_2 = K_1(H + H \ln(2m+2))$-fellow travels with a subpath of q. Therefore we may assume that p_j is split into at most $(2m+1)$ segments, so that each segment asynchronously $K_2 = K_1(H + H \ln(2m+2))$-fellow travels with a segment of another side. By pigeonhole principle, at least one segment of p_j contains at least

$$(6.2) \qquad (M - 2m)/(2m+1) \geq \frac{M}{2m+1} - 2 \geq \frac{M}{3n} - 2 = M_1$$

copies of the word representing h_j. Denote this segment of p_j by p and its fellow traveler by s.

Note that since p_j is (λ, ε)-quasigeodesic, geodesic length of s is at least

$$(6.3) \qquad \lambda^{-1}(M_1|h_1|_X - 2K_2) - \varepsilon.$$

We show below that given sufficiently large lower bound on M, p can fellow travel neither with q_i, nor with r. Choosing

$$(6.4) \qquad M > 3n(\lambda(\varepsilon + 3n^{E+1}) + 2K_2 + 2) = Q_1(n)$$

guarantees $M_1 > \lambda(\varepsilon + 3n^{E+1}) + 2K_2$, so by (6.3) geodesic length of $|s|_X > 3n^{E+1}$, which eliminates the possibility that s is a segment of q_i, $1 \leq i \leq m+1$. Note that $Q_1(n)$ in (6.4) is of degree $E + 2$ in n since $K_2 = K_1(H + H \ln(2m+2)) \leq K_1(H + 3nH)$. The same bound (6.4) also prohibits fellow travel with r since geodesic length of r is at most $n < 3n^{E+1}$.

From (6.4) we conclude that with

(6.5) $$M > Q_1(n) + E,$$

the only possibility is that p fellow travels with a segment of some p_l, $l \neq j$.

By Lemma 6.6, there exists L (depending on X) such that if p K_2-fellow travels with a segment of p_l and $M_1 > nL^{K_2}$, then h_j and h_l are commensurable and form a rectangle $h_j^{k_1} = d^{-1}h_l^{k_2}d$ (see (6.1)) with k_1 between 0 and α_j, and k_2 between 0 and α_l. In that case, α_j and α_l can be replaced by $(\alpha_j - k_1)$ and $(\alpha_l - k_2)$, respectively, preserving the equality $g = b_1 h_1^{\alpha_1} \ldots h_m^{\alpha_m} b_{m+1}$. (See Figure 8.) Note
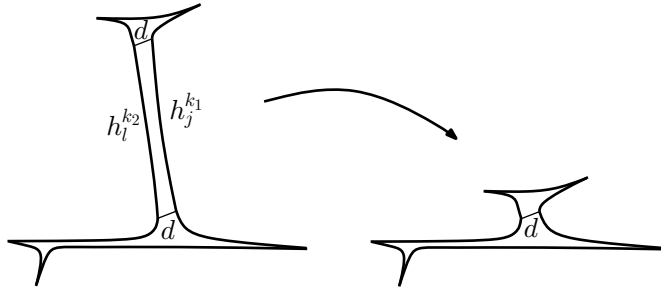

FIGURE 8. Removing rectangle $h_j^{k_1} = d^{-1}h_l^{k_2}d$.

that

$$\begin{aligned} nL^{K_2} &= nL^{K_1(H + H\ln(2m+2))} \\ &= L^{K_1 H} n(2m+2)^{K_1 H \ln L} \\ &\leq L^{K_1 H} n(4n)^{K_1 H \ln L}. \end{aligned}$$

Hence, $M_1 \geq nL^{K_2}$ is guaranteed by

(6.6) $$M > 3n(L^{K_1 H} n(4n)^{K_1 H \ln L} + 2) = Q_2(n),$$

which is of degree $\leq (2 + K_1 H \ln L)$ in n. Consider

(6.7) $$M = Q_1(n) + Q_2(n) + E,$$

which satisfies inequalities (6.4), (6.5) and (6.6). By the argument above, if some $|\varepsilon_i| > M$ and g_i is a torsion element, then ε_i can be replaced with ε_i' where $|\varepsilon_i'| < E < M$. If some $|\varepsilon_i| > M$ and g_i is an infinite order element, then ε_i and some ε_j can be replaced by ε_i' and some ε_j', respectively, where $|\varepsilon_i'| < |\varepsilon_i|$ and $|\varepsilon_j'| < |\varepsilon_j|$.

Repeating this procedure, we eventually obtain that for every $1 \leq i \leq k$, $|\varepsilon_i| < M$. It is only left to note that M in (6.7) is of degree $\max\{E + 2, 2 + K_1 H \ln L\}$ in n, where E, K_1, H, L depend only on the presentation $\langle X \mid R \rangle$. This completes proof of the theorem. $\square$

If infinite order elements $g_1, \ldots, g_m$ are not commensurable, then a stronger version of Theorem 6.7 holds.

Theorem 6.8. *Let $\langle X \mid R \rangle$ be a finite presentation of a hyperbolic group G. Let $w_1, \ldots, w_m$ be words in the alphabet X of total length $|w_1| + |w_2| + \ldots + |w_m| = n$. Suppose that the elements $g_1 = \overline{w_1}, \ldots, g_m = \overline{w_m}$ in G satisfy:*

(a) g_i has infinite order for every $1 \leq i \leq m$.

(b) g_i, g_j are commensurable if and only if $i = j$.

Then there is a polynomial $p(x)$ that depends solely on the presentation $\langle X \mid R \rangle$, such that for any $K \in \mathbb{N}$, if the geodesic length of the product

$$h = g_1^{\alpha_1} \cdots g_m^{\alpha_m}$$

is less than K, then

$$\max\{|\alpha_1|, \ldots, |\alpha_m|\} \leq K \cdot p(n).$$

Proof. We assume $|h|_X < K$ and come up with a lower bound on M that makes this impossible.

For each g_i, $1 \leq i \leq m$, let h_i, c_i be such that $g_i = c_i^{-1} h_i c_i$ and h_i cyclically reduced. Note that $|h_i|_X, |c_i|_X < |g_i|_X \leq n$. Given numbers $\alpha_1, \ldots, \alpha_m$, consider the product

$$h = g_1^{\alpha_1} g_2^{\alpha_2} \cdots g_m^{\alpha_m} = c_1^{-1} h_1^{\alpha_1} c_1 c_2^{-1} h_2^{\alpha_2} c_2 \cdots c_{m-1}^{-1} c_m^{-1} h_m^{\alpha_m} c_m,$$

and $(2m + 2)$-gon with sides $q_1 p_1 q_2 \ldots p_m q_{m+1} r$ where:

- q_1 is labeled by a geodesic word representing c_1^{-1},
- p_i, $1 \leq i \leq m$, is labeled by a (λ, ε)-quasigeodesic word representing $h_i^{\alpha_i}$ (according to Lemma 6.5),
- q_i, $2 \leq i \leq m$, is labeled by a geodesic word representing $c_{i-1} c_i^{-1}$,
- q_{m+1} is labeled by a geodesic word representing c_m,
- r is labeled by a geodesic word representing h.

Assume some $\alpha_j \geq M$, with M to be chosen later. The proof then proceeds similarly to the proof of the Theorem 6.7 using Lemmas 6.4 and 6.3.

Analogously to (6.4),

(6.8) $$M > 3n(\lambda(\varepsilon + 2n + K) + 2K_2 + 2) = P_1(n, K)$$

forbids fellow travel with q_i (since $|q_i| < 2n$) or r (since $|r| < K$). Then

(6.9) $$M > 3n(L^{K_1 H} n(4n)^{K_1 H \ln L} + 2) = P_2(n),$$

similarly to (6.6), allows us to apply Lemma 6.6 if p_j fellow travels with a segment of some p_l, $l \neq j$. Since g_j, g_l are not commensurable, this possibility is also eliminated.

Now notice that

(6.10) $$M = P_1(n, K) + P_2(n)$$

satisfies (6.8) and (6.9), making $|h|_X < K$ impossible. Observe that M in (6.10) is of degree $\max\{2, 2 + K_1 H \ln L\}$ in n, where K_1, H, L ultimately depend only on the presentation $\langle X \mid R \rangle$, and linear in K. □

6.3. **Knapsack optimization problems.** In this section we describe polynomial solutions to **KOP**, **KOP**1, **KOP**2, **SSOP**1, and **SSOP**2 (see Section 2.2) for hyperbolic groups.

By Thereom 6.7, in hyperbolic groups **KP** reduces to **BKP**. Therefore, Theorem 5.13 is enough to give a polynomial time solution to **KOP**. Similarly, by Thereom 6.7, **KOP**1(G, X) in a given hyperbolic group G **P**-time reduces to **SSOP**1(G, X). The following theorem suffices to solve the latter problem in polynomial time.

Theorem 6.9. *Let G be a hyperbolic group given by a finite presentation $\langle X \mid R \rangle$. There exists a polynomial time algorithm that, given $g_1, \ldots, g_k, g \in G$ and a unary $N \in \mathbb{N} \cup \{0\}$, finds $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ such that the distance between g and $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in the Cayley graph $Cay(G, X)$ does not exceed N, or outputs "No solutions" if no such $\varepsilon_1, \ldots, \varepsilon_k$ exist.*

Proof. By a standard argument, it is enough to solve the corresponding decision problem: given $g_1, \ldots, g_k, g \in G$ and a unary $N \in \mathbb{N} \cup \{0\}$, decide whether there exist $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ such that the distance between g and $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in the Cayley graph $Cay(G, X)$ does not exceed N.

We consider graph $\Gamma = \Gamma(w_1, \ldots, w_k, w, N)$ similar to the one in Figure 1, accommodating a ball of radius N centered at w, as in Figure 9.
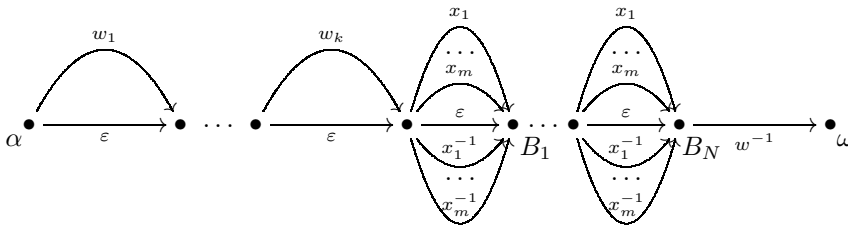

FIGURE 9. The graph $\Gamma(w_1, \ldots, w_k, w, N)$.

It is clear that the problem has a positive answer if and only if $1 \in L(\Gamma)$. By Proposition 5.6, it suffices to check whether the graph

$$\Delta = \mathcal{F}(\mathcal{C}^{O(\log(|w| + \sum |w_i| + mN))}(\Gamma))$$

contains the edge $\alpha \xrightarrow{\varepsilon} \omega$. $\square$

Now we turn to solving **KOP**2(G, X). Again, by Thereom 6.7, it is enough to solve **SSOP**2(G, X), which is achieved using the following statement.

Theorem 6.10. *Let G be a hyperbolic group given by a finite presentation $\langle X \mid R \rangle$. There exists a polynomial time algorithm that, given $g_1, \ldots, g_k, g \in G$ and a unary $N \in \mathbb{N} \cup \{0\}$, finds $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ such that $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ belongs to the segment $[1, g]$, and the distance between g and $g_1^{\varepsilon_1} \ldots g_k^{\varepsilon_k}$ in the Cayley graph $Cay(G, X)$ does not exceed N, or outputs "No solutions" if no such $\varepsilon_1, \ldots, \varepsilon_k$ exist.*

Proof. As in proof of Theorem 6.9, we only need solve the corresponding decision problem.

Recall that hyperbolic groups are strongly geodesically automatic ([12]), which means that they possess an automatic structure, where the language $\mathcal{L}$ accepted by the word acceptor is the set of all geodesic words. Recall further that an equality checker (see, for example, [17]) for an automatic group G is the automaton that accepts the subset $\{(u, v) \mid u =_G v\}$ of $\mathcal{L} \times \mathcal{L}$.

For a given $g \in G$, one can construct in polynomial time an automaton M_g that accepts all geodesic words equal to g in G. Indeed, this can be done by building an automaton product of the equality checker (see [17]) and the automaton Γ_g in Figure 10, where $w = y_1 y_2 \ldots y_{|g|}$ is a geodesic word representing g in generators $X = \{x_1, \ldots, x_m\}$. Further, in the automaton M_g we mark every vertex that is a distance at most N from the terminal one.
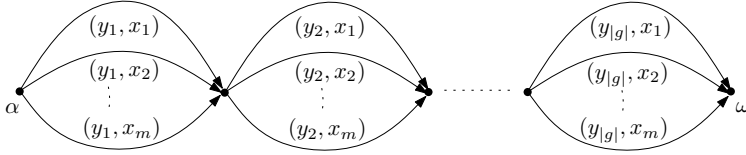
FIGURE 10. The graph Γ_g.
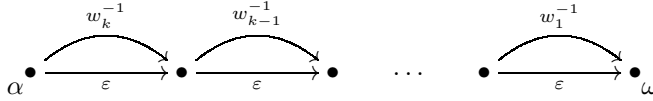
FIGURE 11. The graph Γ.

Let Γ be the automaton displayed in Figure 11. We obtain an automaton $\Delta = \Delta(g_1, g_2, \ldots, g_k, g, N)$ by attaching copies $\Gamma_1, \Gamma_2, \ldots$ of Γ to every marked vertex of M_g, as in Figure 12. We assign the initial vertex of Δ to be the initial vertex α of M_g, and the set of terminal vertices to consist of the terminal vertices $\omega_1, \omega_2, \ldots$ of the copies $\Gamma_1, \Gamma_2, \ldots$.
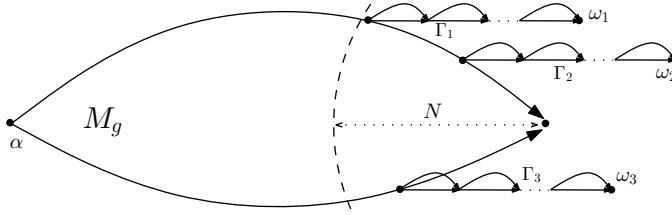
FIGURE 12. The graph Δ.

Notice that the problem has a positive answer if and only if $1 \in L(\Delta)$. By Proposition 5.6, it is enough to check whether there is the edge $\alpha \xrightarrow{\varepsilon} \omega_j$ in $\mathcal{F}(\mathcal{C}^{O(\log l)}(\Delta))$, where l is the number of edges in Δ. It is only left to note that the number of edges in M_g and Γ is polynomial in $\sum |g_i| + |g| + N$, therefore so is l. $\qquad\square$

Corollary 6.11. *Let G be a hyperbolic group given by a finite generating set X. Then* $\mathbf{KOP}(G, X)$, $\mathbf{SSOP}1(G, X)$, $\mathbf{SSOP}2(G, X)$, $\mathbf{KOP}1(G, X)$, $\mathbf{KOP}2(G, X)$ *are in* $\mathbf{P}$.

7. Bounded submonoid membership problem for $F_2 \times F_2$

We proved in Section 5.3 that the bounded submonoid problem is decidable in any hyperbolic group G in polynomial time. In this section we show that taking a direct product does not preserve $\mathbf{P}$-time decidability of $\mathbf{BSMP}$ unless $\mathbf{P} = \mathbf{NP}$. In fact, we prove a stronger result. We show that there exists a (fixed!) subgroup $H = \langle h_1, \ldots, h_k \rangle$ in $F_2 \times F_2$ with $\mathbf{NP}$-complete bounded membership problem.

The bounded GWP for a fixed subgroup $H = \langle h_1, \ldots, h_k \rangle \leq G$**:** Given $g \in G$ and unary $1^n \in \mathbb{N}$ decide if g can be expressed as a product of the form $g = h_{i_1}^{\pm 1} h_{i_2}^{\pm 1} \cdots h_{i_l}^{\pm 1}$, where $l \leq n$ and $1 \leq i_1, \ldots, i_l \leq k$.

Similar to Proposition 2.6, one can show that complexity of the bounded membership problem does not depend on a finite generating set for G, and, hence, we can denote this problem $\mathbf{BGWP}(G; h_1, \ldots, h_k)$.

Proposition 7.1. $\mathbf{BGWP}(G; h_1, \ldots, h_k)$ *is* $\mathbf{P}$-*time reducible to* $\mathbf{BSMP}(G)$. *Therefore, if* $\mathbf{BGWP}(G; h_1, \ldots, h_k)$ *is* $\mathbf{NP}$-*complete and the word problem in* G *is in* $\mathbf{P}$, *then* $\mathbf{BSMP}(G)$ *is* $\mathbf{NP}$-*complete.*

Proof. $(g, 1^n)$ is a positive instance of $\mathbf{BGWP}(G; h_1, \ldots, h_k)$ if and only if $(h_1, \ldots, h_k, h_1^{-1}, \ldots, h_k^{-1}, g, 1^n)$ is a positive instance of $\mathbf{BSMP}(G)$. $\square$

Below we prove that there exists a subgroup $H = \langle h_1, \ldots, h_k \rangle$ in $F_2 \times F_2$ with $\mathbf{NP}$-complete $\mathbf{BGWP}(F_2 \times F_2; h_1, \ldots, h_k)$. In our argument we employ the idea used by Olshanskii and Sapir in [38, Theorems 2 and 7] to investigate subgroup distortions in $F_2 \times F_2$. The argument follows Mikhailova's construction of a subgroup of $F_2 \times F_2$ with undecidable membership problem. We briefly outline that construction as described in [34].

Let $G = \langle X \mid R \rangle$ be a finitely presented group. We may assume that both sets X and R are symmetric, i.e., $X = X^{-1}$ and $R = R^{-1}$. Define a set:

$$(7.1) \qquad D_G = \{(r, 1) \mid r \in R\} \cup \{(x, x^{-1}) \mid x \in X\} \quad \subset \quad F(X) \times F(X).$$

Let H be a subgroup of $F(X) \times F(X)$ generated by D_G. Then for any $w \in F(X)$:

$$(7.2) \qquad\qquad\qquad (w, 1) \in H \quad \Leftrightarrow \quad w = 1 \text{ in } G.$$

In more detail, the following lemma is true.

Lemma 7.2 ([34])**.** *Let* $w = w(X)$. *If*

$$(w, 1) = (u_1, v_1)(u_2, v_2) \ldots (u_n, v_n) \text{ for some } (u_i, v_i) \in D_G,$$

then the word $u_1 \ldots u_n$ *is of the form*

$$w_0 r_1 w_1 r_2 w_2 \ldots w_{m-1} r_m w_m \text{ for some } w_i \in F(X), \ r_i \in R$$

satisfying $w_0 w_1 \ldots w_m =_{F(X)} 1$ *and, hence,*

$$w =_{F(X)} \prod_{i=1}^{m} (w_0 \ldots w_{i-1}) r_i (w_0 \ldots w_{i-1})^{-1}.$$

Moreover, by [38, Lemma 1] we may assume that $|w_0| + \ldots + |w_m| \leq 4E$, where E is the number of edges in the minimal van Kampen diagram for w over $\langle X \mid R \rangle$. Denoting $C = \max\{|r| : r \in R\}$, we get $|w_0| + \ldots + |w_m| \leq 4(Cm + |w|)$, so

$$(7.3) \qquad n \leq m + 2(|w_0| + |w_1| + \ldots + |w_m|) \leq m + 8(Cm + |w|),$$

i.e., the number of elements of D_G necessary to represent $(w, 1)$ is bounded by a polynomial (in fact, linear) function of $|w|$ and m.

Lemma 7.3. *Let* $\langle X \mid R \rangle$ *be finite presentation of a group* G *and* $D_G \subset F(X) \times F(X)$ *the set given by* (7.1). *If the isoperimetric function for* $\langle X \mid R \rangle$ *is bounded by a polynomial* p, *then the word problem in* G *is* $\mathbf{P}$-*time reducible to* $\mathbf{BGWP}(F(X) \times F(X); D_G)$.

Proof. As above, let $C = \max\{|r| : r \in R\}$. For an arbitrary $w \in F(X)$ compute

$$n = p(|w|) + 8(Cp(|w|) + |w|).$$

Now it easily follows from Lemma 7.2 and inequality (7.3) that $w = 1$ in G if and only if $((w, 1), 1^n)$ is a positive instance of $\mathbf{BGWP}(F(X) \times F(X); D_G)$. $\square$

Theorem 7.4. *There is a finitely generated subgroup $H = \langle h_1, \ldots, h_k \rangle$ in $F_2 \times F_2$ such that $\mathbf{BGWP}(F_2 \times F_2; h_1, \ldots, h_k)$ is $\mathbf{NP}$-complete.*

Proof. It is shown in [46] that there exists a finitely presented group G with $\mathbf{NP}$-complete word problem and polynomial Dehn function. Let $D_G = \{h_1, \ldots, h_k\}$ be a subset of $F(X) \times F(X)$ defined by (7.1). By Lemma 7.3, $\mathbf{BGWP}(F(X) \times F(X); D_G)$ is $\mathbf{NP}$-hard. Since $F_2 \times F_2$ contains subgroup isomorphic to $F(X) \times F(X)$, $\mathbf{BGWP}(F_2 \times F_2; D_G)$ is also $\mathbf{NP}$-hard. It is only left to note that the word problem in $F_2 \times F_2$ is $\mathbf{P}$-time decidable, so $\mathbf{BGWP}(F_2 \times F_2; D_G)$ is $\mathbf{NP}$-complete. □

Corollary 7.5. *If G contains $F_2 \times F_2$ as a subgroup, then there exists $\{h_1, \ldots, h_k\} \subseteq G$ such that $\mathbf{BGWP}(G; h_1, \ldots, h_k)$ and $\mathbf{BSMP}(G)$ are $\mathbf{NP}$-hard. If, in addition, the word problem in G is $\mathbf{P}$-time decidable, then $\mathbf{BGWP}(G; h_1, \ldots, h_k)$ and $\mathbf{BSMP}(G)$ are $\mathbf{NP}$-complete.*

Corollary 7.6. *Linear groups $GL(\geq 4, \mathbb{Z})$, braid groups and graph groups whose graph contains an induced square C_4 have $\mathbf{NP}$-complete $\mathbf{BGWP}$ and $\mathbf{BSMP}$.*

References

[1] J. M. Alonso, T. Brady, D. Cooper, V. Ferlini, M. Lustig, M. Mihalik, M. Shapiro, and H. Short, *Notes on word hyperbolic groups*, Group theory from a geometrical viewpoint (Trieste, 1990), World Sci. Publ., River Edge, NJ, 1991, pp. 3–63. Edited by Short. MR1170363 (93g:57001)

[2] Gilbert Baumslag, *On generalised free products*, Math. Z. **78** (1962), 423–438. MR0140562 (25 #3980)

[3] Gilbert Baumslag, *A finitely presented metabelian group with a free abelian derived group of infinite rank*, Proc. Amer. Math. Soc. **35** (1972), 61–62. MR0299662 (45 #8710)

[4] Gilbert Baumslag, *Subgroups of finitely presented metabelian groups*, J. Austral. Math. Soc. **16** (1973), 98–110. MR0332999 (48 #11324)

[5] Gilbert Baumslag, Alexei Myasnikov, and Vladimir Remeslennikov, *Algebraic geometry over groups. I. Algebraic sets and ideal theory*, J. Algebra **219** (1999), no. 1, 16–79, DOI 10.1006/jabr.1999.7881. MR1707663 (2000j:14003)

[6] Gilbert Baumslag, Alexei Myasnikov, and Vladimir Remeslennikov, *Discriminating completions of hyperbolic groups*, Geom. Dedicata **92** (2002), 115–143, DOI 10.1023/A:1019687202544. MR1934015 (2003i:20073)

[7] O. V. Bogopol′skiĭ and V. N. Gerasimov, *Finite subgroups of hyperbolic groups* (Russian, with Russian summary), Algebra i Logika **34** (1995), no. 6, 619–622, 728, DOI 10.1007/BF00739330; English transl., Algebra and Logic **34** (1995), no. 6, 343–345 (1996). MR1400705 (97c:20055)

[8] Noel Brady, *Finite subgroups of hyperbolic groups*, Internat. J. Algebra Comput. **10** (2000), no. 4, 399–405, DOI 10.1142/S0218196700000236. MR1776048 (2001f:20084)

[9] R. M. Bryant and V. A. Roman′kov, *Automorphism groups of relatively free groups*, Math. Proc. Cambridge Philos. Soc. **127** (1999), no. 3, 411–424, DOI 10.1017/S0305004199003898. MR1713119 (2001b:20061)

[10] V. K. Bulitko, *Equations and inequalities in a free group and a free semigroup* (Russian), Tul. Gos. Ped. Inst. Učen. Zap. Mat. Kaf. **2 Geometr. i Algebra** (1970), 242–252. MR0393235 (52 #14045)

[11] J. W. Cannon, W. J. Floyd, and W. R. Parry, *Introductory notes on Richard Thompson's groups*, Enseign. Math. (2) **42** (1996), no. 3-4, 215–256. MR1426438 (98g:20058)

[12] James W. Cannon, *The combinatorial structure of cocompact discrete hyperbolic groups*, Geom. Dedicata **16** (1984), no. 2, 123–148, DOI 10.1007/BF00146825. MR758901 (86j:20032)

[13] Sean Cleary, *Distortion of wreath products in some finitely presented groups*, Pacific J. Math. **228** (2006), no. 1, 53–61, DOI 10.2140/pjm.2006.228.53. MR2263024 (2007k:20085)

[14] S. Dasgupta, C. Papadimitriou, and U. Vazirani, *Algorithms*, McGraw-Hill Science, 2006.

[15] Cornelia Druţu, *Cônes asymptotiques et invariants de quasi-isométrie pour des espaces métriques hyperboliques* (French, with English and French summaries), Ann. Inst. Fourier (Grenoble) **51** (2001), no. 1, 81–97. MR1821069 (2002h:53069)

[16] Michael R. Garey and David S. Johnson, *Computers and Intractability,* A guide to the theory of NP-completeness; A Series of Books in the Mathematical Sciences, W. H. Freeman and Co., San Francisco, Calif., 1979. MR519066 (80g:68056)

[17] S. M. Gersten and H. B. Short, *Small cancellation theory and automatic groups*, Invent. Math. **102** (1990), no. 2, 305–334, DOI 10.1007/BF01233430. MR1074477 (92c:20058)

[18] Mikhael Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. **53** (1981), 53–73. MR623534 (83b:53041)

[19] Mikhael Gromov, *Hyperbolic groups*, Essays in Group Theory, MSRI Publications, vol. 8, Springer, 1985, pp. 75–263.

[20] Derek F. Holt and Sarah Rees, *Solving the word problem in real time*, J. London Math. Soc. (2) **63** (2001), no. 3, 623–639, DOI 10.1017/S0024610701002083. MR1825979 (2002b:20044)

[21] Hans Kellerer, Ulrich Pferschy, and David Pisinger, *Knapsack Problems*, Springer-Verlag, Berlin, 2004. MR2161720 (2006d:90002)

[22] O. Kharlampovich, I. G. Lysënok, A. G. Myasnikov, and N. W. M. Touikan, *The solvability problem for quadratic equations over free groups is NP-complete*, Theory Comput. Syst. **47** (2010), no. 1, 250–258, DOI 10.1007/s00224-008-9153-7. MR2643918 (2011g:68099)

[23] O. Kharlampovich and A. Myasnikov, *Irreducible affine varieties over a free group. I. Irreducibility of quadratic equations and Nullstellensatz*, J. Algebra **200** (1998), no. 2, 472–516, DOI 10.1006/jabr.1997.7183. MR1610660 (2000b:20032a)

[24] O. Kharlampovich, E. Lioutikova, and A. Myasnikov, *Equations in the **Q**-completion of a torsion-free hyperbolic group*, Trans. Amer. Math. Soc. **351** (1999), no. 7, 2961–2978, DOI 10.1090/S0002-9947-99-02010-3. MR1443195 (99j:20039b)

[25] Markus Lohrey and Benjamin Steinberg, *Tilings and submonoids of metabelian groups*, Theory Comput. Syst. **48** (2011), no. 2, 411–427, DOI 10.1007/s00224-010-9264-9. MR2763109 (2012b:20080)

[26] R. Merkle and M. Hellman, *Hiding information and signatures in trapdoor knapsacks*, Inform. Theory, IEEE Trans. **24** (1978), 525–530.

[27] A. G. Miasnikov and A. Nikolaev, *Verbal subgroups of hyperbolic groups have infinite width*, preprint. Available at http://arxiv.org/abs/1107.3719, 2011.

[28] A. G. Myasnikov and V. N. Remeslennikov, *Exponential groups. II. Extensions of centralizers and tensor completion of CSA-groups*, Internat. J. Algebra Comput. **6** (1996), no. 6, 687–711, DOI 10.1142/S0218196796000398. MR1421886 (97j:20039)

[29] A. G. Miasnikov, V. Remeslennikov, and D. Serbin, *Regular free length functions on Lyndon's free* $\mathbb{Z}[t]$*-group* $f^{F[t]}$, Algorithms, Languages, Logic, Contemporary Mathematics, vol. 378, American Mathematical Society, 2005, pp. 37–77.

[30] Alexei G. Myasnikov, Vladimir N. Remeslennikov, and Denis E. Serbin, *Fully residually free groups and graphs labeled by infinite words*, Internat. J. Algebra Comput. **16** (2006), no. 4, 689–737, DOI 10.1142/S0218196706003141. MR2258835 (2007k:20053)

[31] A. Myasnikov, V. Roman'kov, A. Ushakov, and A. Vershik, *The word and geodesic problems in free solvable groups*, Trans. Amer. Math. Soc. **362** (2010), no. 9, 4655–4682. MR2645045 (2011k:20059)

[32] A. G. Miasnikov, V. Shpilrain, and A. Ushakov, *Non-commutative Cryptography and Complexity of Group-theoretic Problems*, Mathematical Surveys and Monographs, AMS, 2011.

[33] Alexei Myasnikov and Alexander Ushakov, *Random van Kampen diagrams and algorithmic problems in groups*, Groups Complex. Cryptol. **3** (2011), no. 1, 121–185, DOI 10.1515/GCC.2011.006. MR2806084 (2012g:20065)

[34] K. A. Mihaĭlova, *The occurrence problem for direct products of groups* (Russian), Dokl. Akad. Nauk SSSR **119** (1958), 1103–1105. MR0100018 (20 #6454)

[35] Andrey Nikolaev, *Membership Problem in Groups Acting Freely on Non-Archimedean Trees*, ProQuest LLC, Ann Arbor, MI, 2010. Thesis (Ph.D.)–McGill University (Canada). MR2890071

[36] Andrey Nikolaev and Denis Serbin, *Membership problem in groups acting freely on* $\mathbb{Z}^n$*-trees*, J. Algebra **370** (2012), 410–444, DOI 10.1016/j.jalgebra.2012.07.038. MR2966848

[37] A. M. Odlyzko, *The rise and fall of knapsack cryptosystems*, Cryptology and computational number theory (Boulder, CO, 1989), Proc. Sympos. Appl. Math., vol. 42, Amer. Math. Soc., Providence, RI, 1990, pp. 75–88. MR1095552 (92f:94016)

[38] Alexander Yu. Ol′shanskii and Mark V. Sapir, *Length and area functions on groups and quasi-isometric Higman embeddings*, Internat. J. Algebra Comput. **11** (2001), no. 2, 137–170, DOI 10.1142/S0218196701000401. MR1829048 (2002b:20058)

[39] A. Yu. Ol′shanskiĭ, *Diagrams of homomorphisms of surface groups* (Russian), Sibirsk. Mat. Zh. **30** (1989), no. 6, 150–171, DOI 10.1007/BF00970919; English transl., Siberian Math. J. **30** (1989), no. 6, 961–979 (1990). MR1043443 (91e:20028)

[40] A. Yu. Ol′shanskiĭ, *Periodic quotients of hyperbolic groups*, Mat. Zametki **182** (1991), 543–567.

[41] Christos H. Papadimitriou, *Computational Complexity*, Addison-Wesley Publishing Company, Reading, MA, 1994. MR1251285 (95f:68082)

[42] Christos H. Papadimitriou and Kenneth Steiglitz, *Combinatorial Optimization: Algorithms and Complexity*, Dover Publications Inc., Mineola, NY, 1998. Corrected reprint of the 1982 original. MR1637890

[43] V. Remeslennikov, *On finitely presented groups*, Fourth All-Union Symposium on the Theory of Groups 1973 (Novosibirsk, USSR), 1973, pp. 164–169.

[44] E. Rips, *Subgroups of small cancellation groups*, Bull. London Math. Soc. **14** (1982), no. 1, 45–47, DOI 10.1112/blms/14.1.45. MR642423 (83c:20049)

[45] N. S. Romanovskiĭ, *The embedding problem for abelian-by-nilpotent groups* (Russian), Sibirsk. Mat. Zh. **21** (1980), no. 2, 170–174, 239. MR569186 (82c:20069)

[46] Mark V. Sapir, Jean-Camille Birget, and Eliyahu Rips, *Isoperimetric and isodiametric functions of groups*, Ann. of Math. (2) **156** (2002), no. 2, 345–466, DOI 10.2307/3597195. MR1933723 (2005b:20077a)

[47] Paul E. Schupp, *Coxeter groups, 2-completion, perimeter reduction and subgroup separability*, Geom. Dedicata **96** (2003), 179–198, DOI 10.1023/A:1022155823425. MR1956839 (2003m:20052)

[48] Adi Shamir, *A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem*, IEEE Trans. Inform. Theory **30** (1984), no. 5, 699–704, DOI 10.1109/TIT.1984.1056964. MR781265 (86m:94032)

[49] V. Shpilrain and A. Ushakov, *Thompson's group and public key cryptography*, Applied Cryptography and Network Security – ACNS 2005, Lecture Notes Comp. Sc., vol. 3531, Springer, 2005, pp. 151–164.

[50] U. U. Umirbaev, *The occurrence problem for free solvable groups* (Russian, with Russian summary), Algebra i Logika **34** (1995), no. 2, 211–232, 243, DOI 10.1007/BF00750164; English transl., Algebra and Logic **34** (1995), no. 2, 112–124. MR1362615 (96k:20063)

[51] A. Ushakov, *Fundamental search problems in groups*, Ph.D. thesis, CUNY/Graduate Center, 2005.

[52] R. Venkatesan and S. Rajagopalan, *Average case intractability of matrix and diophantine problems* (extended abstract), STOC (S. Rao Kosaraju, Mike Fellows, Avi Wigderson, and John A. Ellis, eds.), ACM, 1992, pp. 632–642.

[53] Joseph A. Wolf, *Growth of finitely generated solvable groups and curvature of Riemanniann manifolds*, J. Differential Geometry **2** (1968), 421–446. MR0248688 (40 #1939)

Stevens Institute of Technology, Hoboken, New Jersey 07030
E-mail address: `amiasnik@stevens.edu`

Stevens Institute of Technology, Hoboken, New Jersey 07030
E-mail address: `anikolae@stevens.edu`

Stevens Institute of Technology, Hoboken, New Jersey 07030
E-mail address: `aushakov@stevens.edu`