KNAPSACK PROBLEMS IN PRODUCTS OF GROUPS

ELIZAVETA FRENKEL, ANDREY NIKOLAEV, AND ALEXANDER USHAKOV

Abstract. The classic knapsack and related problems have natural generalizations to arbitrary (non-commutative) groups, collectively called knapsack-type problems in groups. We study the effect of free and direct products on their time complexity. We show that free products in certain sense preserve time complexity of knapsack-type problems, while direct products may amplify it.

Keywords. Subset sum problem, knapsack problem, bounded subgroup membership problem, free products, direct products, hyperbolic groups, nilpotent groups.

2010 Mathematics Subject Classification. 03D15, 20F65, 20F10.

1. Introduction

In [4], the authors introduce a number of certain decision, search and optimization algorithmic problems in groups, such as the subset sum problem, the knapsack problem, and the bounded submonoid membership problem (see Section 1.1 for definitions). These problems are collectively referred to as knapsack-type problems and deal with different generalizations of the classic knapsack and subset sum problems over \( \mathbb{Z} \) to the case of arbitrary groups. In the same work, the authors study time complexity of such problems for various classes of groups, for example for nilpotent, metabelian, hyperbolic groups. With that collection of results in mind, it is natural to ask what is the effect of group constructions on the complexity of knapsack-type problems, primarily the subset sum problem. In the present paper we address this question in its basic variation, for the case of free and direct products of groups.

Solutions to many algorithmic problems carry over from groups to their free products without much difficulty. It certainly is the case with classic decision problems in groups such as the word, conjugacy [2] and membership [7] problems. In some sense, the same expectations are satisfied with knapsack-type problems, albeit not in an entirely straightforward fashion. It turns out that knapsack-type problems such as the aforementioned subset sum problem, the bounded knapsack problem, and the bounded submonoid membership problem share a certain common ground that allows to approach these problems in a unified fashion, and to carry solutions of these problems over to free products. Thus, our research both presents certain known facts about these algorithmic problems in a new light, and widens the class of groups with known complexity of the knapsack-type problems.

Algorithmic problems in a direct product of groups can be dramatically more complex than in either factor, as is the case with the membership problem, first shown by Mikhailova [6]. By contrast, the word and conjugacy problems in direct products easily reduce to those in the factors. In Section 3 we show that direct product does not preserve polynomial time subset sum problem (unless \( \text{P} = \text{NP} \)).
Thus, the subset sum problem occupies an interesting position, exhibiting features of both word problem and membership problem; on the one hand, its decidability clearly carries immediately from factors to the direct product, while, on the other hand, its time complexity can increase dramatically.

Below we provide basic definitions and some of the immediate properties of the problems mentioned above. We refer to [4, 5] for the initial motivation for the study of non-commutative discrete optimization, the set-up of the problems, and initial facts on non-commutative discrete optimization.

1.1. Preliminaries. In this paper we follow terminology and notation introduced in [4]. For convenience, below we formulate the algorithmic problems mentioned in Section 1. We collectively refer to these problems as knapsack-type problems in groups.

Elements in a group $G$ generated by a finite or countable set $X$ are given as words over the alphabet $X \cup X^{-1}$.

**The subset sum problem SSP** $(G, X)$: Given $g_1, \ldots, g_k, g \in G$ decide if
\begin{equation}
  g = g_{\varepsilon_1} \cdots g_{\varepsilon_k}
\end{equation}
for some $\varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$.

**The knapsack problem KP** $(G, X)$: Given $g_1, \ldots, g_k, g \in G$ decide if
\begin{equation}
  g = g_{\varepsilon_1} \cdots g_{\varepsilon_k}
\end{equation}
for some non-negative integers $\varepsilon_1, \ldots, \varepsilon_k$.

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 $g_{i_1}, \ldots, g_{i_s} \in \{g_1, \ldots, g_k\}, s \in \mathbb{N}$:
\begin{equation}
  g = g_{i_1} \cdots g_{i_s}.
\end{equation}

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, the *uniform subgroup membership problem* in $G$.

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. In this case the problem is to verify if the corresponding equalities \(2\) and \(3\) 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, we define the bounded knapsack problem (BKP) for a group $G$ as follows.

**Bounded knapsack problem BKP** $(G, X)$: Given $g_1, \ldots, g_k, g \in G$ and $1^m \in \mathbb{N}$ decide if the equality
\[ g = g_{\varepsilon_1} \cdots g_{\varepsilon_k} \]
holds for some $\varepsilon_i \in \{0, 1, \ldots, m\}$.

This problem is $\mathbf{P}$-time equivalent to SSP in $G$ (we recall the definition of $\mathbf{P}$-time reduction below), 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 \(g = g_1 \cdots g_s\), where \(g_1, \ldots, g_s \in \{g_1, \ldots, g_k\}\) and \(s \leq m\).

Recall that a decision problem can be denoted as \((I, D)\), where \(I\) is the set of all instances of the problem, and \(D \subseteq I\) is the set of positive ones. A decision problem \((I_1, D_1)\) is \(\text{P-time reducible}\) to a problem \((I_2, D_2)\) if there is a \(\text{P-time computable}\) function \(f : I_1 \to I_2\) 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 \(\text{many-to-one P-time reductions}\) or \(\text{Karp reductions}\). Since we mainly use this type of reduction we omit “many-to-one” from the name and call them \(\text{P-time reductions}\). We say that two problems are \(\text{P-time equivalent}\) if each of them \(\text{P-time reduces}\) to the other. Aside from many-to-one reductions, we use the so-called Cook reductions. That is, we say that a decision problem \((I_1, D_1)\) is \(\text{P-time Cook reducible}\) to a problem \((I_2, D_2)\) if there is an algorithm that solves problem \((I_1, D_1)\) using a polynomial number of calls to a subroutine for problem \((I_2, D_2)\), and polynomial time outside of those subroutine calls. Correspondingly, we say that two problems are \(\text{P-time Cook equivalent}\) if each of them \(\text{P-time Cook reduces}\) to the other. In our present work we are primarily interested in establishing whether certain problems are \(\text{P-time decidable}\) or \(\text{NP-complete}\), and thus we make no special effort to use one of the two types of reduction over the other.

Finally we mention that for a problem \(\Pi \in \{\text{SSP, KP, BKP, SMP, BSMP}\}\), \(\Pi(G, X_1)\) is \(\text{P-time equivalent}\) to \(\Pi(G, X_2)\) for any finite generating sets \(X_1, X_2\), i.e. the time complexity of \(\Pi(G)\) does not depend on the choice of a finite generating set of a given group \(G\). We refer the reader to [4] for the proof of the above statement, further information concerning knapsack-type problems and their variations in groups, details regarding their algorithmic set-up, and the corresponding basic facts.

1.2. Results and open questions. Primary goal of the present work is to answer the following basic questions about complexity of knapsack-type problems in free and direct products.

Q1. Assuming \(\text{SSP}(G), \text{SSP}(H) \in \text{P}\), is it true that \(\text{SSP}(G \ast H) \in \text{P}\)?

Q2. If the answer to the above question is positive, is it true that \(\text{KP}(G \ast H) \in \text{P}\)?

Q3. Assuming \(\text{SSP}(G), \text{SSP}(H) \in \text{P}\), is it true that \(\text{SSP}(G \times H) \in \text{P}\)?

Q4. If the answer to the above question is positive, is it true that \(\text{KP}(G \times H) \in \text{P}\)?

We give a partial positive answer to the question Q1. To elaborate, in the context of studying properties of the subset sum problem in free products, it is natural to view this problem, along with the bounded knapsack and the bounded submonoid membership problems, as special cases of a more general algorithmic problem formulated in terms of graphs labeled by group elements, which we call the \textit{acyclic graph problem (AGP)}, introduced in Section 2 below.

In the same section we also establish connection between \(\text{SSP, BKP, BSMP}\) and \(\text{AGP}\), as shown in Figure 1 and show that \(\text{AGP}\) is \(\text{P-time solvable}\) in all known groups where \(\text{SSP}\) is. Further, we show in Section 3 that \(\text{AGP}\) in free products is \(\text{P-time Cook reducible}\) to \(\text{AGP}\) in the factors. As a consequence, we obtain that \(\text{SSP, BKP, BSMP}\) are polynomial time solvable in a wide class of
groups. As an answer to Q2, we show in Section 5 that the (unbounded) knapsack problem in a free product $P$-time reduces to BKP, which allows to conclude that, assuming $AGP(G)$, $AGP(H) \in P$, the knapsack problem $KP(G \ast H)$ is $P$-time solvable if and only if $KP(G)$ and $KP(H)$ are.

We observe that the same is false for direct products, i.e that $AGP(G) \in P$, $AGP(H) \in P$ does not imply $AGP(G \times H) \in P$ (unless $P = NP$). In Section 3 we prove a similar result for $SSP(G \times H)$, which negatively resolves question Q3.

The following questions remain open.

OQ1. Is there a group $G$ with $SSP(G) \in P$ and $NP$-hard $AGP(G)$ (cf. results shown in Figure 1)?

OQ2. Let $F_2$ be a free group of rank 2. Is $SSP(F_2 \times F_2)$ $NP$-complete (cf. Proposition 3.3)?

The authors are grateful to A. Miasnikov for bringing our attention to the problem and for insightful advice and discussions.

2. Acyclic graph problem

Let $G$ be a group and $X = \{x_1, \ldots, x_n\}$ a generating set for $G$.

The acyclic graph problem $AGP(G, X)$: Given an acyclic directed graph $\Gamma$ labeled by letters in $X \cup X^{-1} \cup \{\varepsilon\}$ with two marked vertices, $\alpha$ and $\omega$, decide whether there is an oriented path in $\Gamma$ from $\alpha$ to $\omega$ labeled by a word $w$ such that $w = 1$ in $G$.

Let graph $\Gamma$ have $n$ vertices and $m$ edges. Define $size(\Gamma)$ to be $m + n$. Let total word length of labels of edges of $\Gamma$ be $l$. For a given instance of $AGP(G, X)$, its size is the value $m + n + l$. With a slight abuse of terminology, we will also sometimes use labels that are words rather than letters in $X \cup X^{-1} \cup \{\varepsilon\}$. Note that given such a graph $\Gamma$ of size $m + n + l$, subdividing its edges we can obtain a graph $\Gamma'$ where edges are labeled by letters, with $m + n + l \leq size(\Gamma') \leq (m + l) + (n + l) + l$. Therefore, $1/3 size(\Gamma') \leq size(\Gamma) \leq size(\Gamma')$, so such an abuse of terminology results in distorting the size of an instance of $AGP(G, X)$ by a factor of at most 3.

Note that by a standard argument, if $X_1$ and $X_2$ are two finite generating sets for a group $G$, the problems $AGP(G, X_1)$ and $AGP(G, X_2)$ are $P$-time (in fact, linear time) equivalent. In this sense, the complexity of $AGP$ in a group $G$ does not depend on the choice of a finite generating set. In the sequel we often write $AGP(G)$ instead of $AGP(G, X)$, implying an arbitrary finite generating set. As shown in [4],
complexity of algorithmic problems in a group can change dramatically depending on a choice of infinite generating set. We do not consider infinite generating sets in the present work, and refer the reader to [4] for details of treating those.

We make a note of the following obvious property of AGP.

**Proposition 2.1.** Let $G$ be a finitely generated group and $H \leq G$ its finitely generated subgroup. Then $\mathsf{AGP}(H)$ is $\mathsf{P}$-time reducible to $\mathsf{AGP}(G)$. In particular,

1. If $\mathsf{AGP}(H)$ is $\mathsf{NP}$-hard then $\mathsf{AGP}(G)$ is $\mathsf{NP}$-hard.
2. If $\mathsf{AGP}(G) \in \mathsf{P}$ then $\mathsf{AGP}(H) \in \mathsf{P}$.

Methods used in [4] to treat SSP and BSMP in hyperbolic and nilpotent groups can be easily adjusted to treat AGP as well, as we see in the two following statements.

**Proposition 2.2.** $\mathsf{AGP}(G) \in \mathsf{P}$ for every finitely generated virtually nilpotent group $G$.

*Proof.* Follows immediately from polynomial growth of virtually nilpotent groups [8], similar to the proof of Theorem 3.3 in [4]. □

**Proposition 2.3.** $\mathsf{AGP}(G) \in \mathsf{P}$ for every finitely generated hyperbolic group $G$.

*Proof.* The statement follows immediately from [4, Proposition 5.5]. □

Here we would also like to note that since the word problem straightforwardly reduces to AGP, an obvious prerequisite for $\mathsf{AGP}(G)$ to belong to $\mathsf{NP}$ is to have a polynomial time word problem. Therefore, in the context of investigating time complexity of AGP we are primarily interested in such groups.

We also note that adding or eliminating a direct factor $\mathbb{Z}$ does not change complexity of AGP.

**Theorem 2.4.** Let $G$ be a finitely generated group. Then $\mathsf{AGP}(G)$ and $\mathsf{AGP}(G \times \mathbb{Z})$ are $\mathsf{P}$-time equivalent.

*Proof.* We only have to show the reduction of $\mathsf{AGP}(G \times \mathbb{Z})$ to $\mathsf{AGP}(G)$, since the other direction is immediate by Proposition 2.3.

Since the complexity of AGP in a given group does not depend on a finite generating set, we assume that the group $G \times \mathbb{Z}$ is generated by finitely many elements $(g_1,0), (g_2,0), \ldots,$ and $(1,1)$. Consider an arbitrary instance $(\Gamma, \alpha, \omega)$ of $\mathsf{AGP}(G \times \mathbb{Z})$, where $\Gamma = (V,E)$. Consider a graph $\Gamma^* = (V^*,E^*)$, where $V^* = V \times \mathbb{Z}$ and

$$E^* = \left\{(v,k) \xrightarrow{(h,m)} (v',k+m) \mid \text{for every } (v,k) \in V^* \text{ and } v \xrightarrow{(h,m)} v' \in E \right\},$$

where $(h,m)$ denotes an element of $G \times \mathbb{Z}$, with $h \in G, m \in \{0,1,-1\}$. Let $\Gamma' = (V',E')$ be the minimal connected component of $\Gamma^*$ containing $(\alpha,0) \in V^*$ (or the subgraph of $\Gamma^*$ induced by all vertices in $\Gamma^*$ that can be reached from $(\alpha,0)$). It is easy to see that $|V'| \leq |V| \cdot (2|E| + 1)$.

Moreover, the graph $\Gamma'$ can be constructed in a straightforward way in polynomial time. Finally, it follows from the construction of $\Gamma'$ that $(\Gamma, \alpha, \omega)$ is a positive instance of $\mathsf{AGP}(G \times \mathbb{Z})$ if and only if $(\Gamma', (\alpha,0), (\omega,0))$ is a positive instance of $\mathsf{AGP}(G)$. □
The above statement and Proposition 2.3 provide the following corollary.

**Corollary 2.5.** \( AGP(F_2 \times \mathbb{Z}) \in P \).

Here, and everywhere below, \( F_2 \) denotes the free group of rank 2.

### 2.1. Connection between acyclic graph problem and knapsack-type problems.

**Proposition 2.6.** SSP\((G)\), BKP\((G)\), BSMP\((G)\) are \( P \)-time reducible to \( AGP(G) \).

**Proof.** Let \( w_1, w_2, \ldots, w_k, w \) be an input of SSP\((G)\). Consider the graph \( \Gamma = \Gamma(w_1, w_2, \ldots, w_k, w) \) shown in the Figure 2. We see immediately that \((w_1, \ldots, w_k, w)\) is a positive instance of SSP\((G)\) if and only if \( \Gamma \) is a positive instance of AGP\((G)\). Since BKP\((G)\) \( P \)-time reduces to SSP\((G)\) (see [4]), it is only left to prove that BSMP\((G)\) reduces to AGP\((G)\). Indeed, let \((w_1, w_2, \ldots, w_k, w, 1^n)\) be an input of BSMP\((G)\). Consider the graph \( \Delta = \Delta(w_1, w_2, \ldots, w_k, w, 1^n) \) shown in Figure 3. It is easy to see that \((w_1, w_2, \ldots, w_k, w, 1^n)\) is a positive instance of BSMP\((G)\) if and only if \( \Delta \) is a positive instance of AGP\(\).

**Figure 2.** Graph \( \Gamma(w_1, w_2, \ldots, w_k, w) \), Proposition 2.6

**Figure 3.** Graph \( \Delta(w_1, w_2, \ldots, w_k, w, 1^n) \), Proposition 2.6.

There are \( n + 2 \) vertices in the graph.

Given Proposition 2.6 and results of [4], we immediately see that AGP is NP-complete in the following cases:

- certain metabelian groups (finitely generated free metabelian groups, wreath products of two infinite abelian groups, Baumslag’s group \( B = \langle a, s, t \mid [a, a^t] = 1, [s, t] = 1, a^s = aa^t \rangle \), Baumslag-Solitar groups \( BS(m, n) \) with \( |m| \neq |n|, m, n \neq 0 \),
- Thompson’s group \( F \),
- \( F_2 \times F_2 \),
- linear groups \( GL(n, \mathbb{Z}) \) with \( n \geq 4 \),
- braid groups \( B_n \) with \( n \geq 5 \) (by [3]),
- graph groups whose graph contains an induced square \( C_4 \).

While it still remains to be seen whether AGP reduces to either of the problems in Proposition 2.6 we make note of the following two observations. Firstly, in every case when it is known that those problems are \( P \)-time, so is AGP, as shown in Propositions 2.2 and 2.3. The second observation is that for a given group \( G \), AGP\((G)\) \( P \)-time reduces to either of the problems SSP\((G * F_2)\) or SSP\((G \times F_2)\).
Proposition 2.7. Let $G$ be a finitely generated group. Then $\text{AGP}(G)$ is $\text{P}$-time reducible to $\text{SSP}(G * F_2)$.

Proof. Let $\Gamma$ be a given directed acyclic graph on $n$ vertices with edges labeled by group words in a generating set $X$ of the group $G$. We start by organizing a topological sorting on $\Gamma$, that is enumerating vertices of $\Gamma$ by symbols $V_1$ through $V_n$ so that if there is a path in $\Gamma$ from $V_i$ to $V_j$ then $i \leq j$. This can be done in a time linear in $\text{size}(\Gamma)$ by $\mathbb{1}$. We assume $\alpha = V_1$ and $\omega = V_n$, otherwise discarding unnecessary vertices. We perform a similar ordering of edges, i.e. we enumerate them by symbols $E_1, \ldots, E_m$ so that if there is a path in $\Gamma$ whose first edge is $E_i$ and the last edge $E_j$, then $i \leq j$ (considering the derivative graph of $\Gamma$ we see that this can be done in time quadratic in $\text{size}(\Gamma)$). For each edge $E_i$, $1 \leq i \leq m$, denote its label by $u_i$, its origin by $V_{o(i)}$, and its terminus by $V_{t(i)}$. We similarly assume that $o(1) = 1$ and $t(m) = n$.

Next, we produce in polynomial time $n$ freely independent elements $v_1, \ldots, v_j$ of the free group $F_2 = \langle x, y \rangle$, of which we think as labels of the corresponding vertices $V_1, \ldots, V_n$. For example, $v_j = x^j y x^j$, $j = 1, \ldots, n$, suffice. We claim that

$$g_1 = v_{o(1)} u_1 v_{t(1)}^{-1}, \ g_2 = v_{o(2)} u_2 v_{t(2)}^{-1}, \ldots, \ g_m = v_{o(m)} u_m v_{t(m)}^{-1}; \ g = v_1 v_n^{-1}$$

is a positive instance of $\text{SSP}(G * F_2)$ if and only if $\Gamma$ is positive instance of $\text{AGP}(G)$. (See Figure 4 for an example.) Indeed, suppose there is an edge path $E_{i_1}, \ldots, E_{i_k}$ from $\alpha = V_1$ to $\omega = V_n$ in $\Gamma$ with $u_{i_1} \cdots u_{i_k} = 1$ in $G$. Note that since the above sequence of edges is a path, for each $1 \leq \mu \leq k - 1$, we have $V_{t(\mu)} = V_{o(\mu + 1)}$, so $v_{t(\mu)} = v_{o(\mu + 1)}$. Then the same choice of elements $g_{i_1}, \ldots, g_{i_k}$ gives

$$g_i \cdots g_k = (v_{o(i_1)} u_{i_1} v_{t(i_1)}^{-1})(v_{o(i_2)} u_{i_2} v_{t(i_2)}^{-1})\cdots(v_{o(i_k)} u_{i_k} v_{t(i_k)}^{-1}) = v_{o(i_1)} u_{i_1} (v_{t(i_1)}^{-1} v_{o(i_2)} u_{i_2} v_{t(i_2)}^{-1})v_{o(i_3)} u_{i_3} v_{t(i_3)}^{-1} = v_{o(i_1)} u_{i_1} \cdots u_{i_m} v_{t(i_k)}^{-1} = v_{o(i_1)} v_{t(i_k)}^{-1} = v_1 v_n^{-1} = g.$$

In the opposite direction, suppose in $G * F_2$ the equality

$$g_{i_1} \cdots g_{i_k} = g, \ \ i_1 < \ldots < i_k,$$

Figure 4. Reduction of $\text{AGP}(G)$ to $\text{SSP}(G * F_2)$ and $\text{SSP}(G \times F_2)$. Dotted arrows illustrate the correspondence between edges labeled by $u_i$ and elements $g_i = v_{o(i)} u_i v_{t(i)}^{-1}$.
takes place. Consider the $F_2$-component of this equality:
\[ v_{o(i_1)} v^{-1}_{t(i_1)} \cdot v_{o(i_2)} v^{-1}_{t(i_2)} \cdots v_{o(i_k)} v^{-1}_{t(i_k)} = v_1 v^{-1}_n. \]
Since $v_1, \ldots, v_n$ are freely independent, it is easy to see by induction on $k$ that the latter equality only possible if
\[ v_{o(i_1)} = v_1, \ v_{t(i_1)} = v_{o(i_2)}, \ v_{t(i_2)} = v_{o(i_3)}, \ldots, \ v_{t(i_{k-1})} = v_{o(i_k)}, \ v_{t(i_k)} = v_n, \]
i.e. edges $E_{i_1}, E_{i_2}, \ldots, E_{i_k}$ for a path from $V_1$ to $V_n$ in $\Gamma$. Further, inspecting the $G$-component of the equality $[4]$, we get that $u_{i_1} u_{i_2} \cdots u_{i_k} = 1$, as required in AGP$(G)$.

**Proposition 2.8.** Let $G$ be a finitely generated group. Then AGP$(G)$ is P-time reducible to SSP$(G \times F_2)$.

**Proof.** The proof repeats that of Proposition 2.7 with $G \times F_2$ instead of $G * F_2$. \hfill $\square$

3. AGP and SSP in direct products.

We show in this section that direct product of groups may change the complexity of SSP and AGP dramatically, in contrast with results of Section 2 where we show that free products preserve the complexity of AGP.

**Proposition 3.1.** There exist groups $G, H$ such that AGP$(G), AGP(H) \in P$, but AGP$(G \times H)$ is NP-complete.

**Proof.** It was shown in [4] Theorem 7.4] that BSMP$(F_2 \times F_2)$ is NP-complete. By Proposition 2.6 it follows that AGP$(F_2 \times F_2)$ is NP-complete, while by Proposition 2.3 AGP$(F_2)$ $\in P$. \hfill $\square$

A similar statement can be made about SSP with the help of Proposition 2.8. However, in the next proposition we organize reduction of BSMP$(G)$ to SSP$(G \times \mathbb{Z})$, thus simplifying the “augmenting” group, which allows to make a slightly stronger statement about complexity of SSP in direct products.

**Proposition 3.2.** Let $G$ be a finitely generated group. Then BSMP$(G)$ P-time Cook reduces to SSP$(G \times \mathbb{Z})$.

**Proof.** Let $w_1, w_2, \ldots, w_k, w, 1^n$ be the input of BSMP$(G)$. We construct graphs $\Gamma_m, m = 1, \ldots, n$, with edges labeled by elements of $G \times \mathbb{Z}$ as shown in the Figure 5. Note that a path from $\alpha$ to $\omega$ is labeled by a word trivial in $G \times \mathbb{Z}$ if and only if it passes through exactly $m$ edges labeled by $(w_{i_1}, 1), \ldots, (w_{i_m}, 1)$ and $w_{i_1} \cdots w_{i_m} = w$ in $G$. Therefore, the tuple $w_1, \ldots, w_k, 1^n$ is a positive instance of BSMP$(G)$ if and only if at least one of graphs $\Gamma_1, \ldots, \Gamma_n$ is a positive instance of SSP$(G \times \mathbb{Z})$. \hfill $\square$

**Figure 5.** Reduction of BSMP$(G)$ to SSP$(G \times \mathbb{Z})$. Graph $\Gamma_m$. 

We put $G = F_2 \times F_2$ in the above Proposition 3.2 to obtain the following result.

**Proposition 3.3.** **SSP**($F_2 \times F_2 \times \mathbb{Z}$) is **NP**-complete.

**Proof.** As we mentioned in the proof of Proposition 3.1, **AGP**($F_2 \times F_2$) is **NP**-complete. By Proposition 3.2, the latter **P**-time Cook reduces to **SSP**((($F_2 \times F_2$) × $\mathbb{Z}$)). Therefore, the **SSP**($F_2 \times F_2 \times \mathbb{Z}$) is **NP**-complete. □

The latter proposition answers the question whether direct product preserves polynomial time **SSP**.

**Corollary 3.4.** There exist finitely generated groups $G, H$ such that **SSP**$(G) \in \mathbb{P}$, **SSP**$(H) \in \mathbb{P}$ but **SSP**$(G \times H)$ is **NP**-complete.

**Proof.** By Corollary 2.5, **AGP**($F_2 \times \mathbb{Z}$) is in **P**. Therefore, **SSP**($F_2$) and **SSP**($F_2 \times \mathbb{Z}$) are in **P**, while **SSP**($F_2 \times (F_2 \times \mathbb{Z})$) is **NP**-complete by the above result. □

**Corollary 3.5.** **SSP** is **NP**-complete in braid groups $B_n$, $n \geq 7$, special linear groups $SL(n, \mathbb{Z})$, $n \geq 5$, graph groups whose graph contains the square pyramid $\mathbb{Z}$ (also called the wheel graph $W_5$) as an induced subgraph.

**Proof.** Note that $F_2 \times F_2$ embeds in a braid group $B_n$ with $n \geq 5$ by a result of Makanina [3]. The statement now follows from Propositions 3.2 and 2.1 since all of the listed groups contain $F_2 \times F_2 \times \mathbb{Z}$ as a subgroup. □

It remains to be seen whether **SSP**($F_2 \times F_2$) is **NP**-complete.

4. **AGP** in **FREE PRODUCTS**

**Theorem 4.1.** Let $G, H$ be finitely generated groups. Then **AGP**($G \ast H$) is **P**-time Cook reducible to **AGP**($G$), **AGP**($H$).

**Proof.** Let $G$ be given by a generating set $X$, and $H$ by $Y$. Let $\Gamma = \Gamma_0$ be the given acyclic graph labeled by $\Sigma = X \cup X^{-1} \cup Y \cup Y^{-1} \cup \{\varepsilon\}$. Given the graph $\Gamma_k$, $k \in \mathbb{Z}$, construct graph $\Gamma_{k+1}$ by adding edges to $\Gamma_k$ as follows.

Consider $\Gamma_k$, the maximal subgraph of $\Gamma_k$ labeled by $X \cup X^{-1} \cup \{\varepsilon\}$ (i.e. the graph obtained by removing all edges labeled by $Y \cup Y^{-1}$). For each pair of vertices $v_1, v_2 \in V(\Gamma_k)$ from the same connected component of $\Gamma_k$, decide whether a word equal to $1$ in $G$ is readable as a label of an oriented path in $\Gamma_k$, using the solution to **AGP**($G, X$). Let $E$ be the set of pairs $(v_1, v_2) \in V(\Gamma_k) \times V(\Gamma_k)$ such that the answer to the above question is positive, and there is no edge $v_1 \xrightarrow{\varepsilon} v_2$ in $\Gamma_k$. Construct the graph $\overline{\Gamma}_k$ by adding edges $v_1 \xrightarrow{\varepsilon} v_2$, $(v_1, v_2) \in E$ to the graph $\Gamma_k$. Now consider the maximal subgraph $\overline{\Gamma}_k$ of $\overline{\Gamma}_k$ labeled by $Y \cup Y^{-1} \cup \{\varepsilon\}$ and perform similar operation using the solution to **AGP**($H, Y$), obtaining the graph $\overline{\Gamma}_k = \Gamma_{k+1}$. Note that by the construction, size($\Gamma_{k+1}$) < $2$ size($\Gamma$)².

We claim that a word $w$ equal to $1$ in $G \ast H$ is readable from $\alpha$ to $\omega$ in $\Gamma$ if and only if there is an edge $\alpha \xrightarrow{w} \omega$ in the graph $\Gamma_{\text{size}(\Gamma)}$. Indeed, suppose there is a path in $\Gamma_k$ from $\alpha$ to $\omega$ labeled by a word $w = w_1w_2 \cdots w_m$, with $w_j \in \Sigma$ and at least one nontrivial letter among $w_1, \ldots, w_m$, such that $w = 1$ in $G \ast H$. The normal form theorem for free products guarantees that $w$ has a subword $w' = w_iw_{i+1} \cdots w_j$ of letters in $X \cup X^{-1} \cup \{\varepsilon\}$ or $Y \cup Y^{-1} \cup \{\varepsilon\}$ with $w' = 1$ in $G$ or $H$, respectively, with at least one nontrivial letter among $w_i, \ldots, w_j$. By the construction, the word $w_1 \cdots w_{i-1} \varepsilon w_{j+1} \cdots w_m$ is readable as a label of a path in $\Gamma_{k+1}$ from $\alpha$ to $\omega$. Since
the graph $\Gamma$ is acyclic, $m < \text{size}(\Gamma)$. By induction, a word $\varepsilon^{<\text{size}(\Gamma)}$ is readable as a label of an oriented path in $\Gamma_{\text{size}(\Gamma)-1}$ from $\alpha$ to $\omega$. By the construction, $\Gamma_{\text{size}(\Gamma)}$ contains an edge $\alpha \xrightarrow{\varepsilon} \omega$. The converse direction of the claim is evident. \hfill $\square$

**Corollary 4.2.** If $G, H$ are finitely generated groups such that $\text{AGP}(G), \text{AGP}(H) \in P$ then $\text{AGP}(G \ast H) \in P$.

**Corollary 4.3.** SSP, BKP, BSMP, AGP are polynomial time decidable in free products of finitely generated virtually nilpotent and hyperbolic groups in any finite number.

5. Knapsack problem in free products

It is not clear whether the (unbounded) knapsack problem in general reduces to BKP, or even AGP. However, it was shown in [4] that in the case of hyperbolic groups there is indeed such reduction. In light of results of Section 4, it is natural to ask whether a similar reduction takes place for free products of groups.

For an element $f$ of a free product of groups $G \ast H$, let $\|f\|$ denote the syllable length of $f$, i.e. its geodesic length in generators $G \cup H$ of $G \ast H$. We say that $f$ is simple if $f$ can be conjugated by an element of $G \ast H$ into $G \cup H$, i.e.

$$f = u^{-1}f'u,$$

where $u \in G \ast H, \|f'\| \leq 1$. Otherwise, we say that $f$ is non-simple.

**Lemma 5.1.** Let $G, H$ be groups and let an element $f \in G \ast H$ be non-simple. Then there are $a_1, \ldots, a_r \in G \cup H, b_1, \ldots, b_s \in G \cup H, c_1, \ldots, c_t \in G \cup H, r + t \leq 2\|f\|, s \leq \|f\|$, such that for every integer $n \geq 3$ the normal form of $f^n$ is

$$a_1 \cdots a_r(b_1 \cdots b_s)^{n-2}c_1 \cdots c_t.$$

**Proof.** Follows from the normal form theorem for free products. \hfill $\square$

The statement below is, in some sense, a strengthened big-powers condition for a free product.

**Proposition 5.2.** Let $p(x)$ be the polynomial $p(x) = x^2 + 4x$. Let $G, H$ be groups. If for $f_1, f_2, \ldots, f_m, f \in G \ast H$ there exist non-negative integers $n_1, n_2, \ldots, n_m \in \mathbb{Z}$ such that

$$f_1^{n_1}f_2^{n_2} \cdots f_m^{n_m} = f$$

then there exist such integers $n_1, \ldots, n_m$ with

$$n_i \leq p(\|f_1\| + \|f_2\| + \cdots + \|f_m\| + \|f\|)$$

whenever $f_i$ is non-simple.

**Proof.** For convenience, denote $\|f_1\| + \|f_2\| + \cdots + \|f_m\| + \|f\| = N$ and $f = f_0, -1 = n_0$. For each $f_i$, $i = 0, \ldots, m$, we represent $f_i^{n_i}$ by its normal form $w_i$, using Lemma 5.1 whenever $f_i$ is non-simple and $n_i \geq 3$. Suppose that for some non-simple $f_i, n_i > N^2 + 4N$. We inspect the path traversed by the word $w_1w_2 \cdots w_m w_0$ in the Cayley graph of $G \ast H$ with respect to generators $G \cup H$. Since this word corresponds to the trivial group element, the path must be a loop and thus the word $w_i$ splits in at most $m$ pieces, each piece mutually canceling with a subword of $w_j, j \neq i$. Let $w_i = ab^{m_i-2}c$ as in Lemma 5.1. Then by pigeonhole principle at least one piece contains at least $(n_i - 2 - m)/m \geq N + 1$ copies of the word $b$. Observe that $f_j$ is non-simple and $n_j \geq 3$, otherwise $\|f_j^{n_j}\| \leq 2N$, so it cannot
mutually cancel with $b^{N+1}$ since $\|b^{N+1}\| \geq 2N + 2$. Let $w_j = a'b^{n_j-2}c'$. We note that $\|b\| \leq \|f_i\| \leq N$, $\|b'\| \leq \|f_j\| \leq N$, so $\|b'\| \leq N$ copies of $b$ mutually cancel with $\|b'\| \cdot \|b'\| = \|b\|$ copies of $b'$ (up to a cyclic shift). Therefore replacing $n_i, n_j$ with $n_i - \|b'\|$ and $n_j - \|b\|$, respectively, preserves equality (6). Iterating this process, we may find numbers $n_1, \ldots, n_m$ that deliver equality (6) such that $n_i \leq p(N) = N^2 + 4N$ whenever $f_i$ is non-simple.

We observe that $p(N) = N^2 + 4N$ in the above proposition is monotone on $\mathbb{Z}_{\geq 0}$.

**Proposition 5.3.** If $G, H$ are groups such that $\textbf{KP}(G), \textbf{KP}(H) \in \textbf{P}$, then $\textbf{KP}(G \ast H)$ is $\textbf{P}$-time reducible to $\textbf{BKP}(G \ast H)$.

**Proof.** Let $f_1, f_2, \ldots, f_m, f \in G \ast H$ be an input of $\textbf{KP}(G \ast H)$. For each $f_i$, normal form of $f_i^n$, $n_i \geq 3$, is given by Lemma 5.1 or by simplicity of $f_i$. Suppose some $n_1, n_2, \ldots, n_m$ provide a solution to $\textbf{KP}$, i.e. $f_1^n \cdots f_m^n f^{-1} = 1$ in $G \ast H$. Representing $f^{-1}$ and each $f_i^n$ by their normal forms and combining like terms we obtain (without loss of generality) a product

$$g_1 h_1 g_2 h_2 \cdots g_\ell h_\ell = 1,$$

where each $g_i \in G$ and each $h_i \in H$, and $\ell \leq \|f\| + m \cdot (\max\{\|f_i\|\}) \cdot p(\max\{\|f_i\|\})$ by Proposition 5.2, so $\ell \leq N^2 p(N)$ where $N$ is the total length of the input (i.e. the sum of word lengths of $f_1, f_2, \ldots, f_m, f$). Further, since the product in (7) represents the trivial element, it can be reduced to 1 by a series of eliminations of trivial syllables and combining like terms:

$$g_1 h_1 g_2 h_2 \cdots g_\ell h_\ell = g_1^{(1)} h_1^{(1)} \cdots g_\ell^{(1)} h_\ell^{(1)} = g_1^{(2)} h_1^{(2)} \cdots g_\ell^{(2)} h_\ell^{(2)} = \cdots = g_1^{(\ell)} h_1^{(\ell)} = 1,$$

where the product labeled by $(j)$ is obtained from the one labeled by $(j - 1)$ by a single elimination of a trivial term and combining the two (cyclically) neighboring terms. Observe that each $g_\ell^{(j)}$ is (up to a cyclic shift) a product of the form $g_\alpha g_{\alpha+1} \cdots g_\beta$; similarly for $h_\ell^{(j)}$. Therefore, each $g_\ell^{(j)}$ is of the form

$$g_\ell^{(j)} = d_{1j}^{i_1} d_{2j}^{i_2} \cdots d_{kj}^{i_k},$$

where each $d_{ij}, 1 \leq \mu \leq k_j$ is either

- (NS) one of the syllables involved in Lemma 5.1 or normal form of some $f_1$ or $f_2$, or “u” part of (5), in which case $\delta_{ij} = 1$, or
- (S) the syllable $f'$ in (5) for some $f_\nu$, in which case $\delta_{ij} = n_\nu$.

On the one hand, the total amount of syllables $d_{ij}$ involved in (8) for a fixed $j$ is $k_{1j} + k_{2j} + \cdots + k_{\ell - j + 1}$; On the other hand, it cannot exceed $k_{11} + k_{21} + \cdots + k_{\ell 1}$ since $g_1^{(j)}, g_2^{(j)}, \ldots, g_{\ell - j + 1}^{(j)}$ are obtained by eliminating and combining elements $g_1, g_2, \ldots, g_n$. Taking into account that each $k_{i1} \leq m + 1 \leq N$, we obtain $k_{1j} + k_{2j} + \cdots + k_{\ell j - j + 1} \leq \ell N \leq N^3 p(N)$.

Now, given the equality $g_i^{(j)} = 1$ for some $i, j$, if the option (S) takes place for any $1 \leq \mu \leq k_j$, then the right hand side of the corresponding equality (8) can be represented (via a standard conjugation procedure) as a positive instance of the $\textbf{KP}(G)$ with input of length bounded by $(Nk_{ij})^2 \leq N^8 p^2(N)$. Since $\textbf{KP}(G) \in \textbf{P}$,
it follows that every $n_\nu$ that occurs as some $\delta_{\mu j}$ in some $g^{(j)}_i$ is bounded by a polynomial $p_G(N)$. Similar argument takes place for the $H$-syllables $h^{(j)}_i$, resulting in a polynomial bound $p_H(N)$.

It is only left to note that since for every $1 \leq \nu \leq m$, either $f_\nu$ is non-simple and then $n_\nu$ is bounded by $p(N)$, or it is simple and then $n_\nu$ is bounded by $p_G(N)$ or $p_H(N)$, so every $n_\nu$ is bounded by $p(N) + p_G(N) + p_H(N)$. □

**Theorem 5.4.** If $G,H$ are groups such that $\text{AGP}(G)$, $\text{AGP}(H) \in \text{P}$ and $\text{KP}(G)$, $\text{KP}(H) \in \text{P}$ then $\text{KP}(G * H) \in \text{P}$.

**Proof.** By Proposition 5.3 $\text{KP}(G * H)$ is $\text{P}$-time reducible to $\text{BKP}(G * H)$. In turn, the latter is $\text{P}$-time reducible to $\text{AGP}(G * H)$ by Proposition 2.6. Finally, $\text{AGP}(G * H) \in \text{P}$ by Corollary 4.2. □

**Corollary 5.5.** $\text{KP}$ is polynomial time decidable in free products of finitely generated virtually nilpotent and hyperbolic groups in any finite number.

**References**

[1] A. B. Kahn. Topological sorting of large networks. *Commun. ACM*, 5(11):558–562, 1962.
[2] R. Lyndon and P. Schupp. *Combinatorial Group Theory*. Classics in Mathematics. Springer, 2001.
[3] T. A. Makanina. Occurrence problem for braid groups $B_{n+1}$ with $n+1 \geq 5$. *Mathematical notes of the Academy of Sciences of the USSR*, 29(1):16–17, 1981.
[4] A. G. Miasnikov, A. Nikolaev, and A. Ushakov. Knapsack problems in groups. To appear in Mathematics of Computation. Available at [http://arxiv.org/abs/1302.5671](http://arxiv.org/abs/1302.5671) 2013.
[5] A. G. Miasnikov, A. Nikolaev, and A. Ushakov. Post correspondence problem in groups. To appear in *Journal of Group Theory*. Available at [http://arxiv.org/abs/1310.5246](http://arxiv.org/abs/1310.5246) 2013.
[6] K. A. Mikhailova. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958.
[7] K. A. Mikhailova. The occurrence problem for free products of groups. *Math. USSR-Sb.*, 4:181–190, 1968.
[8] J. Wolf. Growth of finitely generated solvable groups and curvature of Riemannian manifolds. *Journal of Differential Geometry*, 2:421–446, 1968.