On the Knapsack Problem and Semilinear Sets

DISSERTATION
zur Erlangung des Grades eines Doktors
der Naturwissenschaften

vorgelegt von
Michael Figelius, M.Sc.

eingereicht bei der Naturwissenschaftlich-Technischen Fakultät
der Universität Siegen
Siegen 2024

Betreuer und erster Gutachter
Prof. Dr. Markus Lohrey
Universität Siegen

Zweiter Gutachter
PD Dr. Armin Weiß
Universität Stuttgart

Tag der mündlichen Prüfung
12. September 2024

Abstract

In this thesis we analyze the knapsack problem for different group constructions and groups. The knapsack problem, which has become well known in optimization and economics, is considered here in a group-theoretic context as a decision problem. More precisely, the question is whether equations of the form $u_1^{x_1} \cdots u_k^{x_k} v = 1$, where u_i and v are from a group G and the x_i are natural numbers, have a solution.

Of particular interest to us are groups in which the set of solution vectors $(x_1, \ldots, x_k)$ forms a so-called semilinear set for each input. Such groups are called knapsack-semilinear. The set of knapsack-semilinear groups satisfies good closure properties, some of which we discuss in this thesis.

We define the concept of a magnitude and determine in the first part the magnitude of knapsack-semilinear groups under finite extensions, graph products and HNN-extensions or amalgamated products with certain restrictions. It turns out that solvability of knapsack equations of such group constructions is in NP if this is already the case for the base groups.

We then show that certain HNN-extensions of knapsack-semilinear groups over infinite associated subgroups are also knapsack-semilinear, if we restrict ourselves to the case where the isomorphism between the subgroups is the identity. This means, we analyze groups $H = \langle G, t \mid t^{-1}at = a\,(a \in A)\rangle$. An important special case here are the so-called extensions of centralizers. The same applies to central extensions of hyperbolic groups: These are also knapsack-semilinear. As an application, we then conclude that HNN-extensions (of the mentioned form H) of hyperbolic groups over quasiconvex subgroups are knapsack-semilinear.

In the last part of the thesis we consider the knapsack problem for two more cases, but not from the semilinear aspect. For uniformly SENS groups G the knapsack problem for $G \wr \mathbb{Z}$ is Σ_2^p-hard. Here the equations are restricted to the case $x_i \neq x_j$, $i \neq j$. Furthermore, we show that the knapsack problem for $SL_3(\mathbb{Z})$ is already undecidable in the case of a single equation if $x_i = x_j$, $i \neq j$, is allowed.

The results of this thesis are published in [F3], [F4] and [F6].

Zusammenfassung

In dieser Arbeit analysieren wir das Knapsack-Problem für verschiedene Gruppenkonstruktionen und Gruppen. Das Knapsack-Problem, welches in der Optimierung und Wirtschaft bekannt geworden ist, wird hier in einem gruppentheoretischen Zusammenhang als Entscheidungsproblem betrachtet. Genauer geht es um die Frage, ob Gleichungen der Form $u_1^{x_1} \cdots u_k^{x_k} v = 1$, mit u_i und v aus einer Gruppe G und natürlichen Zahlen x_i, eine Lösung haben.

Für uns interessant sind vor allem Gruppen, bei denen die Menge der Lösungsvektoren $(x_1, \ldots, x_k)$ für jeden Input eine sogenannte semilineare Menge bildet. Solche Gruppen heißen knapsack-semilinear. Die Menge der knapsack-semilinearen Gruppen erfüllt gute Abschlusseigenschaften, von denen wir in dieser Arbeit einige diskutieren.

Wir definieren den Begriff der Magnitude und bestimmen im ersten Teil die Magnitude von knapsack-semilinearen Gruppen unter endlichen Erweiterungen, Graphprodukten und HNN-Erweiterungen bzw. amalgamierten Produkten mit bestimmten Einschränkungen. Es stellt sich heraus, dass Lösbarkeit von Knapsack-Gleichungen von solchen Gruppenkonstruktionen in NP ist, wenn dies bereits für die Basisgruppen der Fall ist.

Anschließend zeigen wir, dass auch bestimmte HNN-Erweiterungen von knapsack-semilinearen Gruppen über unendlichen assoziierten Untergruppen knapsack-semilinear sind, wenn wir uns auf den Fall beschränken, dass der Isomorphismus zwischen den Untergruppen die Identität ist. Dies bedeutet, wir analysieren die Gruppen $H = \langle G, t \mid t^{-1}at = a\,(a \in A)\rangle$. Als wichtiger Spezialfall sind hier die sogenannten Erweiterungen von Zentralisatoren zu nennen. Dasselbe gilt für zentrale Erweiterungen von hyperbolischen Gruppen: Auch diese sind knapsack-semilinear. Als Anwendung schließen wir dann noch, dass HNN-Erweiterungen (der genannten Form H) von hyperbolischen Gruppen über quasikonvexen Untergruppen knapsack-semilinear sind.

Im letzten Teil der Arbeit betrachten wir noch das Knapsack-Problem für zwei weitere Fälle, aber nicht vom semilinearen Aspekt. Für uniforme SENS Gruppen G ist das Knapsack-Problem für $G \wr \mathbb{Z}$ bereits Σ_2^p-schwierig. Hierbei sind die Gleichungen eingeschränkt auf den Fall $x_i \neq x_j$, $i \neq j$. Außerdem zeigen wir, dass das Knapsack-Problem für $SL_3(\mathbb{Z})$ im Falle einer einzigen Gleichung schon unentscheidbar ist, wenn $x_i = x_j$, $i \neq j$, erlaubt ist.

Die Ergebnisse dieser Arbeit sind veröffentlicht in [F3], [F4] und [F6].

Acknowledgements

First of all, I would like to thank my doctoral supervisor Markus Lohrey. Despite the very turbulent times I went through, he was always very patient with me and supported me in word and deed when I needed it. Already during my studies, he awakened my interest in theoretical computer science and took me by the hand several times so that I could get into scientific exchange with others very early on (especially at the AlMoTh 2016 and the seminar at Schloss Dagstuhl 2019). Together with Dieter Spreen, whom I would also like to thank, he also made my two research stays in Sydney and New York / Hoboken possible, which were very important for me on many levels.

I would also like to thank the researchers and co-authors I have had the pleasure of meeting and exchanging ideas with over the last few years. First and foremost Armin Weiß, my second reviewer, Georg Zetzsche and Laurent Bartholdi. I got to know all three of them at Schloss Dagstuhl and got on well with them straight away. The collaboration was definitely valuable for me. I was also able to get to know Murray Elder at Dagstuhl and research with him for a while in Sydney. He was also a great host and gave me good advice and support on my first trip abroad of my PhD. I would also like to thank Alexei Miasnikov, Andrey Nikolaev and Alexander Ushakov. They helped me find my way around the Stevens Institute in Hoboken and we had some inspiring conversations that had a great impact on my further research. As pioneers in the field, their contributions were of outstanding importance for this thesis anyway.

The Hölderlin office would not be the same without my wonderful colleagues. I would therefore like to thank Hesam Fathi, Moses Ganardi, Danny Hucke, Rahul Jain, Seungbum Jo, Julio Caesar Juarez Xochitemol, Carl Philipp Reh, Andreas Rosowski, Louisa Seelbach Benkner, Kurt Sieber and Tobias Schüler. They contributed greatly to my creativity and further development and always had good tips, be it for research, for solving a computer problem or for private matters.

A special thanks also goes to my family, especially my wife Tran Thi Cam Van, who accompanies me on all my journeys and shows understanding for all my interests and weaknesses, my son Felix, who helped me to see the world with different eyes and let me enjoy the little things again, and my parents and my sister, as they are an emotional support for me, from whom I have always been able to grow and retreat.

Last but not least, I would like to thank my friends and acquaintances who have always put a smile on my face over the years and with whom I have shared many great moments.

Danksagungen

Zunächst möchte ich meinem Doktorvater Markus Lohrey danken. Trotz der sehr turbulenten Zeit, durch die ich gegangen bin, war er immer sehr geduldig mit mir und hat mich mit Rat und Tat unterstützt, wenn ich es brauchte. Schon während des Studiums weckte er in mir das Interesse an der theoretischen Informatik und hat mich mehrfach an die Hand genommen, damit ich bereits sehr früh in den wissenschaftlichen Austausch mit anderen kommen konnte (hier sind vor allem die AlMoTh 2016 und das Seminar im Schloss Dagstuhl 2019 zu nennen). Er ermöglichte mir außerdem gemeinsam mit Dieter Spreen, dem ich ebenso danken möchte, meine beiden Forschungsaufenthalte in Sydney und New York bzw. Hoboken, die für mich auf vielen Ebenen sehr bedeutend waren.

Ebenfalls danken möchte ich Forschern und Koautoren, die ich in den letzten Jahren kennenlernen und mich mit ihnen austauschen durfte. Allen voran Armin Weiß, meinem zweiten Gutachter, Georg Zetzsche und Laurent Bartholdi. Alle drei habe ich im Schloss Dagstuhl kennengelernt und mich direkt gut mit ihnen verstanden. Die Zusammenarbeit war definitiv wertvoll für mich. Auch mit Murray Elder durfte ich in Dagstuhl kennenlernen und mit ihm eine Zeit lang in Sydney forschen. Als Gastgeber war er ebenso großartig und hat mich auf meiner ersten promotionsbedingten Auslandsreise gut beraten und begleitet. Ein Dank geht auch an Alexei Miasnikov, Andrey Nikolaev und Alexander Ushakov. Sie halfen mir, mich am Stevens Institute in Hoboken zurechtzufinden und wir führten einige inspirierende Unterhaltungen, die einen großen Einfluss auf meine weitere Forschung hatten. Als Pioniere auf dem Gebiet waren ihre Beiträge ohnehin von herausragender Bedeutung für diese Arbeit.

Das Büro am Hölderlin wäre nicht dasselbe ohne meine wunderbaren Arbeitskollegen. Daher danke ich Hesam Fathi, Moses Ganardi, Danny Hucke, Rahul Jain, Seungbum Jo, Julio Caesar Juarez Xochitemol, Carl Philipp Reh, Andreas Rosowski, Louisa Seelbach Benkner, Kurt Sieber und Tobias Schüler. Sie haben zur Kreativität und Weiterentwicklung bei mir sehr beigetragen und hatten immer wieder gute Tipps parat, sei es zur Forschung, für die Lösung eines Computerproblems oder auch für private Belange.

Ein besonderer Dank geht auch an meine Familie, insbesondere meine Frau Tran Thi Cam Van, die mich begleitet auf allen Wegen und Verständnis zeigt für all meine Interessen und Schwächen, meinen Sohn Felix, der mir half die Welt mit anderen Augen wahrzunehmen und mich wieder an kleinen Dingen Freude haben lässt, und meine Eltern, sowie meine Schwester, da sie für mich eine emotionale Stütze sind, an der ich stets wachsen und mich zurückziehen konnte.

Zu guter Letzt danke ich meinen Freunden und guten Bekannten, die mir über viele Jahre stets ein Lächeln aufs Gesicht gezaubert haben und mit denen ich viele großartige Momente teilen durfte.

Contents

Chapter 1

Introduction

Since its very beginning, the area of combinatorial group theory [69] has been tightly connected to algorithmic questions. The word problem for finitely generated (f.g. for short) groups lies at the heart of theoretical computer science itself. Dehn [18] proved its decidability for certain surface groups (before the notion of decidability was formalized). Magnus [71] extended this result to all one-relator groups. After the work of Magnus it took more than 20 years before Novikov [78] and Boone [15] proved the existence of finitely presented groups with an undecidable word problem (Turing tried to prove the existence of such groups but could only provide finitely presented cancellative monoids with an undecidable word problem).

Since the above mentioned pioneering work, the area of algorithmic group theory has been extended in many different directions. More general algorithmic problems have been studied and also the computational complexity of group theoretic problems has been investigated. Miasnikov, Nikolaev, and Ushakov initiated in [74] the systematic investigation of a new class of algorithmic problems that have their origin in discrete optimization problems over the integers. One of these problems is the *knapsack problem*. Miasnikov et al. proposed the following definition for the knapsack problem in a finitely generated group G ($\textsc{Knapsack}(G)$ for short): The input is a sequence of group elements $u_1, \ldots, u_k, v \in G$ (specified by finite words over the generators of G) and it is asked whether there exist natural numbers $n_1, \ldots, n_k \in \mathbb{N}$ such that $u_1^{n_1} \cdots u_k^{n_k} = v$ in G. For the particular case $G = \mathbb{Z}$ (where the additive notation $n_1 \cdot u_1 + \cdots + n_k \cdot u_k = v$ is usually preferred) this problem is NP-complete if the numbers $u_1, \ldots, u_k, v \in \mathbb{Z}$ are given in binary notation [53, 39].[1] On the other hand, if $u_1, \ldots, u_k, v$ are given in unary notation, then the knapsack problem for the integers was shown to be complete for the circuit complexity class TC^0 [27]. Note that the unary notation for integers corresponds to the case where an integer is given by a word over a generating set $\{t, t^{-1}\}$. In one particular case, the knapsack problem was studied for a non-commutative group before the work of Miasnikov et al.: in [4],

[1] Karp in his seminal paper [53] defined knapsack in a slightly different way. NP-completeness of the above version was shown in [39].

it was shown that the knapsack problem for commutative matrix groups over algebraic number fields can be solved in polynomial time. Let us emphasize that we are looking for solutions of knapsack equations in the natural numbers. One might also consider the variant, where the variables $x_1, \ldots, x_k$ take values in $\mathbb{Z}$. This latter version can be easily reduced to our knapsack version (with solutions in $\mathbb{N}$), but we are not aware of a reduction in the opposite direction.[2] Let us also mention that the knapsack problem is a special case of the more general rational subset membership problem [65].

We also consider a generalization of KNAPSACK(G): An exponent equation is an equation of the form $u_1^{x_1} \cdots u_k^{x_k} = v$ as in the specification of KNAPSACK(G), except that the variables $x_1, \ldots, x_k$ are not required to be pairwise different. *Solvability of exponent equations* for G (EXPEQ(G) for short) is the problem where the input is a conjunction of exponent equations (possibly with shared variables) and the question is whether there is a joint solution for these equations in the natural numbers. Equations of this form have received a lot of attention in recent years, see e.g. [4, 9, 11, 13, 25, 30, 31, 58, 62, 68, 32, 76, 74].

1.1 Overview of previous research

Let us give a brief survey of the results that were obtained for the knapsack problem in [74] and successive papers:

- Knapsack can be solved in polynomial time for every hyperbolic group [74]. In [30] this result was extended to free products of any finite number of hyperbolic groups and finitely generated abelian groups. A further generalization was obtained in [62], where the smallest class of groups that can be obtained from hyperbolic groups using the operations of free products and direct products with $\mathbb{Z}$ was considered. It was shown that for every group in this class the knapsack problem belongs to the complexity class LogCFL (a subclass of P).
- There are nilpotent groups of class 2 for which knapsack is undecidable. Examples are direct products of sufficiently many copies of the discrete Heisenberg group $H_3(\mathbb{Z})$ [58], and free nilpotent groups of class 2 and sufficiently high rank [76].
- Knapsack for $H_3(\mathbb{Z})$ is decidable [58]. In particular, together with the previous point it follows that decidability of knapsack is not preserved under direct products. Also, solvability of one exponent equation is decidable, but systems of exponent equations are undecidable for $H_3(\mathbb{Z})$.
- There is a recent paper, in which decidability of KNAPSACK($H_3(\mathbb{Z})$) was used to show that the rational subset membership problem for $H_3(\mathbb{Z})$ is decidable as well [12].

[2] Note that the problem whether a given system of linear equations has a solution in $\mathbb{N}$ is NP-complete, whereas the problem can be solved in polynomial time (using the Smith normal form) if we ask for a solution in $\mathbb{Z}$. In other words, if we consider the knapsack problem for $\mathbb{Z}^n$ with n part of the input, then looking for solutions in $\mathbb{N}$ seems to be more difficult than looking for solutions in $\mathbb{Z}$.

- Knapsack is decidable for every co-context-free group [58], i.e., groups where the set of all words over the generators that do not represent the identity is a context-free language. Lehnert and Schweitzer [60] have shown that the Higman-Thompson groups are co-context-free.
- Knapsack belongs to NP for all virtually special groups (finite extensions of subgroups of graph groups) [67]. The class of virtually special groups is very rich. It contains all Coxeter groups, one-relator groups with torsion, fully residually free groups, and fundamental groups of hyperbolic 3-manifolds. For graph groups (also known as right-angled Artin groups) a complete classification of the complexity of knapsack was obtained in [68]: If the underlying graph contains an induced path or cycle on 4 nodes, then knapsack is NP-complete; in all other cases knapsack can be solved in polynomial time (even in LogCFL).
- Knapsack is NP-complete for non-abelian free solvable groups [F3] and solvable Baumslag-Solitar groups $\mathsf{BS}(1, q)$ [32] with $q > 1$. For Baumslag-Solitar groups $\mathsf{BS}(p, q)$ with $p \neq 1 \neq q$ and $\gcd(p, q) = 1$, decidability of knapsack was shown in [25]. Furthermore, knapsack is NP-complete for every wreath products $G \wr \mathbb{Z}$ with $G \neq 1$ f.g. nilpotent [F3].
- Decidability of knapsack is preserved under finite extensions, HNN-extensions over finite associated subgroups and amalgamated free products over finite subgroups [67].
- In [9], there is a characterization of those wreath products $G \wr H$ for which the knapsack problem is decidable. The characterization is in terms of (i) decidability properties of the groups G and H and (ii) whether G is abelian.

1.2 Content of this thesis

In this thesis, we initiate the systematic study of solution sets of equations $u_1^{x_1} \cdots u_k^{x_k} = v$ in a group G, which we call *knapsack equations*. For a knapsack equation we require that the variables x_i are pairwise different. The *solution set* of this equation is $\{(n_1, \ldots, n_k) \in \mathbb{N}^k \mid u_1^{n_1} \cdots u_k^{n_k} = v \text{ in } G\}$. In the papers [62, 58, 68] it turned out that in many groups the solution set of every knapsack equation is a *semilinear set*. Recall that a subset $S \subseteq \mathbb{N}^k$ is semilinear if it is a finite union of linear sets, and a subset $L \subseteq \mathbb{N}^k$ is linear if there are vectors $v_0, v_1, \ldots, v_\ell \in \mathbb{N}^k$ such that $L = \{v_0 + \lambda_1 v_1 + \cdots + \lambda_\ell v_\ell \mid \lambda_1, \ldots, \lambda_\ell \in \mathbb{N}\}$. Semilinear sets play a prominent role in many areas of computer science and mathematics, e.g. in automata theory and logic. It is known that the class of semilinear sets is closed under Boolean operations and that the semilinear sets are exactly the sets that are first-order definable in Presburger arithmetic (i.e., the structure $(\mathbb{N}, +)$) [35].

We say that a group is *knapsack-semilinear* if for every knapsack equation the set of all solutions is semilinear. Note that in any group G the set of solutions on an equation $u_1^x = v$ is periodic and hence semilinear. This result generalizes to

solution sets of knapsack instances of the form $u_1^x u_2^y = v$ (see Lemma 3.4), but there are examples of knapsack equations with three variables where solution sets (in certain groups) are not semilinear. Moreover, every finitely generated abelian group is semilinear (since solution sets of linear equations are Presburger definable). Nontrivial examples of knapsack-semilinear groups are graph groups [68] (which include free groups and free abelian groups), hyperbolic groups [62], and co-context free groups [58].[3] Obviously, every finitely generated subgroup of a finitely generated knapsack-semilinear group is knapsack-semilinear as well. Furthermore, the class of knapsack-semilinear groups is closed under finite extensions, graph products, amalgamated free products with finite amalgamated subgroups, HNN-extensions with finite associated subgroups (see Chapter 5 to Chapter 7 for these closure properties), certain HNN-extensions over infinite associated subgroups (Chapter 8) and wreath products [31].

In order to get complexity bounds for the knapsack problem, the sole concept of knapsack-semilinearity is not useful. For this purpose, we need a quantitative measure for semilinear sets; see also [17]: For a semilinear set

$$L = \bigcup_{1 \leq i \leq n} \{v_{i,0} + \lambda_1 v_{i,1} + \cdots + \lambda_{\ell_i} v_{i,\ell_i} \mid \lambda_1, \ldots, \lambda_{\ell_i} \in \mathbb{N}\}$$

we call the tuple of all vectors $v_{i,j}$ a *semilinear representation* for L. The *magnitude* of this semilinear representation is the largest number that occurs in some of the vectors $v_{i,j}$. Finally, the magnitude of a semilinear set L is the smallest magnitude among all semilinear representations of L.

In Chapter 5, Chapter 6 and Chapter 7, we prove the closure of the class of knapsack-semilinear groups under

- finite extensions,
- graph products,
- amalgamated free products with finite amalgamated subgroups, and
- HNN-extensions with finite associated subgroups.

The operation of graph product interpolates between direct products and free products. It is specified by a finite graph (V, E), where every node $v \in V$ is labelled with a group G_v. One takes the free product of the groups G_v ($v \in V$) modulo the congruence that allows elements from adjacent groups to commute. Graph products can be seen as a generalization of graph groups (where all G_v are $\mathbb{Z}$), and hence our results of Chapter 6 are a natural continuation of [68]. Amalgamated free products and HNN-extensions are fundamental operations in all areas of geometric and combinatorial group theory; see Section 2.4 for references. A theorem of Seifert and van Kampen links HNN-extensions to algebraic topology. Moreover, HNN-extensions are used in all modern proofs for the undecidability of the word problem in finitely presented groups. For a base group G with two isomorphic subgroups A and B and an isomorphism

[3] Knapsack-semilinearity of co-context free groups is not stated in [58] but follows immediately from the proof for the decidability of knapsack.

$\varphi\colon A \to B$, the corresponding HNN-extension is the group

$$H = \langle G, t \mid t^{-1}at = \varphi(a)\,(a \in A)\rangle. \tag{1.1}$$

Intuitively, it is obtained by adjoing to G a new generator t (the *stable letter*) in such a way that conjugation of A by t realizes φ. The subgroups A and B are also called the *associated subgroups*.

Our proofs showing that the above group constructions preserve knapsack-semilinearity also yield upper bounds for the magnitude of solution sets in terms of (i) the total length of the knapsack equation (measured in the total number of generators) and (ii) the number of variables in the knapsack equation. For this, we introduce a function $\mathsf{K}_G(n, m)$ that yields the maximal magnitude of a solution set for a knapsack equation over G of total length at most n and at most m variables. Roughly speaking, it turns out that finite extensions, amalgamated free products with finite amalgamated subgroups, and HNN-extensions with finite associated subgroups only lead to a polynomial blowup for the function $\mathsf{K}_G(n, m)$ (actually, this function also depends on the generating set for G), whereas graph products can lead to an exponential blowup. On the other hand, if we bound the number of variables by a constant, then also graph products only lead to a polynomial blowup for the function $\mathsf{K}_G(n, m)$.

For arbitrary HNN-extensions, knapsack-semilinearity is not preserved. For instance, the Baumslag-Solitar group $\mathsf{BS}(1, 2) = \langle a, t \mid t^{-1}at = a^2\rangle$ is not knapsack-semilinear [32] but it is an HNN-extension of the knapsack-semilinear group $\langle a\rangle \cong \mathbb{Z}$. This example shows that we have to drastically restrict HNN-extensions in order to get a transfer result for knapsack-semilinearity beyond the case of finite associated subgroups. In Chapter 8 we study HNN-extensions of the form

$$H = \langle G, t \mid t^{-1}at = a\,(a \in A)\rangle, \tag{1.2}$$

where $A \leq H$ is a subgroup. In other words, we take in (1.1) for $\varphi : A \to B$ the identity on A. Intuitively: we add to the group G a free generator t together with commutation identities $at = ta$ for all $a \in A$. This operation interpolates between the free product $G * \langle t\rangle \cong G * \mathbb{Z}$ and the direct product $G \times \langle t\rangle \cong G \times \mathbb{Z}$.

Even HNN-extensions of the form (1.2) with f.g. A are too general for our purpose: if the subgroup membership problem for A is undecidable then H has an undecidable word problem. Hence, we also need some restriction on the subgroup $A \leq G$. We say that G is knapsack-semilinear relative to the subgroup A if for every expression of the form $u_1^{x_1}u_2^{x_2}\cdots u_n^{x_n}v$ (with $u_i, v_i \in G$ and pairwise different variables x_i) the set of all tuples $(c_1, \ldots, c_n) \in \mathbb{N}^n$ such that $u_1^{c_1}u_2^{c_2}\cdots u_n^{c_n}v \in A$ is a semilinear set. Our main result states that if the group G is (i) knapsack-semilinear as well as (ii) knapsack-semilinear relative to the subgroup A, then the HNN-extension H in (1.2) is knapsack-semilinear. In some situations we can even avoid the explicit assumption that G is knapsack-semilinear relative to the subgroup A. HNN-extensions of the form (1.2), where A is the centralizer of a single element $g \in G$ are known as *free rank one extensions of centralizers* and were first studied in [75] in the context of so-called exponential

groups. It is easy to observe that if G is knapsack-semilinear and $A \leq G$ is the centralizer of a finite set of elements, then G is also knapsack-semilinear relative to A. In particular the operation of free rank one extension of centralizers preserves knapsack-semilinearity. A corollary of this result is that every fully residually free group is knapsack-semilinear. The class of fully residually free groups is exactly the class of all groups that can be constructed from $\mathbb{Z}$ by the following operations: taking finitely generated subgroups, free products and free rank one extensions of centralizers. Knapsack-semilinearity of fully residually free groups also follows from the fact that every fully residually free group is virtually special [89].

In Chapter 9 we elaborate knapsack-semilinearity for so called central extensions. A group H is called a *central extension* of a group G, if we have $G = H/K$ for a subgroup $K \leq Z(H)$, where $Z(H)$ is the center of H. We restrict ourselves to the case, where G is a hyperbolic group. A group is hyperbolic if all geodesic triangles in the Cayley-graph are δ-slim for a constant δ. The class of hyperbolic groups has several alternative characterizations (e.g., it is the class of finitely generated groups with a linear Dehn function), which gives hyperbolic groups a prominent role in geometric group theory. Moreover, in a certain probabilistic sense, almost all finitely presented groups are hyperbolic [37, 79]. Also from a computational viewpoint, hyperbolic groups have nice properties: it is known that the word problem and the conjugacy problem can be solved in linear time [29, 45]. In [62] it was shown that hyperbolic groups are knapsack-semilinear. Central extensions of hyperbolic groups are known to have an asynchronously biautomatic structure, which allows us to use certain proof techniques for showing knapsack-semilinearity in case of those central extensions.

In the second part of Chapter 9, we study HNN-extensions of the form (1.2), where G is a central extension of a hyperbolic group (an important special case is where G is hyperbolic). Here we extend the main result of part one of this chapter by showing that (a central extension of) a hyperbolic group is knapsack-semilinear relative to a quasiconvex subgroup. Quasiconvex subgroups in hyperbolic groups are known to have nice properties. Many algorithmic problems are decidable for quasiconvex subgroups, including the membership problem [57], whereas Rips constructed finitely generated subgroups of hyperbolic groups with an undecidable membership problem [81].

Finally, in the end of this thesis (Chapter 10) we want to discuss some computational hardness results. In the first part, we make use so-called *uniformly strongly efficiently non-solvable* groups (uniformly SENS groups) that were recently defined in [F2]. Roughly speaking, a group G is uniformly SENS if there exist nontrivial nested commutators of arbitrary depth that moreover, are efficiently computable in a certain sense (see Section 2.4.8 for the precise definition). The essence of these groups is that they allow to carry out Barrington's argument showing the NC^1-hardness of the word problem for a finite solvable group [5]. It turns out that for these groups G, we can prove that $\textsc{Knapsack}(G \wr \mathbb{Z})$ is Σ_2^p-hard. Wreath products are prominent constructions in group theory and semigroup theory. For groups G and H, their (restricted)

wreath product $G \wr H$ can be roughly described as follows: An element of $G \wr H$ consists of (i) a labeling, which maps each element of H to an element of G and (ii) an element of H, called the *cursor*. Here, the labeling has finite support, meaning all but finitely many elements of H are mapped to the identity of G. Moreover, each element of $G \wr H$ can be written as a product of elements from G and from H. Multiplying on the right by an element $g \in G$ will multiply g to the label of the current cursor position. Multiplying on the right by an element $h \in H$ will move the cursor by multiplying h. Knapsack for wreath products has especially been studied in [31] and also [9]. We also state a few corollaries of this hardness result. For instance, we show that for the famous Thompson's group F, $\textsc{Knapsack}(F)$ is Σ_2^p-hard.

In the second part, we study decidability of an exponent equation for the group $SL_3(\mathbb{Z})$, which is the special linear group consisting of all 3×3 matrices with determinant 1 (equipped with matrix multiplication). Similarly to $H_3(\mathbb{Z})$, which is a subgroup of $SL_3(\mathbb{Z})$, one can ask if knapsack is decidable. It turns out that we can show undecidabilty for one exponent equation, in contrast to $H_3(\mathbb{Z})$, which we already mentioned earlier. The group $SL_3(\mathbb{Z})$ is of particular interest in research, since a lot of problems are unsolved, such as the rational subset membership and the subgroup membership problem. In a certain way, $SL_3(\mathbb{Z})$ is a border case between $SL_2(\mathbb{Z})$ and $SL_n(\mathbb{Z})$ ($n \geq 4$), since the case $n = 2$ is algorithmically easy and for $n \geq 4$, many algorithmic problems are indeed undecidable.

Chapter 2

Preliminaries

2.1 Monoids

Let Σ be a finite alphabet of symbols. As usual, Σ^* denotes the set of all finite words over the alphabet Σ. For a word $w = a_1 a_2 \cdots a_n$ with $a_1, \ldots, a_n \in \Sigma$ we denote with $|w| = n$ the length of w and $\mathsf{alph}(w) = \{a_1, a_2, \ldots, a_n\}$ for the set of symbols that occur in w. For $a \in \Sigma$, we write $|w|_a$ to denote the number of occurrences of a in w. The *free monoid* Σ^* consists of all finite words over Σ and the monoid operation is the concatenation of words. The concatenation of words $u, v \in \Sigma^*$ is simply denoted with uv. A *factor* of a word $w \in \Sigma^*$ is any word u such that $w = suv$ for word some words s, v. The identity element of the free monoid Σ^* is the empty word, which is usually denoted with ε. Here, we prefer to denote the empty word with 1 according to the following convention:

Convention 2.1. *For every monoid M we denote the identity element of M with the symbol 1; even in cases where we deal with several monoids.*

So intuitively, all monoids that we deal with share the same identity element 1. This convention will simplify our notations.

2.1.1 Trace monoids

In the following we introduce some notions from trace theory, see [20, 21] for more details. An *independence alphabet* is an undirected graph (Σ, I) (without loops). Thus, I is a symmetric and irreflexive relation on Σ. The set Σ may be infinite. Note that even in the infinite case, Σ^* consists of all finite words over Σ. The *trace monoid* $\mathbb{M}(\Sigma, I)$ is defined as the quotient

$$\mathbb{M}(\Sigma, I) = \Sigma^* / \{ab = ba \mid (a, b) \in I\}$$

with concatenation as operation and the empty trace 1 as the neutral element. Its elements are called *traces*. We denote by $[w]_I$ the trace represented by the word $w \in \Sigma^*$. Let $\mathsf{alph}([w]_I) = \mathsf{alph}(w)$ and $|[w]_I| = |w|$. Note that $[u]_I = [v]_I$ implies that $|u| = |v|$ and $\mathsf{alph}(u) = \mathsf{alph}(v)$. The *dependence alphabet* associated

with (Σ, I) is (Σ, D), where $D = (\Sigma \times \Sigma) \setminus I$. Note that the relation D is reflexive. For $a \in \Sigma$ let $I(a) = \{b \in \Sigma \mid (a,b) \in I\}$ be the letters that commute with a. For traces $u, v \in \mathbb{M}(\Sigma, I)$ we denote with $u\ I\ v$ the fact that $\mathsf{alph}(u) \times \mathsf{alph}(v) \subseteq I$. The trace u is *connected* if we cannot write $u = vw$ in $\mathbb{M}(\Sigma, I)$ such that $v \neq 1 \neq w$ and $v\ I\ w$.

An *independence clique* is a subset $\Delta \subseteq \Sigma$ such that $(a,b) \in I$ for all $a, b \in \Delta$ with $a \neq b$. A *finite* independence clique Δ is identified with the trace $[a_1 a_2 \cdots a_n]_I$, where $a_1, a_2, \ldots, a_n$ is an arbitrary enumeration of Δ.

The following lemma, which is known as Levi's lemma, is one of the most fundamental facts for trace monoids, see e.g. [21].

Lemma 2.2. *Let $u_1, \ldots, u_m, v_1, \ldots, v_n \in \mathbb{M}(\Sigma, I)$. Then*

$$u_1 u_2 \cdots u_m = v_1 v_2 \cdots v_n$$

if and only if there exist $w_{i,j} \in \mathbb{M}(\Sigma, I)$ $(1 \leq i \leq m,\ 1 \leq j \leq n)$ such that

- *$u_i = w_{i,1} w_{i,2} \cdots w_{i,n}$ for every $1 \leq i \leq m$,*
- *$v_j = w_{1,j} w_{2,j} \cdots w_{m,j}$ for every $1 \leq j \leq n$, and*
- *$(w_{i,j}, w_{k,\ell}) \in I$ if $1 \leq i < k \leq m$ and $n \geq j > \ell \geq 1$.*

The situation in the lemma will be visualized by a diagram of the following kind. The i-th column corresponds to u_i, the j-th row corresponds to v_j, and the intersection of the i-th column and the j-th row represents $w_{i,j}$. Furthermore $w_{i,j}$ and $w_{k,\ell}$ are independent if one of them is left-above the other one.

v_n	$w_{1,n}$	$w_{2,n}$	$w_{3,n}$	$\ldots$	$w_{m,n}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
v_3	$w_{1,3}$	$w_{2,3}$	$w_{3,3}$	$\ldots$	$w_{m,3}$
v_2	$w_{1,2}$	$w_{2,2}$	$w_{3,2}$	$\ldots$	$w_{m,2}$
v_1	$w_{1,1}$	$w_{2,1}$	$w_{3,1}$	$\ldots$	$w_{m,1}$
	u_1	u_2	u_3	$\ldots$	u_m

A consequence of Levi's lemma is that trace monoids are cancellative, i.e., $usv = utv$ implies $s = t$ for all traces $s, t, u, v \in \mathbb{M}(\Sigma, I)$.

A *trace rewriting system* R over $\mathbb{M}(\Sigma, I)$ is just a subset of $\mathbb{M}(\Sigma, I) \times \mathbb{M}(\Sigma, I)$ [20]. We define the *one-step rewrite relation* $\to_R \subseteq \mathbb{M}(\Sigma, I) \times \mathbb{M}(\Sigma, I)$ by: $x \to_R y$ if and only if there are $u, v \in \mathbb{M}(\Sigma, I)$ and $(\ell, r) \in R$ such that $x = u\ell v$ and $y = urv$. With $\xrightarrow{*}_R$ we denote the reflexive transitive closure of $\to_R$. The notion of a confluent and terminating trace rewriting system is defined as for other types of rewriting systems [14]: A trace rewriting system R is called *confluent* if for all $u, v, v' \in \mathbb{M}(\Sigma, I)$ with $u \xrightarrow{*}_R v$ and $u \xrightarrow{*}_R v'$ there exists a trace w with $v \xrightarrow{*}_R w$ and $v' \xrightarrow{*}_R w$. It is called *terminating* if there does not exist an infinite chain $u_0 \to_R u_1 \to_R u_2 \cdots$. A trace u is *R-irreducible* if no trace v with $u \to_R v$ exists. The set of all R-irreducible traces is denoted with $\mathsf{IRR}(R)$. If R is terminating and confluent, then for every trace u, there exists a unique *normal form* $\mathsf{NF}_R(u) \in \mathsf{IRR}(R)$ such that $u \xrightarrow{*}_R \mathsf{NF}_R(u)$ [49].

2.2 Formal languages

More details on finite automata can be found in the standard textbook [48]. A *finite automaton* over the alphabet Σ is a tuple $\mathcal{A} = (Q, I, \delta, F)$, where Q is a finite set of states, $I \subseteq Q$ is the set of initial states, $\delta \subseteq Q \times (\Sigma \cup \{1\}) \times Q$ is the set of transitions, and $F \subseteq Q$ is the set of final states. Note that here, 1 denotes the empty word over Σ. If there is a transition $(p, w, q) \in \delta$, we also denote this by $p \xrightarrow{w} q$. A word $w = a_1 a_2 \cdots a_n$ (here we allow $a_i = 1$) is *accepted by* $\mathcal{A}$ if there are transitions $(q_{i-1}, a_i, q_i) \in \delta$ for $1 \leq i \leq n$ such that $q_0 \in I$ and $q_n \in F$. With $L(\mathcal{A})$ (the language accepted by $\mathcal{A}$) we denote the set of all words in Σ^* accepted by $\mathcal{A}$, which is also called its *language*. The *size* of $\mathcal{A}$ is $|Q|$, the number of its states. A language L is called *regular* if it is accepted by a finite automaton.

A *finite state transducer* $\mathcal{T}$ over the alphabet Σ is a tuple $\mathcal{T} = (Q, I, \delta, F)$ where I and F have the same meaning as for a finite automaton and

$$\delta \subseteq (Q \times \Sigma \times \{1\} \times Q) \cup (Q \times \{1\} \times \Sigma \times Q).$$

A pair $(u, v) \in \Sigma^* \times \Sigma^*$ is accepted by $\mathcal{T}$ if there are transitions $(q_{i-1}, a_i, b_i, q_i) \in \delta$ for $1 \leq i \leq |u| + |v|$ (where $a_i, b_i \in \Sigma \cup \{1\}$) such that $u = a_1 \cdots a_{|u|+|v|}$, $v = b_1 \cdots b_{|u|+|v|}$, $q_0 \in I$ and $q_{|u|+|v|} \in F$. With $R(\mathcal{T})$ we denote the set of all pairs accepted by $\mathcal{T}$. A relation $R \subseteq \Sigma^* \times \Sigma^*$ is a *rational relation* if it is accepted by a finite state transducer.

Let K be a finitely generated abelian group. A *finite state transducer with K-output* (over the alphabet Σ) is a tuple $\mathcal{T} = (Q, I, \delta, F)$. The only difference to an ordinary finite state transducer is that δ is a partially defined function of type

$$\delta : \Big((Q \times \Sigma \times \{1\} \times Q) \cup (Q \times \{1\} \times \Sigma \times Q) \Big) \to K.$$

It defines a mapping

$$f_{\mathcal{T}} : \Sigma^* \times \Sigma^* \to 2^K$$

in the natural way: let $u, v \in \Sigma^*$ as above. Then $\alpha \in K$ belongs to $f_{\mathcal{T}}(u, v)$ if there exist $(q_{i-1}, a_i, b_i, q_i) \in \mathsf{dom}(\delta)$ for $1 \leq i \leq |u| + |v|$ such that $u = a_1 \cdots a_{|u|+|v|}$, $v = b_1 \cdots b_{|u|+|v|}$, $q_0 \in I$, $q_{|u|+|v|} \in F$, and $\alpha = \sum_{1 \leq i \leq |u|+|v|} \delta(q_{i-1}, a_i, b_i, q_i)$. In this thesis, $\mathcal{T}$ will be always such that $f_{\mathcal{T}}(u, v)$ is either empty or a singleton. In this situation, we can view $f_{\mathcal{T}}$ as a partially defined mapping $f_{\mathcal{T}} : \Sigma^* \times \Sigma^* \to K$.

2.3 Complexity theory

We assume some knowledge in complexity theory; in particular the reader should be familiar with the classes P, NP, and coNP. The class Σ_2^p (second existential level of the polynomial time hierarchy) contains all languages $L \subseteq \Sigma^*$ for which there exists a polynomial p and a language $K \subseteq \Sigma^* \# \{0,1\}^* \# \{0,1\}^*$ in P (for a

symbol $\# \notin \Sigma \cup \{0,1\}$) such that $x \in L$ if and only if

$$\exists y \in \{0,1\}^{\leq p(|x|)} \forall z \in \{0,1\}^{\leq p(|x|)} : x\#y\#z \in K.$$

Figure 2.1 gives a good visual overview about many complexity classes, where all of the ones appearing in this thesis (and more) can be found. A precise definition is mostly not needed.

A language A is *nondeterministically polynomial time reducible* to a language B if there exists a nondeterministic polynomial time Turing-machine M that outputs on each computation path after termination a word over the alphabet of the language B and such that $x \in A$ if and only if on input x, the machine M has at least one computation path on which it outputs a word from B. Later we make use of the following lemma:

Lemma 2.3. *If A is nondeterministically polynomial time reducible to B and $B \in \mathsf{NP}$, then also $A \in \mathsf{NP}$ holds.*

2.4 Groups

2.4.1 General definitions for groups

For more details on group theory we refer the reader to [69]. Infinite groups are usually given by presentations. Take an arbitrary non-empty set Ω and let $\Omega^{-1} = \{a^{-1} \mid a \in \Omega\}$ be a set of formal inverses such that $\Omega \cap \Omega^{-1} = \emptyset$. Let $\Sigma = \Omega \cup \Omega^{-1}$. The bijection $a \mapsto a^{-1}$ from Ω to Ω^{-1} can be extended to a natural involution $w \mapsto w^{-1}$ on Σ^*. For this we set $(a^{-1})^{-1} = a$ for $a \in \Omega$ and $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ for $a_1, \ldots, a_n \in \Sigma$. A word $w \in \Sigma^*$ is called *reduced* if it does not contain an occurrence of a word aa^{-1} or $a^{-1}a$ ($a \in \Sigma$). Applying the cancellation rules $aa^{-1} \to 1$ or $a^{-1}a \to 1$ as long as possible, every word $w \in \Sigma^*$ can be mapped to a unique reduced word $\mathsf{red}(w)$. The *free group* $F(\Omega)$ consists of all reduced words together with the group multiplication $u \cdot v = \mathsf{red}(uv)$ for reduced words u and v. The mapping red can be also viewed as a monoid morphism from Σ^* to $F(\Omega)$. For a subset $R \subseteq \Sigma^*$ one defines the group $\langle \Sigma \mid R \rangle$ as the quotient group $F(\Omega)/N_R$, where N_R is the smallest normal subgroup of $F(\Omega)$ that contains $\mathsf{red}(R) \subseteq F(\Omega)$. In other words, N_R is the intersection of all normal subgroups of $F(\Omega)$ that contain $\mathsf{red}(R)$. Clearly, every group is (isomorphic to a group) of the form $\langle \Sigma \mid R \rangle$.

Let G be a group. For $g, h \in G$ we write $[g,h] := g^{-1}h^{-1}gh$ for the commutator of g and h and g^h for $h^{-1}gh$. For subgroups A, B of G we write $[A,B]$ for the subgroup generated by all commutators $[a,b]$ with $a \in A$ and $b \in B$. The order of an element $g \in G$ is the smallest number $z > 0$ with $g^z = 1$ and ∞ if such a z does not exist. The group G is torsion-free, if every $g \in G \setminus \{1\}$ has infinite order.

Let $G = \langle \Sigma \mid R \rangle$ in the following. If Σ is finite then G is called *finitely generated* (f.g. for short) and Σ is called a *finite symmetric generating set* for G.

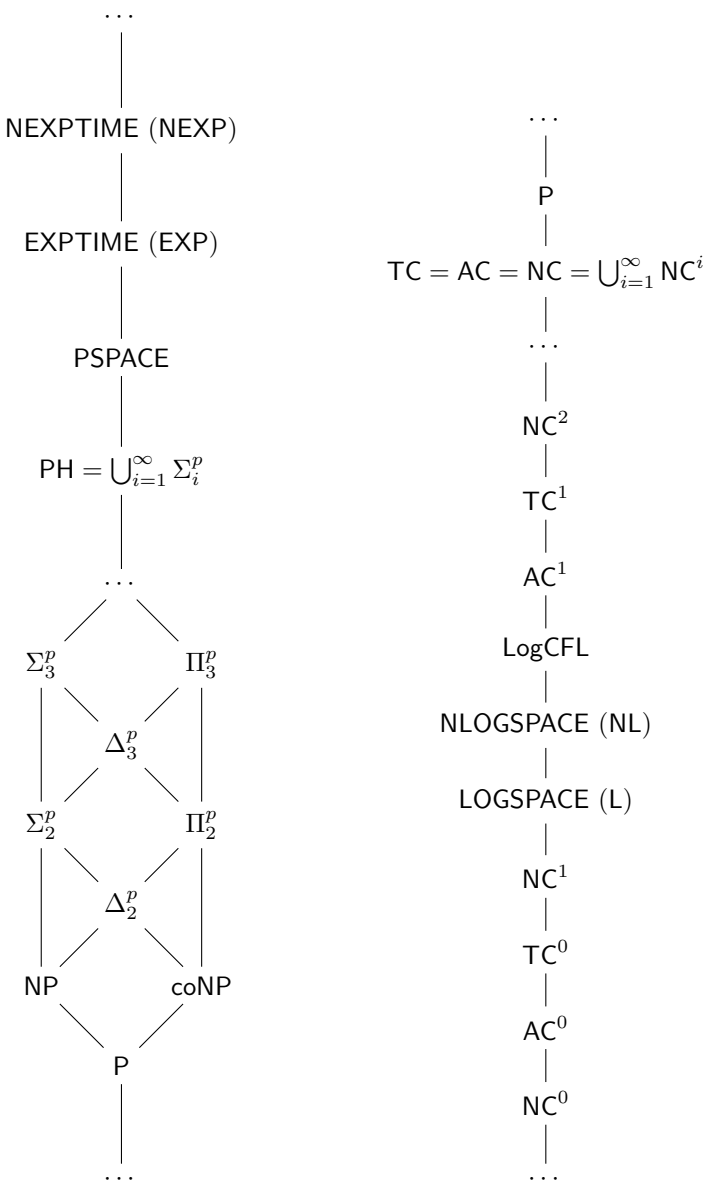

Figure 2.1: Some complexity classes shown in their hierarchy. An edge $\mathcal{C} - \mathcal{C}'$, where $\mathcal{C}$ is above $\mathcal{C}'$, means that $\mathcal{C}$ contains $\mathcal{C}'$

If both Σ and R are finite, then G is called *finitely presented*. The surjective monoid morphism $\mathsf{red}\colon \Sigma^* \to F(\Omega)$ extends to a surjective monoid morphism $h\colon \Sigma^* \to G$, called the *evaluation morphism*. The natural involution on Σ^* allows to use the notations $[g,h] = g^{-1}h^{-1}gh$ and $g^h = h^{-1}gh$ also in case $g, h \in \Sigma^*$. For two words $u, v \in \Sigma^*$ we write $u =_G v$ if $h(u) = h(v)$, in particular if $h(w) = 1$ we also say that $w = 1$ in G. For $g \in G$ we write $\|g\|$ for the length of a shortest word $w \in \Sigma^*$ such that $h(w) = g$. This notation depends on the generating set Σ. Then $\|g\|$ is also called the *geodesic length* of the group element g. For a subset $S \subseteq G$ and $u \in \Sigma^*$ we write $u \in_G S$ if $h(u) \in S$. In the following, when we say that we want to compute a homomorphism $h\colon G_1 = \langle \Sigma_1 \mid R_2 \rangle \to G_2 = \langle \Sigma_2 \mid R_2 \rangle$, we always mean that we compute the images $h(a)$ for $a \in \Sigma_1$.

2.4.2 Graph products

In this subsection we introduce graph products of groups. Graph products are a group construction, which somehow interpolate between direct products and free products. Both, direct products and free products of arbitrarily many groups, can be represented with this group construction as well and hence we are dealing with an actual generalization of both concepts. Our definition of graph products is based on trace monoids (also known as partially commutative monoids), which we discussed in Subsection 2.1.1.

Let us fix a *finite* independence alphabet (Γ, E) and finitely generated groups G_i for $i \in \Gamma$. Let α be the size of a largest clique of the independence alphabet (Γ, E). As usual 1 is the identity element for each of the groups G_i. Let Σ_i be a finite and symmetric generating set of G_i such that $\Sigma_i \cap \Sigma_j = \emptyset$ for $i \neq j$. Also we have the relatorsets R_i, which means $G_i = \langle \Sigma_i \mid R_i \rangle$. We can now define the *graph product* of the G_i with graph (Γ, E) to be the following group:

$$G(\Gamma, E, (G_i)_{i\in\Gamma}) = \left\langle \bigcup_{i\in\Gamma} \Sigma_i \;\middle|\; \bigcup_{i\in\Gamma} R_i \bigcup_{(i,j)\in E} \{[a,b] \mid a \in \Sigma_i, b \in \Sigma_j\} \right\rangle$$

This group presentation is just for better understanding. Later in Chapter 6 we will only work with another definition of graph products, which we will introduce now.

We define a (possibly infinite) independence alphabet as in [23, 59]: Let

$$A_i = G_i \setminus \{1\} \quad \text{and} \quad A = \bigcup_{i\in\Gamma} A_i.$$

We assume that $A_i \cap A_j = \emptyset$ for $i \neq j$. We fix the independence relation

$$I = \bigcup_{(i,j)\in E} A_i \times A_j$$

on A. The independence alphabet (A, I) is the only independence alphabet in this thesis which may be infinite. We will work with traces $t \in \mathbb{M}(A, I)$. For such a trace we need two length measures. The ordinary length of t is $|t|$ as

defined in Section 2.1: If $t = [a_1 \cdots a_k]_I$ with $a_j \in A$ then $|t| = k$. On the other hand, if we deal with computational problems, we need a finitary representations of the elements a_j. Assume that $a_j \in A_{i_j}$. Then, a_j can be written as a word over the alphabet Σ_{i_j}. Let $n_j = \|a_j\|$ be the geodesic length of a_j over Σ_{i_j} (as defined in Subsection 2.4.1). Then $\|t\| = n_1 + n_2 + \cdots + n_k$.

A trace $a \in A$ (i.e., a generator of $\mathbb{M}(A, I)$) is also called *atomic*, or an *atom*. For an atom $a \in A$ that belongs to the group G_i, we write a^{-1} for the inverse of a in G_i; it is again an atom. On $\mathbb{M}(A, I)$ we define the trace rewriting system

$$R = \bigcup_{i \in \Gamma} \Big(\{([aa^{-1}]_I, 1) \mid a \in A_i\} \cup \{([ab]_I, [c]_I) \mid a, b, c \in A_i, ab = c \text{ in } G_i\} \Big). \tag{2.1}$$

The following lemma was shown in [59]:

Lemma 2.4. *The trace rewriting system R is confluent.*

Since R is length-reducing, it is also terminating and hence defines unique normal forms. We define the *graph product* $G(\Gamma, E, (G_i)_{i \in \Gamma})$ as the quotient monoid

$$G(\Gamma, E, (G_i)_{i \in \Gamma}) = \mathbb{M}(A, I)/R.$$

Here we identify R with the smallest congruence relation on $\mathbb{M}(A, I)$ that contains all pairs from R. In the rest of this section, we write G for $G(\Gamma, E, (G_i)_{i \in \Gamma})$. It is easy to see that G is a group. The *inverse* of a trace $t = [a_1 a_2 \cdots a_k]_I \in \mathbb{M}(A, I)$ with $a_i \in A$ is the trace $t^{-1} = [a_k^{-1} \cdots a_2^{-1} a_1^{-1}]_I$. Note that t is well defined: If $[a_1 a_2 \cdots a_k]_I = [b_1 b_2 \cdots b_k]_I$ then $[a_k^{-1} \cdots a_2^{-1} a_1^{-1}]_I = [b_k^{-1} \cdots b_2^{-1} b_1^{-1}]_I$. We can apply this notation also to an independence clique C of (A, I) which yields the independence clique $C^{-1} = \{a^{-1} \mid a \in C\}$.

Note that G is finitely generated by $\Sigma = \bigcup_{i \in \Gamma} \Sigma_i$. If $E = \emptyset$, then G is the *free product*[4] of the groups G_i ($i \in \Gamma$) and if (Γ, E) is a complete graph, then G is the direct product of the groups G_i ($i \in \Gamma$). In this sense, the graph product construction generalizes free and direct products.

Recall that for words $u, v \in \Sigma^*$ we write $u =_G v$ if u and v represent the same element of the group G (Subsection 2.4.1). We use the same notation also for traces $u, v \in \mathbb{M}(A, I)$. In this case, we also say that $u = v$ *in* G. The following lemma is important for solving the word problem in the graph product G:

Lemma 2.5. *Let $u, v \in \mathbb{M}(A, I)$. Then $u =_G v$ if and only if $\mathsf{NF}_R(u) = \mathsf{NF}_R(v)$. In particular we have $u =_G 1$ if and only if $\mathsf{NF}_R(u) = 1$.*

Proof. The if-direction is trivial. Let on the other hand $u, v \in \mathbb{M}(A, I)$ and suppose that $u = v$ in G. By definition this is the case if and only if u and v represent the same element from $\mathbb{M}(A, I)/R$ and are hence congruent with respect to R. Since R produces a normal form for elements from the same congruence class, this implies that $\mathsf{NF}_R(u) = \mathsf{NF}_R(v)$. □

[4] As usual, the free product of groups G_1 and G_2 is denoted by $G_1 * G_2$.

Graph products of copies of $\mathbb{Z}$ are also known as *graph groups* or *right-angled Artin groups*. Graph products of copies of $\mathbb{Z}/2\mathbb{Z}$ are known as *right-angled Coxeter groups*, see [24] for more details.

2.4.3 HNN-extensions

We now introduce the important operation of HNN-extension. In their general form, HNN-extensions have been used to construct groups with an undecidable word problem, which means they may destroy desirable algorithmic properties. HNN-extensions are closely related to amalgamated products, which we will introduce in the next subsection. Later in Chapter 7 we consider the special case of finite associated (resp. identified) subgroups, for which these constructions already play a prominent role, for example, in Stallings' decomposition of groups with infinitely many ends [85] or the construction of virtually free groups [19]. Moreover, these constructions are known to preserve a wide range of important structural and algorithmic properties [2, 42, 51, 52, 54, 55, 63, 64, 72].

Suppose $G = \langle \Sigma \mid R \rangle$ is a finitely generated group with the finite symmetric generating set $\Sigma = \Omega \cup \Omega^{-1}$ and $R \subseteq \Sigma^*$. Fix two isomorphic subgroups A and B of G together with an isomorphism $\varphi\colon A \to B$. Let $t \notin \Sigma$ be a new letter. Then the corresponding *HNN-extension* is the group

$$H = \langle \Sigma \cup \{t, t^{-1}\} \mid R \cup \{t^{-1}a^{-1}t\varphi(a) \mid a \in A\} \rangle$$

(formally, we identify here every element $g \in A \cup B$ with a word over Σ that evaluates to g). This group is usually denoted by

$$H = \langle G, t \mid t^{-1}at = \varphi(a)\ (a \in A) \rangle. \tag{2.2}$$

Intuitively, H is obtained from G by adding a new element t such that conjugating elements of A with t applies the isomorphism φ. Here, t is called the *stable letter* and the groups A and B are the *associated subgroups*. A basic fact about HNN-extensions is that the group G embeds naturally into H [44].

For a subset $S \subseteq G$ of the group G one defines the *centralizer*

$$C(S) = \{h \in G \mid gh = hg \text{ for all } g \in S\}.$$

The HNN-extension $H = \langle G, t \mid t^{-1}at = a\,(a \in C(S)) \rangle$ is an *extension of the centralizer* $C(S)$. Extensions of centralizers were first studied in [75] in the context of exponential groups.

2.4.4 Amalgamated products

The next group construction is strongly related to HNN-extensions. Roughly speaking, one takes two groups and glues them together by a subgroup of both groups. For $i \in \{1, 2\}$, let $G_i = \langle \Sigma_i \mid R_i \rangle$ be a finitely generated group with $\Sigma_1 \cap \Sigma_2 = \emptyset$ and let A be a group that is embedded in each G_i via the injective morphism $\varphi_i\colon A \to G_i$ for $i \in \{1, 2\}$. Then, the *amalgamated product with*

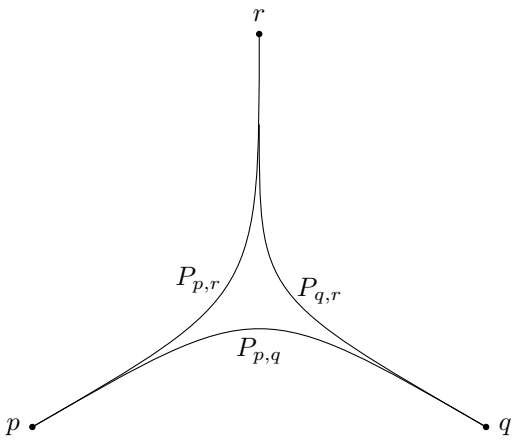

Figure 2.2: The shape of a geodesic triangle in a hyperbolic group

identified (amalgamated) subgroup A is the group

$$\langle \Sigma_1 \uplus \Sigma_2 \mid R_1 \uplus R_2 \cup \{\varphi_1(a)^{-1}\varphi_2(a) \mid a \in A\}\rangle.$$

This group is usually written as

$$\langle G_1 * G_2 \mid \varphi_1(a) = \varphi_2(a)\ (a \in A)\rangle$$

or just $G_1 *_A G_2$. Note that the amalgamated product depends on the morphisms φ_i, although they are omitted in the notation $G_1 *_A G_2$. In this thesis, we just consider finite amalgamated subgroups A.

It is well-known [69, Theorem 2.6, p. 187] that $G_1 *_A G_2$ can be embedded into the HNN-extension

$$H = \langle G_1 * G_2, t \mid t^{-1}\varphi_1(a)t = \varphi_2(a)\ (a \in A)\rangle$$

by the morphism $\Phi\colon G_1 *_A G_2 \to H$ with

$$\Phi(g) = \begin{cases} t^{-1}gt & \text{if } g \in G_1 \\ g & \text{if } g \in G_2. \end{cases}$$

2.4.5 Hyperbolic groups

Hyperbolic groups are groups where the so called Cayley-graph "looks hyperbolic". An easy example is the free group F_2. On the other hand, free abelian groups such as $\mathbb{Z} \times \mathbb{Z}$ are kind of the opposite.

Let G be a finitely generated group with the finite symmetric generating set Σ and let $h : \Sigma^* \to G$ be the evaluation morphism. The *Cayley-graph* of G (with respect to Σ) is the graph $\Gamma = \Gamma(G)$ with node set G and all edges (g, ga) for $g \in G$ and $a \in \Sigma$. We view Γ as a geodesic metric space, where

every edge (g, ga) is identified with a unit-length interval. It is convenient to label the directed edge from g to ga with the generator a. Note that since Σ is symmetric, there is also an edge from ga to g labelled with a^{-1}. Therefore one can view Γ as an undirected graph. The distance between two points p, q is denoted with $d_\Gamma(p, q)$. For $g \in G$ let $|g| = d_\Gamma(1, g)$. For $\kappa \geq 0$ and $g \in G$ let $\mathcal{B}_\kappa(g) = \{h \in G \mid d_\Gamma(g, h) \leq \kappa\}$ be the ball of radius κ around g.

Paths can be defined in a very general way for metric spaces, but we only need paths that are induced by words over Σ. Given a word $w = a_1 a_2 \cdots a_n$ (with $a_i \in \Sigma$), one obtains a unique path $P[w] : [0, n] \to \Gamma$, which is a continuous mapping from the real interval $[0, n]$ to Γ. It maps the subinterval $[i, i+1] \subseteq [0, n]$ isometrically onto the edge $(h(a_1 \cdots a_i), h(a_1 \cdots a_{i+1}))$ of Γ. The path $P[w]$ starts in 1 and ends in $h(w)$ (the group element represented by w). We also say that $P[w]$ is the unique path that starts in 1 and is labelled with the word w. More generally, for $g \in G$ we denote with $g \cdot P[w]$ the path that starts in g and is labelled with w. When writing $u \cdot P[w]$ for a word $u \in \Sigma^*$, we mean the path $h(u) \cdot P[w]$. A path $P : [0, n] \to \Gamma$ of the above form is

- *geodesic* if $d_\Gamma(P(0), P(n)) = n$;
- (λ, ϵ)-*quasigeodesic* if for all points $p = P(a)$ and $q = P(b)$ we have $|a - b| \leq \lambda \cdot d_\Gamma(p, q) + \varepsilon$;
- ζ-*local* (λ, ϵ)-*quasigeodesic* if for all points $p = P(a)$ and $q = P(b)$ with $|a - b| \leq \zeta$ we have $|a - b| \leq \lambda \cdot d_\Gamma(p, q) + \varepsilon$.

A word $w \in \Sigma^*$ is geodesic if the path $P[w]$ is geodesic, which means that there is no shorter word representing the same group element from G. Similarly, we define the notion of (λ, ϵ)-quasigeodesic (resp., ζ-local (λ, ϵ)-quasigeodesic) words. A set (or language) of words $L \subseteq \Sigma^*$ is called geodesic (resp., (λ, ϵ)-quasigeodesic), if every $w \in L$ is geodesic (resp., (λ, ϵ)-quasigeodesic).

A *geodesic triangle* consists of three points $p, q, r \in G$ and geodesic paths $P_1 = P_{p,q}$, $P_2 = P_{p,r}$, $P_3 = P_{q,r}$ (the three sides of the triangle), where $P_{x,y}$ is a geodesic path from x to y. We call a geodesic triangle δ-*slim* for $\delta \geq 0$, if for all $i \in \{1, 2, 3\}$, every point on P_i has distance at most δ from a point on $P_j \cup P_k$, where $\{j, k\} = \{1, 2, 3\} \setminus \{i\}$. Here, we identify a path $P : [0, n] \to \Gamma$ with its image $P([0, n]) \subseteq \Gamma$. The group G is called δ-*hyperbolic*, if every geodesic triangle is δ-slim. Finally, G is hyperbolic, if it is δ-hyperbolic for some $\delta \geq 0$. Figure 2.2 shows the shape of a geodesic triangle in a hyperbolic group. Finitely generated free groups are for instance 0-hyperbolic with respect to a free finite generating set. The property of being hyperbolic is independent of the chosen generating set Σ. The word problem for every hyperbolic group can be decided in real time [45].

Now we are also going to define quasiconvex subgroups: A subset $Q \subseteq G$ is called *quasiconvex* if there exists a constant $\kappa \geq 0$ such that every geodesic path from 1 to some $g \in Q$ is contained in $\bigcup_{h \in Q} B_\kappa(h)$. Later we are only interested in the case that G is a group and Q is a subgroup. The following result can be found in [33] ($h : \Sigma^* \to G$ denotes the evaluation morphism):

Lemma 2.6. *Let G be hyperbolic. A subset $Q \subseteq G$ is quasiconvex if and only if the language of all geodesic words in $h^{-1}(Q)$ is regular.*

2.4.6 Central extensions

Consider a finitely generated group H and let $K \leq Z(H)$ be a subgroup of the center of H. In particular, K is normal in H. Let $G = H/K$ be the quotient group. In this situation, H is called a central extension of G. Note that K is abelian. We write K additively.

Lemma 2.7. *Let H be a central extension of $G = H/K$ with H finitely generated and G finitely presented. Then K is finitely generated.*

Proof. We can choose a finite symmetric generating set Γ for H such that $G = \langle \Gamma \mid R \rangle$ for a finite set of relators R. Let $\phi : \Gamma^* \to H$ be the evaluation morphism. Consider a word $w \in \Gamma^*$ that represents an element of K. Since $w =_G 1$, we can write the word w in the free group $F(\Gamma)$ as

$$w =_{F(\Gamma)} \prod_{i=1}^{n} u_i^{-1} r_i^{\epsilon_i} u_i,$$

with $u_i \in \Gamma^*$, $\epsilon_i \in \{-1, 1\}$, and $r_i \in R$. We have $\phi(R) \subseteq K$. In particular, all elements of $\phi(R)$ are central in H. We obtain

$$w =_H \prod_{i=1}^{n} u_i^{-1} r_i^{\epsilon_i} u_i =_H \prod_{i=1}^{n} r_i^{\epsilon_i}.$$

This shows that the finite set $\phi(R)$ generates K. □

Assume that as above, H is finitely generated and G is finitely presented. Let Σ be a finite symmetric generating set for G. We can identify Σ with a left transversal of K in H. Moreover, let A be a finite generating set for K with $\Sigma \cap A = \emptyset$. Then $\Gamma = \Sigma \cup A$ generates H. Given a word $w \in \Sigma^*$ and $\alpha \in A^*$ we write $w \cdot \alpha$ for the corresponding element of H. Here, α is usually written additively and identified with its Parikh image.

For the following lemma we need the *word search problem* for the finitely presented group G. For this, choose a finite presentation $\langle \Sigma \mid R \rangle$ for G. The input to the word search problem is a word $w \in \Sigma^*$. If $w \neq_G 1$ then the output is NO. Otherwise the output is a representation $w =_{F(\Sigma)} \prod_{i=1}^{n} u_i^{-1} r_i^{\epsilon_i} u_i$ of w in the free group, where $u_i \in \Sigma^*$, $\epsilon_i \in \{-1, 1\}$, and $r_i \in R$. Clearly, the word search problem can be only solved in polynomial time if G has a polynomial Dehn function. Automatic groups (and hence also hyperbolic groups) have a polynomial time solvable word search problem [61, p. 40].

Lemma 2.8. *Let H be a finitely generated central extension of the finitely presented group $G = H/K$. Choose the above generating set $\Gamma = \Sigma \cup A$ for H and let $k = |A|$. Assume that the word search problem for G can be solved in polynomial time. Then given $w \in \Sigma^*$ with $w =_G 1$ we can compute in polynomial*

time $\alpha \in K$ such that $w =_H \alpha$. If $\alpha = (z_1, \ldots, z_k)$ then for every $1 \leq i \leq k$, $|z_i|$ is bounded polynomially in $|w|$.

Proof. Let $\langle \Sigma \mid R \rangle$ be a finite presentation for G. Since $w =_G 1$ and the word search problem for G can be solved in polynomial time, we can compute in polynomial time a representation $w =_{F(\Sigma)} \prod_{i=1}^{n} u_i^{-1} r_i^{\epsilon_i} u_i$ of w in the free group $F(\Sigma)$, where $u_i \in \Sigma^*$, $\epsilon_i \in \{-1, 1\}$, and $r_i \in R$. Note that n is polynomially bounded in $|w|$. For every $r \in R$ there is a fixed element $\alpha(r) \in K$ such that $r =_H \alpha(r)$. Since all elements of R are central in H, we obtain

$$w =_H \prod_{i=1}^{n} u_i^{-1} r_i^{\epsilon_i} u_i =_H \sum_{i=1}^{n} \epsilon_i \cdot \alpha(r_i).$$

The latter sum can be computed in polynomial time. Note that the bit length of all entries in $\sum_{i=1}^{n} \epsilon_i \cdot \alpha(r_i)$ is $\mathcal{O}(\log n) = \mathcal{O}(\log |w|)$. □

We will mainly use Lemma 2.8 for the following situation: Let $u, v \in \Sigma^*$ be given word with $u =_G v$. Then there exists a unique element $\alpha \in K$ such that $u \cdot \alpha =_H v$. Lemma 2.8 allows us to compute this α in polynomial time.

2.4.7 Wreath products

Let G and H be groups. Consider the direct sum $K = \bigoplus_{h \in H} G_h$, where G_h is a copy of G. We view K as the set $G^{(H)}$ of all mappings $f \colon H \to G$ such that $\mathrm{supp}(f) := \{h \in H \mid f(h) \neq 1\}$ is finite, together with pointwise multiplication as the group operation. The set $\mathrm{supp}(f) \subseteq H$ is called the *support* of f. The group H has a natural left action on $G^{(H)}$ given by $hf(a) = f(h^{-1}a)$, where $f \in G^{(H)}$ and $h, a \in H$. The corresponding semidirect product $G^{(H)} \rtimes H$ is the (restricted) *wreath product* $G \wr H$. In other words:

- Elements of $G \wr H$ are pairs (f, h), where $h \in H$ and $f \in G^{(H)}$.
- The multiplication in $G \wr H$ is defined as follows: Let $(f_1, h_1), (f_2, h_2) \in G \wr H$. Then $(f_1, h_1)(f_2, h_2) = (f, h_1 h_2)$, where $f(a) = f_1(a) f_2(h_1^{-1} a)$.

There are canonical mappings

- $\sigma \colon G \wr H \to H$ with $\sigma(f, h) = h$ and
- $\tau \colon G \wr H \to G^{(H)}$ with $\tau(f, h) = f$

In other words: $g = (\tau(g), \sigma(g))$ for $g \in G \wr H$. Note that σ is a homomorphism whereas τ is in general not a homomorphism. Throughout this thesis, the letters σ and τ will have the above meaning, which of course depends on the underlying wreath product $G \wr H$, but the latter will be always clear from the context.

The following intuition might be helpful: An element $(f, h) \in G \wr H$ can be thought of as a finite multiset of elements of $G \setminus \{1_G\}$ that are sitting at certain elements of H (the mapping f) together with the distinguished element $h \in H$, which can be thought of as a cursor moving in H. If we want to compute the product $(f_1, h_1)(f_2, h_2)$, we do this as follows: First, we shift the

finite collection of G-elements that corresponds to the mapping f_2 by h_1: If the element $g \in G \setminus \{1_G\}$ is sitting at $a \in H$ (i.e., $f_2(a) = g$), then we remove g from a and put it to the new location $h_1 a \in H$. This new collection corresponds to the mapping $f_2' \colon a \mapsto f_2(h_1^{-1}a)$. After this shift, we multiply the two collections of G-elements pointwise: If in $a \in H$ the elements g_1 and g_2 are sitting (i.e., $f_1(a) = g_1$ and $f_2'(a) = g_2$), then we put the product $g_1 g_2$ into the location a. Finally, the new distinguished H-element (the new cursor position) becomes $h_1 h_2$.

Clearly, H is a subgroup of $G \wr H$. But also G is a subgroup of $G \wr H$. We can identify G with the set of all mappings $f \in G^{(H)}$ such that $\mathrm{supp}(f) \subseteq \{1\}$. This copy of G together with H generates $G \wr H$. In particular, if $G = \langle \Sigma \rangle$ and $H = \langle \Gamma \rangle$ with $\Sigma \cap \Gamma = \emptyset$ then $G \wr H$ is generated by $\Sigma \cup \Gamma$. In this situation, we will also apply the above mappings σ and τ to words over $\Sigma \cup \Gamma$. We will need the following embedding result:

Lemma 2.9. *Given a unary encoded number d, one can compute in logspace an embedding of $G^d \wr \mathbb{Z}$ into $G \wr \mathbb{Z}$.*

Proof. Let $G = \langle \Gamma \rangle$ and let Γ_i $(0 \leq i \leq d-1)$ be pairwise disjoint copies of Γ, each of which generates a copy of G. For $G^d \wr \mathbb{Z}$ we take the generating set $\{t, t^{-1}\} \cup \bigcup_{i=0}^{d-1} \Gamma_i$, where t generates the right factor $\mathbb{Z}$. We then obtain an embedding $h \colon G^d \wr \mathbb{Z} \to G \wr \mathbb{Z}$ by:

- $h(t) = t^d$ and $h(t^{-1}) = t^{-d}$,
- $h(a) = t^i a t^{-i}$ for $a \in \Gamma_i$.

This proves the lemma. □

2.4.8 Strongly efficiently non-solvable groups

Roughly speaking, a group G is uniformly SENS if there exist nontrivial nested commutators of arbitrary depth that moreover, are efficiently computable in a certain sense. We now give a formal definition of uniformly SENS groups as in [F2].

Let us fix a f.g. group $G = \langle \Sigma \rangle$. Following [F2] we need the additional assumption that the generating set Σ contains the group identity 1. This allows to pad words over Σ to any larger length without changing the group element represented by the word. One also says that Σ is a *standard generating set* for G. The group G is called *strongly efficiently non-solvable (SENS)* if there is a constant $\mu \in \mathbb{N}$ such that for every $d \in \mathbb{N}$ and $v \in \{0,1\}^{\leq d}$ there is a word $w_{d,v} \in \Sigma^*$ with the following properties:

- $|w_{d,v}| = 2^{\mu d}$ for all $v \in \{0,1\}^d$,
- $w_{d,v} = [w_{d,v0}, w_{d,v1}]$ for all $v \in \{0,1\}^{<d}$ (here we take the commutator of words),
- $w_{d,1} \neq 1$ in G.

The group G is called *uniformly strongly efficiently non-solvable* if, moreover,

- given $v \in \{0,1\}^d$, a binary number i with μd bits, and $a \in \Sigma$ one can decide in linear time on a random access Turing-machine whether the i-th letter of $w_{d,v}$ is a.

Here are examples for uniformly SENS groups; see [F2] for details:

- finite non-solvable groups (more generally, every f.g. group that has a finite non-solvable quotient),
- f.g. non-abelian free groups,
- Thompson's group F,
- weakly branched self-similar groups with a f.g. branching subgroup (this includes several famous self-similar groups like the Grigorchuk group, the Gupta-Sidki groups and the Tower of Hanoi groups).

Chapter 3

Knapsack and exponent equations

3.1 General definitions

Let G be a finitely generated group with the finite symmetric generating set Σ. Moreover, let X be a countable infinite set of formal variables that take values from $\mathbb{N}$. For a subset $U \subseteq X$, we use $\mathbb{N}^U$ to denote the set of maps $\nu\colon U \to \mathbb{N}$, which we call *valuations* for U. For valuations $\nu \in \mathbb{N}^U$ and $\mu \in \mathbb{N}^V$ such that $U \subseteq V$ we say that ν extends μ (or μ restricts to ν) if $\nu(x) = \mu(x)$ for all $x \in U$.

An *exponent expression* over Σ is a formal expression of the form $e = u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$ with $k \geq 1$, words $u_i, v_i \in \Sigma^*$ and variables $x_1, \ldots, x_k \in X$. Here, we allow $x_i = x_j$ for $i \neq j$. The words u_i are called the *periods* of e, and we can assume that $u_i \neq 1$ for all $1 \leq i \leq k$. If every variable in an exponent expression occurs at most once, it is called a *knapsack expression*. Alternatively, if we have an equation $e = 1$, we also say *knapsack equation* or *exponent equation* respectively. Let $X_e = \{x_1, \ldots, x_k\}$ be the set of variables that occur in e. For a valuation $\nu : U \to \mathbb{N}$ such that $X_e \subseteq U$ (in which case we also say that ν is a valuation for e), we define $\nu(e) = u_1^{\nu(x_1)} v_1 u_2^{\nu(x_2)} v_2 \cdots u_k^{\nu(x_k)} v_k \in \Sigma^*$. We say that ν is a *G-solution* of the expression e, if $\nu(e)$ evaluates to the identity element 1 of G. With $\mathsf{sol}_G(e)$ we denote the set of all G-solutions $\nu : X_e \to \mathbb{N}$ of e. We can view $\mathsf{sol}_G(e)$ as a subset of $\mathbb{N}^k$. The *length* of e is defined as $\|e\| = \sum_{i=1}^{k} |u_i| + |v_i|$, whereas $k \leq \|e\|$ is its *degree*, $\deg(e)$ for short. We define *solvability of exponent equations over G* (denoted by $\textsc{ExpEq}(G)$) as the following decision problem:

Input A finite list of exponent expressions $e_1, \ldots, e_n$ over Σ.

Question Is $\bigcap_{i=1}^{n} \mathsf{sol}_G(e_i)$ non-empty?

The *knapsack problem for G* ($\textsc{Knapsack}(G)$ for short) is the following decision problem:

Input A single knapsack expression e over Σ.

Question Is $\mathsf{sol}_G(e)$ non-empty?

It is easy to observe that the concrete choice of the generating set Σ has no influence on the decidability and complexity status of these problems.

One could also allow exponent expressions of the form $e = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$. However, since then

$$\mathsf{sol}_G(e) = \mathsf{sol}_G(u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k v_0),$$

this would result in the same class of solution sets. Moreover, we could also restrict to exponent expressions of the form $e = u_1^{x_1} u_2^{x_2} \cdots u_k^{x_k} v$: for $e = u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$ and

$$e' = u_1^{x_1} (v_1 u_2 v_1^{-1})^{x_2} (v_1 v_2 u_3 v_2^{-1} v_1^{-1})^{x_3} \cdots (v_1 \cdots v_{k-1} u_3 v_{k-1}^{-1} \cdots v_1^{-1})^{x_k} v_1 \cdots v_k$$

we have $\nu(e) =_G \nu(e')$ for every valuation ν and hence $\mathsf{sol}_G(e) = \mathsf{sol}_G(e')$.

3.2 Semilinear sets

Fix a dimension $d \geq 1$. All vectors will be column vectors. For a vector $\boldsymbol{v} = (v_1, \ldots, v_d)^\mathsf{T} \in \mathbb{Z}^d$ we define its norm $\|\boldsymbol{v}\| := \max\{|v_i| \mid 1 \leq i \leq d\}$ and for a matrix $M \in \mathbb{Z}^{c \times d}$ with entries $m_{i,j}$ $(1 \leq i \leq c,\ 1 \leq j \leq d)$ we define the norm $\|M\| = \max\{|m_{i,j}| \mid 1 \leq i \leq c,\ 1 \leq j \leq d\}$. Finally, for a finite set of vectors $A \subseteq \mathbb{N}^d$ let $\|A\| = \max\{\|\boldsymbol{a}\| \mid \boldsymbol{a} \in A\}$.

We extend the operations of vector addition and multiplication of a vector by a matrix to sets of vectors in the obvious way. A *linear subset* of $\mathbb{N}^d$ is a set of the form

$$L = L(\boldsymbol{b}, P) := \boldsymbol{b} + P \cdot \mathbb{N}^k$$

where $\boldsymbol{b} \in \mathbb{N}^d$ and $P \in \mathbb{N}^{d \times k}$. We call a set $S \subseteq \mathbb{N}^d$ *semilinear*, if it is a finite union of linear sets. The class of semilinear sets is known to be effectively closed under boolean operations; quantitative results on the descriptional complexity of boolean operations on semi-linear sets can be found in [6].

If a semilinear set S is given as a union $\bigcup_{i=1}^k L(\boldsymbol{b}_i, P_i)$, we call the tuple $\mathcal{R} = (\boldsymbol{b}_1, P_1, \ldots, \boldsymbol{b}_k, P_k)$ a *semilinear representation* of S. For a semilinear representation $\mathcal{R} = (\boldsymbol{b}_1, P_1, \ldots, \boldsymbol{b}_k, P_k)$ we define $\|\mathcal{R}\| = \max\{\|\boldsymbol{b}_1\|, \|P_1\| \ldots, \|\boldsymbol{b}_k\|, \|P_k\|\}$. The *magnitude* of a semilinear set S, $\mathsf{mag}(S)$ for short, is the smallest possible value for $\|\mathcal{R}\|$ among all semilinear representations $\mathcal{R}$ of S.

For a linear set $L(\boldsymbol{b}, P) \subseteq \mathbb{N}^d$ we can assume that all columns of P are different. Hence, if the magnitude of $L(\boldsymbol{b}, P)$ is bounded by s then we can bound the number of columns of P by $(s+1)^d$ (since there are only $(s+1)^d$ vectors in $\mathbb{N}^d$ of norm at most s). No better upper bound is known, but if we allow to split $L(\boldsymbol{b}, P)$ into several linear sets, we get the following lemma from [26]:

Lemma 3.1 (c.f. [26, Theorem 1])**.** *Let $L = L(\boldsymbol{b}, P) \subseteq \mathbb{N}^d$ be a linear set of magnitude $s = \mathsf{mag}(L)$. Then $L = \bigcup_{i \in I} L(\boldsymbol{b}, P_i)$ such that every P_i consists of at most $2d \log(4ds)$ columns from P (and hence, $\mathsf{mag}(L(\boldsymbol{b}, P_i)) \leq s$).*

We also need the following bound on the magnitude for the intersections of semilinear sets:

Proposition 3.2 (c.f. [6, Theorem 4])**.** *Let $K = L(\boldsymbol{b}_1, P_1)$ and $L = L(\boldsymbol{b}_2, P_2)$ ($K, L \subseteq \mathbb{N}^d$) be linear sets of magnitude at most $s \geq 1$. Then the intersection $K \cap L$ is semilinear and*

$$\mathsf{mag}(K \cap L) \leq (12d^2 \log^2(4ds) d^{d/2} s^{d+1} + 1)s \leq \mathcal{O}(d^{d/2+3} s^{d+3}).$$

Proof. By Lemma 3.1 we can write $K = \bigcup_{i \in I_1} L(\boldsymbol{b}_1, P_{1,i})$ and $L = \bigcup_{i \in I_2} L(\boldsymbol{b}_2, P_{2,i})$ where every $P_{1,i}$ ($P_{2,i}$) consists of at most $2d \log(4ds)$ columns from P_1 (P_2). We have $K \cap L = \bigcup_{(i,j) \in I_1 \times I_2} L(\boldsymbol{b}_1, P_{1,i}) \cap L(\boldsymbol{b}_2, P_{2,i})$. From [6, Theorem 4] we get the upper bound $(12d^2 \log^2(4ds) d^{d/2} s^{d+1} + 1)s$ for the magnitude of each intersection $L(\boldsymbol{b}_1, P_{1,i}) \cap L(\boldsymbol{b}_2, P_{2,i})$. □

In the context of knapsack problems (which we will introduce in the next section), we will consider semilinear subsets as sets of mappings $\nu \colon \{x_1, \ldots, x_d\} \to \mathbb{N}$ for a finite set of variables $U = \{x_1, \ldots, x_d\}$. Such a mapping ν can be identified with the vector $(\nu(x_1), \ldots, \nu(x_d))^\mathsf{T}$. This allows to use all vector operations (e.g. addition and scalar multiplication) on the set $\mathbb{N}^U$ of all mappings from U to $\mathbb{N}$. In general, if $*$ is a binary operation on $\mathbb{N}$ (we only use addition or multiplication for $*$) we denote with $f * g$ (for $f, g \in \mathbb{N}^U$) the pointwise extension of the operation $*$ to $\mathbb{N}^U$, i.e., $(f * g)(x) = f(x) * g(x)$ for all $x \in U$. Moreover, for mappings $f \in \mathbb{N}^U$, $g \in \mathbb{N}^V$ with $U \cap V = \emptyset$ we define $f \oplus g \in \mathbb{N}^{U \cup V}$ by $(f \oplus g)(x) = f(x)$ for $x \in U$ and $(f \oplus g)(y) = g(y)$ for $y \in V$. All operations on $\mathbb{N}^U$ will be extended to subsets of $\mathbb{N}^U$ in the standard pointwise way. Note that $\mathsf{mag}(K \oplus L) \leq \max\{\mathsf{mag}(K), \mathsf{mag}(L)\}$ for semilinear sets K, L. If $L \subseteq \mathbb{N}^U$ is semilinear and $V \subseteq U$ then we denote with $L{\restriction_V}$ the semilinear set $\{f{\restriction_V} \mid f \in L\}$ obtained by restricting every function $f \in L$ to the subset V of its domain. Clearly, $L{\restriction_V}$ is semilinear too and $\mathsf{mag}(L{\restriction_V}) \leq \mathsf{mag}(L)$.

The semilinear sets are exactly those sets that are definable in first-order logic over the structure $(\mathbb{N}, +)$ (the so-called *Presburger definable sets*). All the above mentioned closure properties of semilinear sets follow from this characterization. A good survey on semilinear results and Presburger arithmetic with references for the above mentioned results is [41].

We fix an arbitrary enumeration $a_1, \ldots, a_k$ of the alphabet Σ. For $w \in \Sigma^*$ and $1 \leq i \leq k$ let $|w|_{a_i}$ be the number of occurrences of a_i in w. The *Parikh image* of w is the tuple $P(w) = (|w|_{a_1}, \ldots, |w|_{a_k}) \in \mathbb{N}^k$. For a language $L \subseteq \Sigma^*$ its Parikh image is $P(L) = \{P(w) \mid w \in L\}$. The following important result was shown by Parikh [80].

Theorem 3.3. *The semilinear sets are exactly the Parikh images of the regular languages. From a given finite automaton $\mathcal{A}$ one can compute a semilinear representation of $P(L(\mathcal{A}))$.*

3.3 Knapsack-semilinearity

The group G is called *knapsack-semilinear* if for every knapsack expression e over Σ, the set $\mathsf{sol}_G(e)$ is a semilinear set of vectors and a semilinear representation can be effectively computed from e. This implies that for every exponent expression e over Σ, the set $\mathsf{sol}_G(e)$ is semilinear as well and a semilinear representation can be effectively computed from e. To see this, consider an exponent expression $e = u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$ over Σ. Choose pairwise different variables $y_1, y_2, \ldots, y_k$ such that $X_e = \{x_1, \ldots, x_k\} \subseteq \{y_1, \ldots, y_k\}$ and consider the knapsack expression $e' = u_1^{y_1} v_1 u_2^{y_2} v_2 \cdots u_k^{y_k} v_k$. Moreover, define the equivalence relation $R = \{(i,j) \mid 1 \leq i,j \leq k, x_i = x_j\}$. We get

$$\mathsf{sol}_G(e) = (\mathsf{sol}_G(e') \cap \{\nu \mid \nu : \{y_1, \ldots, y_k\} \to \mathbb{N}, \forall (i,j) \in R : \nu(y_i) = \nu(y_j)\})\restriction_{X_e}.$$

Since semilinear sets are effectively closed under intersection and restriction, the effective semilinearity of $\mathsf{sol}_G(e')$ yields the effective semilinearity of $\mathsf{sol}_G(e)$.

Also notice that solvability of exponent equations is decidable for every knapsack-semilinear group. As mentioned in the introduction, the class of knapsack-semilinear groups is very rich. Examples of a groups, where knapsack is decidable but solvability of systems of exponent equations is undecidable are the Heisenberg group $H_3(\mathbb{Z})$ (the group of all upper triangular (3×3)-matrices over the integers, where all diagonal entries are 1) [58] and the Baumslag-Solitar group $\mathsf{BS}(1,2)$ [32]. These groups are not knapsack-semilinear in a strong sense: there are knapsack expressions e such that $\mathsf{sol}_{H_3(\mathbb{Z})}(e)$ (resp. $\mathsf{sol}_{\mathsf{BS}(1,2)}(e)$) is not semilinear. In order to obtain a non-semilinear solution set, one needs a knapsack instance over $H_3(\mathbb{Z})$ (resp. $\mathsf{BS}(1,2)$) with three variables. For two variables, the solutions sets are semilinear for any group. In fact, they have a particularly simple structure:

Lemma 3.4. *Let G be a group and $g_1, g_2, h \in G$ be elements.*

(i) The solution set $S_1 = \{(x,y) \in \mathbb{Z}^2 \mid g_1^x g_2^y = 1\}$ is a subgroup of $\mathbb{Z}^2$. If G is torsion-free and $\{g_1, g_2\} \neq \{1\}$ then S_1 is cyclic.

(ii) The solution set $S = \{(x,y) \in \mathbb{Z}^2 \mid g_1^x g_2^y = h\}$ is either empty or a coset $(a,b) + S_1$ of S_1 where $(a,b) \in S$ is any solution.

Proof. Clearly $(0,0) \in S_1$, and if $g_1^x g_2^y = 1 = g_1^{x'} g_2^{y'}$ then also $g_1^{x-x'} g_2^{y-y'} = 1$. This shows the first part of statement (i). Now assume that G is torsion-free and that $g_1 \neq 1$ (the case $g_2 \neq 1$ is analogous). If $(x,y), (x',y') \in S_1$ then $y'(x,y) - y(x',y') = (xy' - x'y, 0) \in S_1$ and hence $g_1^{xy'-x'y} = 1$. Since G is torsion-free this implies that $xy' - x'y = 0$, i.e. (x,y) and (x',y') are linearly dependent, since $\det \left(\begin{smallmatrix} x & x' \\ y & y' \end{smallmatrix}\right) = 0$. This shows that S_1 is cyclic.

For (ii) let us assume that $S \neq \emptyset$ and take any solution $(a,b) \in S$, i.e. $g_1^a g_2^b = h$. We first show that $(a,b) + S_1 \subseteq S$. Take any $(x,y) \in S_1$, i.e. $g_1^x g_2^y = 1$. Then we obtain $g_1^{a+x} g_2^{b+y} = g_1^a g_1^x g_2^y g_2^b = g_1^a g_2^b = h$ and thus $(a+x, b+y) \in S$.

Finally we claim that $S \subseteq (a,b) + S_1$: Let $(x,y) \in S$, i.e. $g_1^x g_2^y = h$. Since $g_1^{-a} h g_2^{-b} = 1$, we get $g_1^{x-a} g_2^{y-b} = g_1^{-a} (g_1^x g_2^y) g_2^{-b} = g_1^{-a} h g_2^{-b} = 1$ and therefore

$(x-a, y-b) \in S_1$. Hence $S = (a,b) + S_1$. □

Remark 3.5. The requirement that the semilinear representation of the solution set in a knapsack-semilinear group G can be computed effectively is important: There are groups where every knapsack equation has a semilinear solution set, but the semilinear representation cannot be computed. For example, consider a finitely generated torsion group G with an undecidable word problem [1]. Then every knapsack expression over G has a semilinear solution set. However, computing a semilinear representation for $\{n \in \mathbb{N} \mid u^n = 1\}$ for a given word u would allow us to check whether $u = 1$ in G.

For a knapsack-semilinear group G and a finite generating set Σ for G we define two growth functions. For $n, m \in \mathbb{N}$ with $m \leq n$ let $\mathsf{Exp}(n,m)$ be the finite set of all exponent expressions e over Σ such that (i) $\mathsf{sol}_G(e) \neq \emptyset$, (ii) $\|e\| \leq n$ and (iii) $\deg(e) \leq m$. Moreover, let $\mathsf{Knap}(n,m) \subseteq \mathsf{Exp}(n,m)$ be the set of all knapsack expressions in $\mathsf{Exp}(n,m)$. We define the mappings $\mathsf{E}_{G,\Sigma} : \{(n,m) \mid m,n \in \mathbb{N}, m \leq n\} \to \mathbb{N}$ and $\mathsf{K}_{G,\Sigma} : \{(n,m) \mid m,n \in \mathbb{N}, m \leq n\} \to \mathbb{N}$ as follows:

- $\mathsf{E}_{G,\Sigma}(n,m) = \max\{\mathsf{mag}(\mathsf{sol}_G(e)) \mid e \in \mathsf{Exp}(n,m)\}$,
- $\mathsf{K}_{G,\Sigma}(n,m) = \max\{\mathsf{mag}(\mathsf{sol}_G(e)) \mid e \in \mathsf{Knap}(n,m)\}$.

Clearly, if $\mathsf{sol}_G(e) \neq \emptyset$ and $\mathsf{mag}(\mathsf{sol}_G(e)) \leq N$ then e has a G-solution ν such that $\nu(x) \leq N$ for all variables $x \in X_e$. Therefore, if G has a decidable word problem and we have a computable bound on the function $\mathsf{E}_{G,\Sigma}$ then we obtain a nondeterministic algorithm for solvability of exponent equations over G: given an exponent expression e we can guess $\nu : X_e \to \mathbb{N}$ with $\nu(x) \leq N$ for all variables x and then verify (using an algorithm for the word problem), whether ν is indeed a solution.

Let Σ and Σ' be two generating sets for the group G. Then there is a constant c such that $\mathsf{E}_{G,\Sigma}(n,m) \leq \mathsf{E}_{G,\Sigma'}(cn,m)$ and $\mathsf{K}_{G,\Sigma}(n,m) \leq \mathsf{K}_{G,\Sigma'}(cn,m)$. To see this, note that for every $a \in \Sigma$ there is a word $w_a \in (\Sigma')^*$ such that a and w_a are representing the same element in G. Then we can choose $c = \max\{|w_a| \mid a \in \Sigma\}$. Due to this fact, we do not have to specify the generating set Σ when we say that $\mathsf{K}_{G,\Sigma}$ (resp., $\mathsf{E}_{G,\Sigma}$) is polynomially/exponentially bounded. On the other hand, we might simplify the notation to K_G (resp., E_G).

In Chapter 10 we do not care about the degree of the knapsack equations and hence we use the functions $\hat{\mathsf{K}}_{G,\Sigma}(n) = \mathsf{K}_{G,\Sigma}(n,n)$ and $\hat{\mathsf{E}}_{G,\Sigma}(n) = \mathsf{E}_{G,\Sigma}(n,n)$, where we do not specify the degree. For simplicity, we just write $\mathsf{K}_{G,\Sigma}$ (resp., $\mathsf{E}_{G,\Sigma}$), if it is clear from the context.

Furthermore we will need the following lemma:

Lemma 3.6. *Let G be knapsack-semilinear and let*

$$e = v_0 (u_1^{k_1})^{x_1} v_1 (u_2^{k_2})^{x_2} v_2 \cdots (u_d^{k_d})^{x_d} v_d$$

be an exponent expression over G where $k_1, \ldots, k_d \leq k$ and $|v_0 u_1 v_1 \cdots u_d v_d| = n$. Then the magnitude of $\mathsf{sol}_G(e)$ is $(n \cdot \max\{\hat{\mathsf{K}}_G(n), k\} + 1)^{\mathcal{O}(n)}$.

Proof. Let $X = \{x_1, \ldots, x_d\}$ (some of the variables x_i might be equal) and $Y = \{y_1, \ldots, y_d\}$ be a set of d *distinct* variables. Then $\nu\colon X \to \mathbb{N}$ is a solution of $e = 1$ if and only if $\mu\colon Y \to \mathbb{N}$ is a solution of $e' = v_0 u_1^{y_1} v_1 u_2^{y_2} v_2 \cdots u_d^{y_d} v_d = 1$ where $\mu(y_i) = k_i \nu(x_i)$. Notice that e' is a knapsack expression. Hence $\mathsf{sol}_G(e)$ can be obtained as a projection of the intersection of $\mathsf{sol}_G(e')$ with a semilinear set of magnitude $\leq k$ (it has to ensure that $\mu(y_i)$ is a multiple of k_i and that $\mu(y_i)/k_i = \mu(y_j)/k_j$ whenever $x_i = x_j$). Therefore

$$\mathsf{mag}(\mathsf{sol}_G(e)) = (n \cdot \max\{\hat{\mathsf{K}}_G(n), k\} + 1)^{\mathcal{O}(n)}.$$

□

3.4 Relative knapsack-semilinearity

Let $S \subseteq G$ for a finitely generated group G with the finite generating set Σ. We say that G is *knapsack-semilinear relative to* S if for every knapsack expression e over Σ, the set $\{\nu : X_e \to \mathbb{N} \mid \nu(e) \in_G S\}$ is a semilinear set of vectors and a semilinear representation can be effectively computed from e. We are mainly interested in the case where S is a subgroup of G. For sets $S_1, \ldots, S_k \subseteq G$ we say that G is knapsack-semilinear relative to $\{S_1, \ldots, S_k\}$ if for every $1 \leq i \leq k$, G is knapsack-semilinear relative to S_i. Note that G is knapsack-semilinear if and only if it is knapsack-semilinear relative to 1.

Chapter 4

Main results of the thesis

In this chapter we collect all main theorems of this thesis. There are several corollaries from these theorems, which we will discuss in the respective chapters.

The following theorem can be found in Chapter 5.

Theorem 4.1 ([F6]). *Let G be a finitely generated group with a finite symmetric generating set Σ and let H be a finite extension of G (hence, it is finitely generated too) with the finite symmetric generating set $\Sigma' = \Sigma \cup (C \setminus \{1\}) \cup (C \setminus \{1\})^{-1}$, where C is a set of coset representatives with $1 \in C$. Let $\ell = |C|$ be the index of G in H. If G is knapsack-semilinear then H is knapsack-semilinear too and we have the bounds*

$$\begin{aligned} \mathsf{E}_{H,\Sigma'}(n,m) &\leq \ell \cdot \mathsf{E}_{G,\Sigma}(\mathcal{O}(\ell^2 n), m) + 2\ell, \\ \mathsf{K}_{H,\Sigma'}(n,m) &\leq \ell \cdot \mathsf{K}_{G,\Sigma}(\mathcal{O}(\ell^2 n), m) + 2\ell. \end{aligned}$$

The next two theorems are discussed in Chapter 6.

Theorem 4.2 ([F6]). *We denote with α the size of a largest independence clique in the finite graph (Γ, E). If each group G_i, $i \in \Gamma$, is knapsack-semilinear, then their graph product $G = G(\Gamma, E, (G_i)_{i\in\Gamma})$ is knapsack-semilinear as well. Let $\mathsf{K} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the pointwise maximum of the functions $\mathsf{K}_{G_i,\Sigma_i}(n,m)$ for $i \in \Gamma$. Then $\mathsf{E}_{G,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2\}$ with*

$$\begin{aligned} \mathsf{K}_1 &\leq \mathcal{O}\big((\alpha m)^{\alpha m/2+3} \cdot \mathsf{K}(6\alpha m n, \alpha m)^{\alpha m+3}\big), \\ \mathsf{K}_2 &\leq (\alpha m)^{\mathcal{O}(\alpha^2 m)} \cdot n^{\mathcal{O}(\alpha^2 |\Gamma| m)}. \end{aligned}$$

Theorem 4.3 ([F6]). *If the groups G_1 and G_2 are knapsack-semilinear, then $G_1 * G_2$ is knapsack-semilinear as well. Let $\mathsf{K}(n,m)$ be the pointwise maximum of the functions $\mathsf{K}_{G_1,\Sigma_1}$ and $\mathsf{K}_{G_2,\Sigma_2}$. Then for $G = G_1 * G_2$ we have $\mathsf{K}_{G,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2\}$ with*

$$\mathsf{K}_1 = \mathsf{K}(6mn, m) \text{ and } \mathsf{K}_2 \leq \mathcal{O}(mn^4).$$

In Chapter 7 we deal with these two theorems.

Theorem 4.4 ([F6]). *Let A, B be finite subgroups of G and let $\varphi\colon A \to B$ be an isomorphism. If G is knapsack-semilinear, then the HNN-extension H of G (with respect to the isomorphism φ) is knapsack-semilinear as well. Moreover, we have $\mathsf{K}_{H,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2\}$ with*

$$\mathsf{K}_1 = \mathsf{K}_{G,\Sigma}(24mn, m) \text{ and } \mathsf{K}_2 \leq \mathcal{O}(\gamma^2 mn^4),$$

where $\gamma = |A|$.

Theorem 4.5 ([F6]). *Let G_1 and G_2 be finitely generated groups with a common subgroup A. Let $\mathsf{K}(n,m)$ be the pointwise maximum of the functions $\mathsf{K}_{G_1,\Sigma_1}$ and $\mathsf{K}_{G_2,\Sigma_2}$. Furthermore, let $\gamma = |A|$ and let G be the amalgamated product $G_1 *_A G_2$. Then with $\Sigma = \Sigma_1 \cup \Sigma_2$ we have $\mathsf{K}_{G,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2, \mathsf{K}_3\}$ where*

$$\mathsf{K}_1 = \mathsf{K}_{G,\Sigma}(144m^2n, m), \mathsf{K}_2 \leq \mathcal{O}(m^5n^4) \text{ and } \mathsf{K}_3 \leq \mathcal{O}(m \cdot \gamma^2 \cdot n^4).$$

The following two theorems are analyzed in Chapter 8.

Theorem 4.6 ([F4]). *Let $H = \langle G, t \mid t^{-1}at = a \ (a \in A)\rangle$ be an HNN-extension, where G is knapsack-semilinear relative to $\{1, A\}$. Then H is knapsack-semilinear.*

Theorem 4.7 ([F4]). *If G is knapsack-semilinear and H is an extension of a centralizer $C(S)$ with S finite, then H is knapsack-semilinear as well.*

Chapter 9 contains the next three theorems.

Theorem 4.8. *A central extension of a hyperbolic group is knapsack-semilinear.*

Theorem 4.9. *Let H be a central extension of the hyperbolic group G and let $\pi : H \to G$ be the canonical projection. Let $Q \leq G$ be a quasiconvex subgroup of G. Then the HNN-extension $\langle H, t \mid t^{-1}at = a \ (a \in \pi^{-1}(Q))\rangle$ is knapsack-semilinear.*

For the special case $G = H$ we obtain:

Theorem 4.10 ([F4]). *Let G be hyperbolic and $A \leq G$ be a quasiconvex subgroup of G. Then the HNN-extension $\langle G, t \mid t^{-1}at = a \ (a \in A)\rangle$ is knapsack-semilinear.*

Finally, in Chapter 10 we prove these two theorems.

Theorem 4.11 ([F3]). *Let the f.g. group $G = \langle \Sigma \rangle$ be uniformly SENS. Then, $\textsc{Knapsack}(G \wr \mathbb{Z})$ is Σ_2^p-hard.*

Theorem 4.12. *Let $SL_3(\mathbb{Z})$ be the special linear group consisting of all 3×3 matrices over $\mathbb{Z}$ with determinant 1 (equipped with matrix multiplication). It is undecidable if a single exponent equation over $SL_3(\mathbb{Z})$ has a solution.*

Chapter 5

Finite extensions

5.1 Introduction

In this short chapter, we show that knapsack-semilinearity is preserved under one of the most simple group constructions, the finite extensions. We say that H is a *finite extension of* G if G is a finite-index subgroup of H. We also prove transfer result Theorem 5.1, which allows to reduce $\textsc{Knapsack}(H)$ to $\textsc{Knapsack}(G)$ nondeterministically in polynomial time.

5.2 Finite extensions preserve knapsack-semilinearity

First we give a proof of

Theorem 4.1 ([F6])**.** *Let G be a finitely generated group with a finite symmetric generating set Σ and let H be a finite extension of G (hence, it is finitely generated too) with the finite symmetric generating set $\Sigma' = \Sigma \cup (C \setminus \{1\}) \cup (C \setminus \{1\})^{-1}$, where C is a set of coset representatives with $1 \in C$. Let $\ell = |C|$ be the index of G in H. If G is knapsack-semilinear then H is knapsack-semilinear too and we have the bounds*

$$\mathsf{E}_{H,\Sigma'}(n,m) \leq \ell \cdot \mathsf{E}_{G,\Sigma}(\mathcal{O}(\ell^2 n), m) + 2\ell, \tag{5.1}$$

$$\mathsf{K}_{H,\Sigma'}(n,m) \leq \ell \cdot \mathsf{K}_{G,\Sigma}(\mathcal{O}(\ell^2 n), m) + 2\ell. \tag{5.2}$$

Proof. Suppose we are given an exponent expression

$$e = u_1^{x_1} v_1 \cdots u_m^{x_m} v_m \tag{5.3}$$

in H where the u_i and v_i are words over Σ'. Let n be the length of e. We need to show that the solution set is semilinear and that it can be effectively computed (using that G is knapsack-semilinear). Our algorithm to compute such a semilinear representation will make some nondeterministic guesses.

As a first step, we guess which of the variables x_i assume a value smaller than ℓ. For those that do, we can guess the value and merge the resulting power with the v_i on the right. This increases the size of the instance by at most a factor of ℓ, which is a constant. At the end we will compensate this by applying the substitution $n \mapsto \ell n$. Hence, from now on, we only look for H-solutions ν to e where $\nu(x_i) \geq \ell$ for $1 \leq i \leq m$.

Next we guess the cosets of the prefixes of $u_1^{x_1} v_1 \cdots u_m^{x_m} v_m$, i.e., we guess coset representatives $c_1, d_1, \ldots, c_{m-1}, d_{m-1}, c_m \in C$ and restrict to H-solutions ν to e such that $u_1^{\nu(x_1)} v_1 \cdots u_i^{\nu(x_i)} \in G c_i$ and $u_1^{\nu(x_1)} v_1 \cdots u_i^{\nu(x_i)} v_i \in G d_i$ for $1 \leq i \leq m$. Here, we set $d_m = 1$. Equivalently, we only consider H-solutions ν where $d_{i-1} u_i^{x_i} c_i^{-1}$ and $c_i v_i d_i^{-1}$ all belong to G for $1 \leq i \leq m$. Here, we set $d_0 = 1$. We can verify in polynomial time that all $c_i v_i d_i^{-1}$ $(1 \leq i \leq m)$ belong to G. It remains to describe the set of all H-solutions ν for e that fulfill the following constraints for all $1 \leq i \leq m$:

$$d_{i-1} u_i^{\nu(x_i)} c_i^{-1} \in G \text{ and } \nu(x_i) \geq \ell. \tag{5.4}$$

For $1 \leq i \leq m$ consider the function $f_i \colon C \to C$, which is defined so that for each $c \in C$, $f_i(c)$ is the unique element $d \in C$ with $c u_i d^{-1} \in G$. Note that we can compute f_i in polynomial time if G and H are fixed groups (all we need for this is a table that specifies for each $c \in C$ and $a \in \Sigma'$ the coset representative of ca; this is a fixed table that does not depend on the input). Then there are numbers $1 \leq k_i \leq \ell$ such that $f_i^{\ell+k_i}(d_{i-1}) = f_i^{\ell}(d_{i-1})$. With this notation, we have $d_{i-1} u_i^z c_i^{-1} \in G$ if and only if $f_i^z(d_{i-1}) = c_i$ for all $z \in \mathbb{N}$.

We may assume that there is a $z \geq \ell$ with $f_i^z(d_{i-1}) = c_i$; otherwise, there is no H-solution for e fulfilling the above constraints (5.4) and we have a bad guess. Therefore, there is a $0 \leq r_i < k_i$ such that $f_i^{\ell+r_i}(d_{i-1}) = c_i$. This means that for all $z \geq \ell$, we have $d_{i-1} u_i^z c_i^{-1} \in G$ if and only if $f_i^z(d_{i-1}) = c_i$ if and only if $z = \ell + k_i \cdot y + r_i$ for some $y \geq 0$. This allows us to construct an exponent expression over G.

Let $e_i = f_i^{\ell}(d_{i-1})$. Then, the words $d_{i-1} u_i^{\ell} e_i^{-1}$, $e_i u_i^{k_i} e_i^{-1}$, and $e_i u_i^{r_i} c_i^{-1}$ all represent elements of G. Moreover, for all $y_i \geq 0$ and $z_i = \ell + k_i \cdot y_i + r_i$ $(1 \leq i \leq m)$, we have

$$\begin{aligned} u_1^{z_1} v_1 \cdots u_m^{z_m} v_m &= \prod_{i=1}^{m} d_{i-1} u_i^{\ell + k_i \cdot y_i + r_i} c_i^{-1} c_i v_i d_i^{-1} \\ &= \prod_{i=1}^{m} (d_{i-1} u_i^{\ell} e_i^{-1})(e_i u_i^{k_i} e_i^{-1})^{y_i} (e_i u_i^{r_i} c_i^{-1} c_i v_i d_i^{-1}) \end{aligned}$$

and each word in parentheses represents an element of G. Hence, we can define the exponent expression

$$e' = \prod_{i=1}^{m} (d_{i-1} u_i^{\ell} e_i^{-1})(e_i u_i^{k_i} e_i^{-1})^{x_i} (e_i u_i^{r_i} v_i d_i^{-1})$$

over the group G. From the above consideration we obtain

$$\begin{aligned}&\mathsf{sol}_H(e) \cap \{\nu : X_e \to H \mid \nu \text{ satisfies the constraints (5.4)}\} = \\ &\{\nu \mid \nu(x_i) = k_i \cdot \nu'(x_i) + (\ell + r_i) \text{ for some } \nu' \in \mathsf{sol}_G(e')\}. \qquad (5.5)\end{aligned}$$

The set in (5.5) is semilinear by assumption and since all k_i and r_i are bounded by ℓ, we can bound its magnitude by $\ell \cdot \mathsf{mag}(\mathsf{sol}_G(e')) + 2\ell$. Moreover, we have $\deg(e') = \deg(e)$. It remains to bound $\|e'\|$. For this, we first have to rewrite the words $d_{i-1}u_i^\ell e_i^{-1}$, $e_i u_i^{k_i} e_i^{-1}$, and $e_i u_i^{r_i} v_i d_i^{-1}$ (which represent elements of G) into words over Σ. This increases the length of the words only by a constant factor: for every $c \in C$ and every generator $a \in \Sigma'$ there exists a fixed word $w_{c,a} \in \Sigma^*$ and $d_{c,a} \in C$ such that $ca = w_{c,a}d_{c,a}$ holds in H. After this rewriting we have $\|e'\| \leq \mathcal{O}(\ell n)$, which implies $\mathsf{mag}(\mathsf{sol}_G(e')) \leq \mathsf{E}_{G,\Sigma}(\mathcal{O}(\ell n), m)$. This yields the bound $\ell \cdot \mathsf{E}_{G,\Sigma}(\mathcal{O}(\ell n), m) + 2\ell$ for the magnitude of the semilinear set in (5.5). Applying the substitution $n \mapsto \ell n$ from the first step finally yields (5.1). The corresponding bound (5.2) for knapsack expressions can be shown in the same way: Note that in the above transformation of e into e' we do not duplicate variables. □

From the above proof and Lemma 2.3 we also obtain the following complexity transfer result:

Theorem 5.1. *The knapsack problem for a finite extension of a group G is nondeterministically polynomial time reducible to* Knapsack(G).

The consequence of Theorem 5.1 that solvability of the knapsack problem in NP is passed on from G to finite extensions of G has also appeared in the extended abstract of [67].

5.3 Open problems

Despite Theorem 5.1, it is not known, if there exists a finitely generated group G with a finite extension H, such that Knapsack(G) is in P, but Knapsack(H) is NP-complete.

Chapter 6

Graph products

6.1 Introduction

We show that every graph product of knapsack-semilinear groups is again knapsack-semilinear (Section 6.6). Furthermore we will derive bounds for the magnitude. This leads to Theorem 4.2, from which we conclude Theorem 4.3. The latter one is a special case, where we have the most simple graph product $G = G_1 * G_2$ (where G is just a free product of two groups).

As an application of Theorem 4.2, we obtain Theorem 6.21, which states that ExpEq(G) belongs to NP, if G is a graph product of hyperbolic groups. A corollary of the proof of Theorem 4.3 is Theorem 6.24, where we derive that in case of $G = G_1 * G_2$, Knapsack(G) is nondeterministically polynomial time reducible to Knapsack(G_1) and Knapsack(G_2).

The proof techniques used in this chapter, where we break down knapsack equations into smaller two-dimensional pieces and deal with 1-reducible refinements of sequences (defined in Section 6.5) are also used in Chapter 7 and Chapter 8. In Chapter 8 however, we do not obtain bounds on the magnitudes for the HNN-extensions.

6.2 Further definitions

Recall that for a trace $t \in \mathbb{M}(A, I)$, $\mathsf{alph}(t) \subseteq A$ is the set of symbols that occur in t. We define the Γ-*alphabet* of t as

$$\mathsf{alph}_\Gamma(t) = \{i \in \Gamma \mid \mathsf{alph}(t) \cap A_i \neq \emptyset\}.$$

Note that whether $u \; I \; v$ (for $u, v \in \mathbb{M}(A, I)$) only depends on $\mathsf{alph}_\Gamma(u)$ and $\mathsf{alph}_\Gamma(v)$.

Every independence clique of (A, I) has size at most α and hence can be identified with a trace from $\mathbb{M}(A, I)$. Let C_1 and C_2 be independence cliques. We say that C_1 and C_2 are *compatible*, if $\mathsf{alph}_\Gamma(C_1) = \mathsf{alph}_\Gamma(C_2)$. In this case we can write $C_1 = \{a_1, \ldots, a_m\}$ and $C_2 = \{b_1, \ldots, b_m\}$ for some $m \leq \alpha$ such that

for every $1 \leq i \leq m$ there exists $j_i \in \Gamma$ with $a_i, b_i \in A_{j_i}$. Let $c_i = a_i b_i$ in the group G_{j_i}. If $c_i \neq 1$ for all $1 \leq i \leq m$, then C_1 and C_2 are *strongly compatible*. In this case we define the independence clique $C_1 C_2 = \{c_1, \ldots, c_m\}$. Note that $\mathsf{alph}_\Gamma(C_1) = \mathsf{alph}_\Gamma(C_2) = \mathsf{alph}_\Gamma(C_1 C_2)$.

Also we will write G for the graph product $G(\Gamma, E, (G_i)_{i \in \Gamma})$ in this chapter as defined in Subsection 2.4.2. Moreover, we use all notations from Subsection 2.4.2.

6.3 Results from [68]

In this section we state a small modification of results from [68], where the statements are made for finitely generated trace monoids $\mathbb{M}(\Sigma, I)$. We need the corresponding statements for the non-finitely generated trace monoid $\mathbb{M}(A, I)$ from Subsection 2.4.2. The proofs are exactly the same as in [68], one only has to argue with the Γ-alphabet $\mathsf{alph}_\Gamma(t)$ instead the alphabet $\mathsf{alph}(t)$ of traces.

Note that all statements in this section refer to the trace monoid $\mathbb{M}(A, I)$ and not to the corresponding graph product G. In particular, when we write a product $t_1 t_2 \cdots t_n$ of traces $t_i \in \mathbb{M}(A, I)$ no cancellation occurs between the t_i. We will also consider the case that $E = \emptyset$ (and hence $I = \emptyset$), in which case $\mathbb{M}(A, I) = A^*$.

Let $s, t \in \mathbb{M}(A, I)$ be traces. We say that s is a *prefix* of t if there is a trace $r \in \mathbb{M}(A, I)$ with $sr = t$. Moreover, we define $\rho(t)$ as the number of prefixes of t. We will use the following statement from [10].

Lemma 6.1. *Let $t \in \mathbb{M}(A, I)$ be a trace of length n. Then $\rho(t)$ is bounded by $\mathcal{O}(n^\alpha) \leq \mathcal{O}(n^{|\Gamma|})$, where α is the size of a largest clique of the independence alphabet (Γ, E).*

Remark 6.2. It is easy to see that $\rho(t) = n + 1$ if $E = \emptyset$.

Lemma 6.3. *Let $u \in \mathbb{M}(A, I) \setminus \{1\}$ be a connected trace and $m \in \mathbb{N}$, $m \geq 2$. Then, for all $x \in \mathbb{N}$ and traces $y_1, \ldots, y_m$ the following two statements are equivalent:*

(i) $u^x = y_1 y_2 \cdots y_m$.

(ii) There exist traces $p_{i,j}$ $(1 \leq j < i \leq m)$, s_i $(1 \leq i \leq m)$ and numbers $x_i, c_j \in \mathbb{N}$ $(1 \leq i \leq m,\ 1 \leq j \leq m-1)$ such that:

- $y_i = (\prod_{j=1}^{i-1} p_{i,j}) u^{x_i} s_i$ *for all* $1 \leq i \leq m$,
- $p_{i,j}\ I\ p_{k,\ell}$ *if* $j < \ell < k < i$ *and* $p_{i,j}\ I\ (u^{x_k} s_k)$ *if* $j < k < i$,[5]
- $s_m = 1$ *and for all* $1 \leq j < m$, $s_j \prod_{i=j+1}^{m} p_{i,j} = u^{c_j}$,
- $c_j \leq |\Gamma|$ *for all* $1 \leq j \leq m-1$,
- $x = \sum_{i=1}^{m} x_i + \sum_{i=1}^{m-1} c_i$.

[5] Note that since $\mathsf{alph}(p_{i,j}) \subseteq \mathsf{alph}(u)$, we must have $p_{i,j} = 1$ or $x_k = 0$ whenever $j < k < i$.

Note that this implies $\mathsf{alph}_\Gamma(p_{i,j}) \cup \mathsf{alph}_\Gamma(s_i) \subseteq \mathsf{alph}_\Gamma(u)$ for $1 \leq j < i \leq m$.

The proof of Lemma 6.3 is the same as for [68, Lemma 3.3], where the statement is shown for the case of a finite independence alphabet (A, I). In our situation the independency between traces only depends on their Γ-alphabets. This allows to carry over the proof of [68, Lemma 3.3] to our situation by replacing the alphabet $\mathsf{alph}(t)$ of a trace $t \in \mathbb{M}(A, I)$ by $\mathsf{alph}_\Gamma(u)$.

Remark 6.4. In Section 6.6 we will apply Lemma 6.3 in order to replace an equation $u^x = y_1 y_2 \cdots y_m$ (where $x, y_1, \ldots, y_m$ are variables and u is a concrete connected trace) by an equivalent disjunction. Note that the length of all factors $p_{i,j}$ and s_i in Lemma 6.3 is bounded by $|\Gamma| \cdot |u|$ and that $p_{i,j}$ and s_i only contain symbols from u. Hence, one can guess these traces as well as the numbers $c_j \leq |\Gamma|$ (the guess results in a disjunction). We can also guess which of the numbers x_i are zero and which are greater than zero (let K consists of those i such that $x_i > 0$). After these guesses we can verify the independencies $p_{i,j}\ I\ p_{k,\ell}$ $(j < \ell < k < i)$ and $p_{i,j}\ I\ (u^{x_k} s_k)$ $(j < k < i)$, and the identities $s_m = 1$, $s_j \prod_{i=j+1}^{m} p_{i,j} = u^{c_j}$ $(1 \leq j < m)$. If one of them does not hold, the specific guess does not contribute to the disjunction. In this way, we can replace the equation $u^x = y_1 y_2 \cdots y_m$ by a disjunction of formulas of the form

$$\exists x_i > 0\ (i \in K) : x = \sum_{i \in K} x_i + c \wedge \bigwedge_{i \in K} y_i = p_i u^{x_i} s_i \wedge \bigwedge_{i \in [1,m] \setminus K} y_i = p_i s_i,$$

where $K \subseteq [1, m]$, $c \leq |\Gamma| \cdot (m-1)$ and the p_i, s_i are concrete traces of length at most $|\Gamma| \cdot (m-1) \cdot |u|$. The number of disjuncts in the disjunction will not be important for our purpose.

Lemma 6.5. *Let $p, q, u, v, s, t \in \mathbb{M}(A, I)$ with $u \neq 1$ and $v \neq 1$ connected. Let $m = \max\{\rho(p), \rho(q), \rho(s), \rho(t)\}$ and $n = \max\{\rho(u), \rho(v)\}$. Then the set*

$$L(p, u, s, q, v, t) = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid pu^x s = qv^y t\}$$

is a union of $\mathcal{O}(m^8 \cdot n^{4|\Gamma|})$ many linear sets of the form $\{(a + bz, c + dz) \mid z \in \mathbb{N}\}$ with $a, b, c, d \leq \mathcal{O}(m^8 \cdot n^{4|\Gamma|})$. In particular, $L(p, u, s, q, v, t)$ is semilinear. If $|\Gamma|$ is a fixed constant, then a semilinear representation for $L(p, u, s, q, v, t)$ can be computed in polynomial time.

Again, the proof of Lemma 6.5 is exactly the same as the proof of [68, Lemma 3.8]. One simply substitutes $|A|$ by $|\Gamma|$ and $\mathsf{alph}(x)$ by $\mathsf{alph}_\Gamma(x)$.

We will also use the following simplified version of the previous lemma:

Lemma 6.6. *Let $p, q, r, s, u, v \in \Sigma^*$. Then the set*

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid pq^x r = su^y v\}$$

is semilinear and a semilinear representation can be computed from p, q, r, s, u, v.

Remark 6.7. Let us consider again the case $E = I = \emptyset$ in Lemma 6.5. Let $m = \max\{|p|, |q|, |s|, |t|, |u|, |v|\}$. We can construct an automaton accepting pu^*s

of size at most $3m$ and similarly for qv^*t. Hence, we obtain an automaton of size $\mathcal{O}(m^2)$ accepting the language $L = pu^*s \cap qv^*t$. We are only interested in the length of words from L. Let $\mathcal{A}$ be the automaton obtained from the automaton for L by replacing every transition label by the symbol a. The resulting automaton $\mathcal{A}$ is defined over a unary alphabet. Let $P = \{n \mid a^n \in L(\mathcal{A})\}$. By [87, Theorem 1], the set P can be written as a union

$$P = \bigcup_{i=1}^{r} \{b_i + c_i \cdot z \mid z \in \mathbb{N}\}$$

with $r \in \mathcal{O}(m^4)$ and $b_i, c_i \in \mathcal{O}(m^4)$. For every $1 \leq i \leq r$ and $z \in \mathbb{N}$ there must exist a pair $(x, y) \in \mathbb{N} \times \mathbb{N}$ such that

$$b_i + c_i \cdot z = |ps| + |u| \cdot x = |qt| + |v| \cdot y.$$

In particular, $b_i \geq |ps|$, $b_i \geq |qt|$, $|u|$ divides $b_i - |ps|$ and c_i, and $|v|$ divides $b_i - |qt|$ and c_i. We get

$$L(p, u, s, q, v, t) = \bigcup_{i=1}^{r} \left\{ \left(\frac{b_i - |ps|}{|u|} + \frac{c_i}{|u|} \cdot z, \frac{b_i - |qt|}{|v|} + \frac{c_i}{|v|} \cdot z \right) \;\middle|\; z \in \mathbb{N} \right\}$$

and all numbers that appear on the right-hand side are bounded by $\mathcal{O}(m^4)$.

6.4 Irreducible powers in graph products

In this section, we study powers u^n for an irreducible trace $u \in \mathsf{IRR}(R)$. We need the following definitions: A trace $u \in \mathbb{M}(A, I)$ is called *cyclically reduced* if $u \in \mathsf{IRR}(R)$ and there do not exist $a \in A$ and $v \in \mathbb{M}(A, I)$ such that $u = ava^{-1}$. A trace $t \in \mathbb{M}(A, I)$ is called *well-behaved* if it is connected and $t^m \in \mathsf{IRR}(R)$ for every $m \geq 0$.

Lemma 6.8. *Let $u \in \mathsf{IRR}(R)$. If $u^2 \in \mathsf{IRR}(R)$ then $u^m \in \mathsf{IRR}(R)$ for all $m \geq 0$.*

Proof. Assume that $m \geq 3$ is the smallest number, such that $u^{m-1} \in \mathsf{IRR}(R)$ and $u^m \notin \mathsf{IRR}(R)$. Hence we can write $u^m = xaby$ with $x, y \in \mathsf{IRR}(R)$ and $a, b \in A_i$ for some $i \in \Gamma$. Applying Levi's lemma, we get factorizations $x = x_1 x_2 \cdots x_m$ and $y = y_1 y_2 \cdots y_m$ and the following diagram:

y	y_1	y_2	$\cdots$	y_{m-1}	y_m
b			$\cdots$		b
a	a		$\cdots$		
x	x_1	x_2	$\cdots$	x_{m-1}	x_m
	u	u	$\cdots$	u	u

This is in fact the only possibility for the positions of the atoms a and b: If a and b were in the same column then u would contain the factor ab and hence $u \notin \mathsf{IRR}(u)$. Also a and b are not independent, which means b has to

be top-right from a. If a is not in the first column or b is not in the last column, then u^{m-1} is reducible, which contradicts the choice of m. Hence, we have $u = x_1 a y_1 = x_m b y_m$ with $a \ I \ x_m$, $y_1 \ I \ x_m$ and $b \ I \ y_1$. We get $u^2 = x_1 a y_1 x_m b y_m = x_1 a x_m y_1 b y_m = x_1 x_m a y_1 b y_m = x_1 x_m a b y_1 y_m$. Hence $u^2 \notin \mathsf{IRR}(R)$, which is a contradiction. □

Lemma 6.9. *A trace $u \in \mathbb{M}(A, I)$ is well-behaved if and only if it has the following properties:*

- *u is irreducible,*
- *u is not atomic,*
- *u is connected, and*
- *one cannot write u as $u = avb$ such that $a, b \in A_i$ for some $i \in \Gamma$ (in particular, u is cyclically reduced).*

Proof. Clearly, if one the four conditions in the lemma is not satisfied, then u is not well-behaved. Now assume that the four conditions hold for u. By Lemma 6.8, it suffices to show that $u^2 \in \mathsf{IRR}(R)$. Assume that $u^2 = xaby$ with $a, b \in A_i$. Applying Levi's lemma, and using $u \in \mathsf{IRR}(R)$ and $(a, b) \notin I$, we obtain the following diagram:

y	y_1	y_2
b		b
a	a	
x	x_1	x_2
	u	u

From Levi's lemma we also get $b \ I \ y_1$ and $a \ I \ x_2$. But a and b are in the same group, hence $a \ I \ y_1$ and $b \ I \ x_2$ also hold. The first property implies $u = va$ with $v = x_1 y_1$ and the seconds property gives us $u = bw$ with $w = x_2 y_2$. Since u is not atomic, we have $v \neq 1 \neq w$. Now we apply Levi's lemma to $va = bw$, which yields one of the following diagrams:

w	$v = w$	
b		$a = b$
	v	a

w	w'	a
b	b	
	v	a

From the left diagram we get $a \ I \ v$. Hence $u = va$ is not connected, which is a contradiction. From the right diagram we get $u = va = bw'a$ for some trace w', which is a contradiction to our last assumption. This finally proves $u^2 \in \mathsf{IRR}(R)$, hence u is well-behaved. □

Lemma 6.10. *From a trace $u \in \mathbb{M}(A, I)$ one can compute traces $s, t, v_1, \ldots, v_k \in \mathsf{IRR}(R)$, such that the following hold:*

- *every v_i is either atomic or well-behaved,*
- *$u^m =_G s v_1^m \cdots v_k^m t$ for all $m \geq 0$,*
- *$\|s\| + \|t\| + \sum_{i=1}^{k} \|v_i\| \leq 3\|u\|$,*
- *$k \leq \alpha$, where α is the size of a largest clique in (Γ, E).*

Proof. Let $u \in \mathbb{M}(A, I)$. As an initial processing, we can replace every u by $\mathsf{NF}_R(u) \in \mathsf{IRR}(R)$. So we can assume that u is already irreducible. In the next step, we compute irreducible traces s, w, t, such that $u^m =_G sw^m t$ for all $m \geq 0$ and w cannot be written as $w = aw'b$ with $a, b \in A_j$ for some $j \in \Gamma$. For this, we will inductively construct irreducible traces s_i, u_i, t_i (with $0 \leq i \leq \ell$ for some ℓ) such that $u^m =_G s_i u_i^m t_i$ for all $m \geq 0$. Moreover, if $0 \leq i < \ell$ then $|u_i| > |u_{i+1}|$. We start with $u_0 = u$ and $s_0 = t_0 = 1$. Assume that after i steps we already found irreducible traces s_i, u_i, t_i with $u^m =_G s_i u_i^m t_i$ for all $m \geq 0$. If u_i cannot be written in the form $au'b$ with $a, b \in A_j$ for some j, then we are done. Otherwise assume that $u_i = av_ib$ for some $a, b \in A_j$. Let $c \in A_j \cup \{1\}$ such that $c = ba$ in the group G_j. So we get $u_i^m =_G a(v_ic)^m a^{-1}$ for all $m \geq 0$. This means $u^m =_G (s_ia)(v_ic)^m(a^{-1}t_i)$. Hence, we can set $u_{i+1} = v_ic$, $s_{i+1} = \mathsf{NF}_R(s_ia)$ and $t_{i+1} = \mathsf{NF}_R(a^{-1}t_i)$. Note that $|u_{i+1}| = |u_i| - 1$, $\|u_{i+1}\| \leq \|u_i\|$, $\|s_{i+1}\| \leq \|s_i\| + \|a\|$, and $\|t_{i+1}\| \leq \|t_i\| + \|a\|$. This process is terminating after at most $|u|$ steps. Note also that each u_{i+1} is irreducible. When our algorithm is terminating after step ℓ, we set $v = u_\ell$, $s = s_\ell$ and $t = t_\ell$. We have

$$\|s\|, \|t\|, \|v\| \leq \|u\|. \tag{6.1}$$

Finally, we split v into its connected components, i.e., we write $v = v_1 \cdots v_k$, where every v_j is connected and $v_i \; I \; v_j$ for $i \neq j$. We obtain for every $m \geq 0$ the identity $u^m =_G sv_1^m \cdots v_k^m t$ as described in the statement of the lemma. If a v_j is not atomic then it cannot be written as $v_j = bv_j'c$ with $b, c \in A_i$ (otherwise the above reduction process would continue). Thus Lemma 6.9 implies that the non-atomic v_j are well-behaved. Finally, we have $\sum_{i=1}^k \|v_i\| = \|v\| \leq \|u\|$ by (6.1). □

Remark 6.11. If $E = \emptyset$ then we must have $k = 1$ in Lemma 6.10 since $\alpha = 1$. Hence, we obtain s, t, v, where v is either atomic or well-behaved, such that $u^m = sv^m t$ for every $m \geq 0$ and $\|s\| + \|v\| + \|t\| \leq 3\|u\|$.

6.5 Reductions to the empty trace

For the normal form of the product of two R-irreducible traces we have the following lemma, which was shown in [23] (equation (21) in the proof of Lemma 22) using a slightly different notation.

Lemma 6.12. *Let $u, v \in \mathbb{M}(A, I)$ be R-irreducible. Then there exist strongly compatible independence cliques C, D and unique factorizations $u = pCs$, $v = s^{-1}Dt$ such that $\mathsf{NF}_R(uv) = p(CD)t$.*

In the following, we consider tuples over $\mathsf{IRR}(R)$ of arbitrary length. We identify tuples that can be obtained from each other by inserting/deleting 1's at arbitrary positions. Clearly, every tuple is equivalent to a possibly empty tuple over $\mathsf{IRR}(R) \setminus \{1\}$.

Definition 6.13. We define a reduction relation on tuples over $\mathsf{IRR}(R)$ of arbitrary length. Take $u_1, u_2, \ldots, u_m \in \mathsf{IRR}(R)$. Then we have

- $(u_1, u_2, \ldots, u_m) \to (u_1, \ldots, u_{i-1}, u_{i+1}, u_i, u_{i+2}, \ldots, u_m)$ if $u_i \; I \; u_{i+1}$ (a *swapping step*),
- $(u_1, u_2, \ldots, u_m) \to (u_1, \ldots, u_{i-1}, u_{i+2}, \ldots, u_m)$ if $u_i = u_{i+1}^{-1}$ in $\mathbb{M}(A, I)$ (a *cancellation step*),
- $(u_1, u_2, \ldots, u_m) \to (u_1, \ldots, u_{i-1}, a, u_{i+2}, \ldots, u_m)$ if there exists $j \in \Gamma$ with $u_i, u_{i+1}, a \in A_j$, and $a = u_i u_{i+1}$ in G_j (an *atom creation step of type* j).

Moreover, these are the only reduction steps. A concrete sequence of these rewrite steps leading to the empty tuple is a *reduction* of $(u_1, u_2, \ldots, u_m)$. If such a sequence exists, the tuple is called 1*-reducible*.

A reduction of the tuple $(u_1, u_2, \ldots, u_m)$ can be seen as a witness for the fact that $u_1 u_2 \cdots u_m =_G 1$. On the other hand, $u_1 u_2 \cdots u_m =_G 1$ does not necessarily imply that $(u_1, u_2, \ldots, u_m)$ has a reduction. For instance, the tuple (a^{-1}, ab, b^{-1}) has no reduction. But we can show that every sequence which multiplies to 1 in G can be refined (by factorizing the elements of the sequence) such that the resulting refined sequence has a reduction. We say that the tuple $(v_1, v_2, \ldots, v_n)$ is a *refinement* of the tuple $(u_1, u_2, \ldots, u_m)$ if there exists factorization $u_i = u_{i,1} \cdots u_{i,k_i}$ in $\mathbb{M}(A, I)$ such that $(v_1, v_2, \ldots, v_n) = (u_{1,1}, \ldots, u_{1,k_1}, \; u_{2,1}, \ldots, u_{2,k_2}, \; \ldots, u_{m,1}, \ldots, u_{m,k_m})$. In the following, if an independence clique C appears in a tuple over $\mathsf{IRR}(R)$, we identify this clique with the sequence $a_1, a_2, \ldots, a_n$ which is obtained by enumerating the elements of C in an arbitrary way. For instance, $([abcd]_I, \{a, b, c\})$ stands for the tuple $([abcd]_I, a, b, c)$. Let us first prove the following lemma:

Lemma 6.14. *Assume that the tuple $(v_1, v_2, \ldots, v_n)$ is 1-reducible with at most m atom creations of each type. For all $1 \leq i \leq n$ let $v_i = p_i D_i t_i$ be a factorization in $\mathbb{M}(A, I)$ where D_i is an independence clique of (A, I). By refining $p_1, t_1, \ldots, p_n, t_n$ into a total of at most $4n + \sum_{i=1}^{n} |D_i|$ traces, we can obtain a refinement of $(p_1, D_1, t_1, p_2, D_2, t_2, \ldots, p_n, D_n, t_n)$ which is 1-reducible with at most m atom creations of each type.*

Proof. Basically, we would like to apply to $(p_1, D_1, t_1, p_2, D_2, t_2, \ldots, p_n, D_n, t_n)$ the same reduction that reduces $(v_1, v_2, \ldots, v_n)$ to the empty tuple. If we do a swapping step $v_i, v_j \to v_j, v_i$ then we can swap also the order of p_i, D_i, t_i and p_j, D_j, t_j in several swapping steps. Also notice that if v_i is an atom, then the subsequence p_i, D_i, t_i is equivalent to the atom v_i. The only remaining problem are cancellation steps. Assume that v_i and v_j cancel, i.e., $v_i = v_j^{-1}$. The traces t_i and t_j do not necessarily cancel out, and similarly for p_i and p_j and the atoms in D_i and D_j. Hence, we have to further refine p_i, t_i, p_j, t_j using Levi's lemma. Applied to the identity $p_i D_i t_i = t_j^{-1} D_j^{-1} p_j^{-1}$ it yields the following diagram:

p_j^{-1}	$x_{i,j}$	$N_{i,j}$	$z_{i,j}$
D_j^{-1}	$W_{i,j}$	$C_{i,j}$	$E_{i,j}$
t_j^{-1}	$w_{i,j}$	$S_{i,j}$	$y_{i,j}$
	p_i	D_i	t_i

(6.2)

Hence, we get factorizations

$$\begin{aligned} p_i &= w_{i,j} W_{i,j} x_{i,j} && (6.3)\\ t_i &= y_{i,j} E_{i,j} z_{i,j} && (6.4)\\ p_j &= z_{i,j}^{-1} N_{i,j}^{-1} x_{i,j}^{-1} && (6.5)\\ t_j &= y_{i,j}^{-1} S_{i,j}^{-1} w_{i,j}^{-1}. && (6.6) \end{aligned}$$

where $D_i = S_{i,j} \uplus C_{i,j} \uplus N_{i,j}$ and $D_j = E_{i,j}^{-1} \uplus C_{i,j}^{-1} \uplus W_{i,j}^{-1}$. Using these facts and the independencies obtained from the diagram (6.2) shows that the tuple

$$(w_{i,j}, W_{i,j}, x_{i,j}, D_i, y_{i,j}, E_{i,j}, z_{i,j}, z_{i,j}^{-1}, N_{i,j}^{-1}, x_{i,j}^{-1}, D_j, y_{i,j}^{-1}, S_{i,j}^{-1}, w_{i,j}^{-1})$$

is 1-reducible. Hence, by refining p_i, t_i, p_j, and t_j according to the factorizations (6.3), (6.4), (6.5), and (6.6), respectively, we obtain a 1-reducible refinement of $(p_1, D_1, t_1, p_2, D_2, t_2, \ldots, p_n, D_n, t_n)$. Note that $|W_{i,j} \cup E_{i,j}| \leq |D_j|$ and $|N_{i,j} \cup S_{i,j}| \leq |D_i|$. Hence, the $2n$ traces $p_1, t_1, \ldots, p_n, t_n$ are refined into totally at most $4n + \sum_{i=1}^{n} |D_i|$ traces. □

As before, α denotes the size of a largest independence clique in (A, I).

Lemma 6.15. *Let $m \geq 2$ and $u_1, u_2, \ldots, u_m \in \mathsf{IRR}(R)$. If $u_1 u_2 \cdots u_m = 1$ in G, then there exists a 1-reducible refinement of $(u_1, u_2, \ldots, u_m)$ that has length at most $(3\alpha + 4)m^2 \leq 7\alpha m^2$ and there is a reduction of that refinement with at most $m - 2$ atom creations of each type $i \in \Gamma$.*

Proof. The proof of the lemma will be an induction on m. For this we first assume that m is a power of 2. To make the induction work, we slightly strengthen the claim: We will show that there exist factorizations of the u_i with totally at most $f(m) = (\frac{3}{4}\alpha + 1)m^2 - (\frac{3}{2}\alpha + 1)m$ factors such that the resulting tuple is 1-reducible and has a reduction with at most $(m - 2)$ atom creations of each type $i \in \Gamma$. This implies the lemma for the case that m is a power of two.

The case $m = 2$ is trivial (we must have $u_2 = u_1^{-1}$). Let $m = 2n \geq 4$. Then by Lemma 6.12 we can factorize u_{2i-1} and u_{2i} for $1 \leq i \leq n$ as $u_{2i-1} = p_i C_{2i-1} s_i$ and $u_{2i} = s_i^{-1} C_{2i} t_i$ in $\mathbb{M}(A, I)$ such that C_{2i-1} and C_{2i} are strongly compatible independence cliques and $v_i = p_i(C_{2i-1}C_{2i})t_i$ is irreducible. Define the independence clique $D_i = C_{2i-1}C_{2i}$. We have $v_1 v_2 \cdots v_n = 1$ in G. By induction, we obtain factorizations $p_i D_i t_i = v_i = v_{i,1} \cdots v_{i,k_i}$ $(1 \leq i \leq n)$ such that the tuple

$$(v_{i,1}, \ldots, v_{i,k_i})_{1 \leq i \leq n} \tag{6.7}$$

is 1-reducible. Moreover,

$$\sum_{i=1}^{n} k_i \leq \left(\frac{3}{4}\alpha + 1\right) n^2 - \left(\frac{3}{2}\alpha + 1\right) n$$

and there exists a reduction of the tuple (6.7) with at most $n - 2$ atom creations of each type. By applying Levi's lemma to the trace identities

$p_i D_i t_i = v_{i,1} v_{i,2} \cdots v_{i,k_i}$, we obtain factorizations $v_{i,j} = x_{i,j} D_{i,j} y_{i,j}$ in $\mathbb{M}(A, I)$ such that $D_i = \biguplus_{1 \le j \le k_i} D_{i,j}$, $p_i = x_{i,1} \cdots x_{i,k_i}$, $t_i = y_{i,1} \cdots u_{i,k_i}$, and the following independencies hold for $1 \le j < \ell \le k_i$: $y_{i,j}\ I\ x_{i,\ell}$, $y_{i,j}\ I\ a$ for all $a \in D_{i,\ell}$, $a\ I\ x_{i,\ell}$ for all $a \in D_{i,j}$. Note that $D_{i,j}$ can be the empty set.

Let us now define for every $1 \le i \le n$ the tuples $\overline{u}_{2i-1}$ and $\overline{u}_{2i}$ as follows:

- $\overline{u}_{2i-1} = (x_{i,1}, \ldots, x_{i,k_i}, C_{2i-1}, s_i)$
- $\overline{u}_{2i} = (s_i^{-1}, C_{2i}, y_{i,1}, \ldots, y_{i,k_i})$

Thus, the tuple $\overline{u}_i$ defines a factorization of the trace u_i and the tuple $(\overline{u}_1, \overline{u}_2, \ldots, \overline{u}_{2n})$ is a refinement of $(u_1, \ldots, u_{2n})$ of length $2f(n) + 2n(\alpha + 1)$. This tuple can be transformed using n cancellation steps (cancelling s_i and s_i^{-1}) and n atom creations of each type into the sequence

$$(x_{i,1}, \ldots, x_{i,k_i}, D_i, y_{i,1}, \ldots, y_{i,k_i})_{1 \le i \le n}.$$

Using swappings, we finally obtain the sequence

$$(x_{i,1}, D_{i,1}, y_{i,1}, \ldots, x_{i,k_1}, D_{i,k_1}, y_{i,k_1})_{1 \le i \le n}. \tag{6.8}$$

Recall that $v_{i,j} = x_{i,j} D_{i,j} y_{i,j}$. Hence, the tuple (6.8) is a refinement of the 1-reducible tuple (6.7). We are therefore in the situation of Lemma 6.14. By further refining the totally at most $2f(n)$ factors $x_{i,j}$ and $y_{i,j}$ of the traces $u_1, \ldots, u_{2n}$ we obtain a 1-reducible tuple. The resulting refinement of $(u_1, \ldots, u_{2n})$ has length at most

$$\begin{aligned}
& 4 \sum_{i=1}^{n} k_i + \sum_{i=1}^{n} \sum_{j=1}^{k_i} |D_{i,j}| + 2n + 2n\alpha \\
\le\ & 4 \left(\frac{3}{4}\alpha + 1 \right) n^2 - 4 \left(\frac{3}{2}\alpha + 1 \right) n + \sum_{i=1}^{n} |D_i| + 2n + 2n\alpha \\
\le\ & (3\alpha + 4) n^2 - (6\alpha + 4) n + (3\alpha + 2) n \\
=\ & (3\alpha + 4) n^2 - (3\alpha + 2) n \\
=\ & \left(\frac{3}{4}\alpha + 1 \right) m^2 - \left(\frac{3}{2}\alpha + 1 \right) m
\end{aligned}$$

($\sum_{i=1}^{n} k_i + \sum_{i=1}^{n} \sum_{j=1}^{k_i} |D_{i,j}|$ traces from the refinement of the traces $x_{i,j}$ and $y_{i,j}$ by Lemma 6.14, $2n$ traces $s_i^{\pm 1}$, and $2n\alpha$ atoms from the independence cliques C_i). Finally, the total number of atom creations of a certain type is $n + n - 2 = 2n - 2 = m - 2$.

In the general case, where m is not assumed to be a power of two, we can naturally extend the sequence to $u_1, u_2, \ldots, u_\ell$ by possibly adding $u_i = 1$ for $i > m$ to the smallest power of 2. Hence $\ell \le 2m$. Substituting $2m$ for m yields the desired bound. Note that by this process, the number of atom creations will not increase. This concludes the proof of the lemma. □

Since by this result we also get a 1-reducible tuple with at most $\mathcal{O}(m^2)$ many elements for equations $u_1u_2\cdots u_m = 1$ over a graph group, this improves the result of [68].

Remark 6.16. The atom creations that appear in a concrete reduction can be collected into finitely many identities of the form $a_1a_2\cdots a_k =_{G_i} b_1b_2\cdots b_\ell$ (or $a_1a_2\cdots a_kb_\ell^{-1}\cdots b_2^{-1}b_1^{-1} =_{G_i} 1$), where $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_\ell$ are atoms from the initial sequence that all belong to the same group G_i. The new atoms $a_1a_2\cdots a_k$ and $b_1b_2\cdots b_\ell$ are created by at most $m-2$ atom creations. Finally, the two resulting atoms cancel out. Note that $k-1+\ell-1 \leq m-2$, i.e., $k+\ell \leq m$.

In case $E = I = \emptyset$ the quadratic dependence on m in Lemma 6.15 can be avoided:

Lemma 6.17. *Let $m \geq 2$ and $u_1, u_2, \ldots, u_m \in \mathsf{IRR}(R)$. Moreover let $E = I = \emptyset$. If $u_1u_2\cdots u_m = 1$ in the free product G, then there exists a 1-reducible refinement of the tuple $(u_1, u_2, \ldots, u_m)$ that has length at most $7m-12$ and there is a reduction of this refinement with at most $m-2$ atom creations.*

Proof. We prove the lemma by induction on m. The case $m = 2$ is trivial (we must have $u_2 = u_1^{-1}$). If $m \geq 3$ then for the normal form of u_1u_2 there are two cases: either $u_1u_2 \in \mathsf{IRR}(R)$ or $u_1 = pas$ and $u_2 = s^{-1}bt$ for atoms a, b from the same group G_i that do not cancel out. We consider only the latter case. Let $c = ab$ in G_i, i.e., $c \in A_i$. By the induction hypothesis, the tuple $(pct, u_3, \ldots, u_m)$ has a 1-reducible refinement

$$(v_1, \ldots, v_k, w_1, \ldots, w_\ell) \tag{6.9}$$

with $k + \ell \leq 7(m-1) - 12$ and $pct = v_1\cdots v_k$, where the latter is an identity between words from A^*. Moreover, there is a reduction of (6.9) with at most $m-3$ atom creations. Since $pct = v_1\cdots v_k$, one of the v_j $(1 \leq j \leq k)$ must factorize as $v_j = v_{j,1}cv_{j,2}$ such that $p = v_1\cdots v_{j-1}v_{j,1}$ and $t = v_{j,2}v_{j+1}\cdots v_k$, which implies $u_1 = v_1\cdots v_{j-1}v_{j,1}as$ and $u_2 = s^{-1}bv_{j,2}v_{j+1}\cdots v_k$. Therefore we have a 1-reducible tuple of the form

$$(v_1, \ldots, v_{j-1}, v_{j,1}, a, s, s^{-1}, b, v_{j,2}, v_{j+1}, \ldots, v_k, \tilde{w}_1, \ldots, \tilde{w}_\ell), \tag{6.10}$$

where the sequence $\tilde{w}_i$ is w_i unless w_i cancels out with v_j in our reduction of (6.9) (there can be only one such i), in which case $\tilde{w}_i$ is $(v_{j,2})^{-1}, c^{-1}, (v_{j,1})^{-1}$. It follows that the tuple (6.10) is a refinement of $(u_1, u_2, \ldots, u_m)$ with at most $7(m-1)-12+7 = 7m-12$ words, having a reduction with at most $m-2$ atom creations. □

6.6 Graph products preserve knapsack-semilinearity

In this section, we assume that every group G_i ($i \in \Gamma$) is knapsack-semilinear. Recall that we fixed the symmetric generating set Σ_i for G_i, which yields the generating set $\Sigma = \bigcup_{i\in\Gamma} \Sigma_i$ for the graph product G. In this section, we want to show that the graph product G is knapsack-semilinear as well. Moroever, we want to bound the function $\mathsf{E}_{G,\Sigma}$ in terms of the functions $\mathsf{K}_{G_i,\Sigma_i}$. Let $\mathsf{K} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the pointwise maximum of the functions $\mathsf{K}_{G_i,\Sigma_i}(n, m)$. We will bound $\mathsf{E}_{G,\Sigma}$ in terms of K.

Consider an exponent expression $e = u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_m^{x_m} v_m$, where u_i, v_i are words over the generating set Σ. Let g_i (resp., h_i) be the element of G represented by u_i (resp., v_i). We can assume that all u_i and v_i are geodesic words in the graph product G.[6] We will make this assumption throughout this section. Moreover, we can identify each u_i (resp., v_i) with the unique irreducible trace from $\mathsf{IRR}(R)$ that represents the group element g_i (resp., h_i). In addition, for each atom $a \in A$ (say $a \in A_i$) that occurs in one of the traces $u_1, u_2, \ldots, u_m, v_1, \ldots, v_m \in \mathsf{IRR}(R)$ a geodesic word $w_a \in \Sigma_i^*$ that evaluates to a in the group G_i is given. This yields geodesic words for the group elements $g_1, \ldots, g_m, h_1, \ldots, h_m \in G$. The lengths of these words are $\|u_1\|, \ldots, \|u_m\|, \|v_1\|, \ldots, \|v_m\|$ and we have $\|e\| = \|u_1\| + \cdots + \|u_m\| + \|v_1\| + \cdots + \|v_m\|$.

We start with the following preprocessing step.

Lemma 6.18. *Let e be an exponent expression over Σ. From e we can compute a knapsack expression e' with the following properties:*

- $X_e \subseteq X_{e'}$,
- $\|e'\| \leq 3\|e\|$,
- $\deg(e') \leq \alpha \cdot \deg(e)$,
- *every period of e' is either atomic or well-behaved, and*
- $\mathsf{sol}_G(e) = (K \cap \mathsf{sol}_G(e'))\restriction_{X_e}$ *for a semilinear set K of magnitude one.*

Proof. Let $u_1, \ldots, u_m \in \Sigma^*$ be the periods of e. We can view these words as traces $u_1, \ldots, u_m \in \mathbb{M}(A, I)$ that are moreover irreducible. We apply Lemma 6.10 to each power u_i^x in e and obtain an equivalent exponent expression $\tilde{e}$ of degree $n \leq \alpha \cdot m$ and $\|\tilde{e}\| \leq 3\|e\|$. We have $X_{\tilde{e}} = X_e$ and $\mathsf{sol}_G(e) = \mathsf{sol}_G(\tilde{e})$.

We now rename in $\tilde{e}$ the variables by fresh variables in such a way that we obtain a knapsack expression e'. Moreover, for every $x \in X_e$ we keep exactly one occurrence of x in $\tilde{e}$ and do not rename this occurrence of x. This implies that there is a semilinear set $K \subseteq \mathbb{N}^{X_{e'}}$ of magnitude one such that $\mathsf{sol}_G(e) = (K \cap \mathsf{sol}_G(e'))\restriction_{X_e}$. □

In case $E = I = \emptyset$ and that e is a knapsack expression, we can simplify the statement of Lemma 6.18 as follows:

[6] Since the word problem for every G_i is decidable, also the word problem for G is decidable [36], which implies that one can compute a geodesic word for a given group element of G.

Remark 6.19. Assume that $E = I = \emptyset$ and that e is a knapsack expression as in Lemma 6.18. By Remark 6.11 we can compute from e a knapsack expression e' over Σ with the following properties:

- $\|e'\| \leq 3\|e\|$,
- $\deg(e') \leq \deg(e)$,
- every period of e' is either atomic or well-behaved, and
- $\mathsf{sol}_G(e) = \mathsf{sol}_G(e')$.

We now come to the proof of the main technical result of this chapter, Theorem 4.2. As before, we denote with α the size of a largest independence clique in the finite graph (Γ, E).

Theorem 4.2 ([F6])**.** *If each group G_i, $i \in \Gamma$, is knapsack-semilinear, then their graph product $G = G(\Gamma, E, (G_i)_{i\in\Gamma})$ is knapsack-semilinear as well. Let $\mathsf{K} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ be the pointwise maximum of the functions $\mathsf{K}_{G_i,\Sigma_i}(n, m)$ for $i \in \Gamma$. Then $\mathsf{E}_{G,\Sigma}(n, m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2\}$ with*

$$\mathsf{K}_1 \leq \mathcal{O}\big((\alpha m)^{\alpha m/2+3} \cdot \mathsf{K}(6\alpha mn, \alpha m)^{\alpha m+3}\big),$$
$$\mathsf{K}_2 \leq (\alpha m)^{\mathcal{O}(\alpha^2 m)} \cdot n^{\mathcal{O}(\alpha^2|\Gamma|m)}.$$

Proof. Consider an exponent expression $e = u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_m^{x_m} v_m$. Let us denote with $A(e) = \mathsf{alph}(u_1 v_1 \cdots u_m v_m) \subseteq A$ the set of all atoms that appear in the traces u_i, v_i. Finally let $\mu(e) = \max\{\|a\| \mid a \in A(e)\}$ and let $\lambda(e)$ be the maximal length $|t|$ where t is one of the traces $u_1, u_2, \ldots, u_m, v_1, \ldots, v_m$. We clearly have $\mu(e) \leq \|e\|$ and $\lambda(e) \leq \|e\|$.

Let us first assume that e is a knapsack expression (i.e., $x_i \neq x_j$ for $i \neq j$) where every period u_i is either an atom or a well-behaved trace (see Lemma 6.18).

In the following we describe an algorithm that computes a semilinear representation of $\mathsf{sol}_G(e)$ (for e satisfying the conditions from the previous paragraph). At the same time, we will compute the magnitude of this semilinear representation. The algorithm transforms logical statements into equivalent logical statements (we do not have to define the precise logical language; the meaning of the statements should be always clear). Every statement contains the variables $x_1, \ldots, x_m$ from our knapsack expression and equivalence of two statements means that for every valuation $\nu : \{x_1, \ldots, x_m\} \to \mathbb{N}$ the two statements yield the same truth value. We start with the statement $e = 1$. In each step we transform the current statement Φ into an equivalent disjunction $\bigvee_{i=1}^{n} \Phi_i$. We can therefore view the whole process as a branching tree, where the nodes are labelled with statements. If a node is labelled with Φ and its children are labelled with $\Phi_1, \ldots, \Phi_n$ then Φ is equivalent to $\bigvee_{i=1}^{n} \Phi_i$. The leaves of the tree are labelled with semilinear constraints of the form $(x_1, \ldots, x_m) \in L$ for semilinear sets L. Hence, the solution set $\mathsf{sol}_G(e)$ is the union of all semilinear sets that label the leaves of the tree. A bound on the magnitude of these semilinear sets yields a bound on the magnitude of $\mathsf{sol}_G(e)$. Therefore, we can restrict our analysis to a single branch of the tree. We can view this branch as a sequence

of nondeterministic guesses. Some guesses lead to dead branches because the corresponding statement is unsatisfiable. We will speak of a bad guess in such a situation.

Let $N_a \subseteq [1,m]$ be the set of indices such that u_i is atomic and let $N_{\overline{a}} = [1,m] \setminus N_a$ be the set of indices such that u_i is not atomic (and hence a well-behaved trace). For better readability, we write a_i for the atom u_i in case $i \in N_a$. Define $X_a = \{x_i \mid i \in N_a\}$ and $X_{\overline{a}} = \{x_i \mid i \in N_{\overline{a}}\}$. For $i \in N_a$ let $\gamma(i) \in \Gamma$ be the index with $u_i \in A_{\gamma(i)}$.

Step 1: Eliminating trivial powers. In a first step we guess a set $N_1 \subseteq N_a$ of indices with the meaning that for $i \in N_1$ the power $a_i^{x_i}$ evaluates to the identity element of the group $G_{\gamma(i)}$. To express this we continue with the formula

$$\Phi[N_1] = (e[N_1] = 1) \wedge \bigwedge_{i \in N_1} a_i^{x_i} =_{G_{\gamma(i)}} 1, \tag{6.11}$$

where $e[N_1]$ is the knapsack expression obtained from e by deleting all powers $a_i^{x_i}$ with $i \in N_1$. Note that the above constraints do not exclude that a power $u_i^{x_i}$ with $i \in [1,m] \setminus N_1$ evaluates to the identity element. This will not cause any trouble for the following arguments. Clearly, the initial equation $e = 1$ is equivalent to the formula $\bigvee_{N_1 \subseteq N_a} \Phi[N_1]$.

In the following we transform every equation $e[N_1] = 1$ into a formula $\Psi[N_1]$ such that the following hold for every valuation $\nu : \{x_i \mid i \in [1,m] \setminus N_1\} \to \mathbb{N}$:

(1) if $\Psi[N_1]$ is true under ν then $\nu(e[N_1]) =_G 1$,

(2) if $a_i^{\nu(x_i)} \neq_{G_{\gamma(i)}} 1$ for all $i \in N_a \setminus N_1$ and $\nu(e[N_1]) =_G 1$ then $\Psi[N_1]$ is true under ν.

This implies that $\bigvee_{N_1 \subseteq N_a} \Phi[N_1]$ (and hence $e = 1$) is equivalent to the formula

$$\bigvee_{N_1 \subseteq N_a} (\Psi[N_1] \wedge \bigwedge_{i \in N_1} a_i^{x_i} =_{G_{\gamma(i)}} 1).$$

Step 2: Applying Lemma 6.15. We construct the formula $\Psi[N_1]$ from the knapsack expression $e[N_1]$ using Lemma 6.15. More precisely, we construct $\Psi[N_1]$ by nondeterministically guessing the following data:

(i) factorizations $v_i = v_{i,1} \cdots v_{i,\ell_i}$ in $\mathbb{M}(A,I)$ of all non-trivial traces v_i. Each factor $v_{i,j}$ must be nontrivial too.

(ii) "symbolic factorizations" $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$ for all $i \in N_{\overline{a}}$. The numbers k_i and ℓ_i must sum up to at most $28\alpha m^2$ (this number is obtained by replacing m by $2m$ in Lemma 6.15). The $y_{i,j}$ are existentially quantified variables that take values in $\mathsf{IRR}(R)$ and which will be eliminated later.

(iii) non-empty alphabets $A_{i,j} \subseteq \mathsf{alph}(u_i)$ for each symbolic factor $y_{i,j}$ ($i \in N_{\overline{a}}$, $1 \leq j \leq k_i$) with the meaning that $A_{i,j}$ is the alphabet of atoms that appear in $y_{i,j}$.

(iv) a reduction (according to Definition 6.13) of the resulting refined factorization of $u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_m^{x_m} v_m$ with at most $2m-2$ atom creations of each type $i \in \Gamma$.

Note that every factor $a_i^{x_i}$ with $i \in N_a \setminus N_1$ evaluates (for a given valuation) either to an atom from $A_{\gamma(i)}$ or to the identity element. Hence, there is no need to further factorize such a power $a_i^{x_i}$. In our guessed reduction we treat $a_i^{x_i}$ as a symbolic atom (although it might happen that $a_i^{\nu(x_i)} = 1$ for a certain valuation ν; but this will not make the above statements (1) and (2) wrong).

We can also guess $k_i = 0$ in (ii). In this case, we can replace $u_i^{x_i}$ in $e[N_1]$ by the empty trace and add the constraint $x_i = 0$ (note that a well-behaved trace $u_i \neq 1$ represents an element of the graph product G without torsion). Hence, in the following we can assume that the k_i are not zero. Some of the $y_{i,j}$ must be atoms since they take part in an atom creation in our guessed reduction. In this case we have to guess for $A_{i,j}$ a singleton set (but there can be other $y_{i,j}$ that do not take part in an atom creation and for which we guess an $A_{i,j}$ of size one). Every $y_{i,j}$ with $|A_{i,j}| = 1$ is replaced by a nondeterministically guessed atom $a_{i,j}$ from the atoms in u_i.

The guessed alphabetic constraints from (iii) must be consistent with the independencies from our guessed reduction in (iv). This means that if for instance $y_{i,j}$ and $y_{k,\ell}$ are swapped in the reduction then we must have $A_{i,j} \times A_{j,k} \subseteq I$. Here comes a subtle point: Recall that each power a^{x_i} ($i \in N_a \setminus N_1$) evaluates for a given valuation either to an atom from $A_{\gamma(i)}$ or to the identity element. When checking the consistency of the alphabetic constraints with the guessed reduction we make the (pessimistic) assumption that every a^{x_i} evaluates to an atom from $A_{\gamma(i)}$. This is justified below.

For every specific guess in (i)–(iv) we write down the existentially quantified conjunction of the following formulas:

- the equation $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$ from (ii) (every trace-variable $y_{i,j}$ is existentially quantified),
- all trace equations that result from cancellation steps in the guessed reduction,
- all "local" identities that result from the atom creations in the guessed reduction,
- all alphabetic constraints from (iii) and
- all constraints $x_i = 0$ in case we guessed $k_i = 0$ in (ii).

The local identities in the third point involve the above atoms $a_{i,j}$ and the powers $a_i^{x_i}$ for $i \in N_a \setminus N_1$. According to Remark 6.16 they are combined into several knapsack expressions over the groups G_i.

The formula $\Psi[N_1]$ is the disjunction of the above existentially quantified conjunctions, taken over all possible guesses in (i)–(iv). It is then clear that the above points (1) and (2) hold. Point (2) follows immediately from Lemma 6.15. For point (1) note that each of the existentially quantified conjunctions in $\Psi[N_1]$ yields the identity $e[N_1] = 1$, irrespective of whether a power $a_i^{x_i}$ is trivial or not.

So far, we have obtained a disjunction of existentially quantified conjunctions. Every conjunction involves the equations $u_i^{x_i} = y_{i,1} \cdots y_{i,k_i}$ from (ii), trace equations that result from cancellation steps (we will deal with them in step 4 below), local knapsack expressions over the groups G_i, alphabetic constraints for the variables $y_{i,j}$ and constraints $x_i = 0$ (if $k_i = 0$). In addition we have the identities $a_i^{x_i} =_{G_{\gamma(i)}} 1$ $(i \in N_1)$ from (6.11). In the following we deal with a single existentially quantified conjunction of this form.

Step 3: Isolating the local knapsack instances for the groups G_i. In our existentially quantified conjunction we have knapsack expressions $e_1, \ldots, e_q$ over the groups G_j $(j \in \Gamma)$. These knapsack expressions involve the atoms $a_{i,j}$ and the symbolic expressions $a_i^{x_i}$ with $i \in N_a$. Note that every identity $a_i^{x_i} =_{G_{\gamma(i)}} 1$ $(i \in N_1)$ yields the knapsack expression $a_i^{x_i}$. Each of the expressions e_j is built from at most $2m$ atom powers $a_i^{x_i}$ and atoms $a_{i,j}$ (since for every $j \in \Gamma$ there are at most $2m-2$ atom creations of type j) and its degree is at most m (since there are at most m atom powers $a_i^{x_i}$). All atoms a_i and $a_{i,j}$ belong to $A(e)$. This yields the bound $\|e_j\| \leq 2m\mu(e)$ for $1 \leq j \leq q$. We can assume that each expression e_j contains at least one atom power $u_i^{x_i}$ (identities between the explicit atoms $a_{i,j}$ can be directly verified; if they do not hold, one gets a bad guess). Moreover, note that every atom power $a_i^{x_i}$ with $i \in N_a$ occurs in exactly one e_j. Assume that the knapsack expression e_j is defined over the group $H_j \in \{G_i \mid i \in \Gamma\}$. The solution sets $\mathsf{sol}_j = \mathsf{sol}_{H_j}(e_j)$ of these expressions are semilinear by the assumption on the groups G_i. Each sol_j has some dimension $d_j \leq m$ (which is the number of symbolic atoms in e_j), where $\sum_{j=1}^{q} d_j = |N_a|$ and the magnitude of sol_j is bounded by $\mathsf{K}(2m\mu(e), m) \leq \mathsf{K}(2m\|e\|, m)$. Finally, we can combine these sets sol_j into the single semilinear set $S_a = \bigoplus_{j=1}^{q} \mathsf{sol}_j \subseteq \mathbb{N}^{X_a}$ of dimension $|N_a|$ and magnitude at most $\mathsf{K}(2m\|e\|, m)$. Recall that the sets sol_j refer to pairwise disjoint sets of variables. For the variables $x_i \in X_a$ we now obtain the semilinear contraint $(x_i)_{i \in N_a} \in S_a$.

Step 4: Reduction to two-dimensional knapsack instances. Let us now deal with the cancellation steps from our guessed reduction. From these reduction steps we will produce two-dimensional knapsack instances on pairwise disjoint variable sets.

If two explicit factors $v_{i,j}$ and $v_{k,\ell}$ (from (i) in step 2) cancel out in the reduction, we must have $v_{k,\ell} = v_{i,j}^{-1}$; otherwise our previous guess was bad. If a symbolic factor $y_{i,j}$ and an explicit factor $v_{k,\ell}$ cancel out, then we can replace $y_{i,j}$ by $v_{k,\ell}^{-1}$. Before doing this, we check whether $\mathsf{alph}(v_{k,\ell}^{-1}) = A_{i,j}$ and if this condition does not hold, then we obtain again a bad guess. Let S be the set of pairs (i,j) such that the symbolic factor $y_{i,j}$ still exists after this step. On this set S there must exist a matching $M \subseteq \{(i,j,k,\ell) \mid (i,j),(k,\ell) \in S\}$ such that $y_{i,j}$ and $y_{k,\ell}$ cancel out in our reduction if and only if $(i,j,k,\ell) \in M$. We have $(i,j,k,\ell) \in M$ if and only if $(k,\ell,i,j) \in M$.

Let us write the new symbolic factorization of $u_i^{x_i}$ as $u_i^{x_i} = \tilde{y}_{i,1} \cdots \tilde{y}_{i,k_i}$, where every $\tilde{y}_{i,j}$ is either the original symbolic factor $y_{i,j}$ (in case $(i,j) \in S$) or a concrete trace $v_{k,\ell}^{-1}$ (in case $y_{i,j}$ and $v_{k,\ell}$ cancel out in our reduction) or an atom

$a_{i,j} \in \mathsf{alph}(u_i)$ (that was guessed in step 2). It remains to describe the set of all tuples $(x_1, \ldots, x_m)$ that satisfy a statement of the following form: there exist traces $y_{i,j}$ ($(i,j) \in S$) such that the following hold:

(a) $u_i^{x_i} = \tilde{y}_{i,1} \cdots \tilde{y}_{i,k_i}$ in $\mathbb{M}(A, I)$ for all $i \in N_{\overline{a}}$
(b) $\mathsf{alph}(y_{i,j}) = A_{i,j}$ for all $(i,j) \in S$,
(c) $y_{i,j} = y_{k,\ell}^{-1}$ in $\mathbb{M}(A, I)$ for all $(i,j,k,\ell) \in M$
(d) $(x_i)_{i \in N_a} \in S_a$

In the next step, we eliminate the trace equations $u_i^{x_i} = \tilde{y}_{i,1} \cdots \tilde{y}_{i,k_i}$ ($i \in N_{\overline{a}}$). We apply to each of these trace equations Lemma 6.3 (or Remark 6.4). For every $i \in N_{\overline{a}}$ we guess a subset $K_i \subseteq [1, k_i]$, an integer $0 \leq c_i \leq |\Gamma| \cdot (k_i - 1)$ and traces $p_{i,j}, s_{i,j}$ with $\mathsf{alph}(p_{i,j}) \subseteq \mathsf{alph}(u_i) \supseteq \mathsf{alph}(s_{i,j})$ and $|p_{i,j}|, |s_{i,j}| \leq |\Gamma| \cdot (k_i - 1) \cdot |u_i| \leq |\Gamma| \cdot (k_i - 1) \cdot \lambda(e)$, and replace $u_i^{x_i} = \tilde{y}_{i,1} \cdots \tilde{y}_{i,k_i}$ by the following statement: there exist integers $x_{i,j} > 0$ ($j \in K_i$) such that

- $x_i = c_i + \sum_{j \in K_i} x_{i,j}$,
- $\tilde{y}_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}$ for all $j \in K_i$,
- $\tilde{y}_{i,j} = p_{i,j} s_{i,j}$ for all $j \in [1, k_i] \setminus K_i$.

At this point we can check whether the alphabetic constraints $\mathsf{alph}(y_{i,j}) = A_{i,j}$ for $(i,j) \in S$ hold (note that an equation $y_{i,j} = p_{i,j} s_{i,j}$ or $y_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}$ with $x_{i,j} > 0$ determines the alphabet of $y_{i,j}$). Equations $\tilde{y}_{i,j} = p_{i,j} s_{i,j}$, where $\tilde{y}_{i,j}$ is an explicit trace can be checked and possibly lead to a bad guess. From an equation $\tilde{y}_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}$, where $\tilde{y}_{i,j}$ is an explicit trace, we can determine a unique solution for $x_{i,j} > 0$ (if it exists) and substitute this value into the equation $x_i = c_i + \sum_{j \in K_i} x_{i,j}$. Note that we must have $x_{i,j} \leq |\tilde{y}_{i,j}| \leq \lambda(e)$, since $\tilde{y}_{i,j}$ is an atom or a factor of a trace v_k^{-1}. Similarly, an equation $y_{i,j} = p_{i,j} s_{i,j}$ with $(i,j) \in S$ allows us to replace the symbolic factor $y_{i,j}$ by the concrete trace $p_{i,j} s_{i,j}$ and the unique symbolic factor $y_{k,\ell}$ with $(i,j,k,\ell) \in M$ by the concrete trace $s_{i,j}^{-1} p_{i,j}^{-1}$. If we have an equation $y_{k,\ell} = p_{k,\ell} s_{k,\ell}$ then we check whether $s_{i,j}^{-1} p_{i,j}^{-1} = p_{k,\ell} s_{k,\ell}$ holds. Otherwise we have an equation $y_{k,\ell} = p_{k,\ell} u_k^{x_{k,\ell}} s_{k,\ell}$, and we can compute the unique non-zero solution for $x_{k,\ell}$ (if it exists). Note that $x_{k,\ell} \leq |s_{i,j}^{-1} p_{i,j}^{-1}| \leq 2|\Gamma| \cdot (k_i - 1) \cdot \lambda(e) \in \mathcal{O}(|\Gamma|^2 \cdot m^2 \cdot \lambda(e))$. We then replace $x_{k,\ell}$ in the equation $x_k = c_k + \sum_{\ell \in K_k} x_{k,\ell}$ by this unique solution.

By the above procedure, our statement (a)–(d) (with existentially quantified traces $y_{i,j}$) is transformed nondeterministically into a statement of the following form: there exist integers $x_{i,j} > 0$ ($i \in N_{\overline{a}}$, $j \in K_i'$) such that the following hold:

(a) $x_i = c_i' + \sum_{j \in K_i'} x_{i,j}$ for $i \in N_{\overline{a}}$,
(b) $p_{i,j} u_i^{x_{i,j}} s_{i,j} = s_{k,\ell}^{-1} (u_k^{-1})^{x_{k,\ell}} p_{k,\ell}^{-1}$ in $\mathbb{M}(A, I)$ for all $(i,j,k,\ell) \in M'$,
(c) $(x_i)_{i \in N_a} \in S_a$.

Here, $K_i' \subseteq K_i \subseteq [1, k_i]$ is a set of size at most $k_i \leq 28\alpha m^2$, $M' \subseteq M$ is a new matching relation (with $(i,j,k,\ell) \in M'$ if and only if $(k,\ell,i,j) \in M'$), and $c_i' \leq |\Gamma| \cdot (k_i - 1) + k_i \cdot \mathcal{O}(|\Gamma|^2 \cdot m^2 \cdot \lambda(e)) \leq \mathcal{O}(|\Gamma|^3 \cdot m^4 \cdot \lambda(e))$.

Step 5: Elimination of two-dimensional knapsack instances. The remaining knapsack equations $p_{i,j}u_i^{x_{i,j}}s_{i,j} = s_{k,\ell}^{-1}(u_k^{-1})^{x_{k,\ell}}p_{k,\ell}^{-1}$ in (b) are two-dimensional (these equations all have two variables) and can be eliminated with Lemma 6.5. By this lemma, every trace equation

$$p_{i,j}u_i^{x_{i,j}}s_{i,j} = s_{k,\ell}^{-1}(u_k^{-1})^{x_{k,\ell}}p_{k,\ell}^{-1}$$

(recall that all u_i are connected, which is assumed in Lemma 6.5) can be nondeterministically replaced by a semilinear constraint

$$(x_{i,j}, x_{k,\ell}) \in \{(a_{i,j,k,\ell} + b_{i,j,k,\ell} \cdot z, a_{k,\ell,i,j} + b_{k,\ell,i,j} \cdot z) \mid z \in \mathbb{N}\}.$$

For the numbers $a_{i,j,k,\ell}, b_{i,j,k,\ell}, a_{k,\ell,i,j}, b_{k,\ell,i,j}$ we obtain the bound

$$a_{i,j,k,\ell}, b_{i,j,k,\ell}, a_{k,\ell,i,j}, b_{k,\ell,i,j} \in \mathcal{O}(\mu^8 \cdot \eta^{4|\Gamma|}),$$

where, by Lemma 6.1,

$$\mu = \max\{\rho(p_{i,j}), \rho(p_{k,\ell}), \rho(s_{i,j}), \rho(s_{k,\ell})\} \leq \mathcal{O}(|\Gamma|^{2\alpha} \cdot 28^\alpha \cdot m^{2\alpha} \cdot \lambda(e)^\alpha) \quad (6.12)$$

and

$$\eta = \max\{\rho(u_i), \rho(u_k)\} \leq \mathcal{O}(\lambda(e)^\alpha). \quad (6.13)$$

Note that $\rho(t) = \rho(t^{-1})$ for every trace t. Moreover, note that we have the constraints $x_{i,j}, x_{k,\ell} > 0$. Hence, if our nondeterministic guess yields $a_{i,j,k,\ell} = 0$ or $a_{k,\ell,i,j} = 0$ then we make the replacement $a_{i,j,k,\ell} = a_{i,j,k,\ell} + b_{i,j,k,\ell}$ and $a_{k,\ell,i,j} = a_{k,\ell,i,j} + b_{k,\ell,i,j}$. If after this replacement we still have $a_{i,j,k,\ell} = 0$ or $a_{k,\ell,i,j} = 0$ then our guess was bad.

At this point, we have obtained a statement of the following form: there exist $z_{i,j,k,\ell} \in \mathbb{N}$ (for $(i,j,k,\ell) \in M'$) with $z_{i,j,k,\ell} = z_{k,\ell,i,j}$ and such that

(a) $x_i = c'_i + \sum_{(i,j,k,\ell)\in M'}(a_{i,j,k,\ell} + b_{i,j,k,\ell} \cdot z_{i,j,k,\ell})$ for $i \in N_{\overline{a}}$, and

(b) $(x_i)_{i\in N_a} \in S_a$.

Note that the sum in (a) contains $|K'_i| \leq 28m^2\alpha$ many summands (since for every $j \in K'_i$ there is a unique pair (k,ℓ) with $(i,j,k,\ell) \in M'$). Hence, (a) can be written as $x_i = c''_i + \sum_{(i,j,k,\ell)\in M'} b_{i,j,k,\ell} \cdot z_{i,j,k,\ell}$ with

$$\begin{aligned} c''_i &= c'_i + \sum_{(i,j,k,\ell)\in M'} a_{i,j,k,\ell} \\ &\leq \mathcal{O}(|\Gamma|^3 \cdot m^4 \cdot \lambda(e)) + \mathcal{O}(\alpha \cdot m^2 \cdot \mu^8 \cdot \eta^{4|\Gamma|}) \\ &\leq \mathcal{O}(|\Gamma|^{16\alpha+1} \cdot 28^{8\alpha} \cdot m^{16\alpha+2} \cdot \lambda(e)^{8\alpha+4\alpha|\Gamma|}) \\ &\leq \mathcal{O}(|\Gamma|^{16\alpha+1} \cdot 28^{8\alpha} \cdot m^{16\alpha+2} \cdot \|e\|^{8\alpha+4\alpha|\Gamma|}) \end{aligned}$$

(since $\lambda(e) \leq \|e\|$). The bound in the last line is also an upper bound for the numbers $b_{i,j,k,\ell}$. Hence, we have obtained a semilinear representation for $\mathsf{sol}_G(e)$

whose magnitude is bounded by $\max\{\mathsf{K}_1, \mathsf{K}_2\}$, where

$$\mathsf{K}_1 \leq \mathsf{K}(2m\|e\|, m)$$

(this is our upper bound for the magnitude of the semilinear set S_a) and

$$\mathsf{K}_2 \leq \mathcal{O}\big(|\Gamma|^{16\alpha+1} \cdot 28^{8\alpha} \cdot m^{16\alpha+2} \cdot \|e\|^{8\alpha+4\alpha|\Gamma|}\big).$$

Step 6: Integration of the preprocessing step. Recall that so far we only considered the case where e is a knapsack expression having the form of the e' in Lemma 6.18. Let us now consider an arbitrary exponent expression e of degree m. By Lemma 6.18 we have $\mathsf{sol}_G(e) = (K \cap \mathsf{sol}_G(e'))\restriction_{X_e}$ where K is semilinear of magnitude one and e' has degree at most $\alpha \cdot m$ and satisfies $\|e'\| \leq 3\|e\|$. We can apply the upper bound shown so far to e'. Hence, the magnitude of $\mathsf{sol}_G(e')$ is bounded by $\max\{\mathsf{K}'_1, \mathsf{K}'_2\}$, where

$$\mathsf{K}'_1 \leq \mathsf{K}(6\alpha m\|e\|, \alpha m)$$

and

$$\mathsf{K}'_2 \leq \mathcal{O}\big(|\Gamma|^{16\alpha+1} \cdot 28^{8\alpha} \cdot (\alpha m)^{16\alpha+2} \cdot (3\|e\|)^{8\alpha+4\alpha|\Gamma|}\big).$$

It remains to analyze the influence of intersecting with K. For this, we can apply Proposition 3.2, which yields for the magnitude the upper bound $\max\{\mathsf{K}_1, \mathsf{K}_2\}$, where

$$\mathsf{K}_1 \quad \leq \quad \mathcal{O}\big((\alpha m)^{\alpha m/2+3} \cdot \mathsf{K}(6\alpha m\|e\|, \alpha m)^{\alpha m+3}\big)$$

and

$$\begin{aligned} \mathsf{K}_2 \quad &\leq \quad \mathcal{O}\big((\alpha m)^{\alpha m/2+3} \cdot \mathcal{O}\big(|\Gamma|^{32\alpha+3} \cdot 28^{8\alpha} \cdot (\alpha m)^{16\alpha+2} \cdot (3\|e\|)^{8\alpha+4\alpha|\Gamma|}\big)^{\alpha m+3}\big) \\ &\leq \quad (\alpha m)^{\mathcal{O}(\alpha^2 m)} \cdot \|e\|^{\mathcal{O}(\alpha^2|\Gamma| m)}. \end{aligned}$$

This concludes the proof of the theorem. □

Remark 6.20. Assume that G is a fixed graph product (hence, $|\Gamma|$ is a constant). Consider again the case that e is a knapsack expression (i.e., $x_i \neq x_j$ for $i \neq j$) where every period u_i is either an atom or a well-behaved trace. Let $m = \deg(e)$. In the above proof, we show that the set of solutions $\mathsf{sol}_G(e)$ can be written as a finite union

$$\mathsf{sol}_G(e) = \bigcup_{i=1}^{p} \bigoplus_{j=1}^{q_i} \mathsf{sol}_{H_{i,j}}(e_{i,j}) \oplus L_i$$

such that the following hold for every $1 \leq i \leq p$:

- every $H_{i,j}$ is one of the groups G_k and $e_{i,j}$ is a knapsack expression over the group $H_{i,j}$. The variable sets $X_{e_{i,j}}$ $(1 \leq j \leq q_i)$ form a partition of the set X_a (the variables corresponding to atomic periods).
- Every $e_{i,j}$ is a knapsack expression of size at most $2m\|e\|$ and degree at

most m (see step 3 in the above proof).
- The set L_i is semilinear of magnitude $\mathcal{O}\big(|\Gamma|^{16\alpha+1}28^{8\alpha}m^{16\alpha+2}\|e\|^{8\alpha+4\alpha|\Gamma|}\big) = \mathcal{O}\big(m^{16\alpha+2}\|e\|^{8\alpha+4\alpha|\Gamma|}\big)$ (see step 5 in the above proof).

Here, the indices $i \in [1,p]$ correspond to the guessed data in the above prove. Moreover, given $i \in [1,p]$ (i.e., a specific guess), one can compute the knapsack expressions $e_{i,j}$ $(1 \leq j \leq q_i)$ and a semilinear representation of L_i in polynomial time. This yields a nondeterministic reduction of the knapsack problem for the graph product G to the knapsack problems for the groups G_i $(i \in \Gamma)$, assuming the input expression e satisfies the above restriction. Recall that in general, direct products do not preserve decidability of the knapsack problem.

There is an interesting special case, which was already discussed in [68]: If all G_i are $\mathbb{Z}$ (or more general, G_i is not a torsion group), then knapsack is in NP. Since it also has been shown that knapsack is NP-hard if (Γ, E) is not a transitive forest, we have NP-completeness for knapsack of such graph groups. For the same case $(G_i = \mathbb{Z})$ there is a more recent paper, in which NP-completeness has been proven for the uniform version of the knapsack problem, where the independence alphabet (Γ, E) is part of the input (see [66]).

The reader might wonder, whether we can obtain a bound for the function $\mathsf{K}_{G,\Sigma}$ in terms of the function $\mathsf{K}_{G_i,\Sigma_i}$, which is better than the corresponding bound for $\mathsf{E}_{G,\Sigma}$ from Theorem 4.2. This is actually not the case (at least with our proof technique): a power of the form u^x where $u = u_1u_2 \in \mathbb{M}(A,I)$ with $u_1\ I\ u_2$ is equivalent to $u_1^x u_2^x$. Hence, powers u^x with u a non-connected trace naturally lead to a duplication of the variable x (and hence to an exponent expression which is no longer a knapsack expression). This is the reason why we bounded the (in general faster growing) function $\mathsf{E}_{G,\Sigma}$ in terms of the functions $\mathsf{K}_{G_i,\Sigma_i}$ in Theorem 4.2.

An application of Theorem 4.2 is the following:

Theorem 6.21. *Let G be a graph product of hyperbolic groups. Then* $\textsc{ExpEq}(G)$ *belongs to* NP.

Proof. For a hyperbolic group H (with an arbitrary generating set Σ') it was shown in [62] that the function $\mathsf{K}_{H,\Sigma'}(n) = \mathsf{K}_{H,\Sigma'}(n,n)$ is polynomially bounded. Theorem 4.2 yields an exponential bound for the function $\mathsf{E}_{G,\Sigma}(n) = \mathsf{E}_{G,\Sigma}(n,n)$ (note that $|\Gamma|$ and α are constants since we consider a fixed graph product G). A nondeterministic polynomial time Turing machine can therefore guess the binary encodings of numbers $\nu(x) \leq \mathsf{K}_{G,\Sigma}(\|e\|)$ for each variable x of the input exponent expression e. Checking whether ν is a G-solution of e is an instance of the compressed word problem for G. By the main result of [46] the compressed word problem for a hyperbolic group can be solved in polynomial time and by [43] the compressed word problem for a graph product of groups G_i $(i \in \Gamma)$ can be solved in polynomial time if for every $i \in \Gamma$ the compressed word problem for G_i can be solved in polynomial time. Hence, we can check in polynomial time if ν is a G-solution of e. □

For more details about knapsack for hyperbolic groups, see Chapter 9.

6.7 Special case: Free product of two groups

Let us now consider the special case where the graph product is a free product of two groups G_1 and G_2. We give the proof of

Theorem 4.3 ([F6]). *If the groups G_1 and G_2 are knapsack-semilinear, then $G_1 * G_2$ is knapsack-semilinear as well. Let $\mathsf{K}(n,m)$ be the pointwise maximum of the functions $\mathsf{K}_{G_1,\Sigma_1}$ and $\mathsf{K}_{G_2,\Sigma_2}$. Then for $G = G_1 * G_2$ we have $\mathsf{K}_{G,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2\}$ with*

$$\mathsf{K}_1 = \mathsf{K}(6mn, m) \text{ and } \mathsf{K}_2 \leq \mathcal{O}(mn^4).$$

Proof. The proof is similar to the one from Theorem 4.2. We first consider the case where every period u_i is either an atom or a well-behaved word (see Remark 6.19).

Let us go throw the six steps from the proof of Theorem 4.2:

Step 1. This step is carried out in the same way as in the proof of Theorem 4.2.

Step 2. Here we can use Lemma 6.17 instead of Lemma 6.15, which yields the upper bound of $14m$ on the number of factors in our refinement of $u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_m^{x_m} v_m$ (where powers $u_i^{x_i}$ with $i \in N_1$ have been deleted). The number of atom creations (of any type) is at most $2m-2$. We do not have to guess the atom sets $A_{i,j} \subseteq \mathsf{alph}(u_{i,j})$ since there are no swapping steps in Lemma 6.17.

Step 3. This step is copied from the proof of Theorem 4.2. We obtain for the variables x_i with $i \in N_a$ the semilinear constraint $(x_i)_{i \in N_a} \in S_a$ where S_a is of magnitude at most $\mathsf{K}(2m\|e\|, m)$.

Step 4. Also this step is analogous to the proof of Theorem 4.2. Recall that we have the better bound $14m$ on the number of factors in our refinement of $u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_m^{x_m} v_m$. Eliminating the equations $u_i^{x_i} = \tilde{y}_{i,1} \cdots \tilde{y}_{i,k_i}$ $(i \in N_{\overline{a}})$, which are interpreted in A^*, is much easier due to the absence of commutation. For every $i \in N_{\overline{a}}$ we obtain a disjunction of statements of the following form: there exist integers $x_{i,j} \geq 0$ $(1 \leq j \leq k_i)$ such that

- $x_i = c_i + \sum_{j=1}^{k_i} x_{i,j}$,
- $\tilde{y}_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}$ for all $1 \leq j \leq k_i$.

Here, every $p_{i,j}$ is a suffix of u_i, every $s_{i,j}$ is a prefix of u_i and $c_i \leq k_i \leq 14m$. Basically, c_i is the number of factors u_i that are split non-trivially in the factorization $u_i^{x_i} = \tilde{y}_{i,1} \cdots \tilde{y}_{i,k_i}$. We can then carry out the same simplifications that we did in the proof of Theorem 4.2. If $\tilde{y}_{i,j}$ is an explicit word $v_{k,\ell}^{-1}$ then we determine the unique solution $x_{i,j}$ (if it exists) of $\tilde{y}_{i,j} = p_{i,j} u_i^{x_{i,j}} s_{i,j}$ and replace $x_{i,j}$ by that number, which is at most $\lambda(e)$. We arrive at a statement of the following form: there exist integers $x_{i,j} \geq 0$ $(i \in N_{\overline{a}},\ j \in K_i)$ such that the following hold:

(a) $x_i = c_i' + \sum_{j \in K_i} x_{i,j}$ for $i \in N_{\overline{a}}$,

(b) $p_{i,j}u_i^{x_{i,j}}s_{i,j} = s_{k,\ell}^{-1}(u_k^{-1})^{x_{k,\ell}}p_{k,\ell}^{-1}$ in A^* for all $(i,j,k,\ell) \in M$,

(c) $(x_i)_{i\in N} \in S_a$.

Here, $K_i \subseteq [1,k_i]$ is a set of size at most $k_i \leq 14m$, M is a matching relation (with $(i,j,k,\ell) \in M$ if and only if $(k,\ell,i,j) \in M$), and $c_i' \leq 14m + k_i \cdot \lambda(e) \leq \mathcal{O}(m \cdot \lambda(e))$. The words $p_{i,j}$ and $s_{i,j}$ have length at most $\lambda(e)$.

Step 5. The remaining two-dimensional knapsack equations from point (b) are eliminated with Remark 6.7. Every equation

$$p_{i,j}u_i^{x_{i,j}}s_{i,j} = s_{k,\ell}^{-1}(u_k^{-1})^{x_{k,\ell}}p_{k,\ell}^{-1}$$

can be nondeterministically replaced by a semilinear constraint

$$(x_{i,j}, x_{k,\ell}) \in \{(a_{i,j,k,\ell} + b_{i,j,k,\ell} \cdot z, a_{k,\ell,i,j} + b_{k,\ell,i,j} \cdot z) \mid z \in \mathbb{N}\}.$$

where the numbers $a_{i,j,k,\ell}, b_{i,j,k,\ell}, a_{k,\ell,i,j}, b_{k,\ell,i,j}$ are bounded by $\mathcal{O}(\lambda(e)^4)$.

At this point, we have obtained a statement of the following form: there exist $z_{i,j,k,\ell} \in \mathbb{N}$ (for $(i,j,k,\ell) \in M$) with $z_{i,j,k,\ell} = z_{k,\ell,i,j}$ and such that

(a) $x_i = c_i' + \sum_{(i,j,k,\ell)\in M}(a_{i,j,k,\ell} + b_{i,j,k,\ell} \cdot z_{i,j,k,\ell})$ for $i \in N_{\overline{a}}$, and

(b) $(x_i)_{i\in N_a} \in S_a$.

The sum in (a) contains $|K_i| \leq 14m$ many summands. Hence, (a) can be written as $x_i = c_i'' + \sum_{(i,j,k,\ell)\in M'} b_{i,j,k,\ell} \cdot z_{i,j,k,\ell}$ with

$$\begin{aligned} c_i'' &= c_i' + \sum_{(i,j,k,\ell)\in M} a_{i,j,k,\ell} \\ &\leq \mathcal{O}(m \cdot \lambda(e)) + 14m \cdot \mathcal{O}(\lambda(e)^4) \\ &= \mathcal{O}(m \cdot \lambda(e)^4). \end{aligned}$$

We therefore obtained a semilinear representation for $\mathsf{sol}_G(e)$ whose magnitude is bounded by $\max\{\mathsf{K}_1, \mathsf{K}_2\}$, where

$$\mathsf{K}_1 = \mathsf{K}(2m\|e\|, m) \text{ and } \mathsf{K}_2 \leq \mathcal{O}(m\|e\|^4).$$

Step 6. For the preprocessing we apply Remark 6.19. Hence, we just have to replace $\|e\|$ by $3\|e\|$ in the above bounds, which yields the statement of the theorem. □

Remark 6.22. By Theorem 4.3, $\mathsf{K}_{G,\Sigma}$ is polynomially bounded if $\mathsf{K}_{G_1,\Sigma}$ and $\mathsf{K}_{G_2,\Sigma}$ are polynomially bounded. This was also shown in [68].

Remark 6.23. Analogously to Remark 6.20, the above proof shows that the set of solutions $\mathsf{sol}_G(e)$ for $G = G_1 * G_2$ can be written as a finite union

$$\mathsf{sol}_G(e) = \bigcup_{i=1}^{p} \bigoplus_{j=1}^{q_i} \mathsf{sol}_{H_{i,j}}(e_{i,j}) \oplus L_i$$

such that the following hold for every $1 \leq i \leq p$:

- every $H_{i,j}$ is either G_1 or G_2 and $e_{i,j}$ is a knapsack expression over the group $H_{i,j}$. The variable sets $X_{e_{i,j}}$ $(1 \leq j \leq q_i)$ form a partition of the set X_a (the variables corresponding to atomic periods).
- Every $e_{i,j}$ is a knapsack expression of size at most $6m\|e\|$ and degree at most m.
- The set L_i is semilinear of magnitude $\mathcal{O}(mn^4)$.

Here, the indices $i \in [1, p]$ correspond to the guessed data in the above prove. Moreover, given $i \in [1, p]$, one can compute the knapsack expressions $e_{i,j}$ $(1 \leq j \leq q_i)$ and a semilinear representation of L_i in polynomial time.

The above remark and Lemma 2.3 immediately yields the following complexity transfer result (similarly to Theorem 5.1).

Theorem 6.24. *The knapsack problem for $G_1 * G_2$ is nondeterministically polynomial time reducible to* $\textsc{Knapsack}(G_1)$ *and* $\textsc{Knapsack}(G_2)$.

The consequence of Theorem 6.24 that solvability of the knapsack problem in NP is passed on from G_i for $i = 1, 2$ to the free product $G_1 * G_2$ was shown using different methods in the extended abstract [67] (see also the comment after Theorem 7.8).

6.8 Open problems

Despite Theorem 6.24, it is not known, whether there exists a group $G = G_1 * G_2$, such that $\textsc{Knapsack}(G_1)$ and $\textsc{Knapsack}(G_2)$ are in P, but $\textsc{Knapsack}(G)$ is NP-complete. There is a fact which indicates that $\textsc{Knapsack}(G)$ could indeed be more difficult than $\textsc{Knapsack}(G_i)$: We know that $\textsc{Knapsack}(\mathbb{Z})$ is in TC^0, whereas $\textsc{Knapsack}(\mathbb{Z} * \mathbb{Z})$ is LogCFL-complete [68].

Chapter 7

HNN-extensions and amalgamated products over finite subgroups

7.1 Introduction

In this chapter we deal with two constructions that are of fundamental importance in combinatorial group theory [69], namely HNN-extensions and amalgamated products. As mentioned in Section 2.4, HNN-extensions have been used to construct groups with an undecidable word problem, which means they may destroy desirable algorithmic properties. Here we consider the special case of finite associated (resp. identified) subgroups, which preserve a wider range of algorithmic properties. We show that in these cases, knapsack-semilinearity is preserved as well. We make use of similar techniques as in Chapter 6 and hence we even obtain bounds for the magnitudes.

As transfer results, we obtain both Theorem 7.7 and Theorem 7.8. They state that for $H = \langle H', t \mid t^{-1}at = \varphi(a)\ (a \in A)\rangle$ and $G = G_1 *_A G_2$ with A finite, we can conclude that $\textsc{Knapsack}(H)$ reduces to $\textsc{Knapsack}(H')$ and $\textsc{Knapsack}(G)$ reduces to $\textsc{Knapsack}(G_1)$ and $\textsc{Knapsack}(G_2)$ nondeterministically in polynomial time.

In the next chapter, we will consider a different case for a subclass of HNN-extensions with infinite associated subgroups. There we only obtain preservation of knapsack-semilinearity without bounds for the magnitude.

7.2 Further results on HNN-extensions

In this section, we consider arbitrary subgroups A and B of G. This means, any of these results holds for every HNN-extension. To exploit the symmetry of the situation, we use the notation $A(+1) = A$ and $A(-1) = B$. Then, we have $\varphi^\alpha \colon A(\alpha) \to A(-\alpha)$ for $\alpha \in \{+1, -1\}$. We will make use of the (possibly

infinite) alphabet $\Gamma = G\backslash\{1\}$. By $h\colon (\Gamma \cup \{t, t^{-1}\})^* \to H$, we denote the canonical morphism that maps each word to the element of H it represents.

A word $u \in (\Gamma \cup \{t, t^{-1}\})^*$ is called *Britton-reduced* if it does not contain a factor of the form cd with $c, d \in \Gamma$ or a factor $t^{-\alpha}at^{\alpha}$ with $a \in \Gamma^*$, $a \in_G A(\alpha)$ and $\alpha \in \{-1, 1\}$. A factor of the form $t^{-\alpha}at^{\alpha}$ with $a \in \Gamma^*$, $a \in_G A(\alpha)$ and $\alpha \in \{-1, 1\}$ is also called a *pin*. In this general definition it is also important that a is actually a word over Γ. Note that the equation $t^{-\alpha}at^{\alpha} = \varphi^{\alpha}(a)$ allows us to replace a pin $t^{-\alpha}at^{\alpha}$ by $\varphi^{\alpha}(a) \in_G A(-\alpha)$. Since this decreases the number of t's in the word, we can reduce every word to an equivalent Britton-reduced word. We denote the set of all Britton-reduced words in the HNN-extension (2.2) by $\mathsf{BR}(H)$.

For $u \in (\Gamma \cup \{t, t^{-1}\})^*$ we define $\pi_t(u)$ as the projection of the word u onto the alphabet $\{t, t^{-1}\}$ and $\pi_\Gamma(u)$ as the projection of the word u onto the alphabet Γ. Britton's lemma states that if $u =_H 1$ ($u \in (\Gamma \cup \{t, t^{-1}\})^*$) then u contains a pin or $u \in \Gamma^*$ and $u =_G 1$. Note that a consequence of this is that if $u \in_H G$ then u contains a pin or $u \in \Gamma^*$. To see this, note that $u \in_H G$ implies that $uv =_H 1$ for a word $v \in \Gamma^*$. Britton's lemma implies that uv must contain a pin (i.e., u must contain a pin) or $uv \in \Gamma^*$ (i.e., $u \in \Gamma^*$). In particular, a Britton-reduced word that contains $t^{\pm 1}$ cannot represent an element of the base group G.

A word $w \in \mathsf{BR}(H) \setminus \Gamma$ is called *well-behaved*, if w^m is Britton-reduced for every $m \geq 0$. Note that w is well-behaved if and only if w and w^2 are Britton-reduced. Elements of Γ are also called *atomic*.

The *length* of a word $w \in (\Gamma \cup \{t, t^{-1}\})^*$ is defined as usual and denoted by $|w|$. For a word $w = a_1 a_2 \cdots a_k$ with $a_i \in \Gamma \cup \{t, t^{-1}\}$ we define the the *representation length* of w as $\|w\| = \sum_{i=1}^{k} n_i$, where $n_i = 1$ if $a_i \in \{t, t^{-1}\}$ and n_i is the geodesic length of a_i in the group G if $a_i \in \Gamma$.[7]

The following lemma provides a necessary and sufficient condition for equality of Britton-reduced words in an HNN-extension (cf. Lemma 2.2 of [42]):

Lemma 7.1. *Let $u = g_0 t^{\delta_1} g_1 \cdots t^{\delta_k} g_k$ and $v = h_0 t^{\varepsilon_1} h_1 \cdots t^{\varepsilon_\ell} h_\ell$ be Britton-reduced words with $g_0, \ldots, g_k, h_0, \ldots, h_\ell \in G$ and $\delta_1, \ldots \delta_k, \varepsilon_1, \ldots, \varepsilon_\ell \in \{1, -1\}$. Then $u = v$ in the HNN-extension H of G if and only if the following hold:*

- *$k = \ell$ and $\delta_i = \varepsilon_i$ for $1 \leq i \leq k$*
- *there exist $c_1, \ldots, c_{2m} \in A \cup B$ such that:*
  - *$g_i c_{2i+1} = c_{2i} h_i$ in G for $0 \leq i \leq k$ (here we set $c_0 = c_{2k+1} = 1$)*
  - *$c_{2i-1} \in A(\delta_i)$ and $c_{2i} = \varphi^{\delta_i}(c_{2i-1}) \in A(-\delta_i)$ for $1 \leq i \leq k$.*

The second condition of the lemma can be visualized by the diagram from Figure 7.1 (also called a van Kampen diagram, see [69] for more details), where $k = \ell = 4$. Light-shaded (resp. dark-shaded) faces represent relations in G (resp. relations of the form $ct^{\delta} = t^{\delta}\varphi^{\delta}(c)$ with $c \in A(\delta)$). The elements $c_1, \ldots, c_{2k}$ in such a diagram are also called *connecting elements*.

[7] Recall that G is given as $G = \langle \Sigma \mid R \rangle$ and that the geodesic length of $a \in \Gamma$ is defined as the length of the shortest word $w \in \Sigma^*$, which evaluates to a (see Subsection 2.4.1).

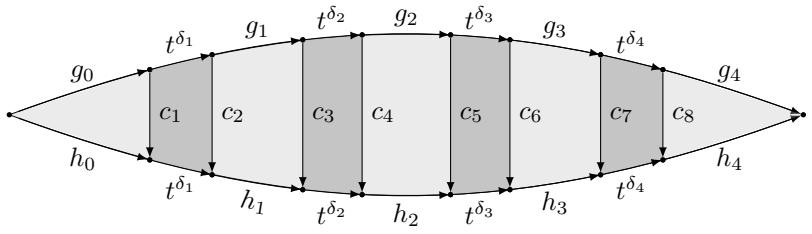

Figure 7.1: A van Kampen diagram witnessing the equality of two Britton-reduced words in the HNN-extension H.

For our purposes, we will need the following lemma (cf. Lemma 2.3 of [42]), which allows us to transform an arbitrary string over the generating set of an HNN-extension into a reduced one:

Lemma 7.2. *Assume that $u = g_0 t^{\delta_1} g_1 \cdots t^{\delta_k} g_k$ and $v = h_0 t^{\varepsilon_1} h_1 \cdots t^{\varepsilon_\ell} h_\ell$ are Britton-reduced words ($g_i, h_j \in G$). Let $m(u,v)$ be the largest number $m \geq 0$ such that*

(a) $A(\delta_{k-m+1}) = A(-\varepsilon_m)$ (we set $A(\delta_{k+1}) = A(-\varepsilon_0) = 1$) and

(b) there is $c \in A(-\varepsilon_m)$ such that

$$t^{\delta_{k-m+1}} g_{k-m+1} \cdots t^{\delta_k} g_k h_0 t^{\varepsilon_1} \cdots h_{m-1} t^{\varepsilon_m} =_H c$$

(for $m = 0$ this condition is satisfied with $c = 1$).

Moreover, let $c(u,v) \in A(-\varepsilon_m)$ be the element c in (b) (for $m = m(u,v)$). Then

$$g_0 t^{\delta_1} g_1 \cdots t^{\delta_{k-m(u,v)}} \gamma(u,v) t^{\varepsilon_{m(u,v)+1}} h_{m(u,v)+1} \cdots t^{\varepsilon_\ell} h_\ell$$

is a Britton-reduced word equal to uv in H, where $\gamma(u,v) \in G$ such that $\gamma(u,v) =_G g_{k-m(u,v)} c(u,v) h_{m(u,v)}$.

The above lemma is visualized in Figure 7.2.

Lemma 7.3. *From a given word $u \in \mathsf{BR}(H)$ we can compute words $s, p, v \in \mathsf{BR}(H)$ such that $u^m =_H s v^m p$ for every $m \geq 0$ and either $v \in G$ or v is well-behaved and starts with $t^{\pm 1}$. Moreover, $\|s\| + \|p\| + \|v\| \leq 3\|u\|$.*

Proof. Let $u \in \mathsf{BR}(H)$. Assume that u is not atomic; otherwise we are done. Let us now consider the word u^2. If u^2 is not Britton-reduced, we can do the following: using Britton-reduction we compute a factorization $u = xyz$ such that $zx =_H g \in G$ and hence $u^2 =_H xygyz$, where moreover x and y are chosen such that the sum $|x| + |z|$ is maximal. Note that either $y = 1$ or y begins and ends with t or t^{-1} (otherwise we could make x or z longer). Moreover, $\|g\| \leq \|u\|$. We obtain the equality $u^m = (xyz)^m =_H x(yg)^m g^{-1} z$ for every $m \geq 0$. We set $s = x$, $v = yg$, and $p = g^{-1}z$. If $y = 1$, we have $v = g \in G$. Now assume that y begins and ends with t or t^{-1}. Since y as a factor of u must be Britton-reduced,

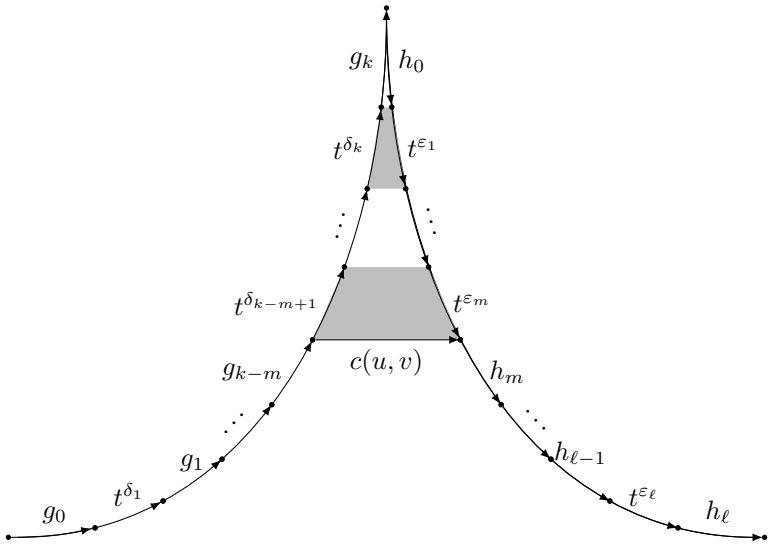

Figure 7.2: The situation from Lemma 7.2.

also $v = yg$ is Britton-reduced. Moreover, $v^2 = ygyg$ must be Britton-reduced, otherwise we could extend the length of x and z in the factorization $u = xyz$. Finally, we have $\|s\| + \|p\| + \|v\| = \|x\| + \|y\| + \|z\| + 2\|g\| \leq 3\|u\|$. □

We now define 1-reducible tuples for HNN-extensions similar to the case of graph products (see chapter 6). Again we identify tuples that can be obtained from each other by inserting/deleting 1's at arbitrary positions.

Definition 7.4. We define a reduction relation on tuples over $\mathsf{BR}(H)$ of arbitrary length. Take $u_1, u_2, \ldots, u_m \in \mathsf{BR}(H)$. Then we have

- $(u_1, u_2, \ldots, u_i, a, u_{i+1}, \ldots, u_m) \to (u_1, \ldots, u_{i-1}, b, u_{i+2}, \ldots, u_m)$ if both u_i and u_{i+1} contain t or t^{-1} and $u_i a u_{i+1} =_H b$ for $a, b \in A \cup B$ (a *generalized cancellation step*),
- $(u_1, u_2, \ldots, u_m) \to (u_1, \ldots, u_{i-1}, g, u_{i+2}, \ldots, u_m)$ if $u_i, u_{i+1} \in \Gamma$ and $g =_G u_i u_{i+1} \in G$.

If $g \neq 1$ then we call the last rewrite step an *atom creation*. A concrete sequence of these rewrite steps leading to the empty tuple is a *reduction* of $(u_1, u_2, \ldots, u_m)$. If such a sequence exists, the tuple is called 1-*reducible*.

A reduction of a tuple $(u_1, u_2, \ldots, u_m)$ can be seen as a witness for the fact that $u_1 u_2 \cdots u_m =_H 1$. On the other hand, $u_1 u_2 \cdots u_m =_H 1$ does not necessarily imply that $u_1, u_2, \ldots, u_m$ has a reduction (as seen for graph products). But we can show that every sequence which multiplies to 1 in H can be refined (by factorizing the elements of the sequence) such that the resulting refined sequence has a reduction. We say that the tuple $(v_1, v_2, \ldots, v_n)$ is a *refinement* of the tuple

$(u_1, u_2, \ldots, u_m)$ if there exist factorizations $u_i = u_{i,1} \cdots u_{i,k_i}$ in $(\Gamma \cup \{t, t^{-1}\})^*$ such that $(v_1, v_2, \ldots, v_n) = (u_{1,1}, \ldots, u_{1,k_1}, \ldots, u_{m,1}, \ldots, u_{m,k_m})$.

Lemma 7.5. *Let $m \geq 2$ and $u_1, u_2, \ldots, u_m \in \mathsf{BR}(H)$. If $u_1 u_2 \cdots u_m = 1$ in H, then there exists a 1-reducible refinement of $(u_1, u_2, \ldots, u_m)$ that has length at most $7m - 12 \leq 7m$ and there is a reduction of this refinement with at most $4m - 8$ atom creations.*

Proof. We prove the lemma by induction on m. The induction is similar to the one of Lemma 6.17. The case $m = 2$ is trivial (we must have $u_2 = u_1^{-1}$). If $m \geq 3$ then by Lemma 7.2 we can factorize u_1 and u_2 in $(\Gamma \cup \{t, t^{-1}\})^*$ as $u_1 = u_1' g_1 r$ and $u_2 = s g_2 u_2'$ such that $rs =_H c \in A \cup B$, $g_1, g_2 \in G$ and $u_1 u_2 =_H u_1' g u_2' \in \mathsf{BR}(H)$ for $g = g_1 c g_2 \in G$. The words r and s are either both empty (in which case we have $c = 1$) or r starts with some t^{ε} and s ends with $t^{-\varepsilon}$.

By induction hypothesis, for the tuple $(u_1' g u_2', u_3, \ldots, u_m)$ there is a 1-reducible refinement

$$(v_1, \ldots, v_k, u_{3,1}, \ldots, u_{3,k_3}, \ldots, u_{m,1}, \ldots, u_{m,k_m}), \tag{7.1}$$

with $4(m-1) - 8$ atom creations, where $k + \sum_{i=3}^{m} k_i \leq 7(m-1) - 12$ and $u_1' g u_2' = v_1 \cdots v_k$ in $(\Gamma \cup \{t, t^{-1}\})^*$. Since $g \in G$, there exists $1 \leq i \leq k$, such that $v_i = v_{i,1} g v_{i,2}$, $u_1' = v_1 \cdots v_{i-1} v_{i,1}$ and $u_2' = v_{i,2} v_{i+1} \cdots v_k$. Now we replace v_i by $v_{i,1}, g, v_{i,2}$ in the above refinement (7.1). If there exists $u_{j,\ell}$ such that v_i and $u_{j,\ell}$ cancel out in a generalized cancellation step in the 1-reduction of (7.1) then there exist $a, b \in A \cup B$ such that $v_{i,1} g v_{i,2} a u_{j,\ell} = v_i a u_{j,\ell} =_H b$. The generalized cancellation replaces $v_i, a, u_{j,\ell}$ by b.

Recall that v_i and $u_{j,\ell}$ are both Britton-reduced. By Lemma 7.1 we can factorize $u_{j,\ell}$ in $(\Gamma \cup \{t, t^{-1}\})^*$ as $u_{j,\ell} = w_1 g' w_2$ such that there exist connecting elements $a', b' \in A \cup B$ with $v_{i,2} a w_1 =_H a'$, $v_{i,1} b' w_2 =_H b$, and $g a' g' =_G b'$; see Figure 7.3. This yields the refined tuple

$$(v_1, \ldots, v_{i-1}, v_{i,1}, g_1, r, s, g_2, v_{i,2}, v_{i+1}, \ldots, v_k, \tilde{u}_{3,1}, \ldots, \tilde{u}_{3,k_3}, \ldots, \tilde{u}_{m,1}, \ldots, \tilde{u}_{m,k_m}),$$

of $(u_1, u_2, \ldots, u_m)$, where $\tilde{u}_{j,\ell} = w_1, g', w_2$ and $\tilde{u}_{p,q} = u_{p,q}$ in all other cases. The length of this tuple is at most $k + 7 + \sum_{i=3}^{m} k_i \leq 7m - 12$. The above tuple is also 1-reducible: First, r, s is replaced by c in a generalized cancellation step. Then, after at most two atom creations[8] we obtain the tuple

$$(v_1, \ldots, v_{i-1}, v_{i,1}, g, v_{i,2}, v_{i+1}, \ldots, v_k, \tilde{u}_{3,1}, \ldots, \tilde{u}_{3,k_3}, \ldots, \tilde{u}_{m,1}, \ldots, \tilde{u}_{m,k_m}).$$

At this point, we can basically apply the fixed reduction of (7.1). The generalized cancellation $v_i, a, u_{j,\ell} \to b$ is replaced by the sequence

$$v_{i,1}, g, v_{i,2}, a, w_1, g', w_2 \to v_{i,1}, g, a', g', w_2 \to v_{i,1}, g a', g', w_2 \to v_{i,1}, b', w_2 \to b$$

[8] Note that each of c, g_1, g_2 can be 1, in which case the number of atom creations is smaller than two.

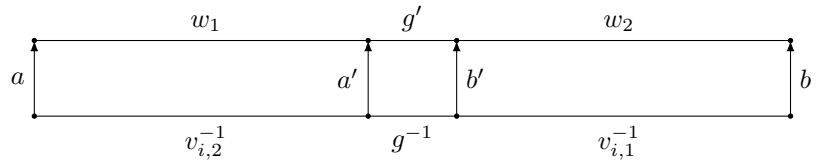

Figure 7.3: The generalized cancellation step for v_i and $u_{j,\ell} = w_1 g' w_2$ in the proof of Lemma 7.5.

which contains at most two atom creations. Hence, the total number of atom creations is at most $4 + 4(m-1) - 8 = 4m - 8$. This concludes the proof of the lemma. □

7.3 Specific results for HNN-extensions over finite associated subgroups

For the rest of this chapter, we only consider the case that A and B are finite groups, so that we may assume that $(A \cup B) \setminus \{1\}$ is contained in the finite generating set Σ. Note that in this case $\|a\| = 1$ for $a \in (A \cup B) \setminus \{1\}$. Also, let γ be the cardinality of A.

Lemma 7.6. *Let $u, v \in \mathsf{BR}(H) \backslash G$ be well-behaved, both starting with $t^{\pm 1}$, $a, b \in A \cup B$, u' (resp., v') be a proper suffix of u (resp., v) and u'' (resp., v'') be a proper prefix of u (resp., v). Let $\mu = \max\{|u|, |v|\}$. Then the set*

$$L(a, u', u, u'', v', v, v'', b) = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid au'u^x u'' =_H v'v^y v''b\}$$

is semilinear. Moreover, one can compute in polynomial time a semilinear representation whose magnitude is bounded by $\mathcal{O}(\gamma^2 \mu^4)$.

Proof. The proof is inspired by the proof of [62, Lemma 8.3] for hyperbolic groups. The assumptions in the lemma imply that for all $x, y \in \mathbb{N}$ the words $au'u^x u''$ and $v'v^y v''b$ are Britton-reduced (possibly after multiplying a and b with neighboring symbols from Γ. For a word $w \in (\Gamma \cup \{t, t^{-1}\})^*$ we define $|w|_{t^{\pm 1}} = |w|_t + |w|_{t^{-1}}$ (the $t^{\pm 1}$-length of w). Clearly, for Britton-reduced words w, w' with $w =_H w'$ we have $|w|_{t^{\pm 1}} = |w'|_{t^{\pm 1}}$.

We will first construct an automaton $\mathcal{A}$ over the unary alphabet $\{\#\}$, where $\#$ is a fresh letter, such that

$$L(\mathcal{A}) = \{\#^\ell \mid \exists x, y \in \mathbb{N} : au'u^x u'' =_H v'v^y v''b, \ell = |au'u^x u''|_{t^{\pm 1}}\}.$$

Moreover, the number of states of $\mathcal{A}$ is $\mathcal{O}(\mu^2 \cdot \gamma)$. Roughly speaking, the automaton $\mathcal{A}$ verifies from left to right the existence of a van Kampen diagram of the form shown in Figure 7.1. Thereby it stores the current connecting element (an element from $A \cup B$). By the assumptions on u and v we can

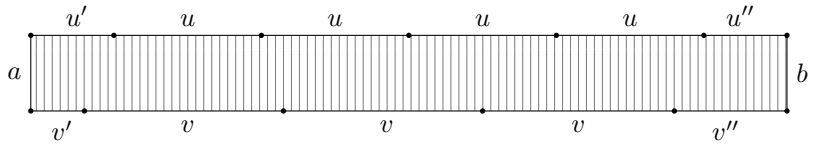

Figure 7.4: In the proof of Lemma 7.6 the automaton stores the connecting elements, i.e. checks the rectangles.

write both words as $u = u_0u_1 \cdots u_{m-1}$, $v = v_0v_1 \cdots v_{n-1}$ where n and m are even, $u_i \in \{t, t^{-1}\}$ for i even and $u_i \in G$ for i odd, and analogously for v. Let us write $u' = u_pu_{p+1} \cdots u_{m-1}$, $u'' = u_0u_1 \cdots u_{q-1}$, $v' = v_rv_{r+1} \cdots v_{n-1}$, $v'' = v_0v_1 \cdots v_{s-1}$. We set $p = m$ if u' is empty and $q = 0$ if u'' is empty and similarly for r and s. We will first consider the case that $p \equiv r \bmod 2$ and $q \equiv s \bmod 2$; other cases are just briefly sketched at the end of the proof.

The state set of $\mathcal{A}$ is

$$Q = \{(c, i, j) \mid c \in A \cup B, 0 \leq i < m, 0 \leq j < n, i \equiv j \bmod 2\}.$$

The initial state is $(a, p \bmod m, r \bmod n)$ and the only final state is $(b, q \bmod m, s \bmod n)$. Finally, $\mathcal{A}$ contains the following transitions for $c_1, c_2 \in A \cup B$ such that $c_1u_i =_H v_jc_2$ (in case i and j are odd, this must be an identity in G since $u_i, v_j \in G$):

- $(c_1, i, j) \xrightarrow{\#} (c_2, i + 1 \bmod m, j + 1 \bmod n)$ if i and j are even,
- $(c_1, i, j) \xrightarrow{1} (c_2, i + 1 \bmod m, j + 1 \bmod n)$ if i and j are odd.

The number of states of $\mathcal{A}$ is $\mathcal{O}(\gamma \cdot \mu^2)$. If $p \equiv r \bmod 2$ does not hold, then we have to introduce a fresh initial state q_0. Assume that for instance p is odd and r is even. Thus u_p belongs to G whereas v_r is t or t^{-1}. Then we add all transitions $q_0 \xrightarrow{1} (c, p + 1 \bmod m, r \bmod n)$ for every $c \in A \cup B$ with $au_p =_G c$. If $q \equiv s \bmod 2$ does not hold, then we have to add a fresh final state q_f.

The rest of the argument is the same as in Remark 6.7, we only have to replace the length of words by the $t^{\pm 1}$-length. We obtain a semilinear representation of $L(a, u', u, u'', v', v, v'', b)$ of magnitude $\mathcal{O}(\gamma^2 \cdot \mu^4)$. □

7.4 HNN-extensions over finite associated subgroups preserve knapsack-semilinearity

Now we can prove

Theorem 4.4 ([F6]). *Let A, B be finite subgroups of G and let $\varphi\colon A \to B$ be an isomorphism. If G is knapsack-semilinear, then the HNN-extension H of G (with respect to the isomorphism φ) is knapsack-semilinear as well. Moreover,*

we have $\mathsf{K}_{H,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2\}$ *with*

$$\mathsf{K}_1 = \mathsf{K}_{G,\Sigma}(24mn, m) \text{ and } \mathsf{K}_2 \leq \mathcal{O}(\gamma^2 mn^4),$$

where $\gamma = |A|$.

Proof. We will follow the idea of the proof of Theorems 4.2 and 4.3, respectively. We first consider the case where every period u_i is either an atom or well-behaved and starts with $t^{\pm 1}$. Again we are going through the six steps. For simplicity, we write K instead of $\mathsf{K}_{G,\Sigma}$.

Step 1. This step is carried out in the same way as in the proof of Theorem 4.2.

Step 2. Here we can use Lemma 7.5 instead of Lemma 6.15, which yields the upper bound of $14m$ on the number of factors in our refinement of $u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_m^{x_m} v_m$ (where powers $u_i^{x_i}$ with $i \in N_1$ have been removed). The number of atom creations is at most $8m - 8$.

Step 3. This step is copied from the proof of Theorem 4.2. We obtain for the variables x_i with $i \in N_a$ the semilinear constraint $(x_i)_{i \in N_a} \in S_a$ where S_a is of magnitude at most $\mathsf{K}(8m\|e\|, m)$.

Step 4. This step is analogous to the proof of Theorem 4.3. The only difference is that the 2-dimensional knapsack instances are produced by the generalized cancellation steps from Definition 7.4. We arrive at a statement of the following form: there exist integers $x_{i,j} \geq 0$ ($i \in N_{\overline{a}}$, $j \in K_i$) such that the following hold:

(a) $x_i = c'_i + \sum_{j \in K_i} x_{i,j}$ for $i \in N_{\overline{a}}$,

(b) $a_{i,j} p_{i,j} u_i^{x_{i,j}} s_{i,j} =_H s_{k,\ell}^{-1} (u_k^{-1})^{x_{k,\ell}} p_{k,\ell}^{-1} b_{i,j}$ for all $(i,j,k,\ell) \in M$,

(c) $(x_i)_{i \in N_a} \in S_a$.

Here, $K_i \subseteq [1, k_i]$ is a set of size at most $k_i \leq 14m$, M is a matching relation (with $(i,j,k,\ell) \in M$ if and only if $(k,\ell,i,j) \in M$), $a_{i,j}, b_{i,j} \in A \cup B$, and $c'_i \leq \mathcal{O}(m \cdot \lambda(e))$. Every word $p_{i,j}$ is a suffix of $u_{i,j}$ and every $s_{i,j}$ is a prefix of $u_{i,j}$. In particular, $p_{i,j}$ and $s_{i,j}$ have length at most $\lambda(e)$.

Step 5. The remaining two-dimensional knapsack equations from point (b) are eliminated with Lemma 7.6. Every equation

$$a_{i,j} p_{i,j} u_i^{x_{i,j}} s_{i,j} =_H s_{k,\ell}^{-1} (u_k^{-1})^{x_{k,\ell}} p_{k,\ell}^{-1} b_{i,j}$$

can be nondeterministically replaced by a semilinear constraint for $x_{i,j}$ and $x_{k,\ell}$ of magnitude $\mathcal{O}(\gamma^2 \lambda(e)^4)$. By substituting these semilinear constraints in the above equations (a) for the x_i (as we did in the proof of Theorem 4.2), we obtain for the variables x_i ($i \in N_{\overline{a}}$) a semilinear constraint of magnitude $\mathcal{O}(m \cdot \gamma^2 \cdot \lambda(e)^4)$. This leads to a semilinear representation for $\mathsf{sol}_H(e)$ of magnitude at most $\max\{\mathsf{K}_1, \mathsf{K}_2\}$, where

$$\mathsf{K}_1 = \mathsf{K}(8m\|e\|, m) \text{ and } \mathsf{K}_2 \leq \mathcal{O}(m \cdot \gamma^2 \cdot \|e\|^4).$$

Step 6. For the preprocessing we can apply Lemma 7.3 to each period u_i. Hence, we just have to replace $\|e\|$ by $3\|e\|$ in the above bounds, which yields the statement of the theorem. □

The following result is obtained analogously to Theorem 5.1 and Theorem 6.24.

Theorem 7.7. *The knapsack problem for $\langle G, t \mid t^{-1}at = \varphi(a)\ (a \in A)\rangle$ (with A finite) is nondeterministically polynomial time reducible to* $\textsc{Knapsack}(G)$.

The consequence of Theorem 7.7 that solvability of the knapsack problem in NP is passed on from G to H was shown using different methods in the extended abstract [67].

7.5 Amalgamated products over finite amalgamated subgroups preserve knapsack-semilinearity

Using our results for free products and HNN-extensions, we can easily deal with amalgamated products. From Theorem 4.4, we can deduce a similar result for amalgamated products, namely

Theorem 4.5 ([F6])**.** *Let G_1 and G_2 be finitely generated groups with a common subgroup A. Let $\mathsf{K}(n,m)$ be the pointwise maximum of the functions $\mathsf{K}_{G_1,\Sigma_1}$ and $\mathsf{K}_{G_2,\Sigma_2}$. Furthermore, let $\gamma = |A|$ and let G be the amalgamated product $G_1 *_A G_2$. Then with $\Sigma = \Sigma_1 \cup \Sigma_2$ we have $\mathsf{K}_{G,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2, \mathsf{K}_3\}$ where*

$$\mathsf{K}_1 = \mathsf{K}_{G,\Sigma}(144m^2n, m), \mathsf{K}_2 \leq \mathcal{O}(m^5n^4) \text{ and } \mathsf{K}_3 \leq \mathcal{O}(m \cdot \gamma^2 \cdot n^4).$$

Proof. For the proof we will make use of Theorem 4.3 for free products and Theorem 4.4 for HNN-extensions.

We remind the reader that $G = G_1 *_A G_2$ can be embedded into

$$H = \langle G_1 * G_2, t \mid t^{-1}\varphi_1(a)t = \varphi_2(a)\ (a \in A)\rangle.$$

Obviously we have $\mathsf{K}_{G,\Sigma}(n,m) \leq \mathsf{K}_{H,\Sigma}(n,m)$. Hence we can calculate the bound by first getting the bound for the free product $G_1 * G_2$ and then proceeding with the HNN-extension. Theorem 4.3 tells us that $\mathsf{J}(n,m) = \mathsf{K}_{G_1*G_2,\Sigma}(n,m) \leq \max\{\mathsf{K}_1', \mathsf{K}_2'\}$, where $\mathsf{K}_1' = \mathsf{K}(6mn, m)$ and $\mathsf{K}_2' \leq \mathcal{O}(mn^4)$. To obtain $\mathsf{K}_{H,\Sigma}(n,m)$, we make use of Theorem 4.4. We have $\mathsf{K}_{H,\Sigma}(n,m) \leq \max\{\mathsf{J}_1, \mathsf{J}_2\}$, where $\mathsf{J}_1 = \mathsf{J}(24mn, m)$ and $\mathsf{J}_2 \leq \mathcal{O}(\gamma^2 mn^4)$. Since the function $\mathsf{J}(n,m)$ appears in J_1, we have to substitute by what we calculated before. More precisely we have to make the substitution $n \mapsto 24mn$ for the values K_1' and K_2'. This yields $\mathsf{K}_{H,\Sigma}(n,m) \leq \max\{\mathsf{K}_1, \mathsf{K}_2, \mathsf{K}_3\}$, where

$$\begin{aligned}
&\mathsf{K}_1 = \mathsf{K}(144m^2n, m),\\
&\mathsf{K}_2 \leq \mathcal{O}(m^5n^4),\\
&\mathsf{K}_3 = \mathsf{J}_2 \leq \mathcal{O}(\gamma^2 mn^4).
\end{aligned}$$

This finishes the proof of the theorem. □

From Theorems 6.24 and 7.7 and the embedding of $G_1 *_A G_2$ in the HNN-extension $\langle G_1 * G_2, t \mid t^{-1}\varphi_1(a)t = \varphi_2(a)\ (a \in A)\rangle$ we obtain:

Theorem 7.8. *The knapsack problem for $G_1 *_A G_2$ (with A finite) is nondeterministically polynomial time reducible to* Knapsack(G_1) *and* Knapsack(G_2).

As before, the consequence of Theorem 7.8 that solvability of the knapsack problem in NP is passed on from G_i for $i = 1, 2$ to the amalgamated product $G_1 *_A G_2$ was shown using different methods in the extended abstract [67].

7.6 Open problems

Despite Theorem 7.7, it is not known, whether there exists an HNN-extension $H = \langle G, t \mid t^{-1}at = \varphi(a)\ (a \in A)\rangle$ with A finite, such that Knapsack(G) is in P, but Knapsack(H) is NP-complete. The same holds for amalgamated products: We have Theorem 7.8, but it is not known, whether there exists a group $G = G_1 *_A G_2$ (A finite), such that Knapsack(G_1) and Knapsack(G_2) are in P, but Knapsack(G) is NP-complete.

Chapter 8

HNN-extensions of the form $\langle G, t \mid t^{-1}at = a\,(a \in A)\rangle$

8.1 Introduction

In the last chapter, we studied HNN-extensions over finite associated subgroups and we obtained preservation of knapsack-semilinearity in this case. The goal of this chapter is show that an HNN-extension

$$H = \langle G, t \mid t^{-1}at = a\,(a \in A)\rangle$$

is knapsack-semilinear provided G is knapsack-semilinear relative to $\{1, A\}$, where A can be an infinite group (Theorem 4.6). So not only do we have restrictions on the isomorphism (φ is the identity), but we also need another condition for the associated subgroup A. We already mentioned in the beginning of the thesis that in general, HNN-extensions over infinite associated subgroups do not preserve knapsack-semilinearity, as the Baumslag-Solitar group $\mathsf{BS}(1,2) = \langle a, t \mid t^{-1}at = a^2\rangle$ is not knapsack-semilinear [32] but it is an HNN-extension of the knapsack-semilinear group $\langle a\rangle \cong \mathbb{Z}$.

As an application of Theorem 4.6, we prove Theorem 4.7, which states that the HNN-extension is knapsack-semilinear, if it is an extension of centralizer and G is knapsack-semilinear. Normally, it is not intuitive to understand the condition of being knapsack-semilinear relative to S, but in this case, we have a very explicit example.

8.2 Special results for HNN-extensions of the form $\langle G, t \mid t^{-1}at = a\,(a \in A)\rangle$

In this chapter, we consider HNN-extensions $H = \langle G, t \mid t^{-1}at = \varphi(a)\ (a \in A)\rangle$, where $A \leq G$ is a subgroup of $G = \langle \Sigma \mid R\rangle$ and $\varphi : A \to A$ is the identity

mapping. Thus, H can be written as

$$H = \langle G, t \mid t^{-1}at = a\ (a \in A)\rangle. \tag{8.1}$$

Let us fix this HNN-extension for the further consideration. As in the last chapter, let us denote with

$$h : (\Gamma \cup \{t, t^{-1}\})^* \to H$$

the evaluation morphism, where $\Gamma = G \setminus \{1\}$.

Recall that a word $u \in (\Gamma \cup \{t, t^{-1}\})^*$ is called *Britton-reduced* if it does not contain a factor of the form $t^{-\alpha}wt^{\alpha}$ with $\alpha \in \{-1, 1\}$, $w \in \Gamma^*$ and $w \in_G A$. Also recall that a factor of the form $t^{-\alpha}wt^{\alpha}$ with $\alpha \in \{-1, 1\}$, $w \in \Gamma^*$ and $w \in_G A$ is called a *pin*, which we can replace by w.

In this special case, we have $H/N(t) \cong G$, where $N(t)$ is the smallest normal subgroup of H containing t. By $\pi_G : H \to G$ we denote the canonical projection. We have $\pi_G(g_0t^{\delta_1}g_1 \cdots t^{\delta_k}g_k) = g_0g_1 \cdots g_k$ for $g_0, \ldots, g_k \in G$. Hence, on the level of words, π_G is computed by the projection $\pi_\Gamma : (\Gamma \cup \{t, t^{-1}\})^* \to \Gamma^*$.

Lemma 8.1. *Let $w \in (\Gamma \cup \{t, t^{-1}\})^*$. Then $w =_H 1$ if and only if $w \in_H G$ and $\pi_\Gamma(w) =_G 1$.*

Proof. If $w =_H 1$, i.e., $h(w) = 1$, then clearly $w \in_H G$. Moreover, by Britton's lemma, w can be reduced to a word from Γ^* using Britton reduction. But this word must be $\pi_\Gamma(w)$. Hence, we have $\pi_\Gamma(w) =_G 1$. On the other hand, if $w \in_H G$ and $\pi_\Gamma(w) =_G 1$, then, again, w can be reduced to $\pi_\Gamma(w) =_G 1$ using Britton reduction, which implies $w =_H 1$. □

We will also need the simplified version of Lemma 7.2:

Lemma 8.2. *Assume that $u = u_0t^{\delta_1}u_1 \cdots t^{\delta_k}u_k$ and $v = v_0t^{\varepsilon_1}v_1 \cdots t^{\varepsilon_\ell}v_\ell$ are Britton-reduced words with $u_i, v_j \in \Gamma^*$. Let $0 \leq m \leq \max\{k, \ell\}$ be the largest number such that*

- *$\delta_{k-i} = -\varepsilon_{i+1}$ for all $0 \leq i \leq m-1$ and*
- *$u_{k-i+1} \cdots u_k v_0 \cdots v_{i-1} \in_G A$ for all $0 \leq i \leq m$ (for $i = 0$ this condition is trivially satisfied).*

Then $w := u_0t^{\delta_1}u_1 \cdots t^{\delta_{k-m}}(u_{k-m} \cdots u_k v_0 \cdots v_m)t^{\varepsilon_{m+1}}v_{m+1} \cdots t^{\varepsilon_\ell}v_\ell$ is a Britton-reduced word with $w =_H uv$.

For simplicity reasons, in this chapter we call *all* words $w \in \mathsf{BR}(H)$ well-behaved (if w^m is Britton-reduced for every $m \geq 0$), and hence every word $w \in \Gamma^*$ is well-behaved (not "atomic").

In the following we assume that G is knapsack-semilinear relative to $\{1, A\}$. For a knapsack expression $e = v_0u_1^{x_1}v_1u_2^{x_2}v_2 \cdots u_k^{x_k}v_k$ over the alphabet $\Sigma \cup \{t, t^{-1}\}$ we define the knapsack expression

$$\pi_\Sigma(e) = \pi_\Sigma(v_0)\pi_\Sigma(u_1)^{x_1}\pi_\Sigma(v_1)\pi_\Sigma(u_2)^{x_2}\pi_\Sigma(v_2) \cdots \pi_\Sigma(u_k)^{x_k}\pi_\Sigma(v_k)$$

over the alphabet Σ. Note that for algorithmic purposes we use the finite symmetric generating set Σ of G instead of Γ for the rest of this chapter. Hence, each $u \in \Gamma$ is represented as a word over Σ.

For an exponent expression $e(x_1, \ldots, x_n)$ over the alphabet $\Sigma \cup \{t, t^{-1}\}$ we call

$$e(x_1, \ldots, x_n) \in_H G$$

a *G-constraint*. If e is an exponent expression over the alphabet Σ, then $e \in_G A$ is called an A-constraint. Since G is knapsack-semilinear relative to A, the set of solutions of an A-constraint is semilinear.

Lemma 8.3. *Let $u, v \in \mathsf{BR}(H)$ be well-behaved, u' (resp., v'') be a proper prefix of u (resp., v) and u'' (resp., v') be a proper suffix of u (resp., v). Let $e = e(z_1, \ldots, z_k)$ be a knapsack expression over the alphabet Σ. Then the set of all $(x, y, z_1, \ldots, z_k) \in \mathbb{N}^{k+2}$ such that the G-constraint*

$$u''u^x u' e(z_1, \ldots, z_k)\, v' v^y v'' \in_H G \tag{8.2}$$

holds is semilinear and a semilinear representation can be effectively computed from the words $u, v, u', u'', v', v'', e$.

Proof. We first claim that by cyclically rotating u and v we can assume that $u'' = v'' = 1$. We only prove this for u'', for v'' we can argue analogously. We can write $u = ru''$ for some word r. Then for all $x \in \mathbb{N}$ we have $u''u^x u' = u''(ru'')^x u' = (u''r)^x u''u'$. The word $u''u'$ is either a prefix of $u''r$ or we can write $u''u' = (u''r)\tilde{u}$ for some prefix $\tilde{u}$ of $u''r$. In the first case, we can simply replace $u''u^x u'$ in (8.2) by $(u''r)^x u''u'$ (note that $u''r$ is well-behaved since it is a cyclic rotation of the well-behaved word $u = ru''$). In the second case (where $u''u' = (u''r)\tilde{u}$ for some prefix $\tilde{u}$ of $u''r$), we replace $u''u^x u'$ in (8.2) by $(u''r)^x \tilde{u}$. If $L \subseteq \mathbb{N}^{\{x, y, z_1, \ldots, z_k\}}$ is the set of solutions of the resulting G-constraint, then the formula $(x + 1, y, z_1, \ldots, z_k) \in L$ describes the set of solution of (8.2). Clearly, a Presburger formula for L immediately yields a Presburger formula for $(x + 1, y, z_1, \ldots, z_k) \in L$.

By the previous paragraph, it suffices to consider the set of solutions of the G-constraint

$$u^x u' e(z_1, \ldots, z_k)\, v' v^y \in_H G.$$

This constraint holds (for certain values of $x, y, z_1, \ldots, z_k$) if and only if $u^x u' e(z_1, \ldots, z_k)\, v' v^y$ can be Britton-reduced to a word from Σ^* which must be $\pi_\Sigma(u^x u' e(z_1, \ldots, z_k)\, v' v^y)$. Since u^x and v^y are Britton-reduced for every $x, y \in \mathbb{N}$ we can apply Lemma 8.2.

Let S_u be the set of suffixes of u that start with $t^{\pm 1}$ and let P_v be the set of prefixes of v that end with $t^{\pm 1}$. We define $S_{u'}$ and $P_{v'}$ analogously. Then by Lemma 8.2 the following formula is equivalent to $u^x u' e(z_1, \ldots, z_n)\, v' v^y \in_H G$ (as usual, $\wedge$ denotes logical conjunction and $\Rightarrow$ denotes logical implication):

$$\pi_t(u^x u') = \pi_t(v'v^y)^{-1} \;\wedge$$
$$\forall x' < x\, \forall y' < y : \bigwedge_{s \in S_u} \bigwedge_{p \in P_v} \pi_t(s\, u^{x'} u') = \pi_t(v' v^{y'} p)^{-1}$$
$$\Rightarrow\; \pi_\Sigma(s\, u^{x'} u'\, e\, v' v^{y'} p) \in_G A$$

$$\bigwedge_{s \in S_u} \bigwedge_{p \in P_{v'}} \pi_t(s\, u^{x'} u') = \pi_t(p)^{-1} \;\Rightarrow\; \pi_\Sigma(s\, u^{x'} u'\, e\, p) \in_G A$$
$$\bigwedge_{s \in S_{u'}} \bigwedge_{p \in P_v} \pi_t(s) = \pi_t(v' v^{y'} p)^{-1} \;\Rightarrow\; \pi_\Sigma(s\, e\, v' v^{y'} p) \in_G A$$
$$\bigwedge_{s \in S_{u'}} \bigwedge_{p \in P_{v'}} \pi_t(s) = \pi_t(p)^{-1} \;\Rightarrow\; \pi_\Sigma(s\, e\, p) \in_G A.$$

Let us explain the intuition behind this formula; see also Figure 8.1 which shows a van Kampen diagram for $u^8 u' e(z_1, \ldots, z_k)\, v' v^5 =_H g$.

The formula $\pi_t(u^x u') = \pi_t(v' v^y)^{-1}$ expresses that every t (resp., t^{-1}) in $u^x u'$ cancels with a t^{-1} (resp., t) in $v' v^y$. If this is not the case, then $u^x u' e(z_1, \ldots, z_k)\, v' v^y$ cannot be Britton-reduced to a word over Σ. The other four lines of the formula ensure that the Britton-reduction of $u^x u' e(z_1, \ldots, z_k)\, v' v^y$ to a word over Σ actually exists. This Britton-reduction proceeds from right to left in Figure 8.1. In each reduction step, the right-most slice in Figure 8.1 is eliminated. Assume that the Britton-reduction has already eliminated the part to the right of the shaded slice. The special form of our HNN-extension (8.1) implies that if a word $w \in (\Sigma \cup \{t, t^{-1}\})^*$ is Britton-reduced to a word over Σ, then we have $w =_H \pi_\Sigma(w)$ (every Britton-reduction step is of the form $t^{-1}at \to a$ or $tat^{-1} \to a$ for $a \in A$). Hence, we must have $a =_G \pi_\Sigma(s\, u^4 u'\, e\, v' v^2 p)$ in Figure 8.1. In order to eliminate the shaded slice, the following must hold:

- a must belong to the subgroup A, i.e., $\pi_\Sigma(s\, u^4 u'\, e\, v' v^2 p) \in_G A$,
- the first letter of s (a suffix of u) must be t (or t^{-1}), and
- the last letter of p (a prefix of v) must be t^{-1} (or t); note that v goes from right to left.

The second line in the above formula ensures that $\pi_\Sigma(s\, u^{x'} u'\, e\, v' v^{y'} p) \in_G A$ whenever $x' < x$, $y' < y$, s is a suffix of u that starts with $t^{\pm 1}$, p is a prefix of v that ends with $t^{\pm 1}$ and $\pi_t(s\, u^{x'} u') = \pi_t(v' v^{y'} p)^{-1}$ holds. This ensures that $s\, u^{x'} u'\, e\, v' v^{y'} p$ is the group element represented by one of the vertical edges in Figure 8.1. The other parts of the above formula deal with the cases where the vertical edge has an endpoint in u' or v'. Altogether this ensures that all the vertical edges in Figure 8.1 represent elements of the subgroup A.

By Lemma 6.6 the solution set of the equation $\pi_t(u^x u') = \pi_t(v' v^y)^{-1}$ (which is interpreted over the free monoid $\{t, t^{-1}\}^*$) is semilinear. To see this let $w = v^{-1}$ and $w' = (v')^{-1}$. Then $\pi_t(u^x u') = \pi_t(v' v^y)^{-1}$ is equivalent to $\pi_t(u)^x \pi_t(u') = \pi_t(w)^y \pi_t(w')$. For the same reason, also the equation $\pi_t(s\, u^{x'} u') = \pi_t(v' v^{y'} p)^{-1}$ is equivalent to a semilinear constraint. The solution sets of the equations $\pi_t(s) = \pi_t(v' v^{y'} p)^{-1}$ and $\pi_t(s) = \pi_t(v' v^{y'} p)^{-1}$ are finite. Moreover, each of

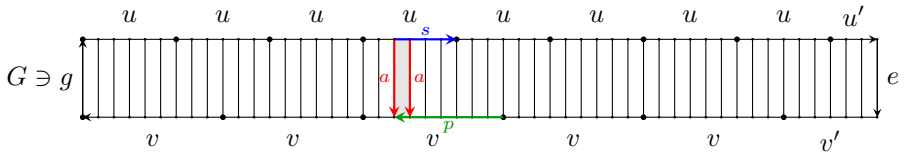

Figure 8.1: The idea behind the proof of Lemma 8.3. The fact that all vertical lines represent elements from the subgroup A is expressed by the formula from the proof.

the A-constraints $(\pi_\Sigma(s\,u^{x'}u'\,e\,v'v^{y'}p) \in_G A$ etc.) is equivalent to a semilinear constraint because G is knapsack-semilinear relative to A. Hence, the above formula is equivalent to a Presburger formula and therefore defines a semilinear set. □

Remark 8.4. There are variations of Lemma 8.3, where the G-constraint has one of the following forms:

$$u'e(z_1,\ldots,z_k)\,v'v^yv'' \in_H G,$$
$$u'u^xu''e(z_1,\ldots,z_k)\,v' \in_H G,$$
$$\text{or } u'e(z_1,\ldots,z_k)\,v' \in_H G$$

with u, u', u'', v, v', v'' as in Lemma 8.3. In all cases, the set of solutions of the G-constraint can be shown to be effectively semilinear using the arguments from the proof of Lemma 8.3.

Here we want to give a slightly different definition compared to Definition 7.4. Instead of 1-reducible tuples, we define G-reducible tuples in a different way.

Definition 8.5. We define a reduction relation on tuples over $\mathsf{BR}(H)$ of arbitrary length. Take $u_1, u_2, \ldots, u_m \in \mathsf{BR}(H)$ and $1 \le i < j \le m$. Then we have

$$(u_1, u_2, \ldots, u_m) \to (u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(u_j), u_{j+1}, \ldots, u_m)$$

if $\pi_t(u_i) \neq 1 \neq \pi_t(u_j)$, $u_{i+1}\cdots u_{j-1} \in \Sigma^*$ and $u_iu_{i+1}\cdots u_{j-1}u_j \in_H G$. Note that this implies that $u_iu_{i+1}\cdots u_{j-1}u_j =_H \pi_\Sigma(u_i)u_{i+1}\cdots u_{j-1}\pi_\Sigma(u_j)$. A concrete sequence of such rewrite steps leading to a tuple where all entries belong to Σ^* is a *G-reduction* of the initial tuple, and the initial tuple is called *G-reducible*. We also say that u_i and u_j *matched in a G-reduction*.

A G-reduction of a tuple $(u_1, u_2, \ldots, u_m)$ can be seen as a witness for the fact that $u_1u_2\cdots u_m \in_H G$. On the other hand, $u_1u_2\cdots u_m \in_H G$ does not necessarily imply that $(u_1, u_2, \ldots, u_m)$ has a G-reduction. But we can show that $u_1u_2\cdots u_m \in_H G$ implies that $(u_1, u_2, \ldots, u_m)$ can refined (by factorizing the u_i) such that the resulting refined tuple has a G-reduction. Moreover, it is important that we have an upper bound on the length of the refined tuple ($4m$ in Lemma 8.6 below) that only depends on m and not on the words $u_1, u_2, \ldots, u_m$.

We say that the tuple $(v_1, v_2, \ldots, v_n)$ is a *refinement* of the tuple $(u_1, u_2, \ldots, u_m)$ if there exist factorizations $u_i = u_{i,1} \cdots u_{i,k_i}$ in $(\Sigma \cup \{t, t^{-1}\})^*$ such that $k_i = 1$ whenever $u_i \in \Sigma^*$ and

$$(v_1, v_2, \ldots, v_n) = (u_{1,1}, \ldots, u_{1,k_1}, \ldots, u_{m,1}, \ldots, u_{m,k_m}).$$

Lemma 8.6. *Let $m \geq 2$ and $u_1, u_2, \ldots, u_m \in \mathsf{BR}(H)$. If $u_1 u_2 \cdots u_m \in_H G$, then there exists a G-reducible refinement of $(u_1, u_2, \ldots, u_m)$ that has length at most $4m$.*

Proof. Let $\overline{u} = (u_1, u_2, \ldots, u_m)$. Let us define $\gamma(\overline{u})$ as the number of pairs (i, j) with $1 \leq i < j \leq m$ such that $u_i u_{i+1} \cdots u_j$ is not Britton-reduced and $u_{i+1} \cdots u_{j-1} \in \Sigma^*$. Note that $\pi_t(u_i) \neq 1 \neq \pi_t(u_j)$ for such a pair (i, j). Moreover, if we have two pairs (i, j) and (k, ℓ) of this form, then either $j \leq k$ or $\ell \leq i$. Let $\theta(\overline{u})$ be the number of i such that $\pi_t(u_i) \neq 1$.

We prove by induction over $\gamma(\overline{u}) + \theta(\overline{u})$ that there exists a G-reducible refinement of $\overline{u}$ that has length at most $2\gamma(\overline{u}) + \theta(\overline{u}) + m \leq 4m$.

The case $m = 2$ is trivial: either $\gamma(u_1, u_2) = \theta(u_1, u_2) = 0$ and $u_1, u_2 \in \Sigma^*$ or $\gamma(u_1, u_2) = 1$, $\theta(u_1, u_2) = 2$ in which case (u_1, u_2) must reduce in one step to $(\pi_\Sigma(u_1), \pi_\Sigma(u_2))$. If $m \geq 3$ then $u_1 u_2 \cdots u_m$ must contain a pin. Since every u_i is Britton-reduced, there must exist $i < j$ such that $u_i u_{i+1} \cdots u_j$ is not Britton-reduced and $u_{i+1} \cdots u_{j-1} \in \Sigma^*$. By Lemma 8.2 we can factorize u_i and u_j in $(\Sigma \cup \{t, t^{-1}\})^*$ as $u_i = u_i' r$ and $u_j = s u_j'$ such that $rs \in_H G$ and $u_i u_{i+1} \cdots u_{j-1} u_j =_H u_i' \pi_\Sigma(r) u_{i+1} \cdots u_{j-1} \pi_\Sigma(s) u_j'$ is Britton-reduced. Note that r and s must contain t or t^{-1}. Moreover, we can assume that either $u_i' = 1$ or u_i' ends with $t^{\pm 1}$ (if u_i' ends with a non-empty word over Σ, we can remove this word from u_i' and add it to r) and, similarly, either $u_j' = 1$ or u_j' begins with $t^{\pm 1}$.

Case 1. u_i' and u_j' both contain $t^{\pm 1}$. Then we have

$$\gamma(u_1, \ldots, u_{i-1}, u_i', \pi_\Sigma(r), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m) < \gamma(\overline{u})$$

since $u_i' \pi_\Sigma(r) u_{i+1} \cdots u_{j-1} \pi_\Sigma(s) u_j'$ is Britton-reduced and u_i' and u_j' both contain $t^{\pm 1}$. Moreover, we have

$$\theta(u_1, \ldots, u_{i-1}, u_i', \pi_\Sigma(r), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m) = \theta(\overline{u}).$$

Hence, we can apply the induction hypothesis to the tuple

$$(u_1, \ldots, u_{i-1}, u_i', \pi_\Sigma(r), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u_j', u_{j+1}, \ldots, u_m). \tag{8.3}$$

It must have a G-reducible refinement of length at most

$$2(\gamma(\overline{u}) - 1) + \theta(\overline{u}) + m + 2 = 2\gamma(\overline{u}) + \theta(\overline{u}) + m.$$

In this refinement $\pi_\Sigma(r), \pi_\Sigma(s) \in \Sigma^*$ will not be factorized into more than one factor. We therefore can take the refinement of (8.3) and replace $\pi_\Sigma(r)$ and $\pi_\Sigma(s)$ by r and s, respectively. This leads to a G-reducible of our original tuple

$\overline{u}$ having length at most $2\gamma(\overline{u}) + \theta(\overline{u}) + m$.

Case 2. $u'_i = 1$ and u'_j begins with $t^{\pm 1}$. Then we have

$$\gamma(u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u'_j, u_{j+1}, \ldots, u_m) \leq \gamma(\overline{u})$$

and

$$\theta(u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u'_j, u_{j+1}, \ldots, u_m) < \theta(\overline{u}).$$

We can therefore apply the induction hypothesis to the tuple

$$(u_1, \ldots, u_{i-1}, \pi_\Sigma(u_i), u_{i+1}, \ldots, u_{j-1}, \pi_\Sigma(s), u'_j, u_{j+1}, \ldots, u_m) \tag{8.4}$$

and obtain a G-reducible refinement of length at most

$$2\gamma(\overline{u}) + \theta(\overline{u}) - 1 + m + 1 = 2\gamma(\overline{u}) + \theta(\overline{u}) + m.$$

Replacing $\pi_\Sigma(u_i)$ by u_i and $\pi_\Sigma(s)$ by s in this refinement yields a G-reducible refinement of $\overline{u}$.

The remaining cases where (i) $u'_j = 1$ and u'_i ends with $t^{\pm 1}$ or (ii) $u'_i = u'_j = 1$ are analogous to case 2. This concludes the proof of the lemma. □

8.3 Knapsack-semilinearity for HNN-extensions of the form $\langle G, t \mid t^{-1}at = a\,(a \in A)\rangle$

Now we are able to prove

Theorem 4.6 ([F4])**.** *Let $H = \langle G, t \mid t^{-1}at = a\ (a \in A)\rangle$ be an HNN-extension, where G is knapsack-semilinear relative to $\{1, A\}$. Then H is knapsack-semilinear.*

Proof. The proof of the theorem is based on ideas from chapter 7. Consider a knapsack expression

$$e(x_2, x_4, \ldots, x_m) = u_1 u_2^{x_2} u_3 u_4^{x_4} u_5 \cdots u_m^{x_m} u_{m+1}$$

with m even (later it will convenient to have only variables with an even index). We can assume that all u_i are Britton reduced. Moreover, by Lemma 7.3, we can assume that every u_i with i even is well-behaved and moreover non-empty (otherwise we can remove the power $u_i^{x_i}$).

In the following we describe an algorithm that computes a semilinear representation of $\mathsf{sol}_H(e)$ in three main steps. The algorithm transforms logical statements into equivalent logical statements (we do not have to define the precise logical language; the meaning of the statements should be always clear). Every statement contains the variables $x_2, x_4, \ldots, x_m$ from our knapsack expression and equivalence of two statements means that for every valuation $\nu : \{x_2, x_4, \ldots, x_m\} \to \mathbb{N}$ the two statements yield the same truth value. We

start with the statement $e(x_2, x_4, \ldots, x_m) =_H 1$ and end with a Presburger formula. In each of the three steps we transform the current statement Φ into an equivalent disjunction $\bigvee_{i=1}^{n} \Phi_i$. We can therefore view the whole process as a branching tree of depth three, where the nodes are labelled with statements. If a node is labelled with Φ and its children are labelled with $\Phi_1, \ldots, \Phi_n$ then Φ is equivalent to $\bigvee_{i=1}^{n} \Phi_i$. The leaves of the tree are labelled with Presburger formulas with free variables $x_2, x_4, \ldots, x_m$. We will concentrate on a single branch of this tree, which can be viewed as a sequence of nondeterministic guesses.

Let $N_\Sigma \subseteq [1, m+1]$ be the set of indices such that $u_i \in \Sigma^*$ and let $N_t = [1, m+1] \setminus N_\Sigma$ be the set of indices such that $\pi_t(u_i) \neq 1$. Moreover, let us define $w_i = u_i$ for i odd and $w_i = u_i^{x_i}$ for i even.

By Lemma 8.1, $e =_H 1$ is equivalent to $e \in_H G \wedge \pi_\Sigma(e) =_G 1$. Since G is knapsack-semilinear, the set $\mathsf{sol}_G(\pi_\Sigma(e))$ is semilinear. Hence, it suffices to show that the set of all $(x_2, x_4, \ldots, x_m) \in \mathbb{N}^{m/2}$ with $e(x_2, x_4 \ldots, x_m) \in_H G$ is semilinear. Here, we will use the assumption that G is knapsack-semilinear relative to A.

Step 1: Applying Lemma 8.6. We construct a disjunction Ψ from the knapsack expression e using Lemma 8.6. More precisely, we construct Ψ by nondeterministically guessing the following data:

(i) symbolic factorizations $w_i = y_{i,1} \cdots y_{i,k_i}$ in $(\Sigma \cup \{t, t^{-1}\})^*$ for all $i \in [1, m+1]$. Here the $y_{i,j}$ are existentially quantified variables that take values in $\mathsf{BR}(H)$. Later, these variables will be eliminated. The guessed k_i must satisfy $k_i \geq 1$ for all i, $k_i = 1$ for all $i \in N_\Sigma$, and $\sum_{1 \leq i \leq m+1} k_i \leq 4(m+1)$.

(ii) a G-reduction (according to Definition 8.5) of the tuple

$$(y_{1,1} \cdots y_{1,k_1}, \ldots, y_{m+1,1} \cdots y_{m+1,k_{m+1}}).$$

For the w_i with i odd we can of course guess concrete words for the variables $y_{i,1}, \ldots, y_{i,k_i}$. Later, we will do this, but in order to simplify the notation, we will still use the names $y_{i,1}, \ldots, y_{i,k_i}$ for these words.

For every specific guess in (i) and (ii) we write down the conjunction of the following formulas:

- the equation $w_i = y_{i,1} \cdots y_{i,k_i}$ from (i) (every variable $y_{i,j}$ is existentially quantified) and
- all G-constraints that result from G-reduction steps in the guessed G-reduction (this will made more precise in Step 2 below).

The formula Ψ is the disjunction of the above existentially quantified conjunctions, taken over all possible guesses in (i) and (ii). This formula is equivalent to the G-constraint $e \in_H G$.

Step 2: Eliminating the equations $w_i = y_{i,1} \cdots y_{i,k_i}$. For an odd i (i.e., $w_i = u_i$) we can eliminate this equation by guessing a concrete factorization

$u_i = u_{i,1} \cdots u_{i,k_i}$ and then replace the equation $w_i = y_{i,1} \cdots y_{i,k_i}$ by the conjunction

$$\bigwedge_{j=1}^{k_i} y_{i,j} = u_{i,j}.$$

For an even i (i.e., $w_i = u_i^{x_i}$) we can eliminate the equation $w_i = y_{i,1} \cdots y_{i,k_i}$ by guessing a symbolic factorization of $u_i^{x_i}$ into k_i factors. A specific guess leads to a formula

$$\bigwedge_{j=1}^{k_i} y_{i,j} = u''_{i,j} u_i^{x_{i,j}} u'_{i,j+1} \ \wedge\ x_i = c_i + \sum_{j=1}^{k_i} x_{i,j}. \tag{8.5}$$

Here, every $u'_{i,j}$ $(2 \leq j \leq k_i)$ is a proper prefix of u_i and every $u''_{i,j}$ $(2 \leq j \leq k_i)$ is a proper suffix of u_i such that either $u_i = u'_{i,j}u''_{i,j}$ or $u'_{i,j} = u''_{i,j} = 1$ for all $2 \leq j \leq k_i$. We set $u'_{i,k_i+1} = u''_{i,1} = 1$ in the above formula. Moreover, c_i is the number of $2 \leq j \leq k_i$ for which $u'_{i,j} \neq 1 \neq u''_{i,j}$ holds. The $u'_{i,j}$ and $u''_{i,j}$ are nondeterministically guessed.

We also guess which of the new exponent variables $x_{i,j}$ are zero and which of the $x_{i,j}$ are non-zero. If we guess $x_{i,j} = 0$, then we replace $x_{i,j}$ in (8.5) by 0. This yields the equation $y_{i,j} = u''_{i,j}u'_{i,j+1}$. If we guess $x_{i,j} > 0$, then we add this constraint to (8.5). After this step, it is determined whether a $y_{i,j}$ contains t or t^{-1} (for i even as well as for i odd). Those $y_{i,j}$ must be matched by G-reduction steps in the G-reduction that we guessed in Step 1. In fact, what we guessed in Step 1 is such a matching.

Step 3: Eliminating G-constraints. Assume that $y_{i,j}$ and $y_{k,\ell}$ are matched in the guessed G-reduction. W.l.o.g. assume that $i < k$ or $i = k$ and $j < \ell$, i.e., (i,j) is lexicographically before (k,ℓ). Then our formula contains the G-constraint

$$y_{i,j} \left(\prod_{(i,j) \prec (p,q) \prec (k,\ell)} \pi_\Sigma(y_{p,q}) \right) y_{k,\ell} \in_H G,$$

where $\prec$ is the strict lexicographic order on pairs of natural numbers. In this constraint, we can replace every $y_{a,b}$ with a even by $u''_{i,j}u_i^{x_{i,j}}u'_{i,j+1}$ (or $u''_{a,b}u'_{a,b+1}$ in case $x_{i,j} = 0$ was guessed), whereas every $y_{a,b}$ with a odd can be replaced by the concrete word $u_{a,b}$. If both $y_{i,j}$ and $y_{k,\ell}$ contain an exponent variable we obtain a G-constraint of the form (8.2). If $y_{i,j}$ or $y_{k,\ell}$ is a concrete word we obtain a G-constraint having one of the three forms listed in Remark 8.4. Lemma 8.3 and Remark 8.4 imply that in each case, the set of solutions of the G-constraint is semilinear. This concludes the proof of the theorem. □

Remark 8.7. It is straightforward to generalize Theorem 4.6 to a multiple HNN-extension

$$H = \langle G, t_1, \ldots, t_n \mid t_i^{-1}at_i = a\ (a \in A_i, 1 \leq i \leq n)\rangle.$$

If G is knapsack-semilinear relative to $\{1, A_1, \ldots, A_n\}$ then H is knapsack-semilinear.

8.4 Application: Extensions of centralizers

Recall the notion of an extension of centralizer from Subsection 2.4.3. We now give a proof for

Theorem 4.7 ([F4]). *If G is knapsack-semilinear and H is an extension of a centralizer $C(S)$ with S finite, then H is knapsack-semilinear as well.*

Proof. We have to show that G is also knapsack-semilinear relative to $C(S)$. Let $e = e(x_1, \ldots, x_n)$ be a knapsack expression. Then $e \in_G C(S)$ is equivalent to $\bigwedge_{a\in S} ea =_G ae$. Note that $ea =_G ae$ is equivalent to $eae^{-1}a^{-1} =_G 1$ and $eae^{-1}a^{-1}$ is an exponent expression. Since G is knapsack-semilinear and semilinear sets are closed under finite intersections, the set of solutions of $\bigwedge_{a\in S} ea = ae$ is semilinear. □

8.5 Open problems

In Theorems 4.6 and 4.7 we obtained knapsack-semilinearity for two types of HNN-extensions. It would be desired to compute bounds on the magnitudes as in Theorem 4.4.

Chapter 9

Central extensions for hyperbolic groups

9.1 Introduction

In this chapter we consider central extensions H of a group $G = H/K$ with K central. We do not want to analyze arbitrary central extensions, but only the ones for hyperbolic groups G. This allows us to deal with asynchronous biautomatic structures, defined in Section 9.3.

The main technical result of this chapter is Theorem 9.10, where we construct a semilinear representation of a Parikh image of $w_1 w_2 \cdots w_n =_H \alpha$. Here, α is from the central subgroup $K \leq H$ and $w_i \in L_i$, where $L_i \subseteq \Sigma^*$ (Σ is a finite generating set of G) is a regular (λ, ϵ)-quasigeodesic language (see Section 2.4). With this theorem, we can prove Theorem 4.8, which states that central extensions for hyperbolic groups are knapsack-semilinear.

In the second part of this chapter, we consider quasiconvex subgroups and we will prove a few transfer results. We show that an HNN-extension

$$H = \langle G, t \mid t^{-1} a t = a \ (a \in A) \rangle$$

is knapsack-semilinear, if G is hyperbolic and $A \leq G$ is a quasiconvex subgroup of G (Theorem 4.10). Theorem 4.9 is a generalization of this theorem, where we obtain a similar statement for the case where G is already a central extension of a hyperbolic group. A special case is where G is a finitely generated free group, since all finitely generated subgroups are quasiconvex.

9.2 Useful lemmas for hyperbolic groups

A word $w \in \Sigma^*$ is *shortlex reduced* if it is the length-lexicographically smallest word that represents the same group element as w. For this, we have to fix an arbitrary linear order on Σ. Note that if $u = xy$ is shortlex reduced then x and

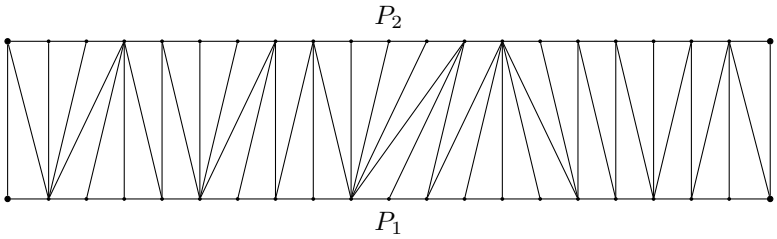

Figure 9.1: Paths that asynchronously $\mathcal{K}$-fellow travel

y are shortlex reduced too. For a word $u \in \Sigma^*$ we denote with $\mathsf{slex}(u)$ the unique shortlex reduced word that represents the same group element as u.

For the rest of the section let G be a δ-hyperbolic group and Σ a symmetric generating set for G.

Lemma 9.1 (c.f. [34, 8.21])**.** *Let $g \in G$ be of infinite order and let $n \geq 0$. Let u be a geodesic word representing g. Then the word u^n is (λ, ϵ)-quasigeodesic, where $\lambda = N|g|$, $\epsilon = 2N^2|g|^2 + 2N|g|$ and $N = |\mathcal{B}_{2\delta}(1)|$.*

Consider two paths $P_1 : [0, n_1] \to \Gamma$, $P_2 : [0, n_2] \to \Gamma$ and let $\mathcal{K}$ be a positive real number. We say that P_1 and P_2 *asynchronously $\mathcal{K}$-fellow travel* if there exist two continuous non-decreasing mappings $\varphi_1 : [0, 1] \to [0, n_1]$ and $\varphi_2 : [0, 1] \to [0, n_2]$ such that $\varphi_1(0) = \varphi_2(0) = 0$, $\varphi_1(1) = n_1$, $\varphi_2(1) = n_2$ and for all $0 \leq t \leq 1$, $d_\Gamma(P_1(\varphi_1(t)), P_2(\varphi_2(t))) \leq \mathcal{K}$. Intuitively, this means that one can travel along the paths P_1 and P_2 asynchronously with variable speeds such that at any time instant the current points have distance at most $\mathcal{K}$. By slightly increasing $\mathcal{K}$ one obtains a ladder graph of the form shown in Figure 9.1, where the edges connecting the horizontal P_1- and P_2-labelled paths represent paths of length at most $\mathcal{K}$ that connect elements from G.

Lemma 9.2 (c.f. [73])**.** *Let P_1 and P_2 be (λ, ϵ)-quasigeodesic paths in Γ_G and assume that P_i starts in g_i and ends in h_i. Assume that $d_\Gamma(g_1, g_2), d_\Gamma(h_1, h_2) \leq h$. Then there exists a computable bound $\mu = \mu(\delta, \lambda, \epsilon, h) \geq h$ such that P_1 and P_2 asynchronously μ-fellow travel.*

Finally, we make use of the following two results from [29].

Lemma 9.3 (c.f. [29, Lemma 3.1])**.** *Let $\zeta = 34\delta + 2$ and assume that $u = u_1u_2$ is shortlex reduced, where $|u_1| \leq |u_2| \leq |u_1| + 1$. Let $\tilde{u} = \mathsf{slex}(u_2u_1)$. If $|\tilde{u}| \geq 2\zeta + 1$ then for every $n \geq 0$, the word $\tilde{u}^n$ is ζ-local $(1, 2\delta)$-quasigeodesic.*

The following lemma is not stated explicitly in [29] but is shown in [29, Section 3.2] (where the main argument is attributed to Delzant).

Lemma 9.4 (c.f. [29])**.** *Let $\zeta = 34\delta + 2$ and assume that u is geodesic such that $|u| \geq 2\zeta + 1$ and for every $n \geq 0$, the word u^n is ζ-local $(1, 2\delta)$-quasigeodesic. Then one can compute $c \in \mathcal{B}_{4\delta}(1)$ and an integer $1 \leq m \leq |\mathcal{B}_{4\delta}(1)|^2$ such that $(\mathsf{slex}(c^{-1}u^m c))^n$ is geodesic for all $n \geq 0$.*

9.3 Asynchronous biautomatic structures

Let G be a f.g. group with the finite symmetric generating set Σ and let $h : \Sigma^* \to G$ be the evaluation morphism. An *asynchronous biautomatic structure* for G consists of a regular language $L \subseteq \Sigma^*$ such that the following holds; see also [28, 77]:

- $G = h(L)$,
- the relation $\{(u, v) \in L \times L \mid u =_G v\}$ is rational, and
- for every generator $a \in \Sigma$ the relations

$$\{(u, v) \in L \times L \mid ua =_G v\} \text{ and } \{(u, v) \in L \times L \mid au =_G v\}$$

  are rational.

If in the last point it is only required that the relation $\{(u, v) \in L \times L \mid ua =_G v\}$ is rational, then L is called an asynchronous automatic structure for G. A f.g. group G is called asynchronously (bi)automatic if it has an asynchronous (bi)automatic structure. We need the following lemma.

Lemma 9.5. *Let L be an asynchronous biautomatic structure for G, let L_1 and L_2 be regular subsets of L and let $v_1, v_2 \in \Sigma^*$. Then the relation*

$$\{(u_1, u_2) \in L_1 \times L_2 \mid v_1 u_1 =_G u_2 v_2\}$$

is rational. Moreover, a finite state transducer for this relation can be effectively computed from the words v_1, v_2 and finite automata for L_1 and L_2.

Proof. It suffices to show that the relation

$$R := \{(u_1, u_2) \in L \times L \mid v_1 u_1 =_G u_2 v_2\}$$

is rational. The corresponding finite state transducer can in addition simulate the automaton for L_1 (resp., L_2) on the first (resp., second) tape. Rationality of the relation R can be shown by induction on $|v_1| + |v_2|$. The case $v_1 = v_2 = 1$ is clear. Assume w.l.o.g. that $v_1 \neq 1$ and let $v_1 = v_1' a$ with $a \in \Sigma$. By induction, the relation $R_1 = \{(u_1', u_2) \in L \times L \mid v_1' u_1' =_G u_2 v_2\}$ is rational. Moreover, the relation $R_2 = \{(u_1, u_1') \in L \times L \mid au_1 =_G u_1'\}$ is rational as well. Finally, we have $R = R_2 \circ R_1$, where $\circ$ is relational composition. The lemma follows since the class of rational relations is closed under relational composition [84]. □

We also need the following result from [47]:

Lemma 9.6. *Let G be a hyperbolic group and let Σ be a finite symmetric generating set for G. Let λ and ϵ be fixed constants. Then the set of all (λ, ϵ)-quasigeodesic words over the alphabet Σ is an asynchronous biautomatic structure for G.*

In [47] it is only stated that the set of all (λ, ϵ)-quasigeodesic words is an asynchronous automatic structure for G. But since for every (λ, ϵ)-quasigeodesic

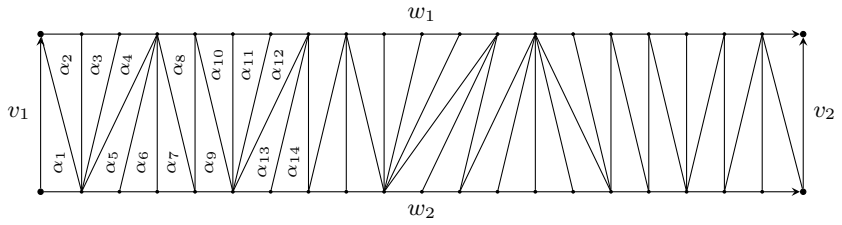

Figure 9.2: The situation from Lemma 9.8.

word $w \in \Sigma^*$ also w^{-1} is (λ, ϵ)-quasigeodesic, it follows easily that the set of all (λ, ϵ)-quasigeodesic words is an asynchronous biautomatic structure for G. With Lemma 9.5 we obtain the following lemma.

Lemma 9.7. *Let G be a hyperbolic group with the finite symmetric generating set Σ and let λ and ϵ be fixed constants. Assume that $L_1, L_2 \subseteq \Sigma^*$ are (λ, ϵ)-quasigeodesic regular languages and $v_1, v_2 \in \Sigma^*$. Then the relation*

$$\{(u_1, u_2) \in L_1 \times L_2 \mid v_1 u_1 =_G u_2 v_2\}$$

is rational. Moreover, a finite state transducer for this relation can be effectively computed from the words v_1, v_2 and finite automata for L_1 and L_2.

In the following let G be a δ-hyperbolic group with the finite symmetric generating set Σ. Let H be a central extension of G with $G = H/K$ and $K \leq Z(H)$. Since hyperbolic groups are finitely presented, Lemma 2.7 implies that K is finitely generated; let A be a finite generating set for K. Let $\pi : H \to G$ be the projection morphism. We can identify every $a \in \Sigma$ with an element from the preimage $\pi^{-1}(a) \subseteq H$ with the constraint that $a^{-1}a = 1$ should also hold in H. Then $\Gamma = \Sigma \cup A$ generates H. As before, we write K additively. Let $|\Sigma| = s$ and $|A| = k$. Elements of K will be written as k-tuples of integers. When we speak of a geodesic (or (ζ-local) (λ, ϵ)-quasigeodesic word) $w \in \Sigma^*$, this is always understood in the hyperbolic group G. Note that such a word w, when viewed as a word over $\Gamma \supseteq \Sigma$ is not necessarily geodesic in the group H.

For the following statements we fix two constants $\lambda \geq 1$ and $\epsilon \geq 0$.

Lemma 9.8. *Assume that $L_1, L_2 \subseteq \Sigma^*$ are (λ, ϵ)-quasigeodesic regular languages and $v_1, v_2 \in \Sigma^*$. Then the function*

$$f : \{(w_1, w_2) \in L_1 \times L_2 \mid v_1 w_1 =_G w_2 v_2\} \to K$$

with $v_1 w_1 =_H w_2 v_2 \cdot f(w_1, w_2)$ can be computed by a finite state transducer with K-output.

Proof. We apply Lemma 9.2 to G. Let $h = \max\{|v_1|, |v_2|\}$ and let $\mu = \mu(\delta, \lambda, \epsilon, h) \geq h$ be the bound from Lemma 9.2. There is a van Kampen diagram as shown in Figure 9.2. The set of states of our transducer $\mathcal{T}$ consists of the set

$\Sigma^{\leq\mu}$ of all words of length at most μ. The initial (resp., final) state of $\mathcal{T}$ is v_1 (resp., v_2). To define the transitions of $\mathcal{T}$ and their outputs, we consider two states $u, v \in \Sigma^{\leq\mu}$ and let $a \in \Sigma$ such that $ua =_G v$ and $ua =_H v \cdot \alpha$. Then we set

$$f_{\mathcal{T}}(u, a, 1, v) = \{\alpha\}. \tag{9.1}$$

Similarly, if $u =_G av$ and $u =_H av \cdot \alpha$ we set

$$f_{\mathcal{T}}(u, 1, a, v) = \{\alpha\}. \tag{9.2}$$

In Figure 9.2 every α_i within a triangle is the element of K that is equivalent to the word obtained by running clockwise around the border of the triangle (starting at the bottom-left corner). This word (which is uav^{-1} in transition (9.1) and $uv^{-1}a^{-1}$ in transition (9.2)) evaluates to the identity in G and therefore evaluates to an element of K in the H. The elements α_i in Figure 9.2 sum up to $v_1 w_1 v_2^{-1} w_2^{-1} \in K$. □

9.4 Parikh images in central extensions of hyperbolic groups

We fix an arbitrary enumeration $a_1, \ldots, a_s$ of the generating set Σ of the hyperbolic group G in order to make Parikh images well-defined. Recall that the semilinear sets are exactly the Parikh images of regular languages (or equivalently, the sets accepted by finite automata with transitions labelled by elements from $\mathbb{N}^k$); see Theorem 3.3. Together with Lemma 9.8 we obtain the next result.

Lemma 9.9. *Assume that $L_1, L_2 \subseteq \Sigma^*$ are (λ, ϵ)-quasigeodesic regular languages and $v_1, v_2 \in \Sigma^*$. Then the set*

$$\{(P(u_1), P(u_2), \alpha) \in \mathbb{N}^{2s} \times K \mid u_1 \in L_1, u_2 \in L_2, v_1 u_1 =_H u_2 v_2 \cdot \alpha\} \tag{9.3}$$

is semilinear. Moreover, a semilinear representation for this set can be effectively computed from the words v_1, v_2 and finite automata for L_1 and L_2.

Proof. By Lemma 9.8 one can construct a finite state transducer $\mathcal{T}$ with K-output such that for all $(u_1, u_2) \in L_1 \times L_2$ with $v_1 u_1 =_G u_2 v_2$ we have $v_1 u_1 =_H u_2 v_2 \cdot f(u_1, u_2)$.

From $\mathcal{T}$ we obtain a finite automaton $\mathcal{A}$, whose transitions are labelled with elements from $\mathbb{N}^{2s} \times K$ as follows: Assume that $\delta_{\mathcal{T}}(p, u, v, q) = \alpha$ where $u, v \in \Sigma \cup \{1\}$ and p, q are states of $\mathcal{T}$. We add in $\mathcal{A}$ a transition from p to q with label $(P(u), P(v), \alpha) \in \mathbb{N}^{2s} \times K$. The initial (resp., final) state of $\mathcal{A}$ is the same as for $\mathcal{T}$. Hence, the lemma follows from Theorem 3.3. □

We now come to our main technical result:

Theorem 9.10. *For $1 \leq i \leq n$ let $L_i \subseteq \Sigma^*$ be a regular (λ, ϵ)-quasigeodesic language. Then the set*

$$\{(P(w_1), \ldots, P(w_n), \alpha) \in \mathbb{N}^{ns} \times K \mid w_i \in L_i \text{ for } 1 \leq i \leq n, w_1 w_2 \cdots w_n =_H \alpha \in K\}$$

is semilinear and a semilinear representation of this set can be computed from finite automata for $L_1, \ldots, L_n$.

We postpone the proof of Theorem 9.10 and first derive some corollaries on knapsack problems.

9.5 Knapsack for central extensions of hyperbolic groups

Theorem 9.11. *Let $S \subseteq \Sigma^*$ be a regular geodesic set and $T \subseteq K$ be a semilinear subset of K. Then H is knapsack-semilinear relative to $h(S) \cdot T \subseteq H$, where $h : \Sigma^* \to H$ is the evaluation morphism.*

The first step for the proof of Theorem 9.11 will be a preprocessing step whose effect is stated in Proposition 9.12 below. We will use the following notations.

Consider a knapsack expression

$$e = (v_0 \cdot \beta_0)(u_1 \cdot \alpha_1)^{x_1}(v_1 \cdot \beta_1)(u_2 \cdot \alpha_2)^{x_2}(v_2 \cdot \beta_2) \cdots (u_k \cdot \alpha_k)^{x_k}(v_k \cdot \beta_k)$$

over H ($v_0, u_1, v_1 \ldots, u_k, v_k \in \Sigma^*$ and $\alpha_1, \beta_1, \ldots, \alpha_k, \beta_k \in K$). We can rewrite it as

$$v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k \cdot (x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k + \beta).$$

with $\beta = \beta_0 + \cdots + \beta_k$. We call $v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k$ (a knapsack expression over G) the G-part of e, and $(x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k + \beta)$ the K-part of e. Note that we write the K-part additively. We say that the G-part of e is (λ, ϵ)-quasigeodesic if all words $v_0, u_1, v_1, \ldots, u_k, v_k$ are geodesics in G and for all $1 \leq i \leq k$ and all $n \geq 0$ the word u_i^n is (λ, ϵ)-quasigeodesic in G. We say that the G-part of e has *infinite order*, if all u_i represent group elements of infinite order in G.

Recall that for a set of variables X and functions $f, h : X \to \mathbb{N}$ we write $f \cdot h$ for the pointwise multiplication of the functions f and h, i.e., $(f \cdot h)(x) = f(x)h(x)$.

Proposition 9.12. *There exist fixed constants λ, ϵ such that from a given knapsack expression e over H one can compute a finite list of knapsack expressions $e_1, \ldots, e_n$ over H with $X_{e_i} = X_e$ and functions $h_1, d_1, \ldots, h_n, d_n : X_e \to \mathbb{N}$ such that*

$$\mathsf{sol}_H(e) = \bigcup_{1 \leq i \leq n} h_i \cdot \mathsf{sol}_H(e_i) + d_i$$

Moreover, the G-part of every e_i is a (λ, ϵ)-quasigeodesic knapsack expression of infinite order.

Proof. We fix the following constants (see Lemma 9.3 and 9.4 for ζ and Lemma 9.1 for N, λ, and ϵ):

- $\zeta = 34\delta + 2$,
- $N = |\mathcal{B}_{2\delta}(1)|$,
- $\lambda = N(2\zeta + 1)$, and
- $\epsilon = 2N^2(2\zeta + 1)^2 + 2N(2\zeta + 1)$.

Consider a knapsack expression

$$e = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_k^{x_k} v_k \cdot (x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k + \beta) \tag{9.4}$$

over H. Let $\tilde{u}_i = \mathsf{slex}(u_i)$. Then there exists $\gamma_i \in K$ with $u_i = u_i' \cdot \gamma_i$. Hence, we can replace every $u_i^{x_i}$ by $\tilde{u}_i^{x_i} \cdot (x_i\gamma_i)$. The term $x_i\gamma_i$ can be moved into the K-part of e. In the following, we assume that the expression e from (9.4) has already the property that every u_i and (by the same reasoning) every v_i is shortlex reduced. Let $g_i \in G$ be the group element represented by the word u_i.

Step 1. In this first step we show how to reduce to the case where all g_i have infinite order in G. In a hyperbolic group G the order of torsion elements is bounded by a fixed constant that only depends on G, see also the proof of [74, Theorem 6.7]. This allows to check for each g_i whether it has finite order, and to compute the order in the positive case. Let $Y \subseteq \{x_1, \ldots, x_k\}$ be those variables x_i such that g_i has finite order. For $x_i \in Y$ let $o_i < \infty$ be the order of g_i. Moreover, let $\gamma_i \in K$ such that $u_i^{o_i} = \gamma_i$ in H.

Let $\mathcal{F}$ be the set of mappings $f : Y \to \mathbb{N}$ such that $0 \leq f(x_i) < o_i$ for all $x_i \in Y$. Consider a concrete mapping $f \in \mathcal{F}$. For this f, we only want to consider those $\nu \in \mathsf{sol}_H(e)$ such that $\nu(x_i) \equiv f(x_i) \bmod o_i$ for every $x_i \in Y$. We therefore replace every $u_i^{x_i}$ ($x_i \in Y$) by

$$u_i^{o_i x_i + f(x_i)} = u_i^{f(x_i)} \cdot x_i\gamma_i.$$

The term $x_i\gamma_i$ can be merged with the K-part of the expression and the word $u_i^{f(x_i)}$ can be merged with the word v_i. In this way we obtain for every mapping $f \in \mathcal{F}$ a knapsack expression e_f over H such that for every power $u_i^{x_i}$ that appears in the G-part of e_f, the word u_i represents an element of infinite order in G.

Finally, we extend every mapping $f \in \mathcal{F}$ to all variables x_i by setting $f(x_i) = 0$ for $x_i \notin Y$. In addition, define the mapping $f_0 : \{x_1, \ldots, x_k\} \to \mathbb{N}$ by $f_0(x_i) = o_i$ for $x_i \in Y$ and $f_0(x_i) = 1$ for $x_i \notin Y$. With this, we can write the set $\mathsf{sol}_H(e)$ as

$$\mathsf{sol}_H(e) = \bigcup_{f \in \mathcal{F}} f_0 \cdot \mathsf{sol}_H(e_f) + f. \tag{9.5}$$

Step 2. We now consider one of the knapsack expression e_f from Step 1. Let us write this expression as

$$e_f = v_0 u_1^{y_1} v_1 u_2^{y_2} v_2 \cdots u_l^{y_l} v_l \cdot (x_1\alpha_1 + x_2\alpha_2 + \cdots + x_k\alpha_k + \beta),$$

where $\{y_1, \dots y_l\} \subseteq \{x_1, \dots x_k\}$. For every $1 \leq i \leq l$, the group element g_i represented by u_i has infinite order in G. We factorize u_i uniquely as $u_i = u_{i,1}u_{i,2}$ where $|u_{i,1}| \leq |u_{i,2}| \leq |u_{i,1}| + 1$, and let $\tilde{u}_i = \mathsf{slex}(u_{i,2}u_{i,1})$. Note that $|\tilde{u}_i| \leq |u_i|$. Let $\beta_i \in K$ such that $u_{i,2}u_{i,1} = \tilde{u}_i \cdot \beta_i$ in K and let $\tilde{g}_i \in G$ be the element of G represented by $\tilde{u}_i$. Since $\tilde{g}_i$ is conjugated to g_i in G, also $\tilde{g}_i$ has infinite order in G. By Lemma 9.1, for every $n \geq 0$, the word $\tilde{u}_i^n$ is (λ_i, ϵ_i)-quasigeodesic in G for $\lambda_i = N|\tilde{u}_i|$, $\epsilon_i = 2N^2|\tilde{u}_i|^2 + 2N|\tilde{u}_i|$. Note that for every $n \geq 0$ we have in H:

$$u_i^n = (u_{i,1}u_{i,2})^n = u_{i,1}(u_{i,2}u_{i,1})^n u_{i,1}^{-1} = u_{i,1}(\tilde{u}_i \cdot \beta_i)^n u_{i,1}^{-1} = u_{i,1}\tilde{u}_i^n u_{i,1}^{-1} \cdot n\beta_i.$$

We can therefore replace $u_i^{y_i}$ by $u_{i,1}\tilde{u}_i^{y_i}u_{i,1}^{-1} \cdot y_i\beta_i$, merge $y_i\beta_i$ with the K-part of e_f and merge $u_{i,1}$ and $u_{i,1}^{-1}$ with the neighboring v_{i-1} and v_i. Let e'_f be the resulting knapsack expression. We have $\mathsf{sol}_H(e_f) = \mathsf{sol}_H(e'_f)$.

For variables y_i with $|\tilde{u}_i| < 2\zeta + 1$, it follows that $\tilde{u}_i^n$ is (λ, ϵ)-quasigeodesic for the constants λ and ϵ defined at the beginning of the proof and we are done with the variable y_i.

Now assume that $|\tilde{u}_i| \geq 2\zeta + 1$. By Lemma 9.3, $\tilde{u}_i^n$ is ζ-local $(1, 2\delta)$-quasigeodesic for every $n \geq 0$. By Lemma 9.4, one can compute $c_i \in \mathcal{B}_{4\delta}(1)$ and an integer $1 \leq m_i \leq |\mathcal{B}_{4\delta}(1)|^2$ such that $(\mathsf{slex}(c_i^{-1}\tilde{u}_i^{m_i}c_i))^n$ is geodesic (and hence $(1,0)$-quasigeodesic) for all $n \geq 0$. Let $\gamma_i \in K$ such that

$$c_i^{-1}\tilde{u}_i^{m_i}c_i \quad =_H \quad \mathsf{slex}(c_i^{-1}\tilde{u}_i^{m_i}c_i) \cdot \gamma_i.$$

Note that for every $n \geq 0$ we obtain

$$\begin{aligned} c_i(\mathsf{slex}(c_i^{-1}\tilde{u}_i^{m_i}c_i))^n c_i^{-1} \cdot n\gamma_i &=_H c_i(\mathsf{slex}(c_i^{-1}\tilde{u}_i^{m_i}c_i) \cdot \gamma_i)^n c_i^{-1} \\ &=_H c_i(c_i^{-1}\tilde{u}_i^{m_i}c_i)^n c_i^{-1} =_H \tilde{u}_i^{m_i n}. \end{aligned}$$

To make the description of the resulting knapsack expression more uniform we set $m_i = 1$, $c_i = 1$, and $\gamma_i = 0$ in case $|\tilde{u}_i| < 2\zeta + 1$. Let $\mathcal{H}$ be the set of all such mappings $h : \{y_1, \dots, y_l\} \to \mathbb{N}$ with $0 \leq h(y_i) \leq m_i - 1$ for all i. For every such h we then produce the knapsack expression $e'_{f,h}$ that is obtained from e'_f by replacing every power $\tilde{u}_i^{y_i}$ by $\tilde{u}_i^{h(y_i)}c_i(\mathsf{slex}(c_i^{-1}\tilde{u}_i^{m_i}c_i))^{y_i}c_i^{-1} \cdot y_i\gamma_i$ (in case $|\tilde{u}_i| < 2\zeta + 1$ this replacement has no effect). Let $h_0 : \{y_1, \dots, y_l\} \to \mathbb{N}$ be the mapping with $h_0(y_i) = m_i$. From the above discussion, we obtain

$$\mathsf{sol}_H(e_f) = \mathsf{sol}_H(e'_f) = \bigcup_{h \in \mathcal{H}} (h_0 \cdot \mathsf{sol}_H(e'_{f,h}) + h).$$

Finally, with (9.5) we obtain

$$\mathsf{sol}_H(e) = \bigcup_{f \in \mathcal{F}} \bigcup_{h \in \mathcal{H}} (f_0 \cdot g_0 \cdot \mathsf{sol}_H(e'_{f,h}) + f_0 \cdot h + f),$$

which concludes the preprocessing. □

Proof of Theorem 9.11. Let e be a knapsack expression over the generating set $\Sigma \cup A$ of H. Let $X = X_e$. We want to find a semilinear representation for the set

$$\{\nu : X \to \mathbb{N} \mid \exists w \in S\, \exists \alpha \in T : \nu(e) =_H w \cdot \alpha\} = \bigcup_{w \in S, \alpha \in T} \mathsf{sol}_H(ew^{-1} \cdot (-\alpha)). \tag{9.6}$$

Consider a knapsack expression e. By Proposition 9.12 one can compute a finite list of knapsack expressions $e_1, \ldots, e_n$ over H and functions $h_i, d_i : X \to \mathbb{N}$ such that

$$\mathsf{sol}_H(e) = \bigcup_{1 \leq i \leq n} (h_i \cdot \mathsf{sol}_H(e_i) + d_i). \tag{9.7}$$

Moreover, every knapsack expression e_i has the property that for every power u^x that appears in the G-part of e_i, the language u^* is (λ, ϵ)-quasigeodesic for some fixed constants λ, ϵ that only depends on the group G.

Consider now for arbitrary $w \in S$ and $\alpha \in T$ the knapsack expression $ew^{-1} \cdot (-\alpha)$. From the construction in the proof of Proposition 9.12 it follows that

$$\mathsf{sol}_H(ew^{-1} \cdot (-\alpha)) = \bigcup_{1 \leq i \leq n} (h_i \cdot \mathsf{sol}_H(e_i w^{-1} \cdot (-\alpha)) + d_i). \tag{9.8}$$

The reason is that in the proof of Proposition 9.12 , every e_i is computed from e by replacing the powers u^x that appear in the G-part of e by small expressions (involving only the exponent variable x). The same replacements are also made for $ew^{-1} \cdot (-\alpha)$, i.e., the replacements in e do not depend on the concrete choice of $w \in S$ and $\alpha \in T$. Therefore, the set in (9.6) is equal to

$$\begin{aligned} \bigcup_{w \in S, \alpha \in T} \mathsf{sol}_H(ew^{-1} \cdot (-\alpha)) &= \bigcup_{w \in S, \alpha \in T} \bigcup_{1 \leq i \leq n} (h_i \cdot \mathsf{sol}_H(e_i w^{-1} \cdot (-\alpha)) + d_i) \\ &= \bigcup_{1 \leq i \leq n} \left(h_i \cdot \left(\bigcup_{w \in S, \alpha \in T} \mathsf{sol}_H(e_i w^{-1} \cdot (-\alpha)) \right) + d_i \right). \end{aligned}$$

The closure properties of semilinear sets imply that the set (9.6) is semilinear provided the set

$$\bigcup_{w \in S, \alpha \in T} \mathsf{sol}_H(e_i w^{-1} \cdot (-\alpha)) = \{\nu : X \to \mathbb{N} \mid \exists w \in S, \alpha \in T : \nu(e_i) =_H w \cdot \alpha\}$$

is semilinear for all $1 \leq i \leq n$.

This shows that it suffices to find a semilinear representation of (9.6) for a knapsack expression

$$e = v_0 u_1^{x_1} v_1 u_2^{x_2} v_2 \cdots u_n^{x_n} v_n \cdot (x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n + \beta),$$

where all $u_i \in \Sigma^*$ have the property that u_i^* is a regular (λ, ϵ)-quasigeodesic language. Clearly, we can also assume that every u_i is non-empty and every v_i is geodesic. Moreover, since $S \subseteq \Sigma^*$ is regular and geodesic, it is easy to see that also S^{-1} is regular and geodesic.

Let $(L_1, \dots, L_m)$ be the tuple of languages $(\{v_0\}, u_1^*, \{v_1\}, \dots, u_n^*, \{v_n\}, S^{-1})$ (with $m = 2(n+1)$). All these languages are regular and (λ, ϵ)-quasigeodesic subsets of Σ^*. By Theorem 9.10, the set

$$\{(P(w_1), \dots, P(w_m), \gamma) \in \mathbb{N}^{ms} \times K \mid w_i \in L_i \text{ for } 1 \leq i \leq m, w_1 \cdots w_m =_H \gamma\}$$

is semilinear and a semilinear representation of this set can be computed. Applying a projection yields a semilinear representation of the set

$$\{(P(w_1), \dots, P(w_n), \gamma) \in \mathbb{N}^{ns} \times K \mid w_i \in u_i^* \text{ for } 1 \leq i \leq n, \\ \exists w \in S : v_0 w_1 v_1 \cdots w_n v_n =_H w \cdot \gamma\}.$$

Choose for every u_i a symbol $a_{j_i} \in \Sigma$ such that $\ell_i := |u_i|_{a_{j_i}} > 0$ (recall that $u_i \neq 1$). Then we project every $P(w_i)$ in the above set to the j_i-th coordinate. The resulting projection is

$$\{(\ell_1 \cdot x_1, \dots, \ell_n \cdot x_n, \gamma) \in \mathbb{N}^n \times K \mid \exists w \in S : v_0 u_1^{x_1} v_1 \cdots u_n^{x_n} v_n =_H w \cdot \gamma\}.$$

The semilinearity of this set easily implies the semilinearity of the set

$$\{(x_1, \dots, x_n, \gamma) \in \mathbb{N}^n \times K \mid \exists w \in S : v_0 u_1^{x_1} v_1 \cdots u_n^{x_n} v_n =_H w \cdot \gamma\}.$$

We finally intersect this set with the set

$$\{(x_1, \dots, x_n, \gamma) \in \mathbb{N}^n \times K \mid \exists \alpha \in T : \gamma = \alpha - (x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n + \beta)\}$$

and project onto $\mathbb{N}^n$. This yields a semilinear representation of the set

$$\{(x_1, \dots, x_n) \in \mathbb{N}^n \mid \exists w \in S \, \exists \alpha \in T : \\ v_0 u_1^{x_1} v_1 \cdots u_n^{x_n} v_n \cdot (x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n + \beta) =_H w \cdot \alpha\}.$$

This concludes the proof. □

With $S = \{1\}$ and $T = \{0\}$, Theorem 9.11 yields Theorem 4.8:

Theorem 4.8. *A central extension of a hyperbolic group is knapsack-semilinear.*

9.6 Quasiconvex subgroups of hyperbolic groups

In this section we want to consider some applications and show that hyperbolic groups are knapsack-semilinear relative to quasiconvex subgroups. Also a similar statement holds for central extensions of hyperbolic groups. We then conclude Theorems 4.9 and 4.10.

Theorem 9.13. *Let H be a central extension of the hyperbolic group G and let $\pi : H \to G$ be the canonical projection. Let $Q \leq G$ be a quasiconvex subgroup of G. Then H is knapsack-semilinear relative to $\pi^{-1}(Q)$.*

Proof. Fix a finite symmetric generating set Σ for G and let $h : \Sigma^* \to G$ be the evaluation morphism. By Lemma 2.6 the set of all geodesic words in $h^{-1}(Q)$ is a geodesic regular language S. As before, we identify Σ with a subset of H. Let K be the central subgroup H such that $G = H/K$. Then, the set $S \cdot K$ represents the preimage $\pi^{-1}(Q)$. By Theorem 9.11, H is knapsack-semilinear relative to $\pi^{-1}(Q)$. □

By setting K to the trivial group, we obtain the following special case:

Theorem 9.14. *Let G be hyperbolic and let A be a quasiconvex subgroup of G. Then G is knapsack-semilinear relative to A.*

It is known that every finitely generated free group F is locally quasiconvex, which means that every finitely generated subgroup of F is quasiconvex.

Corollary 9.15. *Let G be a finitely generated free group and let A be a finitely generated subgroup of G. Then G is knapsack-semilinear relative to A.*

This corollary can actually be generalized. Schupp proved that a group G, which is virtually an orientable surface group of genus at least two or virtually a Coxeter group satisfying a certain reduction hypothesis, is locally quasiconvex [82, Theorem IV]. Since these groups are hyperbolic, it follows that the groups considered by Schupp are knapsack-semilinear relative to any finitely generated subgroup.

Finally, Theorems 4.6, 4.8 and 9.13 yield Theorem 4.9:

Theorem 4.9. *Let H be a central extension of the hyperbolic group G and let $\pi : H \to G$ be the canonical projection. Let $Q \leq G$ be a quasiconvex subgroup of G. Then the HNN-extension $\langle H, t \mid t^{-1}at = a \ (a \in \pi^{-1}(Q))\rangle$ is knapsack-semilinear.*

Furthermore, this theorem together with $K = 1$ implies

Theorem 4.10 ([F4])**.** *Let G be hyperbolic and $A \leq G$ be a quasiconvex subgroup of G. Then the HNN-extension $\langle G, t \mid t^{-1}at = a \ (a \in A)\rangle$ is knapsack-semilinear.*

It is known that every cyclic subgroup of a hyperbolic group is quasiconvex, see e.g. [3]. Hence, for every element $a \in G$ of a hyperbolic group G, the HNN-extension $\langle G, t \mid t^{-1}at = a\rangle$ is knapsack-semilinear. It is also known that if the hyperbolic group G is non-elementary (i.e., it contains a copy of the free group F_2) then the centralizer of an element $g \in G$ is cyclic [3, Lemma 2]. Hence, we obtain Theorem 4.7 for the case of a centralizer of a single element in a non-elementary hyperbolic group.

9.7 Proof of Theorem 9.10

We now come to the proof of Theorem 9.10. Let G be δ-hyperbolic. For $1 \leq i \leq n$ let $L_i \subseteq \Sigma^*$ be a regular (λ, ϵ)-quasigeodesic language. Let $\mathcal{A}_i = (\mathcal{Q}_i, S_i, \delta_i, T_i)$ be a finite automaton for L_i. Without loss of generality, we can assume that

every $q \in \mathcal{Q}_i$ belongs to a path from some initial state $q_0 \in S_i$ to some final state $q_1 \in T_i$. This ensures that every word that labels a path from a state p to a state q is a factor of a word from L_i. Since factors of (λ, ϵ)-quasigeodesic words are (λ, ϵ)-quasigeodesic as well, it follows that every word that labels a path between two states of $\mathcal{A}_i$ is (λ, ϵ)-quasigeodesic.

We want to show that the set

$$\{(P(w_1), \ldots, P(w_n), \alpha) \in \mathbb{N}^{ns} \times K \mid w_i \in L_i \text{ for } 1 \leq i \leq n, w_1 w_2 \cdots w_n =_H \alpha\}$$

is semilinear. For this, we prove a slightly more general statement: For words $v_1, \ldots, v_n \in \Sigma^*$ we consider the set

$$\{(P(w_1), \ldots, P(w_n), \alpha) \in \mathbb{N}^{ns} \times K \mid w_i \in L_i \text{ for } 1 \leq i \leq n, w_1 v_1 \cdots w_n v_n =_H \alpha\}.$$

By induction over n we show that this set is semilinear. For the case $n = 2$ we can directly use Lemma 9.9. This also covers the case $n = 1$ since we can take $L_2 = \{1\}$.

Now assume that $n \geq 3$. We can assume that the words v_i are geodesic. Define the automaton $\mathcal{A}$ as the disjoint union of the automata $\mathcal{A}_i$. Thus, the state set of $\mathcal{A}$ is $\mathcal{Q} = \biguplus_{1 \leq i \leq n} \mathcal{Q}_i$ and the transition set of $\mathcal{A}$ is $\delta = \biguplus_{1 \leq i \leq n} \delta_i$ (the sets of initial and final states of $\mathcal{A}$ are not important). Let us denote for $p, q \in \mathcal{Q}$ with $L_{p,q}$ the set of all finite words that label a path from p to q in the automaton $\mathcal{A}$. The above properties of the automata $\mathcal{A}_i$ ensure that every language $L_{p,q} \subseteq \Sigma^*$ is (λ, ϵ)-quasigeodesic. Note that $L_i = \bigcup_{p \in S_i, q \in T_i} L_{p,q}$. Since the semilinear sets are effectively closed under union, it suffices to show for states $p_i, q_i \in \mathcal{Q}$ $(1 \leq i \leq n)$ that the following set is semilinear:

$$\{(P(w_1), \ldots, P(w_n), \alpha) \in \mathbb{N}^{ns} \mid w_i \in L_{p_i,q_i} \text{ for } 1 \leq i \leq n, w_1 v_1 \cdots w_n v_n =_H \alpha\}.$$

In the following, we denote this set with $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$. We will construct a Presburger formula with free variables $x_{i,j}$ $(1 \leq i \leq n,\ 1 \leq j \leq s)$ and $\bar{\chi}$ for this set. The variables $x_{i,j}$ with $1 \leq j \leq k$ encode the Parikh image of the words from L_{p_i,q_i} and the tuple of variables $\bar{\chi}$ represents an element of the finitely generated abelian group K. Let us write $\bar{x}_i = (x_{i,j})_{1 \leq j \leq k}$ in the following.

Note that $w_1 v_1 \cdots w_n v_n =_H \alpha$ implies $w_1 v_1 \cdots w_n v_n =_G 1$. Recall from Section 2.4.5 the definition of the path $P[w]$ in the Cayley-graph $\Gamma(G)$ for a word $w \in \Sigma^*$. Consider a tuple $(w_1, \ldots, w_n) \in \prod_{i=1}^n L_{p_i,q_i}$ with $w_1 v_1 w_2 v_2 \cdots w_n v_n =_G 1$ and the corresponding $2n$-gon in $\Gamma(G)$ that is defined by the (λ, ϵ)-quasigeodesic paths $P_i = (w_1 v_1 \cdots w_{i-1} v_{i-1}) \cdot P[w_i]$ and the geodesic paths $Q_i = (w_1 v_1 \cdots w_i) \cdot P[v_i]$, see Figure 9.3 for the case $n = 3$. Since all paths P_i and Q_i are (λ, ϵ)-quasigeodesic, we can apply [74, Lemma 6.4]: Every side of the $2n$-gon is contained in the κ-neighborhoods of the other sides, where $\kappa = \xi + \xi \log(2n)$ for a constant ξ that only depends on the constants $\delta, \lambda, \varepsilon$.

Let us now consider the side P_2 of the quasigeodesic $2n$-gon. It is labelled with a word from L_{p_2,q_2}. Its neighboring sides are Q_1 and Q_2, which are labelled

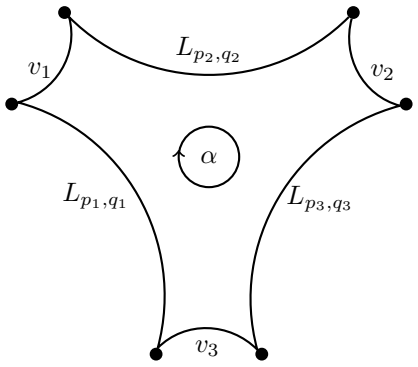

Figure 9.3: The $2n$-gon for $n = 3$ from the proof of Theorem 9.10

with v_1 and v_2, respectively. We distinguish several cases. In each case we cut the $2n$-gon into smaller pieces (m-gons for some $m \leq 2n$) along paths of length $\leq \kappa$ (length $2\kappa + 1$ in Case 2). When we speak of a point on the $2n$-gon, we mean a node of the Cayley graph (i.e., an element of the group G) and not a point in the interior of an edge. Let us emphasize that the cutting process is done in the Cayley-graph of the hyperbolic group G and not the central extension H. But every m-gon in G is a closed loop in the Cayley-graph $\Gamma(G)$ and therefore yields in the central extension H a unique element from the central subgroup K. When we cut our $2n$-gon into smaller m-gons, the K-values of these m-gons have to added in order to yield the K-value of the initial $2n$-gon.

For each of the following six cases we construct a Presburger formula describing a semilinear set. The union of these six sets is $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$.

Case 1: There is a point $a \in P_2$ that has distance at most κ from a point b that does not belong to $P_1 \cup Q_1 \cup Q_2 \cup P_3$. Thus b must belong to one of the paths $Q_3, P_4, \ldots, Q_{n-1}, P_n, Q_n$. Let w be a geodesic word of length at most κ that labels a path from a to b. There are two subcases:

Case 1.1: b belongs to a path Q_i with $3 \leq i \leq n$. The situation is shown in Figure 9.4 for $n = i = 3$. Let T be the set of all tuples $(r, v_{i,1}, v_{i,2}, w)$ such that $r \in \mathcal{Q}$, $v_i = v_{i,1}v_{i,2}$, and $w \in \Sigma^*$ is of length at most κ. By induction, the following two sets are semilinear for every tuple $t = (r, v_{i,1}, v_{i,2}, w) \in T$:

$$\begin{aligned} S_{t,1} &= P(p_1, q_1, v_1, p_2, r, wv_{i,2}, p_{i+1}, q_{i+1}, v_{i+1}, \ldots, p_n, q_n, v_n), \\ S_{t,2} &= P(r, q_2, v_2, p_3, q_3, v_3, \ldots, p_i, q_i, v_{i,1}w^{-1}). \end{aligned}$$

Intuitively, $S_{t,1}$ corresponds to the $2j_1$-gon (when $wv_{i,2}$ is viewed as a single side) on the left of the w-labelled edge in Figure 9.4, whereas $S_{t,2}$ corresponds to the $2j_2$-gon on the right of the w-labelled edge (where $j_1 = n - i + 2$ and $j_2 = i - 1$). Note that $j_1, j_2 \leq n - 1$. We then define the formula

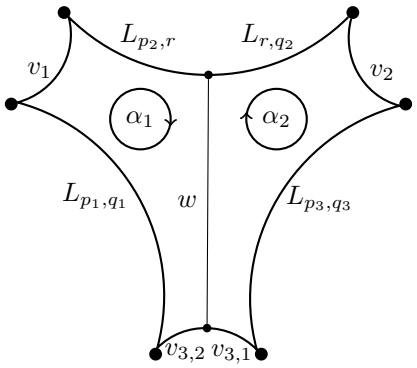

Figure 9.4: Case 1.1 from the proof of Theorem 9.10

$$A_{1.1} = \bigvee_{t\in T} \exists \bar{y}_2, \bar{z}_2, \bar{\chi}_1, \bar{\chi}_2 : (\bar{x}_1, \bar{y}_2, \bar{x}_{i+1}, \ldots, \bar{x}_n, \bar{\chi}_1) \in S_{t,1} \wedge (\bar{z}_2, \bar{x}_3, \ldots, \bar{x}_i, \bar{\chi}_2) \in S_{t,2} \wedge \bar{x}_2 = \bar{y}_2 + \bar{z}_2 \ \wedge \ \bar{\chi} = \bar{\chi}_1 + \bar{\chi}_2.$$

Here $\bar{y}_2, \bar{z}_2$ are s-tuples of new variables, whereas $\bar{\chi}_1, \bar{\chi}_2$ represent elements of K.

The Presburger formula $A_{1.1}$ is one of the six formulas whose union is $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$.

Case 1.2: b belongs to the path P_i, where $4 \leq i \leq n$ (this case can only occur if $n \geq 4$). This case is analogous to Case 1.1. Let T be the set of all tuples (r, r', w) such that $r, r' \in \mathcal{Q}$ and $w \in \Sigma^*$ is of length at most κ. By induction, the following two sets are semilinear for every tuple $t = (r, r', w) \in T$:

$$\begin{aligned} S_{t,1} &= P(p_1, q_1, v_1, p_2, r, w, r', q_i, v_i, p_{i+1}, q_{i+1}, v_{i+1}, \ldots, p_n, q_n, v_n), \\ S_{t,2} &= P(r, q_2, v_2, p_3, q_3, v_3, \ldots, p_{i-1}, q_{i-1}, v_{i-1}, p_i, r', w^{-1}). \end{aligned}$$

Moreover, let $A_{1.2}$ be the formula

$$A_{1.2} = \bigvee_{t\in T} \exists \bar{y}_2, \bar{z}_2, \bar{y}_i, \bar{z}_i, \bar{\chi}_1, \bar{\chi}_2 : (\bar{x}_1, \bar{y}_2, \bar{z}_i, \bar{x}_{i+1}, \ldots, \bar{x}_n, \bar{\chi}_1) \in S_{t,1} \wedge (\bar{z}_2, \bar{x}_3, \ldots, \bar{x}_{i-1}, \bar{y}_i, \bar{\chi}_2) \in S_{t,2} \wedge \bar{x}_2 = \bar{y}_2 + \bar{z}_2 \ \wedge \ \bar{x}_i = \bar{y}_i + \bar{z}_i \ \wedge \ \bar{\chi} = \bar{\chi}_1 + \bar{\chi}_2.$$

Case 2: Every point on P_2 has distance at most κ from a point on $P_1 \cup Q_1 \cup Q_2 \cup P_3$. Since the starting point of P_2 has distance $0 \leq \kappa$ from $P_1 \cup Q_1$ and the end point of P_2 has distance $0 \leq \kappa$ from $Q_2 \cup P_3$, there must be points b_1 on $P_1 \cup Q_1$, b on P_2, and b_2 on $Q_2 \cup P_3$ such that the distance between b_1 and b is at most κ and the distance between b and b_2 is at most $\kappa + 1$. Hence, the distance between b_1 and b_2 is at most $2\kappa + 1$. Let w be a word that labels a geodesic path from b_1 to b_2 (thus, $|w| = \|w\| \leq 2\kappa + 1$). This leads to the following four subcases.

Case 2.1: $b_1 \in Q_1$ and $b_2 \in Q_2$. This case is shown in Figure 9.5. Let T be the set of all tuples $(v_{1,1}, v_{1,2}, w, v_{2,1}, v_{2,2})$ such that $v_1 = v_{1,1}v_{1,2}$, $v_2 = v_{2,1}v_{2,2}$ and

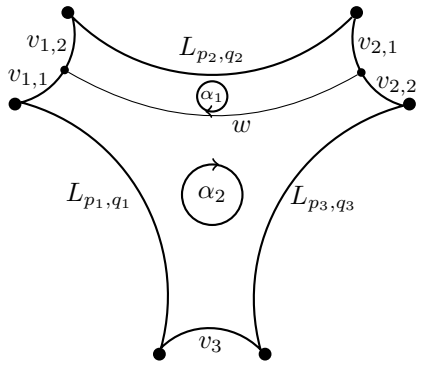

Figure 9.5: Case 2.1 from the proof of Theorem 9.10

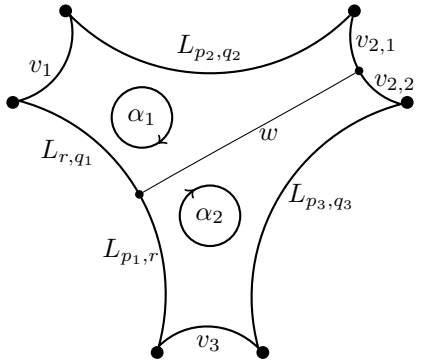

Figure 9.6: Case 2.2 from the proof of Theorem 9.10

$w \in \Sigma^*$ is of length at most $2\kappa + 1$. By induction, the following two sets are semilinear for every tuple $t = (v_{1,1}, v_{1,2}, w, v_{2,1}, v_{2,2}) \in T$:

$$\begin{aligned} S_{t,1} &= P(p_2, q_2, v_{2,1} w^{-1} v_{1,2}), \\ S_{t,2} &= P(p_1, q_1, v_{1,1} w v_{2,2}, p_3, q_3, v_3, \ldots, p_n, q_n, v_n). \end{aligned}$$

We define the formula

$$A_{2.1} = \bigvee_{t \in T} \exists \bar{\chi}_1, \bar{\chi}_2 : (\bar{x}_2, \bar{\chi}_1) \in S_{t,1} \ \wedge \ (\bar{x}_1, \bar{x}_3 \ldots, \bar{x}_n, \bar{\chi}_2) \in S_{t,2} \ \wedge \ \bar{\chi} = \bar{\chi}_1 + \bar{\chi}_2.$$

Case 2.2: $b_1 \in P_1$ and $b_2 \in Q_2$, see Figure 9.6. This case is exactly the same as Case 1.1 with $i = 3$, if we replace the side P_2 in Case 1.1 by P_1; see Figure 9.4.

Case 2.3: $b_1 \in Q_1$ and $b_2 \in P_3$. This case is analogous to Case 2.2.

Case 2.4: $b_1 \in P_1$ and $b_2 \in P_3$, see Figure 9.7. Let T be the set of all tuples $(w_1, w_2, w, r_1, r_2, r_3)$ such that $\|w\| \leq 2\kappa+1$, $\|w_1\| \leq \kappa$, $\|w_2\| \leq \kappa+1$, $w = w_1^{-1} w_2$ in G, and $r_1, r_2, r_3 \in \mathcal{Q}$. By induction, the following three sets are semilinear for

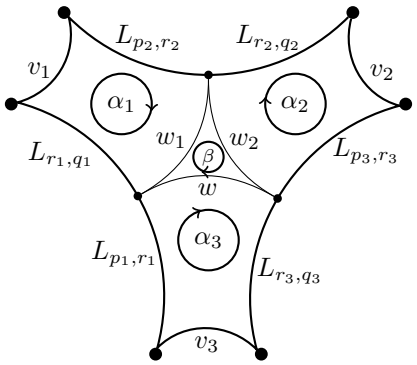

Figure 9.7: Case 2.4 from the proof of Theorem 9.10, where $\beta = \beta(w, w_1, w_2)$.

every tuple $t = (w_1, w_2, w, r_1, r_2, r_3) \in T$:

$$\begin{aligned} S_{t,1} &= P(r_1, q_1, v_1, p_2, r_2, w_1), \\ S_{t,2} &= P(r_2, q_2, v_2, p_3, r_3, w_2^{-1}), \\ S_{t,3} &= P(p_1, r_1, w, r_3, q_3, v_3, p_4, q_4, v_4, \ldots, p_n, q_n, v_n). \end{aligned}$$

For w, w_1, w_2 as above let $\beta(w, w_1, w_2) \in K$ the unique element such that $w^{-1}w_1^{-1}w_2 =_H \beta(w, w_1, w_2)$. We define the formula

$$\begin{aligned} A_{2.4} = \bigwedge_{t \in T} \exists \bar{y}_1, \bar{z}_1, \bar{y}_2, \bar{z}_2, \bar{y}_3, \bar{z}_3, \bar{\chi}_1, \bar{\chi}_2, \bar{\chi}_3 : {} & (\bar{z}_1, \bar{y}_2, \bar{\chi}_1) \in S_{t,1} \wedge \\ & (\bar{z}_2, \bar{y}_3, \bar{\chi}_2) \in S_{t,2} \wedge \\ & (\bar{y}_1, \bar{z}_3, \bar{x}_4, \ldots, \bar{x}_n, \bar{\chi}_3) \in S_{t,3} \wedge \\ & \bigwedge_{i=1}^{3} \bar{x}_i = \bar{y}_i + \bar{z}_i \wedge \\ & \bar{\chi} = \bar{\chi}_1 + \bar{\chi}_2 + \bar{\chi}_3 + \beta(w, w_1, w_2). \end{aligned}$$

This concludes the case distinction.

A tuple $(\bar{x}_1, \ldots, \bar{x}_n, \bar{\chi}) \in \mathbb{N}^{ns} \times K$ belongs to the set $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$ if and only if $A_{1.1} \vee A_{1.2} \vee A_{2.1} \vee A_{2.2} \vee A_{2.3} \vee A_{2.4}$ holds. This yields a Presburger formula for $P(p_1, q_1, v_1, \ldots, p_n, q_n, v_n)$. □

9.8 Generalized cases and open problems

9.8.1 Undecidability for central extensions of abelian groups

Central extensions of abelian groups are the same as 2-step nilpotent groups. Since there exists a finitely generated 2-step nilpotent group H with an undecidable knapsack problem, it follows that knapsack for central extensions of finitely generated abelian groups is in general undecidable.

9.8.2 Malnormality and its role for knapsack-semilinearity

There are still a lot of cases for HNN-extensions where we do not know whether knapsack-semilinearity is preserved. After a very helpful talk with Alexei Miasnikov, we could come up with some very promising conjectures. Very roughly talking, the properties of HNN-extensions of a hyperbolic group are preserved under our conditions, because the resulting group "looks hyperbolic" in a certain way. This means that not too many elements commute and our proofs look very similar to the purely hyperbolic case.

Let us formalize this a bit more. In the paper of Kharlampovich and Miasnikov [56] the property *malnormality* plays a key role in understanding behaviour of HNN-extensions. For a group G, a subgroup $U \leq G$ is called *malnormal* if for all $g \in G \backslash U$ the set $U \cap gUg^{-1}$ is only the identity. If $U \cap gUg^{-1}$ contains only finitely many elements, we call it *conjugate separated*. Let A, B be subgroups of G and let $\varphi : A \to B$ be an isomorphism. The HNN-extension $\langle G, t \mid t^{-1}at = \varphi(a)(a \in A)\rangle$ is called *separated* if (i) either A or B is conjugate separated and (ii) $A \cap gBg^{-1}$ is finite for all $g \in G$.

If G is hyperbolic and H is a separated HNN-extension, where A and B are also quasiconvex, then H is hyperbolic. The same holds when G_1 and G_2 are hyperbolic and A is a quasiconvex associated subgroup, then the amalgamated free product $G_1 *_A G_2$ is hyperbolic. This gives us already more cases, where the HNN-extension preserves knapsack-semilinearity, just by preserving hyberbolism. But it also raises the question, if we can exchange the property hyperbolic by knapsack-semilinear.

Conjecture 9.16. *If G is knapsack-semilinear and H is a separated HNN-extension, where A and B are also quasiconvex, then H is knapsack-semilinear.*

Maybe we have to use *quasiisometrically embedded* instead of quasiconvex in this general case of G being knapsack-semilinear. But this is up to future work to find this out.

We have already discussed that knapsack-semilinearity is preserved, when we restrict the subgroups (for the HNN-extension) or the associated subgroup (for the amalgamation) to be finite. Indeed we can see a similar pattern here: Kharlampovich and Miasnikov have shown that hyperbolicity is also preserved in those two cases.

9.8.3 A generalization via Stallings pregroups

Another way of generalizing our results might be investigating Stallings pregroups (see for example [22, 85, 86]). It is well known that HNN-extensions and amalgamated free products are only special cases of Stallings pregroups. Together with the previously discussed property malnormality, one might come up with some more general theory how knapsack-semilinearity is preserved. Maybe one can even find conditions, where "if and only if" holds.

9.8.4 Further future work

In the literature, central extensions are often defined as short exact sequences of the form $1 \to K \to H \to G \to 1$, where $K \leq Z(H)$. With this definition, one can derive that we can obtain all central extensions of G by K (up to isomorphism) with the cohomology group $H^2(G, K)$ (see e.g. [70]). Hence, by studying homological algebra, one might be able to generalize our results to central extensions of other knapsack-semilinear groups or even obtain bounds for the magnitudes.

In [31] it was shown that the class of knapsack-semilinear groups is also closed under restricted wreath products. It remains to bound the function $\mathsf{K}_{G \wr H}(n, m)$ in terms of the functions $\mathsf{K}_G(n, m)$ and $\mathsf{K}_H(n, m)$. Looking into the proof in [31] reveals that the Presburger formula that describes the solution set for a knapsack equation over $G \wr H$ involves a quantifier alternation. One therefore has to investigate to what extent quantifier alternations blow-up the magnitude of semilinear sets.

More about wreath products in the next chapter.

Chapter 10

Computational hardness results

10.1 Introduction

In the first part of this chapter, Section 10.2, we are going to prove Theorem 4.11. For this we make use so-called *uniformly strongly efficiently non-solvable* groups (uniformly SENS groups) that were recently defined in [F2]. Roughly speaking, a group G is uniformly SENS if there exist nontrivial nested commutators of arbitrary depth that moreover, are efficiently computable in a certain sense (see Subsection 2.4.8 for the precise definition). The essence of these groups is that they allow to carry out Barrington's argument showing the NC^1-hardness of the word problem for a finite solvable group [5].

It has already been shown that for every nontrivial group G, $\textsc{Knapsack}(G \wr \mathbb{Z})$ is NP-hard [31]. So our result, showing that $\textsc{Knapsack}(G \wr \mathbb{Z})$ is Σ_2^p-hard for a uniformly SENS group G, is an extension of this theorem. We also state several corollaries. For instance, we show that for the famous Thompson's group F, $\textsc{Knapsack}(F)$ is Σ_2^p-hard (see Corollary 10.6).

In the second part (Section 10.3) we want to show that the question if one exponent equation over $SL_3(\mathbb{Z})$ has a solution is already undecidable (Theorem 4.12). The proof has not been published before. We want to recall that the question is actually decidable for $H_3(\mathbb{Z})$, but undecidable for systems of exponent equations over $H_3(\mathbb{Z})$ (see [58]). The latter one is shown by a reduction of Hilbert's 10th problem to that problem. This is exactly, what we will do now in case of $SL_3(\mathbb{Z})$.

10.2 Wreath products with difficult knapsack problem

10.2.1 Periodic words over groups

Let $G = \langle \Sigma \rangle$ be a f.g. group. Let G^ω be the set of all functions $f\colon \mathbb{N} \to G$, which forms a group by pointwise multiplication $(fg)(t) = f(t) \cdot g(t)$. A function $f \in G^\omega$ is *periodic* if there exists a number $d \geq 1$ such that $f(t) = f(t+d)$ for all $t \geq 0$. The smallest such number d is called the *period* of f. If $f \in G^\omega$ has period d and $g \in G^\omega$ has period e then fg has period at most $\mathrm{lcm}(d, e)$. A periodic function $f \in G^\omega$ with period d can be specified by its initial d elements $f(0), \ldots, f(d-1)$ where each element $f(t)$ is given as a word over the generating set Σ. The *periodic words problem* $\textsc{Periodic}(G)$ over G is defined as follows:

Input Periodic functions $f_1, \ldots, f_m \in G^\omega$ and a binary encoded number T.

Question Does the product $f = \prod_{i=1}^{m} f_i$ satisfy $f(t) = 1$ for all $t \leq T$?

10.2.2 Some useful results on knapsack-semilinearity of wreath products

For the knapsack problem in wreath products the following result has been shown in [31]:

Theorem 10.1 ([31])**.** *For every nontrivial group G, $\textsc{Knapsack}(G \wr \mathbb{Z})$ is* NP*-hard.*

Important for us is also this result from [31]:

Theorem 10.2 ([31])**.** *If G and H are knapsack-semilinear then also $G \wr H$ is knapsack-semilinear.*

The proof of this result in [31] does not yield a good bound of $\mathsf{K}_{G \wr H}(n)$ in terms of $\mathsf{K}_G(n)$ and $\mathsf{K}_H(n)$ (and similarly for the E-function). In [F3] there is also a bound for the special case that the left factor G is f.g. abelian. For $\mathsf{E}_G(n)$ we then have the following bound, which follows from well-known bounds on solutions of linear Diophantine equations [88]:

Lemma 10.3. *If G is a f.g. abelian group then $\mathsf{E}_G(n) \leq 2^{n^{\mathcal{O}(1)}}$.*

The following proposition is from [31] (see the proof of Proposition 7.2 in [31]).

Proposition 10.4 ([31])**.** *Let G be a f.g. group. There is a non-deterministic polynomial time Turing machine M that takes as input a knapsack expression e over $G \wr \mathbb{Z}$ and outputs in each leaf of the computation tree the following data:*

- *an instance of $\textsc{ExpEq}(G)$ and*
- *a finite list of instances of $\textsc{Periodic}(G)$.*

Moreover, the input expression e has a $(G \wr \mathbb{Z})$-solution if and only if there is a leaf in the computation tree of M such that all instances that M outputs in this leaf are positive.

10.2.3 Applications of Theorem 4.11

Recall Theorem 4.11:

Theorem 4.11 ([F3]). *Let the f.g. group $G = \langle \Sigma \rangle$ be uniformly SENS. Then,* $\textsc{Knapsack}(G \wr \mathbb{Z})$ *is Σ_2^p-hard.*

Before we prove this result we show some applications.

Corollary 10.5. *For the following groups G,* $\textsc{Knapsack}(G \wr \mathbb{Z})$ *is Σ_2^p-complete:*

- *finite non-solvable groups,*
- *non-elementary hyperbolic groups.*[9]

Proof. Finite non-solvable groups and f.g. non-abelian free groups are uniformly SENS [F2]. By Theorem 4.11, $\textsc{Knapsack}(G \wr \mathbb{Z})$ is Σ_2^p-hard. It remains to show that $\textsc{Knapsack}(G \wr \mathbb{Z})$ belongs to Σ_2^p. According to Proposition 10.4, it suffices to show that $\textsc{Periodic}(G)$ and $\textsc{ExpEq}(G)$ both belong to Σ_2^p. The problem $\textsc{Periodic}(G)$ belongs to coNP (since the word problem for G can be solved in polynomial time) and $\textsc{ExpEq}(G)$ belongs to NP. For a finite group this is clear. If G is hyperbolic, then one can reduce $\textsc{ExpEq}(G)$ to the existential fragment of Presburger arithmetic using [62]. □

Theorem 4.11 can be also applied to Thompson's group F. This is one of the most well studied groups in (infinite) group theory due to its unusual properties, see e.g. [16]. It can be defined in several ways; let us just mention the following finite presentation: $F = \langle x_0, x_1 \mid [x_0 x_1^{-1}, x_0^{-1} x_1 x_0], [x_0 x_1^{-1}, x_0^{-2} x_1 x_0^2] \rangle$. Thompson's group F is uniformly SENS [F2] and contains a copy of $F \wr \mathbb{Z}$ [38]. Theorem 4.11 yields

Corollary 10.6. *The knapsack problem for Thompson's group F is Σ_2^p-hard.*

We conjecture that the knapsack problem for F is in fact Σ_2^p-complete. Since F is co-context-free [60], $\textsc{Knapsack}(F)$ is decidable [58].

10.2.4 Proof of Theorem 4.11

We prove Theorem 4.11 in two steps. The second step works for every f.g. group G. Fix this group G and let Σ be a standard generating set for G. Let $\overline{X} = (X_1, \ldots, X_n)$ be a tuple of boolean variables. We identify $\overline{X}$ with the set $\{X_1, \ldots, X_n\}$ when appropriate. A G-program with variables from $\overline{X}$ is a sequence

$$P = (X_{i_1}, a_1, b_1)(X_{i_2}, a_2, b_2) \cdots (X_{i_\ell}, a_\ell, b_\ell) \in (\overline{X} \times \Sigma \times \Sigma)^*.$$

The length of P is ℓ. For a mapping $\alpha : \overline{X} \to \{0, 1\}$ (called an assignment) we define $P(\alpha) \in G$ as the group element $c_1 c_2 \cdots c_\ell$, where $c_j = a_j$ if $X_{i_j} = 1$ and $c_j = b_j$ if $X_{i_j} = 0$ for all $1 \leq j \leq \ell$. We define the following computational problem $\exists\forall\text{-}\textsc{Sat}(G)$:

[9] A hyperbolic group is non-elementary if it is not virtually cyclic. Every non-elementary hyperbolic group contains a non-abelian free group.

Input A G-program P with variables from $\overline{X} \cup \overline{Y}$, where $\overline{X}$ and $\overline{Y}$ are disjoint.

Question Is there an assignment $\alpha : \overline{X} \to \{0,1\}$ such that for every assignment $\beta : \overline{Y} \to \{0,1\}$ we have $P(\alpha \cup \beta) = 1$ (we write $\exists\overline{X}\forall\overline{Y} : P = 1$ for this)?

Lemma 10.7. *Let the f.g. group $G = \langle\Sigma\rangle$ be uniformly SENS. Then, $\exists\forall$-SAT(G) is Σ_2^p-hard.*

Proof. We prove the lemma by a reduction from the following Σ_2^p-complete problem: given a boolean formula $F = F(\overline{X}, \overline{Y})$ in disjunctive normal form, where $\overline{X}$ and $\overline{Y}$ are disjoint tuples of boolean variables, does the quantified boolean formula $\exists\overline{X}\forall\overline{Y} : F$ hold? Let us fix such a formula $F(\overline{X}, \overline{Y})$. We can write F as a fan-in two boolean circuit of depth $\mathcal{O}(\log |F|)$. By [F2, Remark 6.2] we can compute in logspace from F a G-program P over the variables $\overline{X} \cup \overline{Y}$ of length polynomial in $|F|$ such that for every assignment $\gamma : \overline{X} \cup \overline{Y} \to \{0,1\}$ the following two statements are equivalent:

- $F(\gamma(\overline{X}), \gamma(\overline{Y}))$ holds.
- $P(\gamma) = 1$ in G.

Hence, $\exists\overline{X}\forall\overline{Y} : F$ holds if and only if $\exists\overline{X}\forall\overline{Y} : P = 1$ holds. □

Lemma 10.8. *For every f.g. nontrivial group G, $\exists\forall$-SAT(G) is logspace many-one reducible to* KNAPSACK$(G \wr \mathbb{Z})$.

Proof. Let us fix a G-program

$$P = (Z_1, a_1, b_1)(Z_2, a_2, b_2) \cdots (Z_\ell, a_\ell, b_\ell) \in ((\overline{X} \cup \overline{Y}) \times \Sigma \times \Sigma)^* \tag{10.1}$$

where $\overline{X}$ and $\overline{Y}$ are disjoint sets of variables. Let $m = |\overline{X}|$ and $n = |\overline{Y}|$. We want to construct a knapsack expression e over $G \wr \mathbb{Z}$ which has a solution if and only if there is an assignment $\alpha : \overline{X} \to \{0,1\}$ such that $P(\alpha \cup \beta) = 1$ for every assignment $\beta : \overline{Y} \to \{0,1\}$. Let us choose a generator t for $\mathbb{Z}$. Then $\Sigma \cup \{t, t^{-1}\}$ generates the wreath product $G \wr \mathbb{Z}$. First, we compute in logspace the $m+n$ first primes $p_1, \ldots, p_{m+n}$ and fix a bijection $p : \overline{X} \cup \overline{Y} \to \{p_1, \ldots, p_{m+n}\}$. Moreover, let $M = \prod_{i=1}^{m+n} p_i$.

Roughly speaking, the idea is as follows. Each assignment $\alpha\colon \overline{X} \to \{0,1\}$ will correspond to a valuation ν for our expression e. The resulting element $\nu(e) \in G \wr \mathbb{Z}$ then encodes the value $P(\alpha \cup \beta)$ for each $\beta\colon \overline{Y} \to \{0,1\}$ in some position $s \in [0, M-1]$. To be precise, to each $s \in [0, M-1]$, we associate the assignment $\beta_s\colon \overline{Y} \to \{0,1\}$ where $\beta_s(Y) = 1$ if and only if $s \equiv 0 \bmod p(Y)$. Then, $\tau(\nu(e))(s)$ will be $P(\alpha \cup \beta_s)$. This means, $\nu(e) = 1$ implies that $P(\alpha \cup \beta) = 1$ for all assignments $\beta\colon \overline{Y} \to \{0,1\}$.

Our expression implements this as follows. For each $i = 1, \ldots, \ell$, it walks to the right to some position $M' \geq M$ and then walks back to the origin. On the way to the right, the behavior depends on whether Z_i is an existential or a universal variable. If Z_i is existential, we either place a_i at every position (if $\alpha(Z_i) = 1$) or b_i at every position (if $\alpha(Z_i) = 0$). If Z_i is universal, we place a_i

in the positions divisible by $p(Z_i)$; and we place b_i in the others. That way, in position $s \in [0, M-1]$, the accumulated element will be $P(\alpha \cup \beta_s)$.

We define $I_\exists = \{i \in [1,\ell] \mid Z_i \in \overline{X}\}$ and $I_\forall = \{i \in [1,\ell] \mid Z_i \in \overline{Y}\}$. For an existentially quantified variable $X \in \overline{X}$ let $I_X = \{i \in [1,\ell] \mid X = Z_i\}$ be the set of those positions in the G-program P, where the variable X is queried. Moreover, let us write q_i for the prime number $p(Z_i)$. We compute for every $i \in I_\exists$ the words (over the wreath product $G \wr \mathbb{Z}$)

$$u_i = (a_i t)^{q_i} \text{ and } v_i = (b_i t)^{q_i}$$

and for every $i \in I_\forall$ the word

$$w_i = a_i t (b_i t)^{q_i - 1}.$$

Let us now consider the knapsack expression

$$e_1 = \prod_{i=1}^{\ell} f_i t^{-1} (t^{-1})^{z_i} \text{ with } f_i = \begin{cases} u_i^{x_i} v_i^{x_i'} & \text{if } i \in I_\exists, \\ w_i^{y_i} & \text{if } i \in I_\forall. \end{cases}$$

The idea is that in e_1, for each $i \in [1,\ell]$, we go to right with f_i and then we go back to the origin with $t^{-1}(t^{-1})^{z_i}$. If Z_i is existential, we use $f_i = u_i^{x_i} v_i^{x_i'}$ to either place a_i at every position or b_i at every position. If Z_i is universal, we use w_i to place a_i at positions divisible by $q_i = p(Z_i)$ and b_i at the others. Note that the expression itself cannot guarantee that, e.g., (i) $(t^{-1})^{z_i}$ moves exactly onto the origin or (ii) that we either use only u_i or only v_i for each $i \in I_\exists$. Therefore, we ensure these properties temporarily by imposing additional linear equations (Claim 1). In a second step, we shall extend e_1 to get an expression in which a solution will automatically satisfy these linear equations (Claim 2).

Claim 1: $\exists\overline{X}\forall\overline{Y} : P = 1$ holds if and only if there exists a $(G \wr \mathbb{Z})$-solution ν for e_1 with the following properties:

(a) $q_i \cdot \nu(y_i) = \nu(z_i) + 1$ for all $i \in I_\forall$,
(b) $q_i \cdot (\nu(x_i) + \nu(x_i')) = \nu(z_i) + 1$ for all $i \in I_\exists$,
(c) $\nu(z_i) = \nu(z_j)$ for all $i, j \in [1,\ell]$ with $i \neq j$,
(d) $\nu(x_i) = 0$ or $\nu(x_i') = 0$ for all $i \in I_\exists$,
(e) for all $X \in \overline{X}$ and all $i, j \in I_X$ we have: $\nu(x_i) = 0$ if and only if $\nu(x_j) = 0$.

Proof of Claim 1: Assume first that $\exists\overline{X}\forall\overline{Y} : P = 1$ holds. Let $\alpha : \overline{X} \to \{0,1\}$ be an assignment such that for every assignment $\beta : \overline{Y} \to \{0,1\}$, we have $P(\alpha \cup \beta) = 1$ in G.

We have to find a $(G \wr \mathbb{Z})$-solution for e_1 such that the above properties (a)–(d) hold. For this, we set:

- $\nu(z_i) = M - 1$ for all $i \in [1,\ell]$,
- $\nu(y_i) = M/q_i$ for all $i \in I_\forall$,
- $\nu(x_i) = M/q_i$ and $\nu(x_i') = 0$ for all $i \in I_X$, $X \in \overline{X}$ such that $\alpha(X) = 1$,
- $\nu(x_i') = M/q_i$ and $\nu(x_i) = 0$ for all $i \in I_X$, $X \in \overline{X}$ such that $\alpha(X) = 0$.

Then, clearly, (a)–(e) hold. It remains to verify that ν is a $(G \wr \mathbb{Z})$-solution for e_1. Let $h = \tau(\nu(e_1)) \in G^{(\mathbb{Z})}$ and $k = \sigma(\nu(e_1)) \in \mathbb{Z}$. We have $k = 0$ and $h(s) = 1$ for all $s \in \mathbb{Z} \setminus [0, M-1]$. Moreover, for every $s \in [0, M-1]$ we have $h(s) = c_1 c_2 \dots c_\ell$ where

$$c_i = \begin{cases} a_i & \text{if } (i \in I_\forall \text{ and } s \equiv 0 \bmod q_i) \text{ or } (i \in I_X, X \in \overline{X} \text{ and } \alpha(X) = 1) \\ b_i & \text{if } (i \in I_\forall \text{ and } s \not\equiv 0 \bmod q_i) \text{ or } (i \in I_X, X \in \overline{X} \text{ and } \alpha(X) = 0). \end{cases}$$

Here, the a_i and b_i are from (10.1). Hence, there is an assignment $\beta_s : \overline{Y} \to \{0,1\}$ such that $h(s) = P(\alpha \cup \beta_s)$. Thus, $h(s) = 1$ for all $s \in [0, M-1]$, which implies that $\nu(e_1) = 1$ in $G \wr \mathbb{Z}$.

For the other direction, assume that ν is a $(G \wr \mathbb{Z})$-solution for e_1 such that the properties (a)–(e) hold. Let $M' = \nu(z_1) + 1 > 0$. We then have $M' = \nu(z_i) + 1$ for all $i \in [1, \ell]$ by property (c). By properties (a) and (b), M' is divisible by the first $m + n$ primes. This implies that M' is a multiple of M and thus $M' \geq M$.

Let us define an assignment $\alpha : \overline{X} \to \{0,1\}$ as follows, where $i \in I_\exists$:

$$\alpha(Z_i) = \begin{cases} 0 \text{ if } \nu(x_i) = 0 \\ 1 \text{ if } \nu(x_i') = 0 \end{cases}$$

By properties (d) and (e) this defines indeed an assignment $\alpha : \overline{X} \to \{0,1\}$. Moreover, for every position $s \in [0, M'-1]$ we define the assignment $\beta_s : \overline{Y} \to \{0,1\}$ by $\beta_s(Y) = 1$ if $s \equiv 0 \bmod p(Y)$ and $\beta_s(Y) = 0$ otherwise. By the Chinese remainder theorem, for every $\beta : \overline{Y} \to \{0,1\}$ there exists $s \in [0, M'-1]$ with $\beta = \beta_s$. Moreover, the construction of e_1 implies that $\nu(e_1)$ writes $P(\alpha \cup \beta_s)$ into position s. Since $\nu(e_1) = 1$ in $G \wr \mathbb{Z}$ we have $P(\alpha \cup \beta_s) = 1$ for all $s \in [0, M'-1]$, i.e., $P(\alpha \cup \beta) = 1$ for all assignments $\beta : \overline{Y} \to \{0,1\}$. We have shown Claim 1.

In the rest of the proof we construct a knapsack expression e_2 such that each of the variables from e_1 also occurs in e_2. Moreover, the following properties will hold:

- Every $(G \wr \mathbb{Z})$-solution of e_1 that satisfies the properties (a)–(e) extends to a $(G \wr \mathbb{Z})$-solution of e_2.
- Every $(G \wr \mathbb{Z})$-solution of e_2 restricts to a $(G \wr \mathbb{Z})$-solution of e_1 that satisfies the properties (a)–(e).

This implies that e_2 has a $(G \wr \mathbb{Z})$-solution if and only if e_1 has a $(G \wr \mathbb{Z})$-solution that satisfies the properties (a)–(e) if and only if $\exists \overline{X} \forall \overline{Y} : P = 1$ holds.

Let $g \in G$ be any nontrivial element. To construct e_2 it is convenient to work in a wreath product $(\langle g \rangle^d \times G) \wr \mathbb{Z}$ for some d, whose unary encoding can be computed (in logspace) from the input formula $\exists \overline{X} \forall \overline{Y} : F$. By Lemma 2.9 we can compute in logspace an embedding of $(\langle g \rangle^d \times G) \wr \mathbb{Z}$ into $G \wr \mathbb{Z}$. Let ζ_i be the canonical embedding of $\langle g \rangle$ into $\langle g \rangle^d$ that maps g to $(1, \dots, 1, g, 1, \dots, 1)$, where in the latter, g appears in the i-th coordinate. We assume that the coordinates are numbered from 0 to $d-1$. In the following, we write g_i for $\zeta_i(g)$. We set $d = 2\ell + 1$.

We then define the following knapsack expression $e_2 = e_{2,1}e_{2,2}$ where z, z' and $\tilde{X}, \tilde{X}'$ for all $X \in \overline{X}$ appear as fresh variables:

$$\begin{aligned} e_{2,1} &= g_0 g_1 \cdots g_\ell \left(\prod_{X \in \overline{X}} \left(\prod_{i \in I_X} g_{\ell+i} \right)^{\tilde{X}'} \right) t t^z g_1 \cdots g_\ell \cdot \\ &\qquad \left(\prod_{X \in \overline{X}} \left(\prod_{i \in I_X} g_{\ell+i} \right)^{\tilde{X}} \right) t^{-1} (t^{-1})^{z'} g_0^{-1} \\ e_{2,2} &= \prod_{i=1}^{\ell} f_i g_i^{-1} t^{-1} (t^{-1})^{z_i} g_i^{-1} \text{ with } f_i = \begin{cases} u_i^{x_i} g_{\ell+i}^{-1} v_i^{x_i'} & \text{if } i \in I_\exists, \\ w_i^{y_i} & \text{if } i \in I_\forall. \end{cases} \end{aligned}$$

The idea of the construction is that the g_i implement pebbles that can be put on different positions in $\mathbb{Z}$. At the end all pebbles have to be recollected. Note that we only use the pebbles $g_0, g_1, \ldots, g_\ell$ and $g_{\ell+i}$ for $i \in I_\exists$; hence we could reduce the dimension $2\ell + 1$ to $\ell + 1 + |I_\exists|$ but this would make the indexing slightly more inconvenient.

Claim 2: Every $(G \wr \mathbb{Z})$-solution of e_1 that satisfies the properties (a)–(e) extends to a $(G \wr \mathbb{Z})$-solution of e_2.

Proof of Claim 2: Let ν be a $(G \wr \mathbb{Z})$-solution of e_1 that satisfies the properties (a)–(e). Let $M' = \nu(z_1) + 1 > 0$. Hence, $M' = \nu(z_i) + 1$ for all $i \in [1, \ell]$. We then extend ν to the fresh variables in e_2 by:

- $\nu(z) = \nu(z') = M' - 1$,
- for all $X \in \overline{X}$ such that $x_i = 0$ for some (and hence all) $i \in I_X$, we set $\nu(\tilde{X}') = 1$ and $\nu(\tilde{X}) = 0$,
- for all $X \in \overline{X}$ such that $x_i' = 0$ for some (and hence all) $i \in I_X$, we set $\nu(\tilde{X}') = 0$ and $\nu(\tilde{X}) = 1$.

It is easy to check that this yields indeed a $(G \wr \mathbb{Z})$-solution of e_2.

Claim 3: Every $(G \wr \mathbb{Z})$-solution of e_2 restricts to a $(G \wr \mathbb{Z})$-solution of e_1 that satisfies the properties (a)–(e).

Proof of Claim 3: Fix a $(G \wr \mathbb{Z})$-solution ν of e_2. First of all, we must have $\nu(z) = \nu(z')$; otherwise the pebble g_0 will not be recollected. Let $M' = \nu(z) + 1 > 0$. The word $\nu(e_{2,1})$ leaves pebbles $g_1, \ldots, g_\ell$ at positions 0 and M' (it also leaves powers of the pebbles $g_{\ell+i}$ — we will deal with those later) and puts the cursor back to position 0. With the word $\nu(e_{2,1})$ the pebbles at positions 0 and M' have to be recollected. This happens only if $\nu(z_i) = M' - 1$ for all $i \in [1, \ell]$, $q_i \cdot \nu(y_i) = M'$ for all $i \in I_\forall$, and $q_i \cdot (\nu(x_i) + \nu(x_i')) = M'$ for all $i \in I_\exists$. Hence, conditions (a)–(c) hold.

Conditions (d) and (e) are enforced with the pebbles $g_{\ell+i}$ for $i \in I_\exists$. Consider an existentially quantified variable $X \in \overline{X}$. The word $\nu(e_{2,1})$ leaves for every $i \in I_X$ the "pebble powers" $g_{\ell+i}^{\nu(\tilde{X}')}$ and $g_{\ell+i}^{\nu(\tilde{X})}$ at positions 0 and $M' > 0$, respectively. With the word $\nu(e_{2,2})$ exactly one pebble $g_{\ell+i}$ is recollected. Therefore, exactly one of the following two cases has to hold:

- $g^{\nu(\tilde{X}')} = 1$ and $g^{\nu(\tilde{X})} = g$ in G,
- $g^{\nu(\tilde{X}')} = g$ and $g^{\nu(\tilde{X})} = 1$ in G.

Assume first that $g^{\nu(\tilde{X}')} = 1$ and $g^{\nu(\tilde{X})} = g$ in G. Then $\nu(e_{2,1})$ places the pebble $g_{\ell+i}$ at position M' (and it places this pebble at no other position) for all $i \in I_X$. In order to recollect this pebble with $\nu(e_{2,2})$ we must have $\nu(x_i) = M'/q_i = M'/p(X)$ and $\nu(x_i') = 0$ for all $i \in I_X$. If $g^{\nu(\tilde{X}')} = g$ and $g^{\nu(\tilde{X})} = 1$ in G then we must have $\nu(x_i') = M'/q_i = M'/p(X)$ and $\nu(x_i) = 0$ for all $i \in I_X$. This shows that (d) and (e) holds and concludes the proof of Claim 3 and hence the proof of the lemma. □

Theorem 4.11 is now a direct corollary of Lemmas 10.7 and 10.8.

10.3 Undecidability for $SL_3(\mathbb{Z})$

Let us recall Theorem 4.12:

Theorem 4.12. *It is undecidable if a single exponent equation over $SL_3(\mathbb{Z})$ has a solution.*

Proof. The proof is inspired by a construction of Ben-Or and Cleve (see [8] and [61, Theorem 4.16]). In order to reduce Hilbert's 10th problem to exponent equations over $SL_3(\mathbb{Z})$, we need to transform an arbitrary polynomial $p(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ into an expression $e = A_1^{x_{i_1}} \cdots A_\ell^{x_{i_\ell}} B$ with $A_i, B \in SL_3(\mathbb{Z})$ and $x_i \in \mathbb{Z}$ ($1 \leq i_1, \ldots, i_\ell \leq k$) such that $p(x_1, \ldots, x_k) = 0$ has a solution in $\mathbb{Z}$ if and only if $A_1^{x_{i_1}} \cdots A_\ell^{x_{i_\ell}} B = \mathrm{Id}_3$ has a solution in $\mathbb{Z}$, where Id_3 is the 3×3 identity matrix.

More precisely, we have to do the following: For $i, j \in \{1, 2, 3\}$ with $i \neq j$ let $M_{i,j,a}$ be the 3×3 matrix with entry $a \in \mathbb{Z}$ at position (i, j) and 0 at all other positions. Furthermore let $A_{i,j,a} = \mathrm{Id}_3 + M_{i,j,a}$. Then the following simple identities for $M_{i,j,a}$ hold:

(a) $M_{i,j,a} + M_{i,j,b} = M_{i,j,a+b}$

(b) $M_{i,j,a} M_{j,k,b} = M_{i,k,ab}$

(c) $M_{i,j,a} M_{k,\ell,b} = 0$ for $j \neq k$

With these, we get helpful identities regarding $A_{i,j,a}$:

(i) $A_{i,j,a} A_{i,j,b} = A_{i,j,a+b}$

(ii) $(A_{i,j,\varepsilon})^a = A_{i,j,\varepsilon \cdot a}$ for $a \geq 1$, $\varepsilon \in \{-1, +1\}$

(iii) $A_{k,j,-a} A_{i,k,b} A_{k,j,a} A_{i,k-b} = A_{i,j,ab}$, where $\{i, j, k\} = \{1, 2, 3\}$

Identity (i) simulates addition of polynomials, the commutator looking equation (iii) simulates multiplication of polynomials. Let us first prove $(i) - (iii)$: With

$$\begin{aligned} A_{i,j,a} A_{i,j,b} &= (\mathrm{Id}_3 + M_{i,j,a})(\mathrm{Id}_3 + M_{i,j,b}) \\ &= \mathrm{Id}_3 + M_{i,j,a} + M_{i,j,b} + M_{i,j,a} M_{i,j,b} \\ &= \mathrm{Id}_3 + M_{i,j,a+b} \end{aligned}$$

we obtain (i). The third $=$ is true because of $i \neq j$. This immediately implies (ii) (more generally we get $(A_{i,j,a})^k = A_{i,j,a \cdot k}$ for $a \in \mathbb{Z}$ and $k \geq 0$). For (iii) we have

$$\begin{aligned}
&A_{k,j,-a}A_{i,k,b}A_{k,j,a}A_{i,k,-b}\\
=&(\mathrm{Id}_3 + M_{k,j,-a})(\mathrm{Id}_3 + M_{i,k,b})(\mathrm{Id}_3 + M_{k,j,a})(\mathrm{Id}_3 + M_{i,k,-b})\\
=&(\mathrm{Id}_3 + M_{k,j,-a} + M_{i,k,b})(\mathrm{Id}_3 + M_{k,j,a} + M_{i,k,-b})\\
=&\,\mathrm{Id}_3 + M_{k,j,-a} + M_{k,j,a} + M_{i,k,b} + M_{i,k,-b} + M_{i,k,b}M_{k,j,a}\\
=&\,\mathrm{Id}_3 + M_{i,j,ab}.
\end{aligned}$$

The third $=$ holds, since all other products $M_{\dots}M_{\dots}$ vanish due to non-matching indices (see (c)).

Let $p(x_1, \dots, x_k) \in \mathbb{Z}[x_1, \dots, x_k]$ be a polynomial. Remark: It is possible to restrict the x_t to take values in $\mathbb{N}$, since every integer z can be written as $x - y$ with $x, y \in \mathbb{N}$. In such a scenario the number of variables would double, but this is not a problem. For every variable x_t one constructs the following exponential expressions for all $i, j \in \{1, 2, 3\}$ with $i \neq j$ (see (ii)):

- $e_{i,j,x_t} := (A_{i,j,1})^{x_t}$
- $e_{i,j,-x_t} := (A_{i,j,-1})^{x_t}$

In the next step, we focus on monomials in $p(x_1, \dots, x_k)$. We can write p as a sum of monomials $x_1^{d_1}x_2^{d_2}\cdots x_k^{d_k}$ and their negations (possibly with repetitions). Let $m = x_1^{d_1}x_2^{d_2}\cdots x_k^{d_k}$ be a monomial that occurs in $p(x_1, \dots, x_k)$ and assume that all d_i are positive. Since monomials are purely build by multiplication, we use (iii) to obtain the expressions $e_{i,j,m}$ and $e_{i,j,-m}$ for all $i, j \in \{1, 2, 3\}$ with $i \neq j$. For the constant term $c \in \mathbb{Z}$ of $p(x_1, \dots, x_k)$, we can just take $e_{i,j,c} = A_{i,j,c}$ and $e_{i,j,-c} = A_{i,j,-c}$.

Lastly, we have to consider additions of monomials (the constant c included) in order to obtain an expression for the whole polynomial. Here we make use of (i). If we for instance have a polynomial like $p(x, y, z) = x^3y - y^2 + xz^2$, then we use (i) twice to add the three monomials together. And with this example we can also see that we really need $e_{i,j,-m}$, because otherwise it would be difficult to deal with the negative monomial $-y^2$. The expressions $e_{i,j,-m}$ are also needed for multiplications (see (iii)). In the end we obtain the desired expression $e_{1,2,p}$ for the whole polynomial p (we could take any $e_{i,j,p}$ for $i \neq j$). And now it is easy to see that for every valuation $\nu : \{x_1, \dots, x_k\} \to \mathbb{N}$ we have $(\nu(e_{1,2,p}))_{1,2} = p(\nu(x_1), \dots, \nu(x_k))$. Hence, $\mathsf{sol}_{SL_3(\mathbb{Z})}(e_{1,2,p}) \neq \emptyset$ if and only if $p(x_1, \dots, x_k) = 0$ has a solution. This yields the desired reduction and thus the theorem is proven. □

10.4 Open and related problems

Recall we proved that knapsack for Thompson's group F is Σ_2^p-hard. Decidability of knapsack for Thompson's group F follows from [58] and the fact that F is co-context-free. It is shown in [58] that for every co-context-free group the knapsack problem reduces to checking non-universality of the Parikh image of a bounded context-free language. The latter problem belongs to NEXPTIME [50, Theorem 2.10] (see also [40, Corollary 1]). It would be interesting to find better complexity bounds for this problem.

Moreover, there are many open group theoretic problems related to the group $SL_3(\mathbb{Z})$ in particular. For instance, the knapsack, the rational subset membership and the subgroup membership problem seem very difficult to solve. Even though the first problem looks similar to what we just considered, but allowing a variable in an exponent expression to appear only once makes the proof idea of Ben-Or and Cleve already not work.

What can be solved on the other hand are exponent equations for other related groups. We know that $SL_2(\mathbb{Z})$ is knapsack-semilinear[10] (hence exponent equations are decidable) and that some group theoretic problems are undecidable for $SL_n(\mathbb{Z})$, $n \geq 4$, such as the identity problem ([7]) and the subgroup membership problem (since we can embed $F_2 \times F_2$ into this group). It is also unknown whether knapsack is decidable for $SL_n(\mathbb{Z})$, $n \geq 4$.

For the other Heisenberg groups $H_k(\mathbb{Z})$ ($k \geq 4$) we can use the same calculations as in [58] for $H_3(\mathbb{Z})$ and see that one exponent equation is decidable, but systems of exponent equations are undecidable. There is also a very recent result that rational subset membership problem is decidable for $H_3(\mathbb{Z})$, even though the rational subset membership problem remains unsolved for higher order Heisenberg groups (see [12]).

We furthermore know that systems of exponent equations are undecidable for the Baumslag-Solitar groups $\mathrm{BS}(1, q) = \langle a, t \mid t^{-1}at = a^q \rangle$ ($q \geq 2$), but it is not known whether this is also undecidable for only one exponent equation (see [32]).

[10] The group $SL_2(\mathbb{Z}) = \langle S, R \mid S^4 = 1, R^6 = 1, S^2 = R^3 \rangle$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} *_A \mathbb{Z}/6\mathbb{Z}$, where $A = \{\mathrm{Id}, -\mathrm{Id}\}$ (see e.g. [83]). This means, $SL_2(\mathbb{Z})$ is an amalgamated free product of two finite groups. And we proved knapsack-semilinearity in this case (see Chapter 7).

Resulting publications

[F1] Laurent Bartholdi, Michael Figelius, Markus Lohrey, and Armin Weiß. Groups with ALOGTIME-hard word problems and PSPACE-complete circuit value problems. In *35th Computational Complexity Conference (CCC 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.CCC.2020.29.

[F2] Laurent Bartholdi, Michael Figelius, Markus Lohrey, and Armin Weiß. Groups with ALOGTIME-hard word problems and PSPACE-complete compressed word problems. *ACM Transactions on Computation Theory*, 14(3-4):1–41, 2023. doi:10.1145/3569708.

[F3] Michael Figelius, Moses Ganardi, Markus Lohrey, and Georg Zetzsche. The complexity of knapsack problems in wreath products. In *Proceedings of the 47th International Colloquium on Automata, Languages, and Programming, ICALP 2020*, volume 168 of *LIPIcs*, pages 126:1–126:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. doi:10.4230/LIPIcs.ICALP.2020.126.

[F4] Michael Figelius and Markus Lohrey. Exponent equations in HNN-extensions. *Journal of Groups, Complexity, Cryptology*, 14, 2022. doi:10.46298/jgcc.2022.14.2.10521.

[F5] Michael Figelius and Markus Lohrey. Exponent equations in HNN-extensions. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*, pages 293–301, 2022. doi:10.1145/3476446.3535482.

[F6] Michael Figelius, Markus Lohrey, and Georg Zetzsche. Closure properties of knapsack semilinear groups. *Journal of Algebra*, 589:437–482, 2022. doi:10.1016/j.jalgebra.2021.08.016.

Bibliography

[1] Sergei I. Adian. The Burnside problem and related topics. *Russian Mathematical Surveys*, 65(5):805–855, 2010. doi:10.1070/RM2010v065n05ABEH004702.

[2] Reg Allenby and Robert John Gregorac. On locally extended residually finite groups. In *Conference on Group Theory (Univ. Wisconsin-Parkside, Kenosha, Wis., 1972)*, number 319 in Lecture Notes in Mathematics, pages 9–17. Springer, Berlin, 1973. doi:10.1007/BFb0058924.

[3] Goulnara N. Arzhantseva. On quasiconvex subgroups of word hyperbolic groups. *Geometriae dedicata*, 87:191–208, 2001. doi:10.1023/A:1012040207144.

[4] László Babai, Richard Beals, James Cai, Gábor Ivanyos, and Eugene Luks. Multiplicative equations over commuting matrices. In *Proceedings of SODA 1996*, pages 498–507. ACM/SIAM, 1996.

[5] David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *Journal of Computer and System Sciences*, 38:150–164, 1989. doi:10.1016/0022-0000(89)90037-8.

[6] Simon Beier, Markus Holzer, and Martin Kutrib. On the descriptional complexity of operations on semilinear sets. In *Proceedings of the 15th International Conference on Automata and Formal Languages, AFL 2017*, volume 252 of *EPTCS*, pages 41–55, 2017. doi:10.4204/EPTCS.252.8.

[7] Paul Bell and Igor Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *International Journal of Foundations of Computer Science*, 21:963–978, 2010. doi:10.1142/S0129054110007660.

[8] Michael Ben-Or and Richard Cleve. Computing algebraic formulas with a constant number of registers. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 254–257, 1988. doi:10.1145/62212.62236.

[9] Pascal Bergsträßer, Moses Ganardi, and Georg Zetzsche. A characterization of wreath products where knapsack is decidable. In *Proceedings of the 38th International Symposium on Theoretical Aspects of Computer Science,*

STACS 2021, volume 187 of *LIPIcs*, pages 11:1–11:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.STACS.2021.11.

[10] Alberto Bertoni, Giancarlo Mauri, and Nicoletta Sabadini. Membership problems for regular and context free trace languages. *Information and Computation*, 82:135–150, 1989. doi:10.1016/0890-5401(89)90051-5.

[11] Agnieszka Bier and Oleg Bogopolski. Exponential equations in acylindrically hyperbolic groups. *arXiv preprint arXiv:2106.11385*, 2021. doi:10.48550/arXiv.2106.11385.

[12] Corentin Bodart. Membership problems in nilpotent groups. *arXiv preprint arXiv:2401.15504*, 2024. doi:10.48550/ARXIV.2401.15504.

[13] Oleg Bogopolski and Aleksander Ivanov. Decidability problem for exponential equations in finitely presented groups. *Canadian Mathematical Bulletin*, 66(3):731–748, 2023. doi:10.4153/S0008439522000698.

[14] Ronald V. Book and Friedrich Otto. *String–Rewriting Systems*. Springer, 1993. doi:10.1007/978-1-4613-9771-7.

[15] William W. Boone. The word problem. *Annals of Mathematics. Second Series*, 70:207–265, 1959. doi:10.2307/2964151.

[16] John W. Cannon, William J. Floyd, and Walter R. Parry. Introductory notes on Richard Thompson's groups. *L'Enseignement Mathématique*, 42(3):215–256, 1996. doi:10.5169/seals-87877.

[17] Dmitry Chistikov and Christoph Haase. The taming of the semi-linear set. In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016*, volume 55 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 128:1–128:13. Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPIcs.ICALP.2016.128.

[18] Max Dehn. Über unendliche diskontinuierliche Gruppen. *Mathematische Annalen*, 71:116–144, 1911. In German. doi:10.1007/BF01456932.

[19] Warren Dicks and Martin J. Dunwoody. *Groups Acting on Graphs*. Cambridge University Press, 1989.

[20] Voker Diekert. *Combinatorics on Traces*, volume 454 of *Lecture Notes in Computer Science*. Springer, 1990. doi:10.1007/3-540-53031-2.

[21] Voker Diekert and Grzegorz Rozenberg, editors. *The Book of Traces*. World Scientific, 1995. doi:10.1142/2563.

[22] Volker Diekert, Andrew J. Duncan, and Alexei G. Miasnikov. Geodesic rewriting systems and pregroups. In *Combinatorial and geometric group theory*, Trends in Mathematics, pages 55–91. Birkhäuser, 2010. doi:10.1007/978-3-7643-9911-5_3.

[23] Volker Diekert and Markus Lohrey. Word equations over graph products. *International Journal of Algebra and Computation*, 18(3):493–533, 2008. doi:10.1142/S0218196708004548.

[24] Carl Droms. A complex for right-angled Coxeter groups. *Proceedings of the American Mathematical Society*, 131(8):2305–2311, 2003. doi:10.2307/1194256.

[25] Fedor Anatolievich Dudkin and Alexander Victorovich Treyer. Knapsack problem for Baumslag–Solitar groups. *Siberian Journal of Pure and Applied Mathematics*, 18(4):43–55, 2018. doi:10.33048/pam.2018.18.404.

[26] Friedrich Eisenbrand and Gennady Shmonin. Carathéodory bounds for integer cones. *Operations Research Letters*, 34(5):564–568, 2006. doi:10.1016/j.orl.2005.09.008.

[27] Michael Elberfeld, Andreas Jakoby, and Till Tantau. Algorithmic meta theorems for circuit classes of constant and logarithmic depth. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:128, 2011. doi:10.4230/LIPIcs.STACS.2012.66.

[28] David Epstein, James Cannon, Derek Holt, Silvio Levy, Michael Paterson, and William Thurston. *Word Processing in Groups*. Jones and Bartlett, Boston, 1992. doi:10.1201/9781439865699.

[29] David Epstein and Derek Holt. The linearity of the conjugacy problem in word-hyperbolic groups. *International Journal of Algebra and Computation*, 16(02):287–305, 2006. doi:10.1142/S0218196706002986.

[30] Elizaveta Frenkel, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in products of groups. *Journal of Symbolic Computation*, 74:96–108, 2016. doi:10.1016/j.jsc.2015.05.006.

[31] Moses Ganardi, Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack problems for wreath products. In *Proceedings of 35th Symposium on Theoretical Aspects of Computer Science, STACS 2018*, volume 96 of *LIPIcs*, pages 32:1–32:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. doi:10.4230/LIPIcs.STACS.2018.32.

[32] Moses Ganardi, Markus Lohrey, and Georg Zetzsche. Knapsack and the power word problem in solvable Baumslag–Solitar groups. *International Journal of Algebra and Computation*, 33(03):617–639, 2023. doi:10.1142/S0218196723500285.

[33] Stephen M. Gersten and Hamish B. Short. Rational subgroups of biautomatic groups. *Annals of mathematics*, pages 125–158, 1991. doi:10.2307/2944334.

[34] Etienne Ghys and Pierre da la Harpe. *Sur les groupes hyperboliques d'apres Mikhael Gromov*, volume 83. Springer Science & Business Media, 2013. doi:10.1007/978-1-4684-9167-8.

[35] Seymour Ginsburg and Edwin Henry Spanier. Semigroups, Presburger formulas and languages. *Pacific Journal of Mathematics*, 16(2):285–296, 1966. doi:10.2140/pjm.1966.16.285.

[36] Elisabeth R. Green. *Graph Products of Groups*. PhD thesis, The University of Leeds, 1990. URL: https://api.semanticscholar.org/CorpusID:117106161.

[37] Michail L. Gromov. Hyperbolic groups. In Stephen M. Gersten, editor, *Essays in Group Theory*, number 8 in MSRI Publ., pages 75–263. Springer, 1987. doi:10.1007/978-1-4613-9586-7_3.

[38] Victor S. Guba and Mark V. Sapir. On subgroups of the R. Thompson group F and other diagram groups. *Matematicheskii Sbornik*, 190(8):3–60, 1999. doi:10.1070/SM1999v190n08ABEH000419.

[39] Christoph Haase. *On the complexity of model checking counter automata*. PhD thesis, University of Oxford, St Catherine's College, 2011. URL: https://api.semanticscholar.org/CorpusID:45838025.

[40] Christoph Haase. Subclasses of Presburger arithmetic and the weak EXP hierarchy. In *Proceedings of the Joint Meeting of the 23rd EACSL Annual Conference on Computer Science Logic (CSL) and the 29th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–10, 2014. doi:10.1145/2603088.2603092.

[41] Christoph Haase. A survival guide to Presburger arithmetic. *ACM SIGLOG News*, 5(3):67–82, 2018. doi:10.1145/3242953.3242964.

[42] Niko Haubold and Markus Lohrey. Compressed word problems in HNN-extensions and amalgamated products. *Theory of Computing Systems*, 49(2):283–305, 2011. doi:10.1007/978-3-642-03351-3_23.

[43] Niko Haubold, Markus Lohrey, and Christian Mathissen. Compressed decision problems for graph products of groups and applications to (outer) automorphism groups. *International Journal of Algebra and Computation*, 22(8), 2013. doi:10.1142/S0218196712400073.

[44] Graham Higman, Bernhard H. Neumann, and Hanna Neumann. Embedding theorems for groups. *Journal of the London Mathematical Society. Second Series*, 24:247–254, 1949. doi:10.1112/jlms/s1-24.4.247.

[45] Derek Holt. Word-hyperbolic groups have real-time word problem. *International Journal of Algebra and Computation*, 10:221–228, 2000. doi:10.1142/S0218196700000078.

[46] Derek Holt, Markus Lohrey, and Saul Schleimer. Compressed decision problems in hyperbolic groups. In *Proceedings of the 36th International Symposium on Theoretical Aspects of Computer Science, STACS 2019*, volume 126 of *LIPIcs*, pages 37:1–37:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. doi:10.4230/LIPIcs.STACS.2019.37.

[47] Derek Holt and Sarah Rees. Regularity of quasigeodesics in a hyperbolic group. *International Journal of Algebra and Computation*, 13(05):585–596, 2003. doi:10.1142/S0218196703001560.

[48] John E. Hopcroft and Jeffrey D. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison–Wesley, Reading, MA, 1979. doi:10.1145/568438.568455.

[49] Gérard Huet. Confluent reductions: Abstract properties and applications to term rewriting systems. *Journal of the ACM*, 27(4):797–821, 1980. doi:10.1145/322217.322230.

[50] Dung T. Huynh. The complexity of equivalence problems for commutative grammars. *Information and Control*, 66(1-2):103–121, 1985. doi:10.1016/S0019-9958(85)80015-2.

[51] Mark Kambites, Pedro V. Silva, and Benjamin Steinberg. On the rational subset problem for groups. *Journal of Algebra*, 309(2):622–639, 2007. doi:10.1016/j.jalgebra.2006.05.020.

[52] Ilya Kapovich, Richard Weidmann, and Alexei Miasnikov. Foldings, graphs of groups and the membership problem. *International Journal of Algebra and Computation*, 15(1):95–128, 2005. doi:10.1142/S021819670500213X.

[53] Richard M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, New York, 1972. doi:10.7551/mitpress/12274.003.0038.

[54] Abraham Karrass and Donald Solitar. The subgroups of a free product of two groups with an amalgamated subgroup. *Transactions of the American Mathematical Society*, 150:227–255, 1970. doi:10.2307/1995492.

[55] Abraham Karrass and Donald Solitar. Subgroups of HNN groups and groups with one defining relation. *Canadian Journal of Mathematics*, 23:627–643, 1971. doi:10.4153/CJM-1971-070-x.

[56] Olga Kharlampovich and Alexei Miasnikov. Hyperbolic groups and free constructions. *Transactions of the American Mathematical Society*, 350(2):571–613, 1998. doi:10.1090/S0002-9947-98-01773-5.

[57] Olga Kharlampovich, Alexei Miasnikov, and Pascal Weil. Stallings graphs for quasi-convex subgroups. *Journal of Algebra*, 488:442–483, 2017. doi:10.1016/j.jalgebra.2017.05.037.

[58] Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. In *Algebra and Computer Science*, volume 677 of *Contemporary Mathematics*, pages 138–153. American Mathematical Society, 2016. doi:10.1090/conm/677/13625.

[59] Dietrich Kuske and Markus Lohrey. Logical aspects of Cayley-graphs: the monoid case. *International Journal of Algebra and Computation*, 16(2):307–340, 2006. doi:10.1142/S0218196706003001.

[60] Jörg Lehnert and Pascal Schweitzer. The co-word problem for the Higman-Thompson group is context-free. *Bulletin of the London Mathematical Society*, 39(2):235–241, 2007. doi:10.1112/blms/bdl043.

[61] Markus Lohrey. *The Compressed Word Problem for Groups*. SpringerBriefs in Mathematics. Springer, 2014. doi:10.1007/978-1-4939-0748-9.

[62] Markus Lohrey. Knapsack in hyperbolic groups. *Journal of Algebra*, 545:390–415, 2020. doi:10.1016/j.jalgebra.2019.04.008.

[63] Markus Lohrey and Géraud Sénizergues. Theories of HNN-extensions and amalgamated products. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP 2006*, volume 4052 of *Lecture Notes in Computer Science*, pages 681–692. Springer, 2006. doi:10.1007/11787006_43.

[64] Markus Lohrey and Géraud Sénizergues. Rational subsets in HNN-extensions and amalgamated products. *International Journal of Algebra and Computation*, 18(1):111–163, 2008. doi:10.1142/S021819670800438X.

[65] Markus Lohrey, Benjamin Steinberg, and Georg Zetzsche. Rational subsets and submonoids of wreath products. *Information and Computation*, 243:191–204, 2015. doi:10.1007/978-3-642-39212-2_33.

[66] Markus Lohrey, Florian Stober, and Armin Weiß. The power word problem in graph products. *Theory of Computing Systems*, pages 1–62, 2024. doi:10.1007/s00224-024-10173-z.

[67] Markus Lohrey and Georg Zetzsche. Knapsack in graph groups, HNN-extensions and amalgamated products. In *Proceedings of the 33rd International Symposium on Theoretical Aspects of Computer Science, STACS 2016*, volume 47 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 50:1–50:14, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.STACS.2016.50.

[68] Markus Lohrey and Georg Zetzsche. Knapsack in graph groups. *Theory of Computing Systems*, 62(1):192–246, 2018. doi:10.1007/s00224-017-9808-3.

[69] Roger Lyndon and Paul Schupp. *Combinatorial Group Theory*. Springer, 1977. doi:10.1007/978-3-642-61896-3.

[70] Saunders MacLane. *Homology*. Springer Science & Business Media, 2012. doi:10.1007/978-3-642-62029-4.

[71] Wilhelm Magnus. Das Identitätsproblem für Gruppen mit einer definierenden Relation. *Mathematische Annalen*, 106(1):295–307, 1932. doi:10.1007/BF01455888.

[72] Vasileios Metaftsis and Evagelos Raptis. Subgroup separability of graphs of abelian groups. *Proceedings of the American Mathematical Society*, 132(7):1873–1884, 2004. doi:10.1090/S0002-9939-03-07287-3.

[73] Alexei Miasnikov and Andrey Nikolaev. Verbal subgroups of hyperbolic groups have infinite width. *Journal of the London Mathematical Society*, 90(2):573–591, 2014. doi:10.1112/jlms/jdu034.

[74] Alexei Miasnikov, Andrey Nikolaev, and Alexander Ushakov. Knapsack problems in groups. *Mathematics of Computation*, 84:987–1016, 2015. doi:10.1090/S0025-5718-2014-02880-9.

[75] Alexei Miasnikov and Vladimir Remeslennikov. Exponential groups 2: Extensions of centralizers and tensor completion of CSA-groups. *International Journal of Algebra and Computation*, 6(6):687–711, 1996. doi:10.1142/S0218196796000398.

[76] Alexei Mishchenko and Alexander Treier. Knapsack problem for nilpotent groups. *Groups Complexity Cryptology*, 9(1):87–98, 2017. doi:10.1515/gcc-2017-0006.

[77] Walter D. Neumann and Michael Shapiro. Automatic structures and boundaries for graphs of groups. *International Journal of Algebra and Computation*, 4(04):591–616, 1994. doi:10.1142/S0218196794000178.

[78] Pjotr S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *American Mathematical Society, Translations, II. Series*, 9:1–122, 1958. doi:10.1090/trans2/009/01.

[79] Alexander Yu. Ol′shanskiĭ. Almost every group is hyperbolic. *International Journal of Algebra and Computation*, 2(1):1–17, 1992. doi:10.1142/S0218196792000025.

[80] Rohit J. Parikh. On context-free languages. *Journal of the ACM*, 13(4):570–581, 1966. doi:10.1145/321356.321364.

[81] Eliyahu Rips. Subgroups of small cancellation groups. *Bulletin of the London Mathematical Society*, 14:45–47, 1982. doi:10.1112/blms/14.1.45.

[82] Paul E. Schupp. Coxeter groups, 2-completion, perimeter reduction and subgroup separability. *Geometriae Dedicata*, 96:179–198, 2003. doi:10.1023/A:1022155823425.

[83] Jean-Pierre Serre. *Trees*. Springer, 2003. doi:10.1007/978-3-642-61856-7.

[84] David Simplot and Alain Terlutte. Closure under union and composition of iterated rational transductions. *RAIRO-Theoretical Informatics and Applications*, 34(3):183–212, 2000. doi:10.1051/ita:2000114.

[85] John Robert Stallings. *Group Theory and Three-Dimensional Manifolds*. Number 4 in Yale Mathematical Monographs. Yale University Press, 1971. URL: https://www.maths.ed.ac.uk/~v1ranick/papers/stallings1.pdf.

[86] John Robert Stallings. Adian groups and pregroups. In *Essays in group theory*, pages 321–342. Springer, 1987. doi:10.1007/978-1-4613-9586-7_5.

[87] Anthony Widjaja To. Unary finite automata vs. arithmetic progressions. *Information Processing Letters*, 109(17):1010–1014, 2009. doi:10.1016/j.ipl.2009.06.005.

[88] Joachim von zur Gathen and Malte Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society*, 72(1):155–158, 1978. doi:10.2307/2042554.

[89] Daniel T. Wise. Research announcement: the structure of groups with a quasiconvex hierarchy. *Electronic Research Announcements in Mathematical Sciences*, 16:44–55, 2009. doi:10.3934/era.2009.16.44.