Compression Techniques in Group Theory

Markus Lohrey

University of Siegen, Germany, {lohrey}@eti.uni-siegen.de

Abstract. This paper gives an informal overview over applications of compression techniques in algorithmic group theory.

1 Algorithmic problems in group theory

The study of computational problems in group theory goes back more than 100 years. In a seminal paper from 1911, Dehn posed three decision problems [15]: The *word problem*, the *conjugacy problem*, and the *isomorphism problem*. The word and conjugacy problem are defined for a finitely generated group G. This means that there exists a finite subset $\Sigma \subseteq G$ such that every element of G can be written as a finite product of elements from Σ. This allows to represent elements of G by finite words over the alphabet Σ. For the word problem, the input consists of such a finite word $w \in \Sigma^*$ and the goal is to check whether w represents the identity element of G. For the conjugacy problem, the input consists of two finite words $u, v \in \Sigma^*$ and the question is whether the group elements represented by u and v are conjugated. For the isomorphism problem the input consists of two finite group presentations (roughly speaking, two finite descriptions of groups in terms of generators and defining relations) and the question is whether these presentations describe isomorphic groups. Dehn's motivation for studying these abstract group theoretical problems came from topology. In his paper from 1912 [16], Dehn gave an algorithm that solves the word problem for fundamental groups of orientable closed 2-dimensional manifolds, but also realized that his three problems seem to be very hard in general. In [15], he wrote "*Die drei Fundamentalprobleme für alle Gruppen mit zwei Erzeugenden ... zu lösen, scheint einstweilen noch sehr schwierig zu sein.*" (*Solving the three fundamental problems for all groups with two generators seems to be very difficult at the moment.*) When Dehn wrote this sentence, a formal definition of computability was still missing. So, it is not surprising that it took more than 40 years until Novikov [56] and independently Boone [11] proved that the word problem and hence also the conjugacy problem are in general undecidable for finitely presented groups. The isomorphism problems was shown to be undecidable by Adjan [1].

In this paper we are mainly interested in the word problem. Despite the undecidability results from [11,56], for many groups the word problem is decidable. Dehn's result for fundamental groups of orientable closed 2-dimensional manifolds was extended to one-relator groups (finitely generated groups that can be defined by single defining relation) by his student Magnus [49]. Other important classes of groups with a decidable word problem are:

– automatic groups [21] (including important classes like braid groups [4], Coxeter groups, right-angled Artin groups, hyperbolic groups [24]),
– finitely generated linear groups, i.e., finitely generated groups that can be faithfully represented by matrices over a field [58] (including polycyclic groups and nilpotent groups), and
– finitely generated metabelian groups (they can be embedded in direct products of linear groups [65]).

With the rise of computational complexity theory in the 1960's, also the computational complexity of group theoretic problems moved into the focus of research. From the very beginning, this field attracted researchers from mathematics as well as computer science. One of the early results in this context was that for every given $n \geq 0$ there exist groups for which the word problem is decidable but does not belong to the n-th level of the Grzegorczyk hierarchy (a hierarchy of decidable problems) [13]. On the other hand, for many prominent classes of groups the complexity of the word problem is quite low. For instance, for automatic groups, the word problem can be solved in quadratic time [21], and for the subclass of hyperbolic groups the word problem can be solved in linear time (even real time) [31].

For finitely generated linear groups Lipton and Zalcstein [39] (for fields of characteristic zero) and Simon [62] (for prime characteristic) proved in 1977 (resp., 1979) that deterministic logarithmic space (L for short) suffices to solve the word problem. This was the first result putting the word problem for an important class of groups into a complexity class below polynomial time. The class L is located between the classes NC^1 and NC^2 (NC stands for Nick's class after Nicolas Pippenger). The circuit complexity class NC^k consists of all problems that can be solved by uniform polynomial size boolean circuits of bounded fan-in and depth $(\log n)^k$. The class $\mathsf{NC} = \bigcup_{k \geq 1} \mathsf{NC}^k$ is usually identified with the class of problems that have an efficient parallel algorithm. It is a subclass of Ptime and it is a famous open problem whether $\mathsf{NC} = \mathsf{Ptime}$. In his thesis [59] from 1993, Robinson investigated the parallel complexity of word problems in more detail. He proved that for several important classes of groups (nilpotent groups, polycyclic groups, solvable linear groups) the word problem belongs to (subclasses of) NC^1. For the free group of rank two, he proved that the word problem is hard for NC^1 (and since it is linear, the word problem belongs to L). Other groups with low complexity word problems are hyperbolic groups (NC^2 due to Cai [12], which was improved to $\mathsf{LOGCFL} \subseteq \mathsf{NC}^2$ in [40]), Thompson's group V (NC^2 due to Birget [10]), Baumslag-Solitar groups[1] (L due to Weiß [66]) and of course finite groups. A famous result of Barrington [7] says that for every finite non-solvable group the word problem is NC^1-complete. In recent years, also the class $\mathsf{TC}^0 \subseteq \mathsf{NC}^1$ came into the focus of group theorists. Roughly speaking, uniform TC^0 captures the complexity of multiplying two binary encoded integers. It turned out that for many interesting groups the word problem belongs to uniform TC^0. This includes finitely generated solvable linear groups [37] and all subgroups of groups that can be obtained from finitely generated solvable

[1] These are the one-relator groups $\mathsf{BS}(p,q) = \langle a, t \mid t^{-1}a^p t = a^q \rangle$.

linear groups using direct products and wreath products [53]. This includes for instance all metabelian groups and free solvable groups.

2 Compression with straight-line programs

In recent years, compression techniques have led to important breakthroughs concerning the complexity of word problems. The general strategy (which is not restricted to word problems) is to use data compression to avoid the storage of huge intermediate data structures. For solving the word problem in automorphism groups and certain group extensions (in particular, semi-direct products), so called *straight-line programs* turned out to be the right compressed representation. A straight-line program is a context-free grammar that produces only a single word. A typical example is the context-free grammar $S \to ABA$, $A \to CBC$, $B \to CcC$, $C \to DaD$, $D \to bb$. The nonterminal C produces the word $bbabb$, hence B produces $bbabb\,c\,bbabb$. Then, A produces $bbabb\,bbabbcbbabb\,bbabb$. Finally, the start nonterminal S produces

$$bbabbbbabbcbbabbbbabb\,bbabbcbbabb\,bbabbbbabbcbbabbbbabb$$

The length of the word produced by a straight-line program $\mathcal{G}$ can be exponential in the length of $\mathcal{G}$, where the latter is usually defined as the sum of the lengths of all right-hand sides of the grammar (14 in the above example). In other words, straight-line programs allow for exponential compression rates in the best case. Let us just mention that straight-line programs are a very active area in string algorithms and data compression, see for instance [14,42].

Here, we are interested in group theoretical applications of straight-line programs. One of the first such applications is the so-called reachability theorem of Babai and Szemerédi for finite groups [6]. It says that if G is a finite group of order n and $S \subseteq G$ is any generating set of G such that $S = S^{-1}$, then every element $g \in G$ can be defined by a straight-line program with terminal alphabet S and size $\mathcal{O}((\log n)^2)$. Babai and Szemerédi used this result for the solution of subgroup membership problems in finite black-box groups.

2.1 Compressed word problems

Here, we are mainly interested in finitely generated infinite groups. Straight-line programs entered this area with the so-called *compressed word problem*. The compressed word problem for a finitely generated group G is the variant of the word problem for G where the input word is represented by a straight-line program. The compressed word problem can be also explained in terms of circuits. Define a circuit over the group G as a directed acyclic graph, where the nodes of indegree 0 are labelled with group generators and all other nodes have exactly two incoming edges (they have to be ordered in the sense that there is a left and a right incoming edge). Moreover, there is a distinguished output node. Such a circuit computes an element of G in the natural way (every inner node computes the product of the two incoming group elements). Then, the compressed word problem for G is equivalent to the problem whether a given circuit over the group G evaluates to the group identity.

Schleimer [61] observed that the (standard) word problem for every finitely generated subgroup of the automorphism group of a group G is polynomial time reducible to the compressed word problem for G. Similar transfer results hold for semi-direct products and other group extensions. For instance, the word problem for a semi-direct product $K \rtimes Q$ is logspace reducible to (i) the word problem for Q and (ii) the compressed word problem for K [43]. These results make the compressed word problem interesting for the efficient solution of standard word problems. It has been shown before Schleimer's work that the compressed word problem for a free group can be solved in polynomial time (the problem is in fact Ptime-complete) [41]. As a consequence, the word problem for the automorphism group of a free group (which is finitely generated) can be solved in polynomial time [61]. This solved an open problem from [36]. Schleimer's result has drawn interest on the compressed word problem in the combinatorial group theory community. In general, the complexity of the compressed word problem is higher than the complexity of the standard word problem, since the input is given in a more succinct way (we will see concrete examples later). Nevertheless, there are, in addition to free groups, many groups with a polynomial time compressed word problem:

(i) finite groups. It is easy to see that the compressed word problem for a finite group can be solved in polynomial time. Less trivial is the fact that for every finite non-solvable group the compressed word problem is Ptime-complete [9].
(ii) hyperbolic groups [32] and, more generally, groups that are hyperbolic relative to a collection of free abelian subgroups [33]
(iii) fully residually free groups [48],
(iv) right-angled Artin groups [28,45], and, more generally, virtually special groups (finite extensions of subgroups of graph groups) [43]. By the work of Agol, Haglund and Wise [2,26,67], virtually special groups are tightly connected to low dimensional topology and contain many other important classes of groups (Coxeter groups, one-relator groups with torsion, fully residually free groups, and fundamental groups of hyperbolic 3-manifolds).

The polynomial time algorithms from (ii), (iii) and (iv) are all based on the following important result: for two straight-line programs one can check in polynomial time whether they produce the same word. This result has been shown independently in [30,52,57].

For finitely generated virtually nilpotent groups, the compressed word problem belongs to the parallel complexity class NC^2 [37]. Finitely generated virtually nilpotent groups are in fact the larges class of infinite groups, for which the compressed word problem is known to be in NC.

If we allow randomization, we find further examples of groups where the compressed word problem can be parallelized efficiently: for finitely generated free metabelian groups and wreath products of the form $\left(\prod_{i=1}^{k} A_i\right) \wr \mathbb{Z}^n$, where every A_i is either $\mathbb{Z}$ or a cyclic group of prime order, the compressed word problem belongs to the class coRNC^2 (the complement of the randomized version of NC^2) [38]. To show this result, the compressed word problem for $\left(\prod_{i=1}^{k} A_i\right) \wr \mathbb{Z}^n$ is reduced to a special case of *polynomial identity testing* (PIT for short). This is the question, whether a given algebraic circuit over a polynomial ring evaluates to the zero polynomial [60]. It is known that for polynomials over the rings $\mathbb{Z}$ and $\mathbb{Z}_n$, PIT belongs to coRP (the complement of randomized polynomial time) [3,34]. In [38] it was shown that a special case of PIT, where the input circuit is a so-called powerful skew circuit over a polynomial ring $\mathbb{Z}[x]$ or $\mathbb{F}_p[x]$ (p a prime), belongs to coRNC^2. The compressed word problem for $\left(\prod_{i=1}^{k} A_i\right) \wr \mathbb{Z}^n$ is logspace reducible to this special case of PIT.

Using a reduction to the general PIT problem, the compressed word problems for the following groups were shown to be in coRP:

– finitely generated linear groups (which contain the above mentioned virtually special groups), [45,43]
– wreath products of the form $G \wr H$, where G is finitely generated abelian and H is finitely generated virtually abelian [38].

PIT is a famous problem in complexity theory. Proving PIT $\in \mathsf{Ptime}$ would imply spectacular progress on circuit complexity lower bounds [35]. Therefore, complexity theorists believe that proving PIT $\in \mathsf{Ptime}$ will be extremely difficult. In [43] it was shown that PIT can be reduced in logspace to the compressed word problem for the linear group $\mathsf{SL}(3,\mathbb{Z})$ (all (3×3)-matrices over the integers with determinant 1), showing that the two problems are equivalent with respect to logspace reductions. Hence, proving that the compressed word problem for $\mathsf{SL}(3,\mathbb{Z})$ belongs to Ptime seems to be very difficult.

Besides specific classes of groups, also constructions that allow to build new groups from existing groups are important in group theory. For the following important group theoretical constructions the compressed word problem for the constructed group is polynomial time Turing-reducible to the compressed word problems for the constitutent groups: finite group extensions [45,43], HNN extensions with finite associated subgroups [27], amalgamated free products with finite amalgamated subgroups [27], graph products [28].

Another important construction in group theory is the wreath product. We have already seen some positive results for wreath products of abelian groups (at least if we allow randomization). It turns out that the wreath product does not preserve the complexity of the compressed word problem in general. Based on a characterization of the class PSPACE in terms of so-called leaf languages [29], it was shown in [8] that for many groups G the compressed word problem for the wreath product $G \wr \mathbb{Z}$ is PSPACE-complete. Concrete examples of such groups G are finite non-solvable groups and free groups of rank at least two.[2]

[2] In fact, PSPACE-hardness of the compressed word problem for $G \wr \mathbb{Z}$ holds for a quite large class of non-solvable groups, namely all so-called uniformly SENS groups G [8], whereas for every non-abelian group G, the compressed word problem for $G \wr \mathbb{Z}$ is already coNP-hard [43].

Since the compressed word problem for these groups as well as for $\mathbb{Z}$ belongs to L, one obtains two important consequences: (i) wreath products may strictly increase the complexity of the compressed word problem (L is a proper subclass of PSPACE) and (ii) there exist groups for which the compressed word problems is strictly more difficult than the standard word problem (for this one needs the fact that the word problem for a wreath product $G \wr H$ is logspace reducible to the word problems for G and H [63]).

Using the same technique as for wreath products, it was also shown in [8] that the compressed word problem is PSPACE-complete for the Grigorchuk group and Thompson's group F. These groups are famous for their quite unusual properties. Let us just mention that the Grigorchuk group was the first example of a group of intermediate growth. The Grigorchuk group belongs to the rich class of automaton groups (which should not be confused with the class of automatic groups). Recently, examples of automaton groups with an $\mathsf{EXPSPACE}$-complete compressed word problem (and PSPACE-complete word problem) were constructed in [64].

2.2 Power words

In some group theoretical applications, the straight-line programs that appear have a very restricted form: a *power word* has the form $w_1^{n_1} w_2^{n_2} \cdots w_k^{n_k}$, where the exponents $n_1, \dots, n_k$ are integers that are given in binary encoding and the words $w_1, \dots, w_k$ are given explicitly (uncompressed). Using the iterated squaring trick, one can translate a power word into an equivalent straight-line program in logspace. Power words were used in order to solve algorithmic problems for (2×2)-matrix groups. Consider the group $\mathsf{GL}(2, \mathbb{Z})$ of all (2×2)-matrices over the integers with determinant ± 1. The natural representation of elements in this group consists of 4-tuples of binary encoded integers. In [44] it was shown that for this input representation the subgroup membership problem (does a given element of $\mathsf{GL}(2, \mathbb{Z})$ belong to a given finitely generated subgroup of $\mathsf{GL}(2, \mathbb{Z})$?) can be solved in polynomial time. An analogous result was shown in [25] for the modular group $\mathsf{PSL}(2, \mathbb{Z})$. Let us briefly sketch the proof for $\mathsf{GL}(2, \mathbb{Z})$. It is a well-known fact that $\mathsf{GL}(2, \mathbb{Z})$ is virtually-free, i.e., it has a free subgroup of finite index. The connection to power words is made by the observation that a matrix $A \in \mathsf{GL}(2, \mathbb{Z})$ can be translated into a power word $w_1^{n_1} w_2^{n_2} \cdots w_k^{n_k}$ over a fixed (but arbitrarily chosen) finite generating set of $\mathsf{GL}(2, \mathbb{Z})$. Thus, evaluating $w_1^{n_1} w_2^{n_2} \cdots w_k^{n_k}$ in the group $\mathsf{GL}(2, \mathbb{Z})$ yields the matrix A. Therefore, it suffices to show that for every virtually-free group G, the so called power subgroup membership problem for G belongs to Ptime. The power subgroup membership problem for G is the subgroup membership problem for G, where all input elements of G are represented by power words. One can easily get rid off the finite extension, which leaves the power subgroup membership problem for a free group. This problem is finally solved in polynomial using an adaptation of Stallings folding procedure. The ordinary subgroup membership problem for a free group, where all group elements are given by finite words, is known to the Ptime-complete [5].

The proof for $\mathsf{PSL}(2,\mathbb{Z})$ [25] follows the same strategy as for $\mathsf{GL}(2,\mathbb{Z})$. Due to the simpler algebraic structure of $\mathsf{PSL}(2,\mathbb{Z})$ (it is isomorphic to the free product $\mathbb{Z}_2 * \mathbb{Z}_3$), it suffices to solve the power subgroup membership problem for a finitely generated free group, where the input power words have the form $a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k}$ for free generators $a_1, \ldots, a_k$, in polynomial time.

Power words have been also studied in the context of the word problem. The power word problem for a finitely generated group G is the word problem for G, where the input word is given as a power word. In [46] it was shown that the power word problem for a finitely generated free group F_k is logspace reducible to the standard word problem for F_k. Since F_k is a finitely generated linear group, the result of Lipton and Zalcstein [39] implies that the word problem, and hence also the power word problem, for every finitely generated free group can be solved in logspace.

For the following groups, the power word problem even belongs to TC^0:

- wreath products of the form $G \wr \mathbb{Z}$ with G finitely generated nilpotent [22],
- right iterated wreath products of the form $\mathbb{Z}^{n_1} \wr (\mathbb{Z}^{n_2} \wr (\mathbb{Z}^{n_3} \wr \cdots \wr \mathbb{Z}^{n_k}))$ and, as a consequence of the Magnus embedding [50], free solvable groups [22],
- solvable Baumslag-Solitar groups $\mathsf{BS}(1,q)$ [47].

Interestingly, it was shown in [46] that the power word problems for Thompson's group F and all wreath products $G \wr \mathbb{Z}$ with G free of rank at least two or finite non-solvable are coNP-complete.[3] Recall that the compressed word problems for these groups are PSPACE-complete [8]. For the Grigorchuk group the power word problem belongs to L [46], whereas the compressed word problem is again PSPACE-complete [8]. This yields an example of a group, where the compressed word problem is strictly more difficult than the power word problem.

In the commutative setting, power words can be traced back to work from the 1990's. Ge [23] showed that one can verify in polynomial time an identity $\alpha_1^{n_1} \alpha_2^{n_2} \cdots \alpha_n^{n_n} = 1$, where the α_i are elements of an algebraic number field and the n_i are binary encoded integers.

3 Compression beyond straight-line programs

Recall that straight-line programs were applied to word problems for automorphism groups (and certain group extensions) and yield in some cases polynomial time algorithms. This is achieved by representing long words that appear as intermediate results in computations succinctly by straight-line programs. In the best case, a straight-line program allows to represent a word of length n in space $\log n$. For some word problems, this exponential compression is not enough. This holds in particular for groups with extremely fast growing Dehn functions like the Baumslag group or Higman's group. The Dehn functions for these groups have recursive but non-elementary growth. If one tries to solve the word problem naively, one obtains intermediate words of non-elementary length. Therefore, it

[3] coNP-hardness holds for every uniformly SENS group G.

was conjectured that these groups may have very hard word problems. But this turned out to be wrong. For both the Baumslag group [54] as well as Higman's group [17], the word problem can be solved in polynomial time. To prove these results, *power circuits* were introduced in [55]. Power circuits allow to represent huge integers, which arise as exponent towers, succinctly. Moreover, comparison and the arithmetic operations $x+y$ and $x \cdot 2^y$ on numbers that are represented by power circuits can be carried out in polynomial time. Recently, the power circuit technique has been further developed in [51], where it was shown that the word problem for the Baumslag group belongs to NC. Further work on power circuits in the context of group theory can be found in [18].

An even more extreme integer compression is used in [19]. Using the so-called hydra groups, a family of groups G_k ($k \geq 1$) was constructed in [20] such that the Dehn functions of the groups G_k are arbitrarily high in the Ackermann hierarchy. Nevertheless, the word problem for every group G_k can be solved in polynomial time [19].

4 Open problems

Let us conclude with some open problems related to compression in algorithmic group theory:

Linear groups. Recall that the compressed word problem for a finitely generated linear group belongs to coRP. Showing that the compressed word problem for finitely generated linear groups belongs to Ptime seems to be very difficult (it would imply that polynomial identity testing belongs to Ptime). But what about restricted classes of linear groups? Braid groups and solvable linear groups might be good candidates to look at. Within the class of solvable linear groups one might first investigate polycyclic groups or solvable Baumslag-Solitar groups $\mathsf{BS}(1,q)$. Also the power word problem for linear groups might be interesting to look at. The author is not aware of any better upper bound than coRP (the same upper bound as for the compressed word problem for linear groups). Recall that for the solvable and linear Baumslag-Solitar groups $\mathsf{BS}(1,q)$ the power word problem belongs to TC^0 [47]. Is it possible to extend this result to all solvable linear groups?

Baumslag-Solitar groups. Weiß [66] showed that the word problem for every Baumslag-Solitar group $\mathsf{BS}(p,q)$ can be solved in logspace by reducing it in logspace to the word problem for a free group. The same reduction does not work in logspace for the compressed word problem. Currently, the best upper bound for the compressed word problem of a non-solvable Baumslag-Solitar group is PSPACE.

Right iterated wreath products of free abelian groups. Recall that for right iterated wreath products of free abelian groups the power word problem belongs to TC^0 [22]. This gives hope that the compressed word problem for these groups should be not too difficult. Since the word problem belongs to TC^0, a standard argument shows that the compressed word problem for every right iterated wreath product of free abelian groups lies in the counting hierarchy. This makes PSPACE-hardness quite unlikely. The compressed word problem for a wreath product of two free abelian groups belongs to coRP [38]. It would be interesting to see whether this result can be extended to all right iterated wreath products of free abelian groups.

Subgroup membership problems. In [44] it is shown that the subgroup membership problem for a free group can be solved in polynomial time, when all group element are specified by power words. Is it possible to extend this result to the case where all group element are specified by straight-line programs. Straight-line programs are strictly more succinct than power words. On could try to come up with an extension of Stallings' folding procedure to the case where edges are labelled with straight-line programs (the same strategy with power words instead of straight-line programs was successful in [44]).

References

1. Sergei I. Adjan. The unsolvability of certain algorithmic problems in the theory of groups. *Trudy Moskov. Mat. Obsc.*, 6:231–298, 1957. in Russian.
2. Ian Agol. The virtual Haken conjecture. *Documenta Mathematica*, 18:1045–1087, 2013. With an appendix by Ian Agol, Daniel Groves, and Jason Manning.
3. Manindra Agrawal and Somenath Biswas. Primality and identity testing via chinese remaindering. *Journal of the Association for Computing Machinery*, 50(4):429–443, 2003.
4. Emil Artin. Theorie der Zöpfe. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 4(1):47–72, 1925.
5. Jürgen Avenhaus and Klaus Madlener. The Nielsen reduction and P-complete problems in free groups. *Theoretical Computer Science*, 32(1-2):61–76, 1984.
6. László Babai and Endre Szemerédi. On the complexity of matrix group problems I. In *Proceedings of the 25th Annual Symposium on Foundations of Computer Science, FOCS 1984*, pages 229–240, 1984.
7. 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.
8. Laurent Bartholdi, Michael Figelius, Markus Lohrey, and Armin Weiß. Groups with ALOGTIME-hard word problems and PSPACE-complete circuit value problems. In *Proceedings of the 35th Computational Complexity Conference, CCC 2020*, volume 169 of *LIPIcs*, pages 29:1–29:29. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.
9. Martin Beaudry, Pierre McKenzie, Pierre Péladeau, and Denis Thérien. Finite monoids: From word to circuit evaluation. *SIAM Journal on Computation*, 26(1):138–152, 1997.
10. Jean-Camille Birget. The groups of Richard Thompson and complexity. *International Journal of Algebra and Computation*, 14(5-6):569–626, 2004.
11. William W. Boone. The word problem. *Annals of Mathematics. Second Series*, 70:207–265, 1959.

12. Jin-Yi Cai. Parallel computation over hyperbolic groups. In *Proceedings of the 24th Annual Symposium on Theory of Computing, STOC 1992*, pages 106–115. ACM Press, 1992.
13. Frank B. Cannonito. Hierarchies of computable groups and the word problem. *Journal of Symbolic Logic*, 31:376–392, 1966.
14. Moses Charikar, Eric Lehman, Ding Liu, Rina Panigrahy, Manoj Prabhakaran, Amit Sahai, and Abhi Shelat. The smallest grammar problem. *IEEE Transactions on Information Theory*, 51(7):2554–2576, 2005.
15. Max Dehn. Über unendliche diskontinuierliche Gruppen. *Mathematische Annalen*, 71:116–144, 1911. In German.
16. Max Dehn. Transformation der Kurven auf zweiseitigen Flächen. *Mathematische Annalen*, 72:413–421, 1912. In German.
17. Volker Diekert, Jürn Laun, and Alexander Ushakov. Efficient algorithms for highly compressed data: the word problem in Higman's group is in P. *International Journal of Algebra and Computation*, 22(8), 2012.
18. Volker Diekert, Alexei Myasnikov, and Armin Weiß. Conjugacy in Baumslag's group, generic case complexity, and division in power circuits. *Algorithmica*, 76(4):961–988, 2016.
19. Will Dison, Eduard Einstein, and Timothy R. Riley. Taming the hydra: The word problem and extreme integer compression. *International Journal of Algebra and Computation*, 28(7):1299–1381, 2018.
20. Will Dison and Timothey R. Riley. Hydra groups. *Commentarii Mathematici Helvetici*, 88(3):507–540, 2013.
21. David B. A. Epstein, James W. Cannon, Derek F. Holt, Silvio V. F. Levy, Michael S. Paterson, and William P. Thurston. *Word Processing in Groups*. Jones and Bartlett, Boston, 1992.
22. 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.
23. Guoqiang Ge. Testing equalities of multiplicative representations in polynomial time (extended abstract). In *Proceedings of the 34th Annual Symposium on Foundations of Computer Science, FOCS 1993*, pages 422–426, 1993.
24. Mikhail Gromov. Hyperbolic groups. In S. M. Gersten, editor, *Essays in Group Theory*, number 8 in MSRI Publ., pages 75–263. Springer, 1987.
25. Yuri Gurevich and Paul E. Schupp. Membership problem for the modular group. *SIAM Journal on Computing*, 37(2):425–459, 2007.
26. Frédéric Haglund and Daniel T. Wise. Coxeter groups are virtually special. *Advances in Mathematics*, 224(5):1890–1903, 2010.
27. Nico Haubold and Markus Lohrey. Compressed word problems in HNN-extensions and amalgamated products. *Theory of Computing Systems*, 49(2):283–305, 2011.
28. Nico 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.
29. Ulrich Hertrampf, Clemens Lautemann, Thomas Schwentick, Heribert Vollmer, and Klaus W. Wagner. On the power of polynomial time bit-reductions. In *Proceedings of the 8th Annual Structure in Complexity Theory Conference*, pages 200–207. IEEE Computer Society Press, 1993.

30. Yoram Hirshfeld, Mark Jerrum, and Faron Moller. A polynomial algorithm for deciding bisimilarity of normed context-free processes. *Theoretical Computer Science*, 158(1&2):143–159, 1996.
31. Derek Holt. Word-hyperbolic groups have real-time word problem. *International Journal of Algebra and Computation*, 10:221–228, 2000.
32. 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.
33. Derek Holt and Sarah Rees. The compressed word problem in relatively hyperbolic groups. Technical report, arXiv.org, 2020. https://arxiv.org/abs/2005.13917.
34. Oscar H. Ibarra and Shlomo Moran. Probabilistic algorithms for deciding equivalence of straight-line programs. *Journal of the Association for Computing Machinery*, 30(1):217–228, 1983.
35. Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.
36. Ilya Kapovich, Alexei Myasnikov, Paul Schupp, and Vladimir Shpilrain. Generic-case complexity, decision problems in group theory, and random walks. *Journal of Algebra*, 264(2):665–694, 2003.
37. Daniel König and Markus Lohrey. Evaluation of circuits over nilpotent and polycyclic groups. *Algorithmica*, 80(5):1459–1492, 2018.
38. Daniel König and Markus Lohrey. Parallel identity testing for skew circuits with big powers and applications. *International Journal of Algebra and Computation*, 28(6):979–1004, 2018.
39. Richard J. Lipton and Yechezkel Zalcstein. Word problems solvable in logspace. *Journal of the Association for Computing Machinery*, 24(3):522–526, 1977.
40. Markus Lohrey. Decidability and complexity in automatic monoids. *International Journal of Foundations of Computer Science*, 16(4):707–722, 2005.
41. Markus Lohrey. Word problems and membership problems on compressed words. *SIAM Journal on Computing*, 35(5):1210 – 1240, 2006.
42. Markus Lohrey. Algorithmics on SLP-compressed strings: A survey. *Groups Complexity Cryptology*, 4(2):241–299, 2012.
43. Markus Lohrey. *The Compressed Word Problem for Groups.* SpringerBriefs in Mathematics. Springer, 2014.
44. Markus Lohrey. Subgroup membership in GL(2,Z). In *Proceedings of the 38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021*, volume 187 of *LIPIcs*, pages 51:1–51:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
45. Markus Lohrey and Saul Schleimer. Efficient computation in groups via compression. In *Proceedings of Computer Science in Russia, CSR 2007*, volume 4649 of *Lecture Notes in Computer Science*, pages 249–258. Springer, 2007.
46. Markus Lohrey and Armin Weiß. The power word problem. In *Proceedings of the 44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019*, volume 138 of *LIPIcs*, pages 43:1–43:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.
47. Markus Lohrey and Georg Zetzsche. Knapsack and the power word problem in solvable baumslag-solitar groups. In *Proceedings of the 45th International Symposium on Mathematical Foundations of Computer Science, MFCS 2020*, volume 170 of *LIPIcs*, pages 67:1–67:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.

48. Jeremy Macdonald. Compressed words and automorphisms in fully residually free groups. *International Journal of Algebra and Computation*, 20(3):343–355, 2010.
49. Wilhelm Magnus. Das Identitätsproblem für Gruppen mit einer definierenden Relation. *Mathematische Annalen*, 106(1):295–307, 1932.
50. Wilhelm Magnus. On a theorem of Marshall Hall. *Annals of Mathematics. Second Series*, 40:764–768, 1939.
51. Caroline Mattes and Armin Weiß. Parallel algorithms for power circuits and the word problem of the Baumslag group. *CoRR*, abs/2102.09921, 2021.
52. Kurt Mehlhorn, R. Sundar, and Christian Uhrig. Maintaining dynamic sequences under equality-tests in polylogarithmic time. In *Proceedings of the 5th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 1994*, pages 213–222. ACM/SIAM, 1994.
53. Alexei Miasnikov, Svetla Vassileva, and Armin Weiß. The conjugacy problem in free solvable groups and wreath products of abelian groups is in TC^0. *Theory of Computing Systems*, 63(4):809–832, 2019.
54. Alexei Myasnikov, Alexander Ushakov, and Dong Wook Won. The word problem in the Baumslag group with a non-elementary Dehn function is polynomial time decidable. *Journal of Algebra*, 345(1):324–342, 2011.
55. Alexei G. Myasnikov, Alexander Ushakov, and Dong Wook Won. Power circuits, exponential algebra, and time complexity. *International Journal of Algebra and Computation*, 22(6), 2012.
56. Pjotr S. Novikov. On the algorithmic unsolvability of the word problem in group theory. *American Mathematical Society, Translations, II. Series*, 9:1–122, 1958.
57. Wojciech Plandowski. Testing equivalence of morphisms on context-free languages. In *Proceedings of the 2nd Annual European Symposium on Algorithms, ESA 1994*, volume 855 of *Lecture Notes in Computer Science*, pages 460–470. Springer, 1994.
58. Michael O. Rabin. Computable algebra, general theory and theory of computable fields. *Transactions of the American Mathematical Society*, 95:341–360, 1960.
59. David Robinson. *Parallel Algorithms for Group Word Problems.* PhD thesis, University of California, San Diego, 1993.
60. Nitin Saxena. Progress on polynomial identity testing - II. *Electronic Colloquium on Computational Complexity (ECCC)*, 20:186, 2013.
61. Saul Schleimer. Polynomial-time word problems. *Commentarii Mathematici Helvetici*, 83(4):741–765, 2008.
62. Hans-Ulrich Simon. Word problems for groups and contextfree recognition. In *Proceedings of Fundamentals of Computation Theory, FCT 1979*, pages 417–422. Akademie-Verlag, 1979.
63. Stephan Waack. The parallel complexity of some constructions in combinatorial group theory. *Journal of Information Processing and Cybernetics, EIK*, 26:265–281, 1990.
64. Jan Philipp Wächter and Armin Weiß. An automaton group with PSPACE-complete word problem. In *Proceedings of the 37th International Symposium on Theoretical Aspects of Computer Science, STACS 2020*, volume 154 of *LIPIcs*, pages 6:1–6:17. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020.
65. Bertram A. F. Wehrfritz. On finitely generated soluble linear groups. *Mathematische Zeitschrift*, 170:155–167, 1980.
66. Armin Weiß. A logspace solution to the word and conjugacy problem of generalized Baumslag-Solitar groups. In *Algebra and Computer Science*, volume 677 of *Contemporary Mathematics.* American Mathematical Society, 2016.
67. Daniel T. Wise. *The structure of groups with a quasiconvex hierarchy.* Princeton University Press, 2021.