Report from Dagstuhl Seminar 19131

Algorithmic Problems in Group Theory

Edited by

Volker Diekert[1], Olga Kharlampovich[2], Markus Lohrey[3], and Alexei Myasnikov[4]

1 **Universität Stuttgart, DE,** diekert@fmi.uni-stuttgart.de
2 **The City University of New York, US,** okharlampovich@gmail.com
3 **Universität Siegen, DE,** lohrey@eti.uni-siegen.de
4 **Stevens Institute of Technology – Hoboken, US,** amiasnikov@gmail.com

Abstract

Since its early days, combinatorial group theory was deeply interwoven with computability theory. In the last 20 years we have seen many new successful interactions between group theory and computer science. On one hand, groups played an important rule in many developments in complexity theory and automata theory. On the other hand, concepts from these computer science fields as well as efficient algorithms, cryptography, and data compression led to the formulation of new questions in group theory. The Dagstuhl Seminar *Algorithmic Problems in Group Theory* was aimed at bringing together researchers from group theory and computer science so that they can share their expertise. This report documents the material presented during the course of the seminar.

Seminar March 24–29, 2019 – http://www.dagstuhl.de/19131
2012 ACM Subject Classification Theory of computation → Problems, reductions and completeness, Theory of computation → Algebraic complexity theory, Theory of computation → Formal languages and automata theory
Keywords and phrases algorithmic group theory; generic-case complexity; circuit complexity; diophantine theories
Digital Object Identifier 10.4230/DagRep.9.3.83
Edited in cooperation with Georg Zetzsche

1 Executive summary

Volker Diekert
Olga Kharlampovich
Markus Lohrey
Alexei Myasnikov

The field of combinatorial group theory, a part of abstract algebra, is tightly linked to computational problems from its early days. Already in 1911, i.e., 25 years before Turing's work on the halting problem appeared, Max Dehn introduced and investigated three fundamental group theoretical decision problems: the *word problem*, the *conjugacy problem*, and the *isomorphism problem*. Dehn's problems had a strong influence on the development of modern theoretical computer science. It took more that 40 years before the work of Novikov, Boone, Adjan, and Rabin showed the undecidability of Dehn's decision problems in the class of finitely presented groups. Despite these negative results, for many groups the word

problem turned out to be decidable in many important classes of groups. With the rise of 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. Using algorithmic techniques from complexity theory, researchers were able to exhibit highly efficient algorithms for groups, where initially only pure decidability results have been known. A milestone in this context is Lipton and Zalcstein's logspace algorithm for the word problem of finitely generated linear groups. This was the first result putting the word problem for an important class of groups into a complexity class below polynomial time. In the last 10 years, researchers pushed the limits further towards small circuit complexity classes. In particular the class $\mathbf{TC}^0$ turned out be very important in this context. Despite its limited computational power many important group theoretical problems problems were shown to be in $\mathbf{TC}^0$.

Complexity theoretical questions are not the only area where we have seen fruitful interactions between group theory and theoretical computer science in recent years. Other examples can be found in automata theory, data compression, model theory, and reachability problems for infinite state systems. The following paragraphs put some of the seminar talks into the context of these topics and mentions some of the open problems that were discussed during the seminar.

Groups and circuit complexity

Howard Straubing gave an excellent survey on circuit complexity that was particularly addressed to non-experts in complexity theory. Barrington's famous result according to which the word problem for every finite non-solvable groups is hard for $\mathbf{NC}^1$ was explained and several important results centered around the circuit complexity class $\mathbf{TC}^0$ were surveyed. In recent years, $\mathbf{TC}^0$ turned out to be the right class for characterizing the complexity of several group theoretical problems. Two seminar talks presented further examples of group theory problems in $\mathbf{TC}^0$: Armin Weiß gave a talk about the power word problem which is a succinct version of the classical word problem, where powers g^n of group elements with binary encoded integer exponents n are allowed in the input. Despite this succinctness, several power word problems (e.g. for nilpotent groups and certain wreath products of finitely generated abelian groups) can be still solved in $\mathbf{TC}^0$. Moses Ganardi talked on the knapsack problem for finitely generated groups which asks for the solvability of certain exponent equations over a group. Among other results he gave a simple proof showing that the knapsack problem for unary encoded integers is in $\mathbf{TC}^0$. This result generalizes to all finitely generated abelian groups.

Several promising open problems related to the circuit complexity of group theoretical problems were discussed in the open problem sessions: The above mentioned result of Barrington on finite non-solvable groups motivates the question whether the word problem for every finitely generated solvable group is $\mathbf{NC}^1$-hard. Also finding new classes of infinite groups with a word problem in $\mathbf{TC}^0$ is an open research problem that was intensively discussed during the seminar. So far, it is known that solvable linear groups have a word problem in $\mathbf{TC}^0$ and that the class of groups with a word problem in $\mathbf{TC}^0$ is closed under wreath products.

Compression techniques in group theory

Compression techniques turned out to be an important tool for obtaining efficient algorithms in group theory. The general philosophy is trying to avoid storing extremely long words by

computing on a compressed representation of these words. This led to the formulation of several succinct versions of classical group theoretical problems, where the group elements in the input are given a succinct version. The power word problem that was introduced by Armin Weiß (see the previous paragraph) is such a succinct problem. The main result of Armin Weiß' talk was an efficient reduction of the power word problem for a free group to the (ordinary) word problem of a free group. It is open whether similar reductions also exist for right-angeled Artin groups and hyperbolic groups.

In the context of solving equations over groups and monoids, the so-called recompression technique led to several important results in recent years. Arthur Jeż (the inventor of this technique) gave a talk on recompression and outlined his non-deterministic linear time algorithm for solvability of word equations. Ciobanu and Elder presented their recent work on equations in hyperbolic groups where they use recompression in order to show that the set of all solutions for a system of equations over a hyperbolic group is an EDT0L language.

Groups and model theory

This research area directly relates to the previous paragraph. The goal is to understand the first-order theory of groups. Of particular interest is the Diophantine theory. Decidability of the Diophantine theory means that one can decide whether a boolean combination of word equations has a solution. Olga Kharlampovich gave a talk about Diophantine theories of metabelian groups. She proved decidability for several important metabelian groups: Baumslag-Solitar groups $\mathrm{BS}(1, n)$ and wreath products $\mathbb{Z} \wr \mathbb{Z}$ and $\mathbb{Z}_n \wr \mathbb{Z}$. Albert Garreta continued this topic and talked about Diophantine theories of solvable groups. He presented a large class of solvable groups (containing for instance all finitely generated non-virtually abelian nilpotent groups and all polycyclic groups that are not virtually metabelian) for which the Diophantine theory is at least as hard as the Diophantine theory of a suitable ring of algebraic integers. This leads to the conjecture that for each member of his family the Diophantine theory is undecidable.

Montserrat Casals-Ruiz talked on the positive theory of groups acting on trees. The positive theory of a group contains all negation-free statements from the full first-order theory. Montserrat Casals-Ruiz proved that many natural examples of groups acting on trees have the same positive theory as a free group of rank two. Ilya Kazachkov presented new results on the full first-order theory of free products and, more generally, graph products of groups. He showed that under certain conditions, elementary equivalent free products (meaning that their first-order theories coincide) must have elementary equivalent factors.

Groups and automata

Besides complexity of algorithmic problems, a very interesting connection between group theory and theoretical computer science is provided by automata theory, using the very flexible and algorithmically efficient finite state automata to somehow describe an infinite group. This led to the development of automatic groups and automaton groups. Automaton groups are a subclass of so-called self-similar groups. Laurent Bartholdi gave a talk on algorithmic results on self-similar groups and outlined the proof of a recent breakthrough result of Bartholdi and Mitrofanov stating that there exist self-similar groups with an undecidable word problem. For the particular case of automaton groups the word problem belongs to **PSPACE**. The question whether there exist automaton groups with a **PSPACE**-complete word problem was intensively discussed during the seminar. Recently, as a direct outcome of the seminar, an automaton group with this property was constructed by Jan Philipp

Wächter and Armin Weiß [An automaton group with PSPACE-complete word problem, arXiv, 2019. https://arxiv.org/abs/1906.03424]. Volodia Nekrashevych presented in his talk a generalization of automaton groups based on non-deterministic synchronous automata-transducers and discussed their algorithmic properties and relationship to dynamical systems.

Reachability problems

The study of reachability problems for matrix semigroups has a long tradition in theoretical computer science. Formulated in terms of algebra, the reachability problem is equivalent to the subsemigroup membership problem. Several variants and generalization (rational subset membership problem, knapsack problem) have been recently investigated as well. Igor Potapov gave a survey talk on recent progress on the matrix reachability problem from a computer science perspective. Georg Zetzsche presented several new decidability results for the rational subset membership problem in wreath products. Moses Ganardi talked on wreath products as well, but put the focus on the knapsack problem.

The above talks and the open problem session identified several interersting open problems related to reachability problems. An outstanding open problem in this context asks whether the submonoid membership problem for the group $\mathrm{GL}_3(\mathbb{Z})$ is decidable. Recently it was shown that the submonoid membership problem for the Heisenberg group (a subgroup of $\mathrm{GL}_3(\mathbb{Z})$) is decidable, This result suggests two generalizations: (i) the rational subset membership problem for Heisenberg groups and (ii) the submonoid membership problem for groups of unitriangular integer matrices. In both case it is open whether the problem is decidable. Georg Zetzsche mentioned in his talk the submonoid membership problem and the rational subset membership problem in the Baumslag-Solitar group $\mathrm{BS}(1,2)$ as open research problems.

Concluding remarks and future plans

The seminar was well received as witnessed by the high rate of accepted invitations. There was a good balance between participants from computer science and pure mathematics, and this mixture led to many active discussions and the discovery of new connections and promising open problems. The organizers regard this seminar as a great success. With steadily increasing interactions between such researchers, we foresee another seminar focusing on the interplay between computer science and group theory. Finally, the organizers wish to express their gratitude to the Scientific Directors of the Dagstuhl Centre for their support of the seminar.

2 Table of Contents

3 Overview of talks

3.1 Decision problems in self-similar and automata groups

Laurent Bartholdi (Institute of Advanced Studies, ENS Lyon, FR & Universität Göttingen, DE)

Joint work of Laurent Bartholdi, Ivan Mitrofanov

A self-similar group is a group acting on a regular rooted tree, in such a way that the action on subtrees are given recursively by a permutation and by elements of the group itself. Thus such a group is "presented" by a table giving, for each generator, its permutation of the top branches and, for each branch, a word in the generators giving recursively the action on it.

We show that very little can be deduced from such a "self-similar presentation": in particular, the word problem is not decidable.

The proof uses a reduction to Minsky machines.

3.2 On the positive theory of groups acting on trees

Montserrat Casals-Ruiz (University of the Basque Country, ES & Ikerbasque – Bilbao, ES)

Joint work of Montserrat Casals-Ruiz, Albert Garreta, Ilya Kazachkov, Javier de la Nuez

Many classical problems in group theory revolve around laws, verbal subgroups and their width. Results run from the generalisation of the classical Ore's Conjecture, proven by Liebeck, O'Brien, Shalev and Tiep, stating that every verbal subgroup has uniformly bounded width in the class of finite simple groups to the Bestvina-Bromberg-Fujiwara result showing that all verbal subgroups of an acylindrically hyperbolic group have infinite width.

In this talk, we will address these questions in a more general setting from the model-theoretic perspective. More precisely, we will discuss the positive theory of groups acting on trees. As a corollary, we will deduce that many interesting classes of groups have trivial positive theory, namely all acylindrically hyperbolic groups acting on trees and most one-relator groups including non-solvable Baumslag-Solitar groups. We also provide the first examples of finitely generated simple groups with trivial positive theory and so in particular, with all verbal subgroups of infinite width.

3.3 One relator quotients of partially commutative groups.

Andrew Duncan (Newcastle University, GB)

Joint work of Andrew Duncan, Arye Juhasz

A generalisation of Magnus's Freiheitssatz to one relator quotients of partially commutative (right angled Artin) groups is stated. The theorem holds for arbitrary pc groups, as long as certain conditions on the relator hold. In particular the relator must be at least a 3rd power;

but this is not sufficient. Sufficient conditions are detailed. (Some improvements in the proof were obtained as a result of discussions at the workshop).

For certain graphs (cycle graphs with an added 3-cycle) it can been seen that almost all cyclically reduced words in the corresponding pc group satisfy the conditions stated in our theorem. This depends on the fact that such groups have very well behaved normal forms for elements. This allows us to compute asymptotic densities, of subsets of the group, and show the theorem nearly always holds.

3.4 Conjugacy problems in $\mathrm{GL}(n, \mathbb{Z})$

Bettina Eick (TU Braunschweig, DE)

Joint work of Bettina Eick, Tommy Hofmann, Eamonn O'Brien
Main reference Bettina Eick, Tommy Hofmann, Eamonn O'Brien: "The conjugacy problem in GL(n,Z)". To appear in J. London Math. Soc., 2019.

Let T, T' be two invertible rational matrices. The *rational conjugacy problem* asks to decide if there exists $g \in \mathrm{GL}(n, \mathbb{Q})$ satisfying $g^{-1}Tg = T'$ and, if so, then to determine one such g. It is well-known that this problem can be solved readily using a variation of the Gaussian elimination algorithm.

The *integral conjugacy problem* asks to decide if there exists $g \in \mathrm{GL}(n, \mathbb{Z})$ satisfying $g^{-1}Tg = T'$ and, if so, then to determine one such matrix g. This problem is significantly harder to solve than its rational analogue. Dual to the integral conjugacy problem is the *integral centralizer problem* which asks to determine a finite generating set for $C_{\mathbb{Z}}(T) = \{g \in \mathrm{GL}(n, \mathbb{Z}) \mid g^{-1}Tg = T\}$. Grunewald [4] and Sarkisyan [5] both proved independently that the integral conjugacy and centralizer problems are decidable. Neither of their algorithms for this purpose appears to be practical.

This talk describes a first *practical* algorithm to solve both the integral conjugacy and centralizer problems. The algorithm is based on Grunewald's ideas [4] and improves these in various ways. An implementation in Magma [1] is available.

The talk ends by noting two related open problems. First, Sarkisyan [5] also proved that the *multiple integral conjugacy problem* is decidable; that is, given two lists $T_1, \ldots, T_m$ and $T'_1, \ldots, T'_m$ of integral matrices, decide if there exists $g \in \mathrm{GL}(n, \mathbb{Z})$ with $g^{-1}T_i g = T'_i$ for $1 \leq i \leq m$. A practical algorithm to solve this problem and to find an explicit conjugating element g are still open. Secondly, Grunewald & Segal [3] proved that the *subgroup conjugacy problem* for unitriangular subgroups of $\mathrm{GL}(n, \mathbb{Z})$ is decidable. A practical algorithm to solve this problem and to compute the centralizer in $\mathrm{GL}(n, \mathbb{Z})$ of a unitriangular subgroup is a still open problem.

References

1 W. Bosma, J. Cannon, and C. Playoust. The MAGMA algebra system I: The user language. *J. Symb. Comput.*, 24:235–265, 1997.
2 B. Eick, T. Hofmann, and E. O'Brien. The conjugacy problem in $\mathrm{GL}(n, \mathbb{Z})$. To appear in J. London Math. Soc., 2019.
3 F. Grunewald and D. Segal. Some general algorithms, I: Arithmetic groups. *Ann. Math.*, (112):531–583, 1980.

4 F. J. Grunewald. Solution of the conjugacy problem in certain arithmetic groups. In *Word problems, II (Conf. on Decision Problems in Algebra, Oxford, 1976)*, volume 95 of *Stud. Logic Foundations Math.*, pages 101–139. North-Holland, Amsterdam-New York, 1980.
5 R. A. Sarkisjan. The conjugacy problem for collections of integral matrices. *Mat. Zametki*, 25(6):811–824, 956, 1979.

3.5 On the intersection problem for free-abelian by free groups

Jordi Delgado Rodríguez (University of Porto, PT)

Joint work of Jordi Delgado Rodríguez and Enric Ventura Capell
Main reference Jordi Delgado, "Extensions of Free Groups: Algebraic, Geometric, and Algorithmic Aspects", Ph.D. Thesis, Universitat Politècnica de Catalunya, Sept. 2017.
URL https://www.researchgate.net/publication/319902473_Extensions_of_free_groups_algebraic_geometric_and_algorithmic_aspects

The idea of using covering spaces to understand subgroups of the free group $\mathbb{F}_n$ goes back to the eighties with the seminal work of Stallings in [2]. It soon became clear that this theory admitted a neat description in terms of automata (labeled digraphs), and was very convenient to attack algorithmic problems. The success of this interpretation (of subgroups as automata) generated a growing interest in extending Stallings machinery to other families of groups.

In [1, Chapter 5], we extend Stallings theory to free-abelian by free groups ($\mathbb{Z}^m \rtimes \mathbb{F}_n$) by "enriching" the arcs in the automata with abelian labels and modifying accordingly the folding process. This approach provides a clean description of the subgroups of $\mathbb{Z}^m \rtimes \mathbb{F}_n$ as "enriched automata", and an efficient solution to the membership problem within this family.

However, obstructions appear when we try to adapt to our scheme the pullback construction to describe intersections of subgroups. I will discuss the obtained results for $\mathbb{Z}^m \times \mathbb{F}_n$ and where the difficulties lie to extend our proof to the general case.

This is joint work with Enric Ventura.

References

1 J. Delgado. *Extensions of free Groups: algebraic, geometric, and algorithmic aspects*. Ph.D. Thesis. Universitat Politècnica de Catalunya (Sept. 2017).
2 J. R. Stallings. *Topology of Finite Graphs*. Inventiones Mathematicae 71 (Mar. 1983), pp. 551–565.

3.6 Solving equations in hyperbolic groups

Laura Ciobanu (Heriot-Watt University – Edinburgh, GB) and Murray Elder (University of Technology Sydney, AU)

Joint work of Laura Ciobanu, Murray Elder
Main reference Laura Ciobanu, Murray Elder: "Solutions sets to systems of equations in hyperbolic groups are EDT0L in PSPACE", ICALP 2019

For a group G, solving equations where the coefficients are elements in G and the solutions take values in G can be seen as akin to solving Diophantine equations in number theory, answering questions from linear algebra or more generally, algebraic geometry. Moreover, the

question of satisfiability of equations fits naturally into the framework of the first order theory of G. In these talks we will give a short overview of what is known about the satisfiability of equations in infinite non-abelian groups, with an emphasis on free and hyperbolic groups.

More precisely, in the first talk (Ciobanu) we will outline the approaches of Rips & Sela [2], and Dahmani & Guirardel [1] to solving equations in hyperbolic groups. In the second talk (Elder) we will show that the full set of solutions to systems of equations and inequations in a hyperbolic group, with or without torsion, as shortlex geodesic words, is an EDT0L language whose specification can be computed in $\mathbf{NSPACE}(n^2 \log n)$ for the torsion-free case and $\mathbf{NSPACE}(n^4 \log n)$ in the torsion case.

References

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

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

3.7 Knapsack problems for wreath products

Moses Ganardi (Universität Siegen, DE)

Joint work of Moses Ganardi, Daniel König, Markus Lohrey, Georg Zetzsche
Main reference Moses Ganardi, Daniel König, Markus Lohrey, Georg Zetzsche: "Knapsack Problems for Wreath Products", in Proc. of the 35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France, LIPIcs, Vol. 96, pp. 32:1–32:13, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2018.
URL http://dx.doi.org/10.4230/LIPIcs.STACS.2018.32

In recent years, knapsack problems for (in general non-commutative) groups have attracted attention. We study the knapsack problem for wreath products. It turns out that decidability of knapsack is not preserved under wreath product. On the other hand, the class of knapsack-semilinear groups, where solutions sets of knapsack equations are effectively semilinear, is closed under wreath product. As a consequence, we obtain the decidability of knapsack for free solvable groups. Finally, it is shown that for every non-trivial abelian group G, knapsack (as well as the related subset sum problem) for the wreath product $G \wr \mathbb{Z}$ is **NP**-complete.

3.8 Equations in solvable groups

Albert Garreta (University of the Basque Country – Bilbao, ES)

Joint work of Albert Garreta, Alexei Miasnikov, Denis Ovchinnikov

We study the Diophantine problem (decidability of systems of equations) in different families of solvable groups. Whe show that for any group G in each of these families there exists a ring of algebraic integers O that is interpretable in G by systems of equations. This reduces the Diophantine problem of O –conjectured undecidable– to the same problem in G, and it leads us to conjecture that the Diophantine problem in G is undecidable. The families where such result is obtained include all finitely generated non-virtually abelian nilpotent groups and all

polycyclic groups that are not virtually metabelian. Note that the Diophantine problem of virtually abelian groups has long been known to be decidable (their first-order theory is). We also show undecidability of the Diophantine problem in free solvable groups and in 'most' nilpotent groups by studying asymptotic properties of random nilpotent groups.

3.9 Automaticity for graphs of groups, and applications

Susan Hermiller (University of Nebraska – Lincoln, US)

Joint work of Susan Hermiller, Derek F. Holt, Sarah Rees, Tim Susse
Main reference Susan Hermiller, Derek F. Holt, Sarah Rees, Tim Susse: "Automaticity for graphs of groups", CoRR, Vol abs/1905.05943, 2019.
URL https://arxiv.org/abs/1905.05943

In this I will discuss new closure properties for the class of automatic groups with respect to taking fundamental groups of graphs of groups. Applications include automaticity of fundamental groups of graphs of groups in which each vertex group is either a graph product group, a Coxeter group, or an Artin group of sufficiently large type, and each edge group is a subgraph product or special subgroup, respectively, in its adjacent edge groups. The constructions are used to find automatic structures for a new family of Artin groups, and new automatic structures for acylindrical graphs of groups that are hyperbolic relative to abelian subgroups, including fundamental groups of 3-manifolds with hyperbolic pieces. This is joint work with Derek Holt, Sarah Rees, and Tim Susse.

3.10 Satisfiable word equations are context-sensitive

Artur Jeż (University of Wroclaw, PL)

Main reference Artur Jez: "Word Equations in Nondeterministic Linear Space", in Proc. of the 44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland, LIPIcs, Vol. 80, pp. 95:1–95:13, Schloss Dagstuhl – Leibniz-Zentrum fuer Informatik, 2017.
URL http://dx.doi.org/10.4230/LIPIcs.ICALP.2017.95

Word equations are an important problem on the intersection of formal languages and algebra. Given two sequences consisting of letters and variables we are to decide whether there is a substitution for the variables that turns this equation into true equality of strings. The computational complexity of this problem remains unknown, with the best lower and upper bounds being **NP** and **PSPACE**. Recently, a novel technique of recompression was applied to this problem, simplifying the known proofs and lowering the space complexity to (nondeterministic) $O(n \log n)$. In this talk I will show that word equations are in nondeterministic linear space, thus the language of satisfiable word equations is context-sensitive. The algorithm uses the known recompression-based algorithm and additionally employs Huffman coding for letters. The proof, however, uses analysis of how the fragments of the equation depend on each other as well as a new strategy for nondeterministic choices of the algorithm, which uses several new ideas to limit the space occupied by the letters.

3.11 Generic-case complexity of Whitehead's algorithm, revisited

Ilya Kapovich (City University of New York, US)

Main reference Ilya Kapovich: "Generic-case complexity of Whitehead's algorithm, revisited", CoRR, Vol. abs/1903.07040, 2019.
URL https://arxiv.org/abs/1903.07040

We generalize to a much larger class of random processes, including group random walks and graph random walks, the previously known generic-case complexity results regarding the behavior of Whitehead's algorithm algorithm for the automorphic equivalence problem in free groups. The main tool used is the machinery of geodesic currents and the geometric intersection number between currents and $\mathbb{R}$-trees.

3.12 On the elementary theory of graph products of groups

Ilya Kazachkov (University of the Basque Country, ES & Ikerbasque – Bilbao, ES

When studying the model theory of groups, it is natural to ask which group-theoretic constructions preserve the elementary theory. In 1959, Feferman and Vaught studied the first-order properties of direct products and showed, in particular, that the direct products of elementarily equivalent groups are elementarily equivalent. In contrast, invariance of the elementary equivalence for free products of groups was a long-standing conjecture which was recently solved by Sela (2017).

In this talk, we will first address the converse question: given two elementary equivalent free products of groups (or more generally, graph product of groups), when are the factors elementarily equivalent? We discuss some sufficient conditions and use our results to describe finitely generated groups elementarily equivalent to RAAGs whose underlying graph is a transitive forest.

3.13 Equations and model theory in one relator groups

Olga Kharlampovich (The City University of New York, US)

Joint work of Olga Kharlampovich, Laura Lopez, Alexei Miasnikov

O. Kharlampovich gave a talk about results with L. Lopez and A. Miasnikov on solvability of equations in some classes of metabelian groups like Baumslag Solitar groups $BS(1, k)$, and wreath products $\mathbb{Z} \wr \mathbb{Z}$ and $\mathbb{Z}_n \wr \mathbb{Z}$. Some model theoretic questions for one relator groups were also discussed.

3.14 Malcev's problems, weak second order logic, and bi-interpretability

Alexei Myasnikov (Stevens Institute of Technology – Hoboken, US)

Joint work of Olga Kharlampovich, Alexei Myasnikov, Mahmood Sohrabi

Malcev's problems on definable subgroups of a free non-abelian group F were solved a few years ago by Kharlampovich and Myasnikov and also by Perin, Pillay, Sklinos, and Tent. It turned out that only cyclic subgroups are definable proper subgroups of F. Similar results hold for torsion-free hyperbolic groups. On the other hand, in finitely generated abelian groups only subgroups of finite index and the trivial subgroup are definable. One may consider the following question: what are finitely generated infinite groups where all finitely generated subgroups are definable? Furthermore, are there any interesting infinite groups G where finitely generated subgroups are uniformly definable, i.e., for each natural n there exists a first-order formula $D_n(x, y_1, \ldots, y_n)$ such that for any elements $g_1, \ldots, g_n$ in G the formula $D_n(x, g_1, \ldots, g_n)$ defines in G the subgroup generated by $g_1, \ldots, g_n$? Surprisingly, there is a wide variety of finitely generated infinite groups with uniformly definable subgroups. Such questions are part of a much bigger problem about the expressive power of the first-order logic in groups (or rings, or arbitrary structures). I will discuss this problem and its connections with the weak second order logic and bi-interpretability.

3.15 Non-deterministic automata and group theory

Volodia Nekrashevych (Texas A&M University – College Station, US)

The class of groups generated by synchronous deterministic automata has been studied for a long time (see, for example, the extensive literature on the Grigorchuk group and its analogs). It was recently discovered that non-deterministic versions of such automata also generate interesting groups, and provide substantially new properties. For example, the author has constructed examples of simple torsion groups of intermediate growth using such automata. We will discuss algorithmic problems related to non-deterministic synchronous automata-transducers, their applications to dynamical systems (for example they appear naturally in the study of hyperbolic dynamical systems) and to group theory.

3.16 Reachability problems in matrix semigroups

Igor Potapov (University of Liverpool, GB)

A large number of naturally defined decision problems on matrices are still unanswered despite the long history of matrix theory. Originally in Arthur Cayley's "A Memoir on the Theory of Matrices" in 1858, the notion of a matrix arises naturally from abbreviated notations for a set of linear equations where he also defined associated operation of multiplication,

notions of determinant, inverse matrices, etc. Nowadays questions on matrices and matrix problems emerge in much larger context as they appear in the analysis of various digital processes, verification problems [18], in the context of control theory questions [2]. Moreover problems on matrix products have been associated with several long standing open problems in algebraic number theory and transcendence theory, Nash equilibria, in the theory of joint spectral radius and its applications [9, 14, 18, 19].

Many simply formulated and elementary problems for matrices are inherently difficult to solve even in dimension two, and most of these problems become undecidable in general starting from dimension three or four [6, 4, 7, 9, 10, 20]. Only few decidability results are known so far, see for example [1, 12, 5, 11, 13, 21, 22, 23].

Let us given a finite set of square matrices (known as a generator) which is forming a multiplicative semigroup S. The classical computational problems for matrix semigroups are:

- Membership (Decide whether a given matrix M belong to a semigroup S) and two special cases such as: Identity (i.e. if M is the identity matrix) and Mortality (i.e. if M is the zero matrix) problems
- Vector reachability (Decide for a given vectors u and v whether exist a matrix M in S such that $M \cdot u = v$)
- Scalar reachability (Decide for a given vectors u, v and a scalar L whether exist a matrix M in S such that $u^T \cdot M \cdot v = L$)
- Freeness (Decide whether every matrix product in S is unique, i.e. whether it is a code) and some variants of the freeness such as finite freeness problem, the recurrent matrix problem, the unique
- factorizability problem, vector freeness problem, vector ambiguity problems, etc.

The undecidability proofs in matrix semigroups are mainly based on various techniques and methods for embedding universal computations into matrix products. The case of dimension two is the most intriguing since there is some evidence that if these problems are undecidable, then this cannot be proved directly using previously known constructions. Due to a severe lack of methods and techniques the status of decision problems for 2×2 matrices (like membership, vector reachability, freeness) is remaining to be a long standing open problem not only for matrices over algebraic, complex, rational numbers but also for integer matrices.

Recently, a new approach of translating numerical problems of 2×2 integer matrices into variety of combinatorial and computational problems on words and automata over group alphabet and studying their transformations as specific rewriting systems [11, 13] have led to a few results on decidability and complexity for some subclasses:

- The membership problem for 2×2 nonsingular integer matrices is decidable [23]. The algorithm relies on a translation of numerical problems on matrices into combinatorial problems on words. It also makes use of some algebraic properties of well-known subgroups of $\mathrm{GL}(2, \mathbb{Z})$ and various new techniques and constructions that help to convert matrix equations into the emptiness problem for intersection of regular languages.
- The Identity problem in $\mathrm{SL}(2, \mathbb{Z})$ is **NP**-complete [8, 5]. Our **NP** algorithm is based on various new techniques that allow us to operate with compressed word representations of matrices without explicit exponential expansion.
- The vector reachability problem over a finitely generated semigroup of matrices from $\mathrm{SL}(2, \mathbb{Z})$ and the point to point reachability (over rational numbers) for fractional linear transformations, where associated matrices are from $\mathrm{SL}(2, \mathbb{Z})$ are decidable [21].

Similar techniques have been applied to show that the freeness problem is co-NP-hard [16] as well as to study the complexity of other freeness problems such as finite freeness problem, the recurrent matrix problem, the unique factorizability problem, vector freeness problem, vector ambiguity problems, etc [15].

There are still many open problems in special cases of dimension three where in general many problems become undecidable. In the seminal paper of Paterson in 1970 [20], an injective morphism from pairs of words into 3×3 integral matrices was used to prove the undecidability of the mortality problem, and later led to many undecidability results of matrix problems in dimension three. In [17] it was shown that there is no embedding from pairs of words into 3×3 integral matrices with determinant one, i.e., into $\mathrm{SL}(3, \mathbb{Z})$, which provides strong evidence that computational problems in $\mathrm{SL}(3, \mathbb{Z})$ may be decidable, as all known undecidability techniques for low-dimensional matrices are based on encoding of Turing machine computations via Post's Correspondence Problem (PCP), which cannot be applied in $\mathrm{SL}(3, \mathbb{Z})$ following the results of [17]. In the case of the PCP encoding, matrix products extended by right multiplication correspond to a Turing machine simulation, and the only known proof alternatives rely on recursively enumerable sets and Hilbert's Tenth Problem, but provide undecidability for matrix equations of very high dimensions. [3].

References

1. László Babai, Robert Beals, Jin-yi Cai, Gábor Ivanyos, and Eugene M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '96, pages 498–507, Philadelphia, PA, USA, 1996. Society for Industrial and Applied Mathematics.
2. Vincent D. Blondel, John N. Tsitsiklis. A survey of computational complexity results in systems and control. Automatica 36(9): 1249-1274 (2000)
3. Paul Bell, Vesa Halava, Tero Harju, Juhani Karhumäki, Igor Potapov: Matrix Equations and Hilbert's Tenth Problem. IJAC 18(8): 1231-1241 (2008)
4. Paul C. Bell, Mika Hirvensalo, and Igor Potapov. Mortality for 2x2 matrices is NP-hard. In Branislav Rovan, Vladimiro Sassone, and Peter Widmayer, editors, *Mathematical Foundations of Computer Science 2012*, volume 7464 of *Lecture Notes in Computer Science*, pages 148–159. Springer Berlin Heidelberg, 2012.
5. Paul C. Bell, Mika Hirvensalo, and Igor Potapov. The Identity Problem for Matrix Semigroups in SL2(Z) is NP-complete. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, pages 187-206, 2017.
6. Paul Bell and Igor Potapov. On undecidability bounds for matrix decision problems. *Theoretical Computer Science*, 391(1-2):3–13, 2008.
7. Paul C. Bell and Igor Potapov. On the undecidability of the identity correspondence problem and its applications for word and matrix semigroups. *Int. J. Found. Comput. Sci.*, 21(6):963–978, 2010.
8. Paul C. Bell and Igor Potapov. On the computational complexity of matrix semigroup problems. *Fundam. Inf.*, 116(1-4):1–13, January 2012.
9. Vincent D. Blondel, Emmanuel Jeandel, Pascal Koiran, and Natacha Portier. Decidable and undecidable problems about quantum automata. *SIAM J. Comput.*, 34(6):1464–1473, June 2005.
10. Julien Cassaigne, Vesa Halava, Tero Harju, and François Nicolas. Tighter undecidability bounds for matrix mortality, zero-in-the-corner problems, and more. *CoRR*, abs/1404.0644, 2014.
11. Christian Choffrut and Juhani Karhumaki. Some decision problems on integer matrices. *RAIRO-Theor. Inf. Appl.*, 39(1):125–131, 2005.
12. Esther Galby, Joël Ouaknine, and James Worrell. On Matrix Powering in Low Dimensions. In Ernst W. Mayr and Nicolas Ollinger, editors, *32nd International Symposium on Theoretical Aspects of Computer Science (STACS 2015)*, volume 30 of *Leibniz International*

Proceedings in Informatics (LIPIcs), pages 329–340, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

13 Yuri Gurevich and Paul Schupp. Membership problem for the modular group. *SIAM J. Comput.*, 37(2):425–459, May 2007.

14 Raphael Jungers. The Joint Spectral Radius. Theory and Applications, Lecture Notes in Control and Information Sciences, Springer, 146pp, 2009

15 Sang-Ki Ko, and Igor Potapov Vector Ambiguity and Freeness Problems in SL(2,Z), Theory and Applications of Models of Computation: 14th Annual Conference, TAMC 2017, Bern, Switzerland, April 20-22, 2017, Proceedings, 2017, LNCS Springer, 373–388.

16 Sang-Ki Ko, and Igor Potapov. Matrix Semigroup Freeness Problems in SL(2,Z). SOFSEM 2017: Theory and Practice of Computer Science: 43rd International Conference on Current Trends in Theory and Practice of Computer Science, 2017, LNCS Springer, 268–279.

17 Sang-Ki Ko, Reino Niskanen, Igor Potapov: On the Identity Problem for the Special Linear Group and the Heisenberg Group. ICALP 2018: 132:1-132:15

18 Joël Ouaknine, João Sousa Pinto, and James Worrell. On termination of integer linear loops. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '15, pages 957–969. SIAM, 2015.

19 Joël Ouaknine and James Worrell. On the positivity problem for simple linear recurrence sequences,. In *Automata, Languages, and Programming – 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part II*, pages 318–329, 2014.

20 M. S. Paterson. Unsolvability in 3x3 matrices. *Studies in Applied Mathematics*, 49(1):pp.105–107, 1970.

21 Igor Potapov and Pavel Semukhin. Vector reachability problem in SL(2, Z). MFCS 2016. 84:1-84:14, LIPICS, 2016

22 Igor Potapov, Pavel Semukhin: Membership Problem in GL(2, Z) Extended by Singular Matrices. MFCS 2017: 44:1-44:13

23 Igor Potapov and Pavel Semukhin. Decidability of the membership problem for 2 x 2 integer matrices. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2017, Barcelona, Spain, Hotel Porta Fira, January 16-19*, pages 170–186, 2017.

3.17 Conjugator length

Timothy Riley (Cornell University – Ithaca, US)

Joint work of Martin Bridson, Timothy Riley, Andrew Sale

The conjugator length function of a finitely generated group G maps a natural number n to the minimal N such that if u and v are words representing conjugate elements of G with the sum of their lengths at most n, then there is a word w of length at most N such that $uw = wv$ in G. I will explore why this function is important, will describe some recent results with Martin Bridson and Andrew Sale on how it can behave, and will highlight some of the many open questions about conjugator length.

3.18 Unconditionally secure public key transport (with possible errors)

Vladimir Shpilrain (City University of New York, US)

Joint work of Mariya Bessonov, Dima Grigoriev, Vladimir Shpilrain

We offer what seems to be the first public key transport scheme whose security is not based on any computational assumptions but rather on the presence of several "decoy" keys that cannot be positively distinguished from the real key even by a computationally unbounded (passive) adversary. More specifically, we consider a scenario where one party wants to transmit a secret key to another party in the presence of a computationally unbounded (passive) adversary. The legitimate parties succeed with probability close to 1 (although strictly less than 1), while a computationally unbounded passive adversary succeeds in correctly recovering the secret key with significantly lower probability.

3.19 On the group of automorphisms of a context-free graph.

Géraud Sénizergues (University of Bordeaux, FR)

Joint work of Géraud Sénizergues, Armin Weiß

Context. A famous theorem from [Muller-Schupp, JCSS 1983] establishes that a group G has a *context-free* word-problem if and only if it is *virtually-free* of finite type. A key-notion emerging from this work on the links between groups and formal languages, is the notion of *context-free graph*, which generalizes the Cayley-graphs of context-free groups. This notion and its links with second-order monadic logics was studied in [Muller-Schupp, TCS 1985]. Later on, it was shown by [L. Pelecq, TCS 1995] that the automorphism-group of a deterministic context-free graph is a context-free group. We discuss here two problems about the automorphism-groups of context-free graphs (thus skipping the hypothesis about determinism).

Problems. Let Γ be a *context-free* graph.

- Problem 1: What is the algebraic structure of the group $G := \mathrm{Aut}(\Gamma)$?
- Problem 2: Describe the equivalence $\sim_G$ over the vertices of Γ. Is this relation, in general, a *rational* relation?

(Problem 2 was raised in [G. Sénizergues, ICALP 1996]).

Results. A recent proof of Muller and Schupp's theorem was given by [Diekert and Weiß, 2017] and consists in showing that, if the Cayley-graph of a group G is context-free, then the equivalence classes of its "optimal cuts" (in some adequate technical sense) are the vertices of a simplicial tree T, endowed with a natural action of the group G, whose vertex-stabilizers are finite.
From Bass-Serre theory of group-actions on trees, it follows that G is virtually-free.

1. We give a variant of this proof by constructing, from the tree T, a *tiling* of the Cayley-graph of G, with only one elementary tile P, which is finite, and a tiling group $H < G$. By some version of the "combination lemma" (originating in a work of [F. Klein 1883]), we conclude that H is free and $[G : H] = \mathrm{card}(P) < \infty$.

2. We adapt the above proof to the situation where Γ is a context-free graph and G is a group acting transitively on Γ (possibly with infinite stabilizers). In this case G has a *three-fold decomposition* as

   $$G = H \cdot F \cdot S$$

   where H is a free group of finite type, F is a finite subset and S is the stabilizer of some vertex (hence a profinite group). We show that the equivalence $\sim_G$ over Γ is a rational relation.
3. We sketch an extension to the case where Γ is a context-free graph and G is its group of automorphisms. In this case G has again a three-fold decomposition as

   $$G = H \cdot F \cdot S$$

   where H is a free group of finite type, F is a finite subset and S is the stabilizer of some vertex.

We are currently working on the proof that the equivalence $\sim_G$ over Γ is a rational relation.

3.20 Coarse computabilty and closures of Turing degrees

Paul E. Schupp (University of Illinois – Urbana Champaign, US)

Coarse computabilty studies how well arbitrary sets can be approximated in terms of computable sets. Computabilty theory studies Turing degrees. We use coarse computabilty to put the study of some questions about Turing degrees into a complete metric space. We consider only subsets of the natural numbers $\mathbb{N}$ so asymptotic density is classical asymptotic density from number theory. Define two sets A and to be *coarsely similar* if their symmetric difference $A \triangle B$ has density 0. This relation is an equivalence relation, so we consider the space $\mathcal{S}$ of coarse similarity classes. There is a pseudo-metric defined on $\mathcal{P}(\mathbb{N})$ by setting $\delta(A, B)$ to be the upper density of their symmetric difference. Then δ is a metric on the space $\mathcal{S}$. This metric was introduced by Besicovitch in studying almost periodic functions.

Although the space $\mathcal{S}$ is very nonseparable and noncompact, it turns out to be both complete and contractible, two very useful properties. Define the *core*, $\kappa(\boldsymbol{d})$, of a Turing degree $\boldsymbol{d}$ to be the family $\{[A]\}$ of all classes such that A is coarsely computable from $\boldsymbol{d}$. That is, given total information about about a set in $\boldsymbol{d}$ we can compute a set which is coarsely equivalent to A. The closure $\overline{\boldsymbol{d}}$ of the degree $\boldsymbol{d}$ is the closure of $\kappa(\boldsymbol{d})$ in the metric topology. There are now some very interesting interactions between computabilty ideas and the metric topology.

3.21 Homological finiteness in one-relator monoids

Benjamin Steinberg (City University of New York, US)

Joint work of Benjamin Steinberg, Robert Gray

Motivated by the longstanding open problem of deciding the word problem for one-relator monoids, Kobayashi asked in 2000 whether all one-relator monoids are of type FP_∞. This is a necessary condition for admitting a finite complete rewriting system (Kobayashi was interested in whether all one-relator monoids admit finite complete rewriting systems). In this talk, we discuss recent progress by the speaker and Robert Gray on solving Kobayashi's problem using topological methods. Note that Lyndon proved in the fifties that all one-relator groups are of type FP_∞.

3.22 A primer of low-depth circuit complexity

Howard Straubing (Boston College, US)

Howard Straubing presented a survey on low-depth circuit complexity and its connection with finite groups and semigroups. The key result, dating back to work of Barrington and Thérien in the 1980's and 1990's, is essentially this: A circuit family belonging to the classes $\mathbf{AC}^0$ (resp. $\mathbf{CC}^0$, $\mathbf{ACC}^0$, $\mathbf{NC}^1$) can be replaced by a family of circuits, each with a SINGLE gate and polynomially many wires, that computes products in an aperiodic finite monoid (resp. solvable group, monoid containing only solvable groups, non-solvable finite group). Questions of strict inclusions between these complexity classes, and various subclasses thereof, are therefore equivalent to establishing the relative computing power of different families of finite groups and semigroups. In spite of a surge of progress some 30 years ago, most of these remain open problems.

3.23 Ramanujan cubical complexes and non-residually finite CAT(0) groups in any dimension

Alina Vdovina (Newcastle University, GB)

Ramanujan graphs were first considered by Lubotzky, Phillips, Sarnak to get graphs with optimal spectral properties. In our days the theory of expander graphs and, in particular, Ramanujan graphs is well developed, but the questions is what is the best definition of a higher-dimensional expander is still wide open. There are several approaches, suggested by Gromov, Lubotzky, Alon and others, but the cubical complexes were not much investigated from this point of view. In this talk I will give new explicit examples of cubical Ramanujan complexes and discuss possible developments.

3.24 How to compute the stable image of an endomorphism?

Enric Ventura Capell (UPC – Barcelona Tech, ES)

Let F be a finitely generated free group and let g be an endomorphism of F, given by the images of a free basis of F. The stable image of g, denoted $\mathrm{Im}(g^\infty)$, is defined as the intersection of $\mathrm{Im}(g^n)$ for all $n > 0$. It is known that this stable image is always finitely generated (in fact, with rank bounded by that of F), invariant under g, and that the restriction of g on it is always bijective (I'll give short proofs for these facts). The question (open as far as I know) is "can you compute generators for $\mathrm{Im}(g^\infty)$?" This is interesting because a positive answer would have as a consequence the computability of the fixed subgroup of g, a (hard?) open problem. Note that the computability of $\mathrm{Fix}(g)$ in the case when g is an automorphism has been resolved by strongly using the train-track machinery; in presence of non-trivial kernel this aproach doesn't work (unless further developments of the train track techniques allow) and so computation of the fixed subgroup of an endomorphism is an open problem.

3.25 `stallings_graphs`, a Sagemath package to experiment with subgroups of free groups

Pascal Weil (CNRS & University of Bordeaux, FR)

URL http://www.labri.fr/perso/weil/software/

Pascal Weil presented a SageMath package to compute with finitely generated subgroups of free groups. SageMath is an open source free non-commercial mathematical software system. This package, `stallings_graphs`, is available on Pascal's webpage. In this package, the internal representation of a finitely generated subgroup is a tuple of partial injections on some set of the form $[0, ..., n]$, one for each generator of the ambient free group; which is to say that a finitely generated subgroup is represented by its Stallings graph.

The literature abounds in efficient algorithms using this representation, and many are already part of the package: computation of the rank, of a basis, of the intersection of two subgroups, of conjugates; as well as decision of the finite index property, conjugacy, malnormality. Future work will involve automorphism-related algorithms, including the decision of the free factor property.

3.26 The power word problem in free groups

Armin Weiß (Universität Stuttgart, DE)

Joint work of Markus Lohrey, Armin Weiß
Main reference Markus Lohrey, Armin Weiß: "The power word problem", CoRR, Vol. abs/1904.08343, 2019.
URL https://arxiv.org/abs/1904.08343

We introduce a new succinct variant of the word problem in a finitely generated group G, which we call the power word problem: the input word may contain powers p^x, where p is a finite word over generators of G and x is a binary encoded integer. While being more general than the ordinary word problem, the power word problem is a restriction of the compressed word problem, where the input word is represented by a straight-line program (i.e., an algebraic circuit over G). The main result states that the power word problem for a finitely generated free group F is $\mathbf{AC}^0$-Turing-reducible to the word problem for F. Moreover, for a wreath product $G \wr \mathbb{Z}$, where G is either free of rank at least two or finite non-solvable, the power word problem is complete for **coNP**. This contrasts with the situation where G is abelian: then the power word problem is shown to be in $\mathbf{TC}^0$.

In the talk, first an introduction into circuit complexity and its relation to group theory is given. The second part of the talk outlines the proof of the above mentioned main result.

3.27 Regular subsets of wreath products

Georg Zetzsche (MPI-SWS – Kaiserslautern, DE)

In theoretical computer science, an immensely popular concept for algorithmically working with sets of finite words is that of *regular languages*, which can be characterized in terms of finite automata, finite monoids, and monadic second-order logic (MSO). This popularity stems from an abundance of closure and decidability properties: For example, they are closed under Boolean operations and contain every finitely generated submonoid.

There have been several attempts at finding analogous concepts in infinite groups. Examples include the recognizable subsets and the rational subsets [1]. Let G be a finitely generated group. A subset $S \subseteq G$ is called *recognizable* if it is a union of cosets with respect to some finite-index normal subgroup of G. The class of *rational subsets* of G is the smallest class of subsets that (i) contains the empty set, (ii) contains every singleton $\{g\}$ with $g \in G$, (iii) is closed under finite unions: if $A, B \subseteq G$ are rational, then so is $A \cup B$, and (iv) is closed under the Minkowski product: if $A, B \subseteq G$ are rational, then so is $AB = \{ab \mid a \in A,\ b \in B\}$, and (iv) is closed under taking finitely generated submonoids: if $A \subseteq G$ is rational, then so is the submonoid of G generated by A.

In the case of free groups or abelian groups, rational subsets have similarly nice properties as regular languages of finite words: For free groups, their automata representation naturally generalizes Stallings graphs and for abelien groups, they coincide with the first-order definable sets. However, in general, both the recognizable sets and the rational subsets lack important features: While the recognizable subsets are closed under Boolean operations and have decidable membership for every G, they have limited expressiveness (e.g. not every singleton is recognizable). Rational subsets, on the other hand, are in general not closed under the

Boolean operations. However, they are expressive in the sense that they encompass all finitely generated subsemigroups.

In this talk, I describe a class of subsets of groups $H \wr F$, where H is finite and F is free. This class of subsets, which are dubbed *regular subsets*, has several appealing properties:

- Every rational subset of $H \wr F$ is regular.
- Emptiness and membership are decidable for regular subsets.
- The regular subsets are closed under Boolean operations.
- Regular subsets can be characterized using MSO over the Cayley graph of the free group. Via Rabin's theorem, this yields decidability of a number of properties. For example, it is decidable whether a given regular subset is recognizable. In particular, it is decidable whether a given finitely generated subgroup of $H \wr F$ has finite index.

Moreover, these constructions yield an elementary algorithm to decide membership in a given rational subset of $H \wr F$. This answers an open problem from [2]: Therein, it was shown that membership in rational subsets of $H \wr F$ is decidable, but it was left open whether this problem is primitive recursive. Another consequence is that not only membership in rational subsets is decidable, but emptiness of any given Boolean combination.

Note that such a notion of regular subsets is unlikely to exist for much more general wreath products $K \wr G$: In order for membership in rational subsets of $K \wr G$ to be decidable, either K or G has to be a torsion group [2] and there is evidence that G has to be virtually free [2].

References

1 L. Bartholdi and P. V. Silva. Rational subsets of groups. arXiv preprint arXiv:1012.1532, 2010.
2 M. Lohrey, B. Steinberg, and G. Zetzsche. Rational subsets and submonoids of wreath products. *Information and Computation*, (243):101–204, 2015.

4 Open problems

4.1 Asymptotics of words in partially commutative groups

Andrew Duncan (Newcastle University, GB)

Find methods of estimating the size of naturally occuring subsets of elements of partially commutative groups (e.g. cyclically reduced; with no left divisor in a given parabolic subgroup).

Articles containing examples of existing results along these lines are listed in the bibliography below. These all apply to the class of partially commutative groups which map canonically onto braid groups.

References

1 J. Debois and S. Nechaev. Statistics of reduced words in locally free and braid groups *J. Statist. Phys.*, 88:2767–2789, 1997.
2 A. Vershik. Dynamic growth theory in groups: entropy, boundaries, example, *Uspehi Mat. Nauk*, 55 issue 4 (334), p. 59–128, 2002.

4.2 Open problems for integral matrix groups

Bettina Eick (TU Braunschweig, DE)

Problem 1. Let $(T_1, \ldots, T_m)$ and $(T'_1, \ldots, T'_m)$ be two lists of rational matrices. The *multiple integral conjugacy problem* asks to decide if there exists $g \in \mathrm{GL}(n, \mathbb{Z})$ satisfying $g^{-1}T_i g = T'_i$ for $1 \leq i \leq m$ and, if so, then to determine one such g. Sarkisyan (1979) proved that this problem is decidable, but no practical or efficient algorithm is known.

Problem 2. Let $U, V \leq \mathrm{GL}(n, \mathbb{Z})$ be two unitriangular groups. The *subgroup integral conjugacy problem* asks to decide if there exists $g \in \mathrm{GL}(n, \mathbb{Z})$ satisfying $g^{-1}Ug = V$ and, if so, then to determine one such g. Grunewald & Segal (1980) proved that this problem is decidable. Still open is the problem to determine a practical or efficient algorithm for this purpose.

Problem 3. Let T be an invertible rational matrix. Eick, Hofmann and O'Brien (2019) exhibited a practical algorithm to compute a finite set of generators for the centralizer $C_{\mathrm{GL}(n,\mathbb{Z})}(T)$. As this centralizer is an arithmetic group, it follows that it is finitely presented. Develop a practical method to determine such a finite presentation.

4.3 Deciding whether a finitely generated subgroup has finite index

Ilya Kapovich (City University of New York, US)

Problem. Let $\mathcal{G}$ be a "reasonable" class of finitely presented groups with solvable word problem. [E.g. RAAGs, mapping class groups, toral relatively hyperbolic groups, limit groups, 3-manifold groups, $C(4) - T(4)$ small cancellation groups, etc]

Let $G \in \mathcal{G}$ be a group given by a finite presentation $G = \langle X | R \rangle$.

1. Is there an algorithm that, given a finite set of words $v_1, \ldots, v_k \in F(X)$ generating a subgroup $H = \langle v_1, \ldots, v_k \rangle \leq G$, decides whether or not $[G : H] < \infty$?
2. A variation of the same problem: Is there an algorithm that, given a finite set of words $v_1, \ldots, v_k \in F(X)$ generating a subgroup $H = \langle v_1, \ldots, v_k \rangle \leq G$ such that it is known that H is quasi-isometrically embedded in G, decides whether or not $[G : H] < \infty$

Note. It is known that for $\mathcal{G}$ being the class of word-hyperbolic groups, problem (1) is in general undecidable (because of counter-examples given by the Rips construction) but problem (2) is decidable.

4.4 Distinct Baumslag-Solitar groups in the same one-relator group

Olga Kharlampovich (The City University of New York, US)

Let p, q, r, s be different prime numbers. Can a one-relator group contain $\mathrm{BS}(p, q)$ and $\mathrm{BS}(r, s)$ at the same time?

4.5 Membership problems for groups of unitriangular matrices

Markus Lohrey (Universität Siegen, DE)

In a recent paper, Colcombet, Ouaknine, Semukhin and Worrell [On reachability problems for low-dimensional matrix semigroups, arXiv 2019. https://arxiv.org/abs/1902.09597] proved that the subsemigroup membership problem for Heisenberg groups is decidable. The n-dimensional Heisenberg group consists of all integer matrices where all entries on the main diagonal are one, and all entries that do not belong to the main diagonal, to the first row, or to the last column are zero. This result leads to the question whether the following two problems are decidable as well.

- the subsemigroup membership problems for groups $\mathrm{UT}_n(\mathbb{Z})$ of n-dimensional unitriangular integer matrices (matrices where all entries on the main diagonal are one, and all entries below the main diagonal are zero),
- the rational subset membership problem for Heisenberg groups (it is known that the rational subset membership problem for $\mathrm{UT}_n(\mathbb{Z})$ is undecidable if n is sufficiently large).

4.6 Is there an algorithm to compute the stable image of an endomorphism of a free group?

Enric Ventura Capell (UPC – Barcelona Tech, ES)

Problem. Is there an algorithm to compute the stable image of an endomorphism of a free group?

Discussion. Let F be a finitely generated free group and let g be an endomorphism of F, given by the images of a free basis of F. The stable image of g, denoted $\mathrm{Im}(g^\infty)$, is defined as the intersection of $\mathrm{Im}(g^n)$ for all $n > 0$. It is known that this stable image is always finitely generated (in fact, with rank bounded by that of F). The problem consists on computing a free basis for $\mathrm{Im}(g^\infty)$ from the given g.

One can easily compute recursively the Stallings graph (and so a free basis) for $\mathrm{Im}(g)$, $\mathrm{Im}(g^2)$, $\mathrm{Im}(g^3)$, etc. And it is not difficult to see that the Stallings graph for $\mathrm{Im}(g^\infty)$ is a subgraph of $\mathrm{Im}(g^n)$ for some big enough n. What remains is to be able to decide how tall must we go up this tower of graphs and, whence there, how to choose the appropriate subgraph (out of the finitely many ones).

Inspecting the example $a \mapsto a^2$, $b \mapsto b$, (with $\mathrm{Im}(g^\infty) = \langle b \rangle$), it seems that the problem is about detecting which parts of the graph grow to infinite, and cut them in finite time. Maybe the problem is related to the following question: can we define a dynamic notion of stable image including the points at infinity ? (in the previous example, this extended stable image should be something like "$\langle b, a^\infty \rangle$".

The answer to this problem has a direct application: the computability of the fixed subgroup of arbitrary endomorphisms (the corresponding problem for automorphisms has been solved making strong use of train track techniques).

4.7 Rational subsets of Baumslag-Solitar groups $\mathrm{BS}(1, q)$

Georg Zetzsche (MPI-SWS – Kaiserslautern, DE)

Background. The motivation for my problem comes from rational subsets of Baumslag-Solitar groups $\mathrm{BS}(1, q)$ (see abstract 3.27 for a definition of rational subsets): If the answer to the problem is *yes*, then this yields a notion of regular subsets of $\mathrm{BS}(1, q)$ that has similar properties as the regular subsets of wreath products $H \wr F$ as described in abstract 3.27. In particular, a positive answer would imply that membership in rational subsets of $\mathrm{BS}(1, q)$ is decidable. Even more: Emptiness of given Boolean combinations of rational subsets would be decidable.

Setting. Consider the ring $\mathbb{Z}[\frac{1}{q}]$ and its additive submonoid $\mathbb{N}[\frac{1}{q}]$, which consists of all numbers $a = \sum_{i=-m}^{n} a_i q^i$ for some $m, n \in \mathbb{N}$ and $a_{-m}, a_{-m+1}, \ldots, a_n \in \{0, \ldots, q-1\}$. This representation is unique if we require that $a_{-m} > 0$ or $m = 0$ and also $a_n > 0$ or $n = 0$. In this situation, we represent the number $\sum_{i=-m}^{n} a_i q^i$ by the word

$$a_{-m}\ a_{-m+1}\ \cdots\ a_{-1}\ \bullet\ a_0\ \cdots\ a_n$$

over the finite alphabet $\Sigma = \{0, \ldots, q-1, \bullet\}$. Here, the symbol $\bullet$ can be thought of as the radix point. Let $\iota \colon \mathbb{N}[\frac{1}{q}] \to \Sigma^*$ be the map that yields the word representation of each number. We call a subset $A \subseteq \mathbb{N}[\frac{1}{q}]$ *automatic* if $\iota(A)$ is a regular language.

Problem. Suppose $A \subseteq \mathbb{N}[\frac{1}{q}]$ is automatic. Is then A^*, the submonoid generated by A, effectively automatic? Here, *effectively* means that given an automaton for $\iota(A)$, one can compute an automaton for $\iota(A^*)$.

Discussion. If A is in fact a subset of $\mathbb{N}$ (meaning only non-negative powers of q have non-zero coefficients), then this is well-known to be true: Every submonoid of $\mathbb{N}$ is ultimately periodic and thus automatic (and if given an automaton for $\iota(A)$, standard methods yield an automaton for $\iota(A^*)$). This means, if $A \subseteq \mathbb{N}$, then even the assumption that A be automatic is not needed for automaticity of $\iota(A^*)$. In the general case $A \subseteq \mathbb{N}[\frac{1}{q}]$, this assumption cannot be dropped: There exists a submonoid of $\mathbb{N}[\frac{1}{q}]$ that has an undecidable membership problem and is thus not automatic.

5 Discussion on future directions

5.1 Results of the plenary discussion

On the last day, there was a plenary discussion, moderated by Alexei Myasnikov, on future topics of research on Algorithmic Problems in Group Theory. This section provides a (somewhat restructured) short summary on the directions suggested by the participants.

1. Properties of algorithms
   a. What is the *complexity* of problems that are known to be decidable?
   b. A currently active field in algorithmics is *fine-grained complexity*, which studies the degrees of polynomials in polynomial time algorithms.
   c. Which problems have *practical* algorithms?
2. Equations: Solvability & estimates on solutions
   a. Diophantine problem for braid groups
   b. Diophantine problem for the Grigorchuk group
   c. Diophantine problem for $\mathrm{B}(n, m)$ (Burnside groups)
   d. Linear groups:
      i. Particular equations
      ii. Knapsack problem (and other parametric equations)
   e. Word equations with length constraints (which are examples of non-regular constraints)
3. Isomorphism problems
   a. Isomorphism problem for f.g. nilpotent groups.
   b. Isomorphism problem for f.g. polycyclic groups.
   c. What about quasi-isomorphism?
4. Reachability problems
   a. Post-Correspondence Problem for free groups: Given $(u_1, ..., u_n)$ and $(v_1, ..., v_n)$ in F, does there exist a word $w(x_1, ..., x_n) \neq 1$ so that $w(u_1, ..., u_n) = w(v_1, ..., v_n)$?
5. Reductions between problems
   a. For each group G, study reductions between decision problems: Which problems can be reduced to which, and with which kinds of reductions?
6. Formal languages
   a. Word problems: Alexei Myasnikov suggested that rather than formal language classes strictly from computer science (regular, context-free, context-sensitive, etc.), one should consider classes arising from algebra.
   Murray Elder pointed out that people had done work on this. An example is the notion of G-automata [3], where G is a group acting like a "counter". For instance, if $G = \mathbb{Z}^d$, then one obtains blind d-counter automata; if G is a free group of rank ≥ 2, G-automata are equivalent to pushdown automata. In a G-automaton, each transition is labeled by a letter from the alphabet to read, and a group element to multiply the counter by. A run of the automaton is valid if the product of its group elements is $1 \in G$. The resulting language classes have appealing closure properties: For instance, whether the word problem of a group H is accepted by some G-automaton does not depend on the chosen generating set for H.
   These automata have also been generalized to monoids and have been studied under the name *valence automata* [2].

b. Word problem via multiplication tables: Gilman proved a group G has a context-free multiplication table if and only if G is word hyperbolic [1].
   Here, a *multiplication table* (MT) is a language of triples of group elements written in some regular normal form. A triple (u, v, w) belongs to the language if $uvw = 1$ in the group. In other words, the entry in row u and column v is w. So we can ask: Which groups have a regular MT (the finite ones) or an indexed MT (many groups do, the Heisenberg group, solvable Baumslag-Solitar groups, etc.), a poly-context-free MT, or an MT accepted by a G-automaton?
c. Rename EDT0L: Should we find a different term for EDT0L languages? It was suggested to call them "rationally endomorphic" and to call ET0L "non-deterministic rationally endomorphic".

7. Probabilistic aspects

References

1 R. H. Gilman. On the definition of word hyperbolic groups. *Mathematische Zeitschrift* 242.3, p. 529–541, 2002.

2 H. Fernau and R. Stiebe. Sequential grammars and automata with valences. *Theoretical Computer Science* 276.1-2, p. 377–405, 2002.

3 V. Mitrana and R. Stiebe. The accepting power of finite automata over groups. *New Trends in Formal Languages*, p. 39–48, Springer, 1997.

Participants

- Yago Antolin
Universidad Autónoma de Madrid, ES
- Laurent Bartholdi
Institute of advanced Studies, ENS Lyon, FR & Universität Göttingen, DE
- Montserrat Casals-Ruiz
University of the Basque Country – Biblao, ES
- Laura Ciobanu
Heriot-Watt University – Edinburgh, GB
- Jordi Delgado Rodriguez
University of Porto, PT
- Volker Diekert
Universität Stuttgart, DE
- Andrew Duncan
Newcastle University, GB
- Bettina Eick
TU Braunschweig, DE
- Murray Elder
University of Technology – Sydney, AU
- Michal Ferov
University of Newcastle – Callaghan, AU
- Michael Figelius
Universität Siegen, DE
- Moses Ganardi
Universität Siegen, DE
- Albert Garreta Fontelles
University of the Basque Country – Biblao, ES
- Susan Hermiller
University of Nebraska – Lincoln, US
- Artur Jez
University of Wroclaw, PL
- Ilya Kapovich
City University of New York, US
- Ilya Kazachkov
University of the Basque Country, ES & Ikerbasque – Bilbao, ES
- Olga Kharlampovic
City University of New York, US
- Manfred Kufleitner
Loughborough University, GB
- Markus Lohrey
Universität Siegen, DE
- Alexei Myasnikov
Stevens Institute of Technology – Hoboken, US
- Volodymyr Nekrashevych
Texas A&M University – College Station, US
- Gretchen Ostheimer
Hofstra University – Hempstead, US
- Igor Potapov
University of Liverpool, GB
- Timothy Riley
Cornell University – Ithaca, US
- Paul E. Schupp
University of Illinois – Urbana Champaign, US
- Géraud Sénizergues
University of Bordeaux, FR
- Vladimir Shpilrain
City University of New York, US
- Rachel Skipper
Binghamton University, US
- Tatiana Smirnova-Nagnibeda
University of Geneva, CH
- Benjamin Steinberg
City University of New York, US
- Howard Straubing
Boston College, US
- Svetla Vassileva
Champlain Regional College – St. Lambert, CA
- Alina Vdovina
Newcastle University, GB
- Enric Ventura Capell
UPC – Barcelona Tech, ES
- Pascal Weil
University of Bordeaux, FR
- Armin Weiß
Universität Stuttgart, DE
- Georg Zetzsche
MPI-SWS – Kaiserslautern, DE