Final report for NKFIH K109185

We have published or submitted 28 papers with the help of the project's funding, many of them is a joint effort by multiple people from the grant, and some of them already have several citations. The main topics of these papers are the following:

(1) Extended and straight line complexity questions
(2) Combinatorics of words over finite semigroups
(3) Foundation for alternative models of computation
(4) Computational and model theoretic aspects of homogeneous relational structures
(5) Combinatorial problems

1. Extended and straight line complexity questions

We investigated aspects of the equivalence problem, and also the equation solvability problem in the paper "The complexity of the equivalence and equation solvability problems over meta-Abelian groups", which has been published in Journal of Algebra. Here, we show a general method to investigate meta-Abelian groups. To this end, we introduce the module sigma equivalence and module sigma equation solvability problems for finite, commutative, unital rings, and prove that for such rings these problems are decidable in polynomial time. Based on these results, we prove that the equivalence problem is decidable in polynomial time for semidirect products of Abelian groups. Further, for a vast class of meta-Abelian groups we prove that the equation solvability problem is decidable in polynomial time, as well. This method generalizes all earlier existing results for solvable, non-nilpotent groups.

Attila Földvári, the PhD student of Gábor Horváth, published two papers in computational complexity of the equation solvability and the equivalence problem over groups and rings. The complexity of the equation solvability problem is known for nilpotent groups, for not solvable groups and for some semidirect products of Abelian groups. In the first paper he provides a new polynomial time algorithm for deciding the equation solvability problem over certain semidirect products, where the first factor is not necessarily Abelian. The main idea is to represent such groups as matrix groups, and reduce the original problem to the equation solvability problem over the underlying field. Further, this new method is applied to give a much more efficient algorithm for equation solvability over nilpotent rings than previously existed.

In the other paper (published in Journal of Algebra) he investigates the computational complexity of nilpotent groups. So far the fastest algorithm to decide whether or not an equation of length n has a solution over a nilpotent group G was running in $O\left(n^{|G|^{|G|^{\cdots|G|^{|G|}}}}\right)$ time. Here the height of the tower is the nilpotency class of G. He proves that one can decide in $O\left(n^{\frac{1}{2}|G|^2\log|G|}\right)$ time whether an equation of length n has a solution over G. The key ingredient of the proof is to represent group expressions using the polycyclic presentation of p-groups.

In a submitted paper, Gábor Horváth and Attila Földvári provide a polynomial time algorithm for deciding the equation solvability problem over finite groups that are semidirect products of a p-group and an Abelian group. As a consequence, we obtain a polynomial time algorithm for deciding the equivalence problem over semidirect products of a finite nilpotent group and a finite Abelian group. The key ingredient of the proof is to represent group expressions using a special polycyclic presentation of these finite solvable groups.

We have obtained several results about the structure of polynomials over rings, for example in the published paper "Polynomial equivalence of finite rings." We prove that $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p[t]/(t^n)$ are polynomially equivalent if and only if $n \leq 2$ or $p^n = 8$. For the proof, employing Bernoulli numbers, we explicitly provide the polynomials which compute the carry-on part for the addition and multiplication in base p. As a corollary, we characterize finite rings of p^2 elements up to polynomial equivalence.

Gábor Horváth with his MSc and BSc students investigated polynomial functions over commutative finite rings and published two papers. In the paper 'Polynomial functions over finite commutative rings' we prove a necessary and sufficient condition for a function being a polynomial function over a finite, commutative, unital ring. Furthermore, we give an algorithm running in quasilinear time that determines whether or not a function given by its function table can be represented by a polynomial, and if the answer is yes then it provides one such polynomial.

For the results in the second paper, Gábor Horváth's BSc students won the first prize in the final of the Hungarian National Scientific Competition (OTDK) in 2017. Let $PPol(R)$ denote the group of permutation polynomial functions over the finite, commutative, unital ring R under composition. We generalize numerous results about permutation polynomials over Z_{p^n} to local rings by treating them under a unified manner. In particular, we provide a natural wreath product decomposition of permutation polynomial functions over the maximal ideal M and over the finite field R/M. We characterize the group of permutation polynomial functions over M whenever the condition $M^{|R/M|} = \{0\}$ applies. Then we derive the size of $PPol(R)$, thereby generalizing the same size formulas for Z_{p^n}. Finally, we completely characterize when the group $PPol(R)$ is solvable, nilpotent, or Abelian.

Furthermore, Gábor Horváth is a coauthor in the published paper "Non-synthesizable varieties." A variety is a closed translation invariant linear subspace in the vectorspace of continuous functions from a compact group to the complex numbers. We say that spectral synthesis holds for a variety if all its finite dimensional subvarieties generate a dense subspace in it. Using a ring theoretic approach we reprove that over any Abelian group of infinite torsion free rank there exists a variety for which spectral synthesis does not hold.

2. Combinatorics of words over finite semigroups

Kamilla Kátai-Urbán, András Pongrácz and Csaba Szabó have finished their work on the fine- and generative spectra of all varieties of monounary algebras. This result is a follow-up on our earlier papers "The number of rooted trees of given depth" and "The number of monounary algebras". In this paper, we give asymptotic or log-asymptotic estimations for the growth rate of the fine- and generative spectra of all varieties of monounary algebras. These results provided infinitely many examples of spectra that is bigger than any polynomial and smaller than any exponential function. Before this paper, only some sporadic examples were known with such asymptotic behaviour.

The question of whether finite inverse monoids admit a finite F-inverse cover was first proposed by Henckell and Rhodes, and has become one of the biggest open problems regarding finite inverse semigroups since. K. Auinger and M. Szendrei have translated the problem to the language of group varieties and graphs. Gábor Horváth, Kamilla Kátai-Urbán and Csaba Szabó started to work on F-inverse cover problem with Mária Szendrei and Nóra Szakács. We investigated whether varieties of nilpotent groups satisfy the conditions, and we did not find a counterexample in this case.

3. Foundation for alternative models of computation

We considered functionally complete groups in the paper "Length of polynomials over finite groups", which has been published in Journal of Computer and System Sciences. Here, we study the length of polynomials over finite simple non-Abelian groups needed to realize Boolean functions. We apply the results for bounding the length of 5-permutation branching programs recognizing a Boolean set. Moreover, we present upper and lower bounds on the length of shortest polynomials computing an arbitrary n-ary Boolean or general function on these groups, or a function given by another polynomial. Further, we provide upper and lower bounds for the length of shortest realizing polynomials for arbitrary polynomial functions over nilpotent groups.

With several coauthors we investigated interaction computing in the paper "Symmetry structure in discrete models of biochemical systems: natural subsystems and the weak control hierarchy in a new model of computation driven by interactions", which has been published in the prestigious Philosophical Transactions of the Royal Society of London, and is partly an application of the results published in "Length of polynomials over finite groups". A biological system can be naturally described by a finite state automaton, and one can consider its corresponding transition monoid. The decomposition theorem of Krohn and Rhodes states that this monoid is a divisor (homomorphic image of a submonoid) of the wreath product of aperiodic semigroups and simple groups. Further, the simple groups occurring as factors of this wreath product are divisors of the transition monoid. Now, if any of these simple factors is nonabelian, then the biological system is capable (in theory) to compute an arbitrary function. We examine such biological examples according to their mathematical behaviour. Moreover, we set the mathematical foundations of the recursively modelled interaction machines.

Gábor Horváth with two coauthors investigated the maximal subgroups and the complexity of the flow semigroup of digraphs. The paper is published in International Journal of Algebra and Computation. The flow semigroup, introduced by John Rhodes, is an invariant for digraphs and a complete invariant for graphs. We refine and prove Rhodes's conjecture on the structure of the maximal groups in the flow semigroup for finite, antisymmetric, strongly connected graphs. Building on this result, we investigate and fully describe the structure and actions of the maximal subgroups of the flow semigroup acting on all but k points for all finite digraphs and graphs for all $k \geq 1$. A linear algorithm is presented to determine these so-called 'defect k groups' for any finite (di)graph. Finally, we prove that the Krohn-Rhodes complexity of the flow semigroup of a 2-vertex connected (and strongly connected di)graph with n vertices is $n-2$, completely confirming Rhodes's conjecture for such (di)graphs.

4. Computational and model theoretic aspects of homogeneous relational structures

András Pongrácz has submitted 4 papers on reducts of different homogeneous structures. Three of these are already published, another one is still in review, waiting for the editor to make a final decision.

We studied reducts of the homogeneous binary branching tree with several coauthors. A partial order is called semilinear if the upper bounds of each element are linearly ordered and any two elements have a common upper bound. There exists, up to isomorphism, a unique countable existentially closed semilinear order, which we denote by S. We study the reducts of S, that is, the relational structures with domain S, all of whose relations are first-order definable in S. Our main result is a classification of the model-complete cores of the reducts of S. From this, we also obtain a classification of reducts up to first-order interdefinability, which is equivalent to a classification of all permutation groups that contain the automorphism group of S and are closed in the full symmetric group with respect to the point-wise convergence topology.

In a submitted paper, the Henson graphs are considered. For $n > 2$, let $(H_n; E)$ denote the n-th Henson graph, i.e., the unique countable homogeneous graph with exactly those finite graphs as induced subgraphs that do not embed the complete graph on n vertices. We show that for all structures with domain H_n whose relations are first-order definable in $(H_n; E)$ the constraint satisfaction problem is either in P or is NP-complete. We moreover show a similar complexity dichotomy for all structures whose relations are first-order definable in a homogeneous graph whose reflexive closure is an equivalence relation. Together with earlier results, in particular for the random graph, this completes the complexity classification of constraint satisfaction problems of structures first-order definable in countably infinite homogeneous graphs: all such problems are either in P or NP-complete. An extended abstract appeared in the proceedings of International Colloquium on Automata, Languages, and Programming (ICALP 2016, Rome), which is one of the strongest conferences in computer science.

An equality language is a relational structure with infinite domain whose relations are first-order definable in equality. In the paper "The complexity of counting quantifiers on equality languages" we classify the extensions of the quantified constraint satisfaction problem over equality languages in which the native existential and universal quantifiers are augmented by some subset of counting quantifiers. In doing this, we find ourselves in various worlds in which dichotomies or trichotomies subsist. This paper is published in Theoretical Computer Science, ranked Q1 in computer science, and an extended abstract appeared in the proceedings of Computability in Europe (CiE 2016, Paris), a very prestigious conference.

The published paper "Reducts of the random partial order" was one of the first applications of a theoretical method for classifying reducts of a structure up to first-order interdefinability. The paper already has 6 independent citations, and it appeared in Advances in Mathematics, which is a Q1 ranked journal in Mathematics commonly regarded as one of the best general journals.

András Pongrácz with two coauthors initiated a new topic, automatic continuity and homeomorphicity of clone homomorphisms and clone isomorphisms. This is applicable in theoretical computer science. In the paper "Projective clone homomorphisms" the authors investigate the existence of a continuous clone homomorphism from a given clone to the clone of projections, provided that a (not necessarily continuous) homomorphism exists. The non-existence of a clone homomorphism to the trivial clone is usually easy to verify by certain identities that hold in the clone. On the other hand, the existence of a continuous clone homomorphism to the trivial clone implies that the corresponding CSP problem is NP-complete. In this paper, it is shown that the two problems (existence of a homomorphism or a continuous homomorphism to the trivial clone) are equivalent for a wide class of clones. The paper is accepted in Journal of Symbolic Logic, which is ranked Q1 in two categories, logic and philosophy, as well. This paper is the natural continuation of another one with the same set of authors, which was published in Transactions of the American Mathematical Society, another Q1 ranked journal in Mathematics and Applied Mathematics, as well.

In the paper "Functional reducts of Boolean algebras" Csaba Szabó together with his students examines the first order reducts of the homogeneous Boolean-algebra. Let $\mathbf{B} = (B, \wedge, \vee, 0, 1, \neg)$ denote the countable atomless Boolean algebra. It is known that this structure is unique up to isomorphism. It is easy to check that $\mathbf{B}$ is a homogeneous and universal object in the class of countable Boolean algebras and is ω-categorical which means that every countable structure with the same first order theory is isomorphic to $\mathbf{B}$. In the paper 37 first-order definable reducts of $\mathbf{B}$ is described, and at the moment it looks hopeless to describe all of them. Hence, the following definition is introduced: For an algebra $\mathfrak{A} = (A, f_1, \ldots, f_n)$ the algebra $\mathfrak{B} = (A, t_1, \ldots, t_k)$ is called a functional reduct if each t_j is a term function of $\mathfrak{A}$. The functional reducts of the countable homogeneous Boolean algebra are up to first-order interdefinability. There are 13 such reducts and all of them are described via their structures and group of automorphisms, and, surprisingly, they form a lattice among all reducts. The paper is not pointing exactly to the verification of Thomas' conjecture because, although $\mathbf{B}$ is an algebra of finite signature, it cannot be presented on a finite relational language.

In the paper "Permutation groups containing infinite linear groups and reducts of infinite dimensional linear spaces over the two element field" the same trio describes the first order reducts of the countably infinite dimensional vectorspace over the two element field. The ideas involve mostly group theoretic arguments, and it is shown, that there are four supergroups of the automorphism group of the vectorspace in the symmetric group, implying two nontrivial reducts.

The results of these two papers have been published in Hungarian, as well, in 4 papers in Matematikai Lapok, to popularize Mathematical research.

In the paper "Infinitely many reducts of homogeneous structures" it is shown that the countably infinite dimensional pointed vector space (the vector space equipped with a constant) over a finite field has infinitely many first order definable reducts. This implies that the countable homogeneous Boolean-algebra has infinitely many reducts. Although the result is surprising, it is not a rejection of Thomas' conjecture, As we mentioned earlier these structures are of finite signature, but not of finite relational language. The age of the reducts are strongly connected to the Reed – Muller codes.

5. Combinatorial problems

The paper "Compositions of complements of graphs" is in the line of papers counting trees. Connected partitions of graphs (as graph compositions) are natural generalizations of compositions of integers and partitions of the finite sets. A connected partition of a graph G is a partition of its vertex set such that each induced subgraph is connected. In earlier research it was called connected compositions of graphs. We find a polynomial, the defect polynomial of the graph that describes the connected partition numbers of the complements of graph with respect to any complete graph. The defect polynomial is calculated for several classes of graphs as cycles or matchings.

The paper "On the Complexity and Topology of Scoring Games: of Pirates and Treasure" is about the combinatorial game Pirates and Treasure, which is played between two players, Left and Right, on a finite, simple, undirected weighted graph. The vertices of the graph correspond to islands, and a weight function on the vertices indicates the amount of treasure the island has. Left player has n ships, Right player has m ships, in pre-defined vertices. Each turn, the current player moves one of his ships into an adjacent, non-visited vertex, and the weight of the vertex is added to the current points of the player. If a player in his turn cannot move, the game ends. Left moves first. The player who collects more treasures (points) than his opponent wins the game. It is shown that it is $PSPACE$-complete to decide whether or not Left has a winning strategy in the Pirates and Treasure game. Moreover, it is also $PSPACE$-complete to decide whether or not Left has a winning strategy when we assume that the two players are moving in different components of the graph. For a fixed graph G, topological and convexity properties of weightings are analyzed. Among other things it is shown that the winning space of Left is connected, but not always convex.

András Pongrácz has recently started to investigate combinatorial problems related to Markov chains.

He recently submitted his first paper in this area "Discordant voting for the knights of the round table". This is about a particular example of the so-called discordant push and pull voting protocols, namely on cycle graphs. Given a graph whose vertices are coloured red and blue, we define a process that is divided into rounds. In each round we identify the discordant vertices, i.e., those which have a neighbour of the opposite colour. One such vertex u is picked uniformly at random, and then we pick one of its neighbours v of the opposite colour uniformly at random, and change the color of v to that of u. This way we obtain the discordant push protocol. The pull process is similar, except in the end of the above description, it is the colour of u that is changed. The processes terminate when a consensus is reached, that is, all vertices have the same colour; the expected time this takes is denoted by T. It was proven with advanced methods that on the n-cycle $T \leq 33n^2$ from any initial state, but computer simulations suggested that the worst case is when red and blue vertices alternate, and that in this case T is asymptotically $n^2/4$. We have verified this asymptotic estimation by showing that from a state with b blue and r red vertices (no matter how they are distributed in the cycle) the expected time to reach consensus is $T = br + O(n^{3/2})$. The improvement is achieved by an elementary method. Furthermore it is shown in the paper that the probability that the colour blue wins is close to the proportion of the blue vertices in the initial state. More precisely, $|P(\text{blue wins}) - p/n| \leq k/4n$ where k is the number of maximal monochromatic arcs in the initial state. Similar results are shown for the random graph $G(n, p)$, as well. The paper version is not yet accepted, but an extended abstract will be published in the proceedings of ICCSE'18.

The other submitted paper “Voting protocols on the star graph” is a continuation of this project. We obtained asymptotic estimations for the expected runtime of the discordant push and pull protocols on the star graph. The star graph is a particularly interesting case in terms of such protocols. Usually, the push protocol is much faster than the pull protocol. However, in case of the star graph the expected time to reach consensus with the discordant push protocol is about $\log n$ times bigger as it is for the discordant pull protocol.