Algebra and algorithms

January 21, 2021

Explicit isomorphisms

We proposed a randomized polynomial time algorithm which finds an explicit isomorphism between central simple algebras over pure transcendental extensions of degree one of finite fields. While an analogous result over the rationals is only known for algebras of constant dimension, this algorithm works efficiently for an arbitrary dimension. The result, among others, has interesting applications to factorization problems in skew polynomial rings. Our result has appeared in the article IKR18FCM.

We developed a randomized polynomial time algorithm for computing isometrics of quadratic forms over the aforementioned function fields. The new algorithm is based on a suitable splitting of the form into two forms and finding a common value the two forms both represent. The result makes use of an effective formula on the number of fixed degree irreducible polynomials in a given residue class over finite fields. The above method is then applied for computing a Witt decomposition of a quadratic form, for computing an explicit isometry between quadratic forms, and finding zero divisors in quaternion algebras over quadratic extensions over these fields. We reported on our result in the article IKR19FFA.

Péter Kutas defended his PhD. thesis entitled The Explicit Isomorphism Problem at the Central Europen University in 2017. His supervisors were Gábor Ivanyos and Lajos Rónyi.

We proposed various zero knowledge protocols based on the algorithmic problem of finding isomorphisms between central simple algebras over number fields given by structure constants. We also designed a protocol which is based on the hardness of finding an element with a prescribed minimal polynomial in a central simple algebra given by structure constants. This protocol allows arbitrarily long challenges and thus can be turned into a digital signature scheme. These results are in the manuscript KK2019arX.

We applied techniques from the theory of algebras with involutions to computational problems such as constructing simultaneous isometry of tuples of quadratic forms. Over a finite base field we proposed a randomized polynomial time algorithm to compute an explicit solution to this problem. The result can be applied to computing isomorphisms between certain nilpotent groups of class two and to attack an authentication scheme - proposed by Patarin - based on the problem called Isomorphism of Polynomials with One Secret (IP1S). We reported on these results in the preliminary conference paper IQ18PS and then in the full journal article IQ19JC.

Mathematical and algorithmic problems in communication egineering

In TRVGy17IEEE we investigated Shared Risk Link Groups (SRLGs) in communication networks. A Shared Risk Link Group (SRLG) in the setting of communication networks is a failure the network is prepared for, which contains a set of links subject to a common risk of single failure. During planning a backbone network the list of SRLGs must be defined very carefully, because leaving out one likely failure event will significantly degrade the observed reliability of the network. In practical cases the list of SRLGs is simply defined as the list of all single link or node failures. Regional failures manifested at multiple locations of the network, which are physically close to each other. A common belief is that the number of possible regional failure events are too large to be listed as SRLGs. In the paper they have shown the opposite if the size of the regional failure is bounded. A fast systematic approach is given to generate the list of SRLGs that cover every possible regional failure of a given size, and shown that the list has a modest size in terms of the basic parameters of

the network (number of nodes, number of edge intersections, maximal number of links in a regional failure). Extensive simulations suggest practical relevance of the approach.

In the paper BTPRB-KM17TN we proposed a new proactive recovery scheme against single edge failures for unicast connections in transport networks. The new scheme is a generalisation of diversity coding where the source data AB is split into two parts A and B and three data flows A, B and their exclusive OR (XOR) $A \oplus B$ are sent along the network between the source and destination node of the connection. By ensuring that two data flows out of the three always operate even if a single edge fails, the source data can be instantaneously recovered at the destination node. In contrast with diversity coding we do not require the three data flows to be routed along three disjoint paths; however, in our scheme a data flow is allowed to split into two parallel segments and later merge back. Thus, our Generalised Diversity Coding (GDC) scheme can be used in sparse but still 2-connected network topologies.

In the KHTRR18IEEE paper we suggested a new EGH filter to replace the hash functions with simple functions by using prime numbers. We generalized a construction of Eppstein Goodrich and Hirschberg. The new EGH filter ensures a false positive free zone for a subset of elements in a finite set. We generalize the filter to support listing of the elements.

We give several algorithms to determine the integer roots of a polynomial of degree d with integer coefficients. As an application, we study Bloom filters and their variants, which are widely used as space efficient probabilistic data structures for representing set systems and are very popular in networking applications. We propose a data structure, called EGH filter, that supports the Bloom filter operations and besides it can guarantee false positive free operations for a finite universe and a restricted number of elements stored in the filter. We evaluate the performance of our data structure in comparison with the traditional Bloom filters. Our solution is based on recently developed combinatorial group testing techniques.

Given the increase in natural disasters and malicious attacks with geographically extensive impact, considering only independent single link failures is often insufficient. In the paper TVHBHKR18IEEE, we built a stochastic model of geographically correlated link failures caused by disasters, in order to estimate the hazards a network may be prone to, and to understand the complex correlation between possible link failures. We developed a pre-computation process, which enables us to succinctly represent the joint probability distribution of link failures. In particular, we generated a moderate sized data structure to represent the joint failure probability of any set of links.

In PBTB-KKR20TN we contiuned our earlier work on generalized diversity coding as a proactive recovery scheme against single edge failures for unicast connections in transport networks. In this paper, we investigated the corresponding routing problem to calculate capacity-efficient routes for the necessary subflows. We propose a polynomial-time algorithm for topologies without capacity constraints on the links and without capability limitations of the nodes. We show that with node limitations the presented algorithm (as well as a minimum cost disjoint path-pair) provides a 4/3-approximation for the routing problem. Some related simulation results are also presented.

In TRVGy20TN continued our earlier work on regional failures and extended the results which appeared in INFOCOM 17. Regional failures often cause the breakdown of multiple elements of the network, which are physically close to each other. In the first article, we showed that operators should prepare a network for only a small number of possible regional failure events. In particular, we gave an approach to generate the list of shared risk link groups (SRLGs) that hit by a possible circular disk shaped disaster of a given radius r. We proved that this list has manageable size. We proposed a polynomial algorithm to enumerate the list of SRLGs and showed that its worst-case time complexity is asymptotically optimal under some practical restrictions. Finally, through extensive simulations, we demonstrated that this list in practice has only a linear size.

In VTHBHKOVR21IEEE (accepted in IEEE JSAC, a C1 journal with impact factor over 10) we considered in detail the computational aspects of the problem. We proposed efficient data structures and algorithms to implement the probabilistic models developed earlier. We gave numerical evaluation of the proposed methods on the basis of real seismic hazard data.

In THPHR21IEEE we considered the task of reducing the vulnerability of communication networks against regional failures, which are failures of multiple nodes and links in a region due to a natural disaster.

The paper defines a novel design framework, called Geometric Network Augmentation (GNA), which determines a set of node pairs and the new cable routes to be deployed between each of them to have the surviving network always remain connected when a regional failure of a given size occurs. We provide mathematical analysis and efficient heuristic algorithms that are built on the latest computational geometry tools and combinatorial optimization techniques. Through extensive simulation we show that augmentation with just a small number of new cable routes will achieve the desired resilience.

Multi-sense word embeddings (MSEs) model different meanings of word forms with different vectors. In BKMN16ProcEVSR we proposed two new methods for evaluating MSEs by their degree of semantic resolution, measuring the detail of the sense clustering. One method is based on monolingual dictionaries, and the other exploits the principle that words may be ambiguous as far as the postulated senses translate to different words in some other language.

In distributional semantics we derive the embedding from a corpus, and the corpus is just a sample from the entire distribution. We analyze the noise of the obtained vectors and other sources of noise, and how much the considerations of compositionality are affected by noise. This is described in the poster BKKN16ESSL.

The distribution of sentence length in ordinary language is not well captured by the existing models. In BK19MOL we surveyed previous models of sentence length and presented our random walk model that offers both a better fit with the data and a better understanding of the distribution. We developed a generalization of KL divergence, discussed measuring the noise inherent in a corpus, and presented a hyperparameterfree Bayesian model comparison method that has strong conceptual ties to Minimal Description Length modeling. The models we obtained require only a few dozen bits, orders of magnitude less than the naive nonparametric MDL models would.

We also investigated the learning of weights of a finite state automaton for morphological analysis. We developed a large-scale optimizer which can learn the weights of a full HFST model even for morphologically rich languages (Finnish, Hungarian). This has not been published yet, but we developed a software BK19GITHUB.

Some combinatorial applications of commutative algebra and algebraic varieties

In DKMSz16MN we established connection between functions on Newton-Okounkov bodies and Seshadri constants of line bundles on algebraic surfaces.

In DKMSz16AM we related the Segre-Harbourne-Gimigliano-Hirschowitz Conjecture to the rationality of one-point Seshadri constants on blow ups of the projective plane. We also studied the Segre-Harbourne-Gimigliano-Hirschowitz Conjecture.

In an earlier work the Hegedűs and Rónyai described Gröbner bases of the ideal of polynomials over a field, which vanish on the set of characterisic vectors of the complete d-unifom set family over the ground set $[n]$. In particular, it turns out that the standard monomials of the above ideal are ballot monomials. Here they give a partial extension of this fact. A set family is a linear Sperner system if the characteristic vectors satisfy a linear equation with positive integer coefficients a_i. In the paper HR18AU it is proved that the lexicographic standard monomials for linear Sperner systems are also ballot monomials, provided that the sequence a_i is nondecreasing. As an application, a conjecture of Frankl is confirmed in the special case of linear Sperner systems.

A set system F shatters a given set S if all subsets of S can be obtained as the intersection of S with a suitable elment of F. The Sauer-Shelah lemma states that in general, F shatters at least $|F|$ s ets. A set sytstem is called shattering-extremal if it shatters exactly $|F|$ sets. In earlier work an algebraic characterization of shattering-extremal set systems was given, which offered the possibility to generalize the notion of extremality to general finite vector systems. In MR17ENDM we generalized the results obtained for set systems to this more general setting. An application is also given.

Projective norm graphs $NG(q,t)$ provide tight constructions for the Turán number of a complete bipartite graphs $K_{t,s}$ with $s > (t-1)!$. The determination of the largest integer s_t, such that the projective norm

graph $NG(q,t)$ contains K_{t,s_t} for all large enough prime powers q, is an important open question with far-reaching general consequences. We settled the case $t = 4$. Along the way we also developed methods to count the copies of any fixed 3-degenerate subgraph, and found that projective norm graphs are quasirandom with respect to this parameter. Some of these results also extended the work of Alon and Shikhelman on generalized Turán numbers. This was published in BMRSz19AMUC, which is the volume of the conference EUROCOMB 2019. At this conference T. Mészáros gave a talk with title "Exploiting projective norm graphs".

In an earlier paper we solved a question posed by J. E. Littlewood: we proved the existence of seven mutually touching infinite cylinders of radius 1 in the Euclidean 3-space. In the conference paper BRT-LL17MFIOOK we explained this result and discussed the related problems. It is very likely that there exists a "large" algebraic curve of solutions. We have some progress in this direction.

Recently Petrov and Pohoata have developed a new algebraic method which combines the Croot-Lev-Pach Lemma from additive combinatorics and Sylvester's Law of Inertia for real quadratic forms. In the paper HR20M we extended their work and proved upper bounds for the size of s-distance sets in various real algebraic sets. This way we obtained a novel and short proof for the bound of Delsarte-Goethals-Seidel on spherical s-distance sets and a generalization of a bound by Bannai-Kawasaki-Nitamizu-Sato on s-distance sets on unions of spheres. In our arguments we used the method of Petrov and Pohoata together with some Gröbner basis techniques.

In the paper MN19DCC, the authors gave a detailed description of the combinatorial and geometric structure of the sets of full points in abstract unitals of finite order. The results use heavily the concept of full points of abstract unitals, that has been introduced by Korchmáros, Siciliano and Szőnyi as a tool for the study of projective embeddings of abstract unitals. Using the GAP package UnitalSZ MN18GAP it was possible to compute the full points and the corresponding group of perspectivities for many small abstract unitals. In some cases, dual 3-nets, embedded in abstract unitals of order 4 were found, both of classical and non-classical type.

In N20arX it was shown that the Ree unital $R(q)$ has an embedding in a projective plane over a field F if and only if $q = 3$ and $GF(8)$ is a subfield of F. In this case, the embedding is unique up to projective linear transformations. Besides elementary calculations, the proof uses the classification of the maximal subgroups of the simple Ree groups.

In KNT19IEEE a class of algebraic-geometry codes defined over the Hermitian curve in the finite projective plane of order q^2 was studied. It was proved that for a range of parameters, these codes have better minimum distance compared with true values of 1-point Hermitian codes. Moreover, for a subrange of these parameters, it was shown that the automorphism group of the codes is isomorphic to $PGU(3,q)$. The method is based on the explicit determination of bases of Riemann-Roch spaces, and the geometry of the intersections of the Hermitian curves $H(q)$ and $H(q^3)$.

In KN2020AC we studied the behavior of the true dimension of the subfield subcodes of Hermitian codes. Our motivation was to use these classes of linear codes to improve the parameters of the McEliece cryptosystem, such as key size and security level. The McEliece scheme is one of the promising alternative cryptographic schemes to the current public key schemes since in the last four decades, they resisted all known quantum computing attacks. By computing and analyzing a data collection of true dimensions of subfield subcodes, we concluded that they can be estimated by the extreme value distribution function. These theoretical results were motivated by numerical experiments using the GAP package HERmitian KN19GAP by the same two authors.

In the paper KN21AIMS the authors presented new values of the true dimension of subfield subcodes of 1-point Hermitian codes, including the case when the subfield is not binary. Hermitian codes are algebraic-geometric (AG) codes defined over the Hermitian curve over the finite field $GF(q^2)$. Their decoding algorithms can correct up to $(d-1)/2$ errors, where d is Goppa's designed minimum distance. Subfield subcodes of AG codes are good candidates for the use in post-quantum cryptosystems, provided their true parameters such as dimension and minimum distance can be determined.

In MN21DAM a new way to obtain Steiner 2-designs from known ones was presented. Starting with a block B of a 2-design D one forms the incidence structure D_B whose points are those of D not in B and whose blocks are those of D meeting B exactly once. Then a resolution of D_B is used in order to provide a remarkably simple construction (paramodification) of another 2-design. By iteratively performing paramodifications on known unitals of order $q = 3$ or 4, computationally 173 new examples are obtained with $q = 3$ and 25641 with $q = 4$.

In KN21PDM it was shown that no orthogonal arrays $OA(16u, 11, 2, 4)$ exist with $u = 6$ and $u = 7$. This solves an open problem of the NSUCRYPTO International Olympiad in Cryptography 2018. This result allows us to determine the minimum weights of certain higher-order correlation-immune (CI) Boolean functions. Low weight t-CI Boolean functions have practical importance in cryptography, since they resist the Siegenthaler attack.

Algorithms for discovering and exploiting hidden algebraic properties

We developed a deterministic polynomial time algorithm for computing the noncommutative rank of a linear matrix. (A linear matrix is a matrix whose entries are linear polynomials in several variables and its noncommutative rank is the rank of the matrix, considered as a matrix over the free skewfield generated by the variables.) Our result was one of the key contributions to a recent breakthrough in computational invariant theory with remarkable consequences in other areas of mathematics. In IQS17CC we reported on a weaker version of our result. The final, stronger version appeared in the conference paper IQS17LIPI and in the journal article IQS18CC.

In 2018 there was a workshop at the Institute for Advanced Study in Princeton on the breakthrough where Gábor Ivanyos was an invited speaker the above result and its background.

On the result Gábor Ivanyos also gave an invited talk at the minisymposium on Efficient Algorithms for Geometric Invariant Theory organized in the framework of the SIAM Conference on Applied Algebraic Geometry (SIAMAG 19) (Bern, Switzerland 9-13 July, 2019). The costs of travel were covered by this NKFIH grant.

The paper IR18EN is a brief news item on our research related to quantum algorithmic applications of some weaker, but algorithmically effective versions of the Chevalley-Warning theorem from number theory.

We presented an algorithm for learning a linear function from a sample whose distribution depends only on the value taken by the function. The complexity is simply exponential in the number of values taken by the sample elements with nonzero probability and polynomial in the rest of the parameters. As an application, we obtained polynomial-time quantum algorithms for certain generalized shift problems, including, as a special case, the hidden subgroup problem in a class of metabelian groups. We reported on these results in IPS18LIPI.

We presented a detailed description of our methods (basic ideas appeared in an earlier conference paper) to determine the complexity of constraint satisfaction problems in a certain non-conventional computational model and extended them to cover certain interesting problems such as deciding graph properties (IKQSS18JCSS).

Representations of semigroups, groups and algebras

In N16ACTA we characterized and constructed left equalizer simple semigroups. By the left equalizer of a non-empty subset H of a semigroup S we mean the set of all elements $s \in S$ with condition $|xH| = 1$. A semigroup S is called left equalizer simple if, for an arbitrary non-empty subset H of S, the left equalizer of H is either empty or is equal to S. In the paper we characterize and construct left equalizer simple semigroups. The importance of the results of our paper is shown by a result of P.M. Cohn published in 1956: a semigroup S is embeddable into a left simple semigroup without idempotents if and only if S is a left equalizer simple semigroup which does not contain any idempotent elements.

Let S be a semigroup and F be a field. For an ideal J of the semigroup algebra $F[S]$ of S over F, let ϱ_J denote the restriction (to S) of the congruence on $F[S]$ defined by the ideal J. In the paper NZ16CA we shown that if S is a semilattice or a rectangular band then $J \mapsto \varrho_J$ is a homomorphism of the semigroup

$(Con(F[S]);\circ)$ into the relations semigroup $(B_S;\circ)$ if and only if S is a congruence permutable semigroup, that is, $\alpha\circ\beta=\beta\circ\alpha$ is satisfied for all congruences α and β of S, where $\circ$ denotes the usual composition of binary relations.

In N16IJA we proved that, for any similar algebraic structures A_i, $i\in I$, the ultraproduct of the $\wedge$-semilattices of all congruences of A_i, $i\in I$ is embeddable into the $\wedge$-semilattice of all congruences of the ultraproduct of A_i $i\in I$. We applied this result for factor algebras and for ultrapowers.

In Z16ACTA we gave an upper bound for $|Y|$, where Y is a subsemilattice of a finite semilattice indecomposable semigroup. Our investigation was based on our new results proved in this paper which characterize finite semilattice indecomposable semigroups with a zero by only using the properties of its semigroup algebra.

The notion of the graphon (a symmetric measurable fuzzy set of $[0,1]^2$) was introduced by L. Lovász and B. Szegedy in 2006 to describe limit objects of convergent sequences of dense graphs. In the paper N18arX we proved that the set of all fuzzy sets of $[0,1]^2$ is a right regular band with respect to the operation $\circ$ defined by

$$(f\circ g)(s,t)=\vee_{(x,y)\in[0,1]^2}(f(x,y)\wedge g(s,t));\quad (s,t)\in[0,1]^2,$$

and the set of all graphons is a left ideal of this band.

An element a of a semigroup S is said to be a middle unit of S if $xay=xy$ is satisfied for every $x,y\in S$. In the paper NN20IJA we constructed semigroups in which every element is a middle unit.

Let σ be a binary relation on a non empty finite set A. Let $P_\sigma(A)$ denote the probability that a randomly selected couple $(a,b)\in A\times A$ belongs to σ. In the paper NT20arX we investigated $P_\sigma(A)$ when A is a semigroup and σ is the kernel of the right regular matrix representation of S.

In the paper N20CMUC we gave a semigroup theoretical characterization of congruence permutable G-sets (G is a group).

In the paper NT19arX we investigated the right regular representation of special Rees matrix semigroups without zero over the members of sequences

$$S/\alpha^{(0)},S/\alpha^{(1)},\dots,S/\alpha^{(n)},\dots$$

of factor semigroups of semigroups S, where $\alpha^{(0)}=\alpha$ is an arbitrary congruence on S and, for a non-negative integer n, $\alpha^{(n+1)}$ is the congruence on S defined by: $(a,b)\in\alpha^{(n+1)}$ if and only if $(xa,xb)\in\alpha^{(n)}$ for all $x\in S$. We proved further results on the considered type of Rees matrix semigroups.

A mapping from a set S to the unit interval $[0,1]$ is called a fuzzy set of S. It is known that the set $\mathcal{F}(S)$ of all fuzzy sets of a semigroup S is a semigroup under the operation $\circ$ defined by

$$(f\circ g)(s)=\begin{cases}\vee_{s=xy}(f(x)\wedge g(y)), & \text{if } s\in S^2\\ 0, & \text{otherwise.}\end{cases}$$

For every element a of a semigroup S, we defined an operation $\star$ on the set $\mathcal{F}^*(D_a)$ of all fuzzy sets of the set D_a of all divisors of a in S, and proved that this operation is associative. The main result of the paper N19arX is that, for every semigroup S, the semigroup $(\mathcal{F}(S);\circ)$ is a subdirect product of the semigroups $(\mathcal{F}^*(D_a);\star)$, $a\in S$.

In 2018 Attila Nagy successfully defended the theses of his dissertation "Congruence permutable semigroups in special classes of semigroups" submitted to the Hungarian Academy of Sciences for the degree "Doctor of the HAS".

In 1956, P.M. Cohn gave necessary and sufficient conditions for a semigroup to be embeddable into a left simple semigroup. The conditions differ essentially according to whether or not the semigroup contains an idempotent element. The main purpose of the paper N19PP1 was to show how to construct idempotent-free semigroups which can be embedded into left simple semigroups.

In the paper N19PP we focused on Rees matrix rings $\mathcal{M}(R; I, \Lambda; P)$ in which the set I has exactly one element. For a ring R, let $Ann_r(R)$ and $(Ann_r(R) :_r R)$ denote the right annihilator of R and the right colon ideal of $Ann_r(R)$, respectively. The main result of our paper is that, for every choice function P defined on the collection of all cosets of $Ann_r(R)$, the factor ring of the Rees matrix ring $\mathcal{M}(R; I, R/Ann_r(R); P)$ modulo its right annihilator is isomorphic to the Rees matrix ring

$$\mathcal{M}(R/(Ann_r(R) :_r R); I, R/Ann_r(R); P'),$$

in which P' is defined by

$$P' : a + Ann_r(R) \mapsto a + (Ann_r(R) :_r R);\ a \in R.$$

In 2019 Márton Zubor, a PhD student of Attila Nagy, defended successfully his PhD. The title of his thesis was "Commutative substructures of special algebraic structures".

The aim of the paper HSZZ17JA was to generalise the notion of p-stability (p is an odd prime) in finite group theory to fusion systems. We first compared the different definitions of p-stability for groups and examined properties of p-stability concerning subgroups and factor groups. Motivated by Glauberman's theorem, we studied the question of how $Qd(p)$ is involved in finite simple groups. We proved that with a single exception a simple group involving $Qd(p)$ has a subgroup isomorphic to either $Qd(p)$ or a central extension of $Qd(p)$ by a cyclic group of order p. Then we defined p-stability for fusion systems and characterised some of its properties. We proved a fusion theoretic version of Thompson's maximal subgroup theorem. We introduced the notion of section p-stability both for groups and fusion systems and proved a version of Glauberman's theorem to fusion systems. We also examined the relationship between solubility and p-stability for fusion systems and determined the simple groups whose fusion systems are $Qd(p)$-free.

In the paper HSz19JA we investigated p-stable fusion systems, where p is an odd prime. We examined realisable fusion systems and proved a generalisation of a result of G. Glauberman. Then we proved that p-stability is determined by the normaliser systems of centric radical subgroups. Finally, we proved that all p-stable fusion systems are realisable provided there exists a stable p-functor.

In 2017 Erzsébet Horváth made her habilitation in BME. Her thesis topics belong to representation theory of finite groups: questions about monomiality, blocks and depth.

In GHH17IJGT we proved that Maschke property holds for coprime action on iterated wreath product P_n of cyclic groups of order p, i.e. the Sylow p-subgroups of symmetric groups S_{p^n}, where we also proved that a stronger form of Maschke property holds. We applied these results to describe which normal partition subgroups of P_n have complements. We also described abelian subgroups of largest size in P_n.

In HHP19CA we determined the combinatorial and the ordinary depth of the maximal subgroups of the simple Ree groups ${}^2G_2(q)$. As an application of these calculations, we determine the subdegrees of primitive actions of the groups ${}^2G_2(q)$. We also improved an earlier estimate of Burness, Liebeck, and Shalev on the base size of "non-standard" primitive actions of ${}^2G_2(q)$ on the coset space of maximal subgroups from 3 to 2. This is part of the PhD dissertation of the third author, which was defended successfully in 2016.

In JBH20IJGT we proved that for each positive integer n exist a group G and a subgroup H such that the ordinary depth $d(H, G)$ is $2n$. This solves the open problem posed by Lars Kadison whether even ordinary depth larger than 6 can occur. The first series of examples of arbitrarily large even depth is given in JBH20SW which is to appear in the conference volume of the Spring Wind conference. That construction was giving a depth series of 2^n.

In the paper JHH20JGT, we determined the TI subgroups of the simple Suzuki groups $Sz(q)$. More generally, we determined those nontrivial subgroups that are disjoint from some of their conjugates. It turns out that the latter are exactly those subgroups that have ordinary depth 3. The Sylow 2-subgroups of simple Suzuki groups belong to the class of so-called Suzuki 2-groups, which have been studied extensively by Higman. These results were extended later by Goldschmidt, Shaw, Shult, Gross, Wilkens and Bryukhanova.

As a corollary of our investigations, we get some interesting results for the Sylow 2-subgroups of Suzuki groups, as well. We related this to an open problem on Suzuki 2-groups, and we asked a question concerning that. We also gave some characterization of Suzuki groups.

A group G has a Frobenius graphical representation (GFR) if there is a simple graph whose full automorphism group is isomorphic to G and it acts on the vertices as a Frobenius group. In particular, any group G with GFR is a Frobenius group and the graph Cayley. The existence of an infinite family of groups with GFR whose Frobenius kernel is a non-abelian 2-group has been an open question. In KN20AMC a positive answer was given by showing that the Higman group $A(f, q0)$ has a GFR for an infinite sequence of f and $q0$.

In BHHK20JA we investigated the Loewy structure of the fixpoint algebra of the group algebra of the additive group of a finite field F under the action of a subgroup of the multiplicative group of F. In this paper, we introduced a class of certain algebras of finite dimension over a field. All these algebras are split, symmetric and local. In BHHK21IEJA we continued to investigate their Loewy structure. We found that in many cases their Loewy length is equal to an upper bound established in BHHK20JA, but we also constructed examples where we have a strict inequality. The algebras considered here include certain rings of fixpoints under the action of particular finite groups. Thus we may consider the results in this paper as a contribution to the general theory of fixpoint rings.

In LM17CA we proved that every standard Koszul (not necessarily graded) standardly stratified algebra is also Koszul. This generalizes a similar result on quasi-hereditary algebras.

Let A be a standard Koszul standardly stratified algebra and X an A-module. The paper LM16CMJ investigated conditions which imply that the module $Ext^*_A(X)$ over the Yoneda extension algebra A^* is filtered by standard modules. In particular, we proved that the Yoneda extension algebra of A is also standardly stratified. This is a generalization of similar results on quasi-hereditary and on graded standardly stratified algebras.

The publications LM16MHI and LM16MHII are online lecture notes on Representation theory of rings and groups I-II at the Budapest University of Technology and Economics for an MSc course on this topic.

In 2018 András Magyar defended successfully his PhD. The title of his dissertation was "Standard Koszul Algebras".

Some additive questions from number theory

In the last few years, we studied the connections between the basic concepts of Additive combinatorics such as Sidon sets, additive bases and additive complements. Moreover, we investigated the properties of additive representation functions. We gave a necessary and sufficient condition to the multiplicativity of the linear combination of some additive representation functions. We generalized our earlier results about the difference sequence of additive representation functions. We characterized the partitions of the natural numbers into two sets affording identical representation functions and we partially described the structure of the sets, which have coinciding representation functions. Furthermore, we studied the existence of a minimal complement to eventually periodic sets and we gave necessary and sufficient conditions for it. We generalized the construction of Danzer to k-fold additive complements. On the other hand, we proved the existence of a h-Sidon set which is an asymptotic basis of order $2h + 1$. We also proved the existence of dense generalized weak Sidon sets formed by pefect powers. Furthermore, we proved the existence of an asymptotic basis of order $2k + 1$ such that all the sums formed by at least one and at most $k - 1$ terms are different. Moreover, we proved some partial results on a conjecture of Erdős about sets without pairwise coprime integers. We invesigated generalized Stanley sequences as well. In our proofs we used analytic, combinatorial and probabilistic tools combined with elementary ideas. We developed a group testing algorithm based on the Chinese remainder theorem and we applied it to avoid falsie positive free zones of Bloom filters. Finally, we constructed a Zero knowledge protocol which is based on the explicit isomorphism problem between algebras.

In more detail:

In KS17RJ we gave a necessary and sufficient condition to the multiplicativity of the two terms linear combination of certain additive representation functions.

In KS17DM we investigated that partitions of the set of natural numbers into two sets such that the corresponding additive representation functions are identical. We solved a recent problem of Chen and Lev.

Stanley sequences are defined by the greedy algorithm. If we have the first few elements of the sequence then we add the smallest possible element such that the obtained set does not contain a k terms arithmetic progression. In the paper KSQ18ACTA we proved some results about various generalizations of Stanley sequences.

A set of integers W is called additive complement of the set of intgers C if their sumset is the set of integers. In the paper KSQ19JCT we studied the existence of minimal additive complement of an eventually periodic set. We partially solved a problem of Nathanson.

In 1962 Erdős conjectured that maximal cardinality of the set of nonnegative integers up to n, which does not contain $k+1$ pairwise coprime integers is the number of positive integers up to n which are not divisible by the first k primes. Recently Chen and Zhou proved some results about this conjecture. In the paper KSQ18SJDM we solved an open problem of Chen and Zhou and proved several related results about the conjecture.

In the paper KS20INT we partially described the structure of the sets, which have coinciding representation functions.

In the paper KS19ACTA we generalized some statements about the difference sequence of the two terms additive representation functions. By using the block function we investigate the regularity property of the linear combination of additive representation functions.

Let $h, k \geq 22$ be integers. We say a set A of positive integers is an asymptotic basis of order k if every large enough positive integer can be represented as the sum of k terms from A. A set of positive integers A is called $B_h[g]$ set if all positive integers can be represented as the sum of h terms from A at most g times. In the paper KS21DM we proved the existence of $B_h[1]$ sets which are asymptotic bases of order $2h+1$ by using probabilistic methods. We solved a problem of J. Cilleruelo by proving the existence of a dense subset A of positive integers such that the number of representations of a positive integer n as a positive defiite quadratic form with two variables is bounded. We extended this result to positive definite quadratic forms with more than two variables as well.