FINAL REPORT ON THE NKFIH PROJECT OTKA K120154

Summary. In the framework of this project we have written 29 articles with acknowledgment to the support of the NKFIH indicated. To help the evaluation we have to admit that some 1/3rd of these do not fit in the research plan of the proposal. 12 of our papers already appeared in Q1 journals, 7 in Q2 journals, the rest are either submitted or in the form of a manuscript. In this report we focus on some of our main results related to the proposal.

Stability results play an important role in Galois geometries. A typical stability theorem looks as follows. We have a certain class of structures, defined by some combinatorial properties. There exists some result classifying the extremal objects of the class. Then a stability theorem assures that an almost extremal object of the class, e.g. a point set of size close to the extremal value, can be obtained only by slight modifications of an extremal, classified object (e.g. deleting or adding some points from/to it). The resultant method, developed by Szőnyi and Weiner, became very fruitful and resulted in many stability theorems. This is a method based on bivariate polynomials associated to point sets; the results of algebraic shape are then translated back to the original, geometric language. In [6] we generalize the method for the multidimensional case and show some new applications.

A hypergraph is linear if any two edges intersect in at most one vertex. A long-standing conjecture of Erdős, Faber and Lovász states that every n-uniform linear hypergaph with n edges has a proper vertex-coloring using n colors. In [8] we propose an algebraic framework to the problem and formulate a corresponding stronger conjecture. Using the Combinatorial Nullstellensatz, we reduce the Erdős–Faber–Lovász conjecture to the existence of nonzero coefficients in certain polynomials. These coefficients are in turn related to the number of orientations with prescribed in-degree sequences of some auxiliary graphs. We prove the existence of certain orientations of these graphs, which verifies a necessary condition for our algebraic approach to work.

According to Snevily's ex-conjecture, if $A = \{a_1, \dots, a_k\}$ and $B = \{b_1, \dots, b_k\}$ are k-element subsets of a finite group of odd order, then there is a permutation π such that the elements $a_1 + b_{\pi(1)}, \dots, a_k + b_{\pi(k)}$ are all distinct. This was first verified for cyclic groups of prime order by Alon, extended to all cyclic groups by Károlyi et al. and settled completely by Arsovsky. In [5] we prove a variant for cyclic groups of prime order, where A, B are multisets, which may lead to an analogue of Arsovsky's theorem to non-commutative groups via group extensions. The proof involves the use of Vandermonde-type polynomials.

Let R denote a finite ring of m elements given by its addition and multiplication tables and let $x_1, \dots, x_n$ be non-commuting variables. A polynomial over R in these variables can be represented in different ways. The equation solvability problem asks if there is a substitution where two polynomials attain the same value, or equivalently, if a polynomial has a root in R^n. This problem is known to be NP-complete for non-nilpotent rings. Horváth proved that if R is nilpotent, the problem can be solved in polynomial time (in terms of n), but the exponent in his solution was enormous. In [10] we give an $O(n^{m \log m})$-time algorithm, in fact we show that the whole range of a given polynomial can be computed in this time. The hidden constant factor depends only on m and the complexity of the way the polynomial is represented. The first step of our proof is a result in additive combinatorics, which we prove by the polynomial method.

In [1] we prove, among others, that if all points of an $n \times \cdots \times n$ grid in Euclidean d-space is covered by a set of at most $2n-3$ hyperplanes, then it contains a subset of n hyperplanes parallel to one of the coordinate hyperplanes, which already cover the whole grid. Although an elementary proof in now available, we first discovered this result using the strongest version of the Combinatorial Nullstellensatz and lacunary polynomials.

Consider the hypercube $[0,1]^d$. The weight of a vertex is the number of its nonzero coordinates. According to an old theorem of Alon and Füredi, if one wants to cover by hyperplanes all vertices except the origin, one needs at least d hyperplanes. In [11] we prove that if a hypersurface covers all vertices except those of weight not exceeding w (which it does not cover), then its degree must be at least $d - w$. The proof relies heavily on the polynomial method and works over arbitrary fields.

In [3] we propose the following variants of a problem of Erdős. What is the maximum number of triangles of unit area, maximum area or minimum area, that can be determined by an arrangement of n planar lines? We prove that the order of magnitude for the maximum occurrence of unit areas lies between $\Omega(n^2)$ and $O(n^{9/4})$. This result is strongly connected to additive combinatorial results and Szemerédi–Trotter type incidence theorems. Next we show an almost tight bound for the maximum number of minimum area triangles. Finally we present lower and upper bounds for the maximum area and distinct area problems by combining algebraic, geometric and combinatorial techniques.

Consider the 3-dimensional affine space over the finite field of p elements, p a prime. A set of p^2 points is called a cylinder if they lie on p parallel lines. According to the cylinder conjecture, if a set of p^2 points meets every plane in a number of points divisible by p, then it is a cylinder. In a weaker version one assumes that there are more than p directions, which are not determined by the point set. In [4] we solve these conjectures for small values of p with the help of Rédei polynomials, the Combinatorial Nullstellensatz and exhaustive computer search.

There are many examples for point sets in finite geometry, which behave almost regularly in some well-defined sense, for instance they have almost regular line-intersection numbers. In [2] we investigate point sets of a desarguesian affine plane, for which there exist some parallel classes of lines, such that almost all lines of one parallel class intersect our set in the same number of points (possibly modulo the characteristic). The lines with exceptional intersection numbers are called renitent, and the behavior of these lines are studied using polynomials and algebraic curves over finite fields. As a consequence of our results, we also prove geometric properties of certain linear codes over finite fields.

Minimal codewords in linear codes were originally studied in connection with decoding algorithms and have been used for determining the access structure in code-based secret sharing schemes. In a linear code, a codeword is minimal if its support does not contain the support of any codeword other than its scalar multiples. A code is minimal if its codewords are all minimal. Minimal linear codes turned out to be in one-to-one correspondence with special types of blocking sets of projective spaces over a finite field. In [7] we determine, up to a small constant factor, the minimal length of minimal codes of dimension k over the

q-element Galois field, which is linear in both q and k. The lower bound follows by the Alon–Füredi Theorem and the Combinatorial Nullstellensatz.

For positive integers ℓ and m, let $f(\ell, m)$ denote the maximum cardinality of a set $A \subset [1, \ell]$ such that $m \notin \Sigma(A)$ (the set of subset sums of A). The study of this function was initiated by Erdős and Graham. Let $\mathrm{snd}(m)$ denote the smallest positive integer that does not divide m. Alon proved that $f(\ell, m) \leq c(\varepsilon) \cdot \ell/\mathrm{snd}(m)$ for every $\ell^{1+\varepsilon} < m < \ell^2/\ln^2 \ell$, and conjectured that in fact $f(\ell, m) = (1 + o(1)) \cdot \ell/\mathrm{snd}(m)$ holds for $\ell^{1.1} < m < \ell^{1.9}$ as $\ell \to \infty$. This was verified by Vu and Wood. In [9] we prove that for every $\varepsilon > 0$, there is an $\ell_0 = \ell_0(\varepsilon)$ such that if $\ell \geq \ell_0$, then

$$f(\ell, m) = \left\lfloor \frac{\ell}{\mathrm{snd}(m)} \right\rfloor + \mathrm{snd}(m) - 2$$

holds for any $(280 + \varepsilon)\ell \ln \ell < m < \ell^2/(8 + \varepsilon) \ln^2 \ell$, thus determining the exact value of $f(\ell, m)$ and essentially improving all previous results on the topic. In the same paper we also prove an old conjecture of Lev, proving that if n is large enough, $\ell \leq 2n - 6$ and $A \subset [1, \ell]$ is a set of n integers, then

$$[2\ell - 2n + 1, \sigma(A) - (2\ell - 2n + 1)] \subseteq \Sigma(A),$$

where $\sigma(A)$ denotes the sum of the elements of A. The proof depends on the Dias da Silva–Hamidoune theorem and subtle combinatorial arguments, thus the algebraic method only appears in the background.

References

[1] J. Borbély and Gy. Károlyi, Covering Cartesian products by hyperplanes, *manuscript*

[2] B. Csajbók, P. Sziklai, and Zs. Weiner, Renitent lines, *European Journal of Combinatorics*, submitted

[3] G. Damásdi, L. Martinez-Sandoval, D.T. Nagy, and Z.L. Nagy, Triangle areas in line arrangements, *Discrete Mathematics* **143** (2020) 112105, 11 pages

[4] J. De Beule, J. Demeyer, S. Mattheus, and P. Sziklai, On the cylinder conjecture, *Designs, Codes and Cryptography* **87** (2019) 879–893

[5] A. Gáspár and G. Kós, A Snevily-type inequality for multisets, *Acta Mathematica Hungarica* **164** (2021) 46–50

[6] N. Harrach, P. Sziklai, L. Storme and M. Takáts, Resultant methods in higher dimensions, *manuscript*

[7] T. Héger and Z.L. Nagy, Short minimal codes and covering codes via strong blocking sets in projective spaces, *IEEE Transactions on Information Theory* **68** (2021) 881–890

[8] O. Janzer and Z.L. Nagy, Coloring linear hypergraphs: the Erdős–Faber–Lovász conjecture and the Combinatorial Nullstellensatz, *Designs, Codes and Cryptography* **90** (2022) 1991–2001

[9] Gy. Károlyi, Long arithmetic progressions in subset sums and a conjecture of Alon, *Journal of Number Theory*, submitted

[10] Gy. Károlyi and Cs. Szabó, valuation of polynomials over finite rings via additive combinatorics, *Publicacions Matématiques*, **66** (2022) 197–205

[11] P. Sziklai and Zs. Weiner, Covering all but the low weight vertices of the hypercube, *Journal of Combinatorial Theory A*, **193** (2023) 105671, 6 pages