Final report on OTKA project K129335

In this final report we have only included publications on which the financial support of OTKA project K129335 is acknowledged. (Other publications of the participants were either written before the start of this project, or they are not related to the topics of the project, and therefore not listed.) In the list below we give a short description of each paper, and use the numbering given in the list of publications in the online version of final report at the OTKA homepage. Most of the papers have already been published, while some of the recent ones are submitted for publication (in the latter case we have given 2024 as the year of prospective publication).

(1) In this paper some links between the density of a set of integers and the density of its sumset, product set and set of subset sums are presented.

(2) Let $A = \{a_1, a_2, \dots\}$ $(a_1 < a_2 < \dots)$ be an infinite sequence of nonnegative integers, and let $R_{A,2}(n)$ denote the number of solutions of $a_x + a_y = n$ $(a_x, a_y \in A)$. P. Erdős, A. Sárközy and V. T. Sós proved that if $\lim_{N\to\infty} \frac{B(A,N)}{\sqrt{N}} = +\infty$ then $|\Delta_1(R_{A,2}(n))|$ cannot be bounded, where $B(A,N)$ denotes the number of blocks formed by consecutive integers in A up to N and Δ_l denotes the l-th difference. Their result was extended to $\Delta_l(R_{A,2}(n))$ for any fixed $l \geq 2$. In this paper we give further generalizations of this problem.

(3) For a set of nonnegative integers A, denote by $R_A(n)$ the number of unordered representations of the integer n as the sum of two different terms from A. In this paper we partially describe the structure of the sets, which have coinciding representation functions.

(4) Let $C, W \subset \mathbb{Z}$. If $C + W = \mathbb{Z}$, then the set C is called an additive complement to W in $\mathbb{Z}$. If no proper subset of C is an additive complement to W, then C is called a minimal additive complement. Let $X \subset \mathbb{N}$. If there exists a positive integer T such that $x + T \in X$ for all sufficiently large integers $x \in X$, then we call X eventually periodic. In this paper, we study the existence of a minimal complement to W when W is eventually periodic or not. This partially answers a problem of Nathanson.

(5) In the first part of the paper, we investigate the subset sums of a special type of pseudo- recursive sequences. In the second part, we use our results for an encryption algorithm.

(6) We present a number of new methods which provide lower bounds for several infinite families of progression-free sets in certain Abelian groups.

(7) We show that an additive Hilbert cube (in prime fields) of sufficiently large dimension always meets certain kinds of arithmetic sets, namely, product sets and reciprocal sets of sumsets satisfying certain technical conditions.

(8) We present a new proof of a theorem of Shparlinski on the notion of additive energy of sets, and derive some structure theorems for dense sets.

(9) We discuss the following questions, and give partial results: for which values of n can we color the positive integers with precisely n colors in such a way that for any a, the numbers $a, 2a, \ldots, na$ all get different colors?

(10) 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 this paper we prove the existence of $B_h[1]$ sets which are asymptotic bases of order $2h+1$ by using probabilistic methods.

(11) We improve results of the first author on the representation function $R_2(A, N)$ for certain sets of positive integers A.

(12) Let $l_1, l_2, \ldots$ be a countable collection of lines in $\mathbb{R}^d$. For any $t \in [0, 1]$ we construct a compact set Γ with Hausdorff dimension $d - 1 + t$ which projects injectively into each l_i, such that the image of each projection has dimension t.

(13) Let A be a finite, nonempty subset of an abelian group. We show that if every element of A is a sum of two other elements, then A has a nonempty zero-sum subset. That is, a (finite, nonempty) sum-full subset of an abelian group is not zero-sum-free.

(14) Suppose that for some unit vectors $b_1, \ldots, b_n$ we have that for any $j \neq k$ b_j is either orthogonal to b_k or unbiased to it. We prove that if n=d(d+1), then these vectors necessarily form a complete system of mutually unbiased bases.

(15) By constructing suitable nonnegative exponential sums, we give upper bounds on the cardinality of any set B_q in cyclic groups such that the difference set avoids cubic residues modulo q.

(16) In 1978 Nathanson obtained several results on sumsets contained in infinite sets of integers. Later the author investigated how big a Hilbert cube avoiding a given infinite sequence of integers can be. In the present paper we concentrate on densities and Hilbert cubes, Hilbert cubes which avoid given sets, and degenerate Hilbert cubes. The aim is to collect some results in the past and some related recent problems.

(17) We investigate properties of Boolean functions given by number theoretical constructions.

(18) We propose a new identification system based on algorithmic problems related to computing isomorphisms between central simple algebras. We design a statistical zero knowledge protocol which relies on the hardness of computing isomorphisms between orders in division algebras which generalizes a protocol by Hartung and Schnorr, which relies on the hardness of integral equivalence of quadratic forms.

(19) Does there exist an asymptotic basis of order k where all the subset sums with at most l terms are pairwise distinct with the exception of finitely number of cases as long as $l \leq k - 1$? In this paper, we prove the existence of an asymptotic basis of order $2k+1$ and all the sums of at most k elements

of this asymptotic basis are pairwise different except for "small" numbers by using probabilistic tools

(20) Two infinite sets A and B of nonnegative integers are called additive complements if their sumset contains every nonnegative integer. In this paper we solve a problem of Chen and Fang by extending an earlier construction of Danzer.

(21) Bloom filters and their variants are widely used as space efficient probabilistic data structures for representing set systems and are very popular in networking applications. They support fast element insertion and deletion, along with membership queries with the drawback of false positives. Bloom filters can be designed to match the false positive rates that are acceptable for the application domain. However, in many applications a common engineering solution is to set the false positive rate very small, and ignore the existence of the very unlikely false positive answers. This paper is devoted to close the gap between the two design concepts of unlikely and not having false positives. 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 refer to the limited universe and filter size as the false positive free zone of the filter. We describe necessary conditions for the false positive free zone of a filter and generalize the filter to support listing of the elements. We evaluate the performance of the filter in comparison with the traditional Bloom filters. Our data structure is based on recently developed combinatorial group testing techniques.

(22) In this paper, we prove that a lower bound of the first author concerning representation functions is nearly best possible.

(23) The original knapsack problem is well known to be NP-complete. In a multidimensional version one has to decide whether a $p \in \mathbb{N}^k$ is in a sumset-sum of a set $X \subseteq \mathbb{N}^k$ or not. In this paper we are going to investigate a communication complexity problem related to this.

(24) In this paper, we prove some Erdős–Fuchs-type theorems about the error terms appearing in approximation formula for representation functions.

(25) Let d be a positive integer and $U \subset \mathbb{Z}^d$ finite. Using methods of analytic inequalities we study generalizations of the notion of doubling constant of U.

(26) We improve the best known upper bound on the density of a planar measurable set A containing no two points at unit distance to 0.25442. We use a combination of Fourier analytic and linear programming methods to obtain the result. The estimate is achieved by means of obtaining new linear constraints on the autocorrelation function of A utilizing triple-order correlations in A, a concept that has not been previously studied.

(27) We investigate additive properties of sets A, where $A = \{a_1, a_2, \ldots, a_k\}$ is a monotone increasing set of real numbers, and the differences of consecutive elements are all distinct. It is known that $|A + B| \geq c|A||B|^{1/2}$ for any finite set of numbers B. The bound is tight up to the constant multiplier. We give a new proof to this result using bounds on crossing numbers of

geometric graphs. We construct examples showing the limits of possible improvements. In particular, we show that there are arbitrarily large sets with different consecutive differences and sub-quadratic sumset sizes.

(28) We study sets C, D of nonnegative integers such that their representation functions coincide, $R_C(n) = R_D(n)$.

(29) A system of linear equations over a finite field F_q is said to be common if, among all two- colorings of F_q^n , the uniform random coloring minimizes the number of monochromatic solutions asymptotically. The notion of common systems of linear equations was introduced by Saad and Wolf, as an analogue to the well-studied notion of common graphs. Fox, Pham and Zhao characterized the common systems consisting of one equation. We study systems consisting of two equations over the binary field F_2. We characterize, up to a finite number of cases, which systems with an odd number of variables are common. Our characterization answers a question by Kamcev, Liebenau and Morrison in the affirmative way whether there exist common systems of equations that are not translation invariant.

(30) We study generic properties of topological groups in the sense of Baire category. First we investigate countably infinite (discrete) groups. We extend a classical result of B. H. Neumann, H. Simmons and A. Macintyre on algebraically closed groups and the word problem. I. Goldbring, S. E. Kunnawalkam and Y. Lodha proved that every isomorphism class is meager among countably infinite (discrete) groups. In contrast, we show that there is a comeager isomorphism class among countably infinite (discrete) abelian groups. Then we turn to compact metrizable abelian groups. We use Pontryagin duality to show that there is a comeager isomorphism class among compact metrizable abelian groups. We discuss its connections to the countably infinite (discrete) case. Finally, we study compact metrizable groups. We prove that the generic compact metrizable group is neither connected nor totally disconnected; also it is neither torsion-free nor a torsion group.

(31) In this paper we fully settle Fuglede's conjecture for convex bodies affirmatively in all dimensions, i.e. we prove that if a convex body is a spectral set then it is a convex polytope which can tile the space by translations.

(32) In this note we present a counterexample to the lights out problem, that is, for every odd prime we construct a simple graph G with vertex set V such that there does not exist elements $x_v \in F_p$ such that $\sum_{u \in N[v]} x_u \neq 0$ for each $v \in V$.

(33) The additive energy plays a central role in combinatorial number theory. We show an uncertainty inequality which indicates how the additive energy of support of a Boolean function, its degree and subcube partition are related.

(34) In this note we give an overview of the currently known best lower and upper bounds on the size of a subset of Z_m^n avoiding k-term arithmetic progression. We will focus on the case when the length of the forbidden progression is 3. We also formulate some open questions.

(35) We show that sets avoiding 6-term arithmetic progressions in Z_6^n have size at most 5.709^n.

(36) In this paper we prove the existence of a set A formed by perfect powers with almost possible maximal density such that $R_{A,h}(n)$ is bounded by using probabilistic methods

(37) We study some variants of the Erdős similarity problem. We pose the question if every measurable subset of the real line with positive measure contains a similar copy of an infinite geometric progression. We construct a compact subset E of the real line such that 0 is a Lebesgue density point of E, but E does not contain any (non-constant) infinite geometric progression. We give a sufficient density type condition that guarantees that a set contains an infinite geometric progression.

(38) In this paper, we study a Ramsey-type problem for equations of the form $ax+by = p(z)$. We show that if certain technical assumptions hold, then any 2-colouring of the positive integers admits infinitely many monochromatic solutions to the equation $ax + by = p(z)$.

(39) In this paper we show that the largest possible size of a subset of F_q^n avoiding right angles, that is, distinct vectors x, y, z such that $x - z$ and $y - z$ are perpendicular to each other is at most $O(n^{q-2})$. This improves on the previously best known bound due to Naslund and refutes a conjecture of Ge and Shangguan.

(40) We extend a results of Ruzsa and Chen-Fang on exact additive complements of positive integers A, B.

(41) By improving upon previous estimates on a problem posed by L. Moser, we prove a conjecture of Erdős that the density of any measurable planar set avoiding unit distances cannot exceed $1/4$. Our argument implies the upper bound of 0.2470.

(42) The aim of this note is two-fold. In the first part of the paper we are going to investigate an inverse problem related to additive energy. In the second, we investigate how dense a subset of a finite structure can be for a given additive energy.

(43) We prove that under the prime-tuple hypothesis, the set of signed primes is a sumset.

(44) We find large subsums of the MĂśbius function for divisors of an integer.

(45) It is well known that a classical Fubini theorem for Hausdorff dimension cannot hold; that is, the dimension of the intersections of a fixed set with a parallel family of planes do not determine the dimension of the set. Here we prove that a Fubini theorem for Hausdorff dimension does hold modulo sets that are small on all Lipschitz graphs.

(46) In this paper, we study how dense a multiplicative basis of order h for Z_+ can be, improving on earlier results. Upon introducing the notion of a *multiplicative complement*, we present some tight density bounds.

(47) It was recently proved that the Fuglede conjecture holds for the class of convex bodies in $\mathbb{R}^d$. The proof was based on a new geometric necessary condition for spectrality, called "weak tiling". In this paper we study further properties of the weak tiling notion, and present applications to convex bodies, non-convex polytopes, product domains and Cantor sets of positive measure.

(48) In an earlier paper the notion of so-called pseudo-recursive sequences was introduced, which generalize bracket sequences. In the present article, Boolean functions are defined on hypergraphs with edges having big intersections induced by bracket sequences and hypergraphs that are thinly intersecting. These Boolean functions related to combinatorial number theory are new in this area.

(49) 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 a sum of k terms from A. A set of positive integers is called Sidon set if all the two-term sums formed by the elements are different. Many years ago P. Erdős, A. SĂĄrközy and V. T. Sós asked whether there exists a Sidon set which is an asymptotic basis of order 3. In this paper we prove the existence of a Sidon set with positive lower density of the three fold sumset by using probabilistic methods.

(50) We construct a continuously differentiable curve in the plane that can be covered by a collection of lines such that every line intersects the curve at a single point and the union of the lines has Hausdorff dimension 1. We show that for twice differentiable curves this is impossible. In that case, the union of the lines must have Hausdorff dimension 2. If we use only tangent lines then the differentiability of the curve already implies that the union of the lines must have Hausdorff dimension 2, unless the curve is a line. We also construct a continuous curve, which is in fact the graph of a strictly convex function, such that the union of (one sided) tangent lines has Hausdorff dimension 1.

(51) This article shines new light on the classical problem of tiling rectangles with squares efficiently with a novel method. With a twist on the traditional approach of resistor networks, we provide new and improved results on the matter using the theory of Diophantine Approximation, hence overcoming long-established difficulties, such as generalizations to higher-dimensional analogues. The universality of the method is demonstrated through its applications to different tiling problems. These include tiling rectangles with other rectangles, with their respective higher-dimensional counterparts, as well as tiling equilateral triangles, parallelograms, and trapezoids with equilateral triangles.

(52) In this paper our interest is in all possible sizes of hA when A is a nonbasis of order h in G of maximum size; we provide the complete answer when $h = 2$ or $h = 3$.

(53) We consider the question which compact metric spaces can be obtained as a Lipschitz image of the middle third Cantor set, or more generally, as a Lipschitz image of a subset of a given compact metric space.

(54) Two infinite sets A and B of non-negative integers are called *perfect additive complements of non-negative integers*, if every non-negative integer can be uniquely expressed as the sum of elements from A and B. In this paper, we define a Lagrange-like spectrum of the perfect additive complements (L for short). As a main result, we obtain the smallest accumulation point of the set L and prove that the set L is closed. Other related results and problems are also contained.

(55) An asymptotic basis A of order h is minimal if no proper subset of A is an asymptotic basis of order h. Concerning minimal asymptotic bases, in this paper we give some generalizations of a result of Chen and Chen, and recent result of Ling and Tang, and also recent result of Sun.

(56) We study subsets of F_p^n that do not contain progressions of length p.

(57) In this paper, we focus on the function SX, where $SX = \limsup \max\{A(x), B(x)\}/\sqrt{x}$, which was introduced by Erdős and Freud in 1984. As a main result, we determine the value of SX for perfect additive complements and further fix the infimum.

(58) In this paper, we determine the sets A, B such that the representation function $r_{A,B}(n) = 1$ for every nonnegative integer n.

(59) In this paper, following Erdős and Freud's work, we explore properties of "disjoint" sets A, B, i.e. sets such that $A - A$ and $B - B$ only intersect in 0.

(60) We discuss the relation of tiling, weak tiling and spectral sets in finite elementary p-groups $(Z_p)^d$.

(61) In this paper we prove that if A and B are infinite subsets of positive integers such that every positive integer n can be written as $n = ab$, then $\lim A(x)B(x)/x = \infty$.

(62) We study the problem of finding the true dimension of trace codes and their duals, which is relevant for the size of the public key of various code-based cryptographic protocols.

(63) We are looking for integer sets that resemble classical Cantor set and investigate the structure of their sum sets.

(64) In this paper we resolve the Alon-Jaeger-Tarsi conjecture for sufficiently large primes.

(65) Recently, the first two authors proved the Alon-Jaeger-Tarsi conjecture on non-vanishing linear maps, for large primes. We extend their ideas to address several other related conjectures.

(66) We introduce a new family of fractal dimensions by restricting the set of diameters in the coverings in the usual definition of the Hausdorff dimension. Among others, we prove that this family contains continuum many distinct dimensions, and they share most of the properties of the Hausdorff dimension, which answers negatively a question of Fraser. On the other hand, we also prove that among these new dimensions only the Hausdorff dimension behaves nicely with respect to Hölder functions, which supports a conjecture posed by Banaji obtained as a natural modification of Fraser's

question. We also consider the supremum of these new dimensions, which turns out to be an other interesting notion of fractal dimension.

(67) Moser constructed a set A of nonnegative integers such that $R_{A,\lambda}(n) = 1$ holds for every nonnegative integer n. In this paper we generalize this result.

(68) Bell and Shallit recently gave a counterexample for a conjecture of Dombi. In this paper we improve their result.

(69) In this paper we prove the existence of $B_h[1]$ sets which are asymptotic bases of order $2h$ by using probabilistic methods.

(70) In this paper, we study the structure of sets A and B such that their representation functions are equal, and A, B satisfy some further prescribed properties.

(71) In this paper we prove that many well-known formulations of the Kakeya conjecture are indeed equivalent.