Final report for PD115978 (Applications of Combinatorics in Multiplicative Number Theory)

Péter Pál Pach

The results achieved during the framework of the project are contained in 13 papers: 9 of these have already appeared, 4 are under review. The papers were published in prestigious general (Mathematics) journals (including Annals of Mathematics, Bulletin of the LMS) and in top specialized journals (including Combinatorica, JCTA). The PI gave 22 talks at international conferences and workshops (e.g. Workshop on Algebraic Methods in Combinatorics, Harvard; London Colloquia in Combinatorics; Joint International Meeting of the Chinese Mathematical Society and the American Mathematical Society, Shanghai), at 13 occasions as an invited speaker. Furthermore, the PI gave 16 seminar talks at universities in the UK, Hungary, Austria and Germany. Now, we continue with the description of the results.

The most important result is developing, jointly with Croot and Lev, a new variant of the polynomial method to solve a question in Additive Combinatorics, namely to prove that sets avoiding nontrival 3-term arithmetic progressions in $\mathbb{Z}_4^n$ are exponentially small: $r_3(\mathbb{Z}_4^n) \leq 3.611^n$. This improved upon the result of Sanders which was of the form $r_3(\mathbb{Z}_4^n) \leq \frac{4^n}{n(\log n)^c}$. This "exponential saving" was the first of a kind for problems of this sort. The above mentioned paper, titled "Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small", appeared in Annals of Mathematics.

Less then one week after submitting this paper to arXiv, Ellenberg and Gijswijt showed that the method can be adapted to the case of $\mathbb{F}_3^n$, too, known as the "cap set problem". Tao in his 2007 blog post refers to the problem as "perhaps his favourite open question". Gowers writes on his blog that "the argument has a magic quality that leaves one wondering how on earth anybody thought of it. I'm referring particularly to the Croot-Lev-Pach lemma here" and describes it as "a major new technique to add to the toolbox".

Since then the method had several applications including:

- the solution of the cap set problem in $\mathbb{F}_3^n$ (Ellenberg-Gijswijt, Annals paper) and an extension (Ellenberg, Discrete Analysis paper)
- the proof of the Erdős-Szemerédi sunflower conjecture (the currently best bound was given by Naslund and Sawin in their paper in Forum of Mathematics, Sigma)
- tight bound for Green's arithmetic triangle removal lemma (Fox-Lovász, Advances paper) and an extension to k-cycles (Fox-Lovász-Sauermann, JCTA paper)
- Sárközy's theorem in function fields (Green, Quarterly Journal of Mathematics paper)

- growth rate of tri-colored sum-free sets (Kleinberg-Sawin-Speyer, Discrete Analysis paper)
- group theoretic approach to matrix multiplication (Blasiak-Church-Cohn-Grochow-Naslund-Sawin-Umans, Discrete Analysis paper)

Grochow wrote in a paper (which appeared in the Bulletin of the AMS) devoted to the technique and some applications of it that "the Cap Set Conjecture was developed as a keystone problem whose solution was expected to unlock the mysteries of many other problems in combinatorics and number theory. And indeed, as evidenced by the long list of applications already, the technique used to resolve the Cap Set Conjecture had precisely the desired effect! (It may be worth noting that almost none of these applications follow as corollaries of the result itself; they only followed by using the Croot-Lev-Pach technique.)"

The paper has already 65 citations, served as the main topic of several conferences and workshops, moreover world-leading mathematicians devoted blog posts to it (including Cameron, Kalai, Gowers, Tao).

In the paper titled "Caps and progression-free sets in $\mathbb{Z}_m^n$" (joint with Elsholtz) we improved on the known bounds in several cases related to the above topic. Let $r_k(\mathbb{Z}_m^n)$ denote the largest possible size of a subset of the group $\mathbb{Z}_m^n$ which avoids (nontrivial) k-term arithmetic progressions. We give lower bound constructions, which e.g. include that $r_3(\mathbb{Z}_m^n) \geq C_m \frac{((m+2)/2)^n}{\sqrt{n}}$, when m is even. When $m = 4$ this is of order at least $3^n/\sqrt{n} \gg |G|^{0.7924}$. Moreover, if the progression-free set $S \subset \mathbb{Z}_4^n$ satisfies a technical condition, which dominates the problem at least in low dimension, then $|S| \leq 3^n$ holds. Furthermore, we present a number of new methods which cover lower bounds for several infinite families of parameters m, k, n, which includes for example: $r_6(\mathbb{Z}_{125}^n) \geq (85-o(1))^n$. For $r_3(\mathbb{Z}_4^n)$ we determine the exact values, when $n \leq 5$, e.g. $r_3(\mathbb{Z}_4^5) = 124$, and for $r_4(\mathbb{Z}_4^n)$ we determine the exact values, when $n \leq 4$, e.g. $r_4(\mathbb{Z}_4^4) = 128$. It's worth noting that our general lower bound construction for $r_3(\mathbb{Z}_4^n)$ gives the exact value in all the cases when the exact value is known (that is, for $n \leq 5$). The paper is under review.

In the paper titled "Multiplicative bases and an Erdős problem" (joint with Sándor) we investigated how small the density of a multiplicative basis of order h can be in $\{1, 2, \ldots, n\}$ and in $\mathbb{N}$. Furthermore, a related problem of Erdős was also studied: How dense can a set of integers be, if none of them divides the product of h others? These questions are partially related to multiplicative Sidon-sequences, namely, here we also used some factorization lemmata. Some of the results improve the results of Chan, Győri, Sárközy and Raikov. The paper appeared in Combinatorica.

In another joint paper with Sándor, titled "On infinite multiplicative Sidon sets" we studied the asymptotic density of infinite multiplicative Sidon sets. In 1938 Erdős showed that the size of the largest multiplicative Sidon set in $\{1, 2, \ldots, n\}$ is between $\pi(n) + c_1 n^{3/4}/(\log n)^{3/2}$ and $\pi(n) + c_2 n^{3/4}$ (with some positive constants c_1 and c_2). 31 years later Erdős himself improved this upper bound to $pi(n) + c_2 n^{3/4}/(\log n)^{3/2}$. Hence, in the lower- and upper bounds not only the main terms are the same, but the error terms

only differ in a constant factor. In this paper We investigated the maximal possible asymptotic density of an *infinite* multiplicative Sidon set. Namely, we proved that if A is an infinite multiplicative Sidon set, then $\liminf \frac{|A(n)|-\pi(n)}{n^{3/4}/(\log n)^3}$ is always finite, and constructed an infinite multiplicative Sidon set for which $\liminf \frac{|A(n)|-\pi(n)}{n^{3/4}/(\log n)^3}$ is positive. Hence, here – similarly to the result of Erdős – the "error term" is determined up to a constant factor, but this error term is smaller than the error term of the finite case (the exponent of $\log n$ is -3 instead of $-3/2$). Note that it is not difficult to see that in the lim sup version of the problem the error term of the finite case can be reached easily by repeating the finite construction in larger and larger blocks. The paper appeared in the European Journal of Combinatorics.

In the paper titled "The number of multiplicative Sidon sets of integers" (joint with Liu) we showed that the number of multiplicative Sidon subsets of $\{1, 2, \dots, n\}$ is $T(n) \cdot 2^{\Theta(\frac{n^{3/4}}{(\log n)^{3/2}})}$ for a certain function $T(n) \approx 2^{1.815\pi(n)}$ which we specify. This is a rare example in which the order of magnitude of the lower order term in the exponent is determined. It resolves the enumeration problem for multiplicative Sidon sets initiated by Cameron and Erdős in the 80s. We also investigate its extension for generalised multiplicative Sidon sets. Denote by S_k, $k \geq 2$, the number of multiplicative k-Sidon subsets of $\{1, 2, \dots, n\}$. We showed that $S_k(n) = (\beta_k + o(1))^{\pi(n)}$ for some β_k we define explicitly. The paper appeared in the Journal of Combinatorial Theory, Series A.

In the paper titled "The number of maximum primitive sets of integers" (joint with Liu and Palincza) we studied another counting type question, where the forbidden pattern is of multiplicative nature. Namely, we counted the number of primitive subsets of $\{1, 2, \dots, n\}$ and the number of n-element primitive subsets of $\{1, 2, \dots, 2n\}$. The former problem was also first investigated by Cameron and Erdős, the latter one – where an additional difficulty arises – was asked by Bishnoi. We showed that in both cases the answer is of the form $(c + o(1))^n$ (with two different constants c). Furthermore, we gave an algorithm for approximating this constant c. We also investigated another related problem of Cameron and Erdős. They showed that the number of sets containing pairwise coprime integers in $\{1, 2, \dots, n\}$ is between $2^{\pi(n)} \cdot e^{(\frac{1}{2}+o(1))\sqrt{n}}$ and $2^{\pi(n)} \cdot e^{(2+o(1))\sqrt{n}}$. We showed that neither of these bounds is tight: there are in fact $2^{\pi(n)} \cdot e^{(1+o(1))\sqrt{n}}$ such sets. The paper is under review.

In the paper titled "An improved upper bound for the size of the multiplicative 3-Sidon sets" the PI proved that the largest possible size of a multiplicative 3-Sidon set in $\{1, 2, \dots, n\}$ is at most $\pi(n) + \pi(n/2) + n^{2/3}(\log n)^{2^{1/3}-1/3}$. Here the main term $\pi(n) + \pi(n/2)$ is tight, the exponent $2/3$ is also tight, so the gap between the lower and upper bounds is in the exponent of $\log n$, this paper tightened this gap. The paper appeared in the International Journal of Number Theory.

Moreover, we shall mention some progress in terms of lower bounds, too. Namely, for the 5-Sidon case using an idea from the research plan of this project, Vizer and the PI

could improve on the lower bound. This work is in progress and will be continued after the end of this project.

In the paper titled "Monochromatic solutions to the equation $x + y = z^2$ in the interval $[N, cN^4]$" the PI gave a new, shorter proof for the existence of infinitely many monochromatic solutions of the equation $x + y = z^2$ for any 2-colouring of the integers. This question of Csikvári, Gyarmati and Sárközy was answered by Green and Lindqvist in 2016, who gave a 30 pages long proof. Green and Lindqvist describe their proof as "complicated and involves a surprisingly large number of tools from additive combinatorics and number theory". Our proof is rather short, uses different combinatorial ideas, and results in a slightly stronger statement: While Green and Lindqvist remark that their proof could be adapted to show the existence of a monochromatic solution in the interval $[n, cn^8]$, our proof implies the existence of such a solution in $[n, cn^4]$, and shows that the exponent 4 can not be further improved. The paper appeared in the Bulletin of the London Mathematical Society.

Recently, building on the technique developed in the previously described paper, the PI, jointly with Liu and Sándor, managed to extend the result to polynomials of higher degree in place of z^2. (Green and Lindqvist's technique could be adapted only to a class of 2-degree polynomials.) Namely, the PI and his coauthors proved that (under the necessary assumption that $p(1)p(2)$ is even) for any 2-colouring of $\mathbb{N}$ the equation $x + y = p(z)$ has infinitely many monochromatic solutions. Their method also provides a lower bound for the number of monochromatic solutions with $x, y, z \in \{1, 2, \dots, n\}$: the number of such monochromatic solutions is at least $n^{2/d^3 - o(1)}$, where $d = \deg p$. The paper, titled "Polynomial Schur's Theorem", is under review.

In the paper titled "On the density of sumsets and product sets" (joint with Hegyvári and Hennecart) we investigated the connection between the density of a subset of the positive integers and densities of sumsets, product sets, set of subset sums. In this paper we have given a partial answer to a question of Ruzsa by showing that under a certain condition on the set A the density of the set of the subset sums of A exists. We also proved that for every α and β (with $0 < \alpha < \beta < 1$) there is a set of integers having density 0 such that the lower- and upper asymptotic density of the product set AA is α and β, respectively. The paper appeared in the Australasian Journal of Combinatorics.

In the paper titled "Coloring the n-smooth numbers with n colors" (joint with Caicedo and Chartier) we addressed the following question: For which values of n is it possible to colour the positive integers using precisely n colours in such a way that for any a, the numbers $a, 2a, \dots, na$ all receive different colors? In case of an affirmative answer the result would be the strenghtening of a theorem of Balasubramanian and Soundararajan (the problem was formerly known as Graham's conjecture). The relationship of the two problems can be described as follows. Graham's conjecture can be stated in such a way that the clique number of a certain graph on the positive integers is n. (In this graph there are a lot of cliques of size n, so the conjectural part was that there is no larger clique.) The above mentioned problem can be reformulated as stating that the chromatic number

of this graph is also at most n. In the paper we showed that the answer is affirmative, if n is of the form $p-1$, $(p-1)/2$ or p^2-p (where p is a prime). (We shall note that no counterexample is known yet, and the first open case is $n = 195$.)

We also presented different reformulations of the problem (for instance, tiling $\mathbb{Z}^r$ with translates of a certain set) and its relationship with other questions (e.g. Pilz's conjecture). The paper is under review.

In the paper titled "Normal forms under Simons congruence" the PI investigated an algebraic problem about the combinatorics of words. Simon's congruence relates the words having the same subwords of length at most k. In this paper a normal form is presented for the equivalence classes for every k. Before, such a normal form was known only for $k = 1, 2, 3, 4$. As an application, using this normal form the number of equivalence class could be determined. The paper appeared in the Semigroup Forum.