Juin 2022

Séminaire BOURBAKI 73^e année, 2021–2022, nº 1196, p. 547 à 581 doi: 10.24033/ast.1197

RECENT PROGRESS ON BOUNDS FOR SETS WITH NO THREE TERMS IN ARITHMETIC PROGRESSION

[after Bloom and Sisask, Croot, Lev, and Pach, and Ellenberg and Gijswijt]

by Sarah Peluse

Introduction

Van der Waerden's theorem (VAN DER WAERDEN, 1927), one of the foundational results of Ramsey theory, states that if the integers are partitioned into finitely many sets, then one of these sets must contain nontrivial arithmetic progressions,

$$x, x+y, \dots, x+(k-1)y, \tag{1}$$

of all lengths. Here *nontrivial* means that $y \neq 0$ in (1). Motivated by van der Waerden's result, ERDŐS and TURÁN (1936) conjectured that every subset of the integers with positive upper density must contain arithmetic progressions of all lengths, or, equivalently, that any subset A of the first N integers containing no k-term arithmetic progressions satisfies $|A| = o_k(N)$. Thus, van der Waerden's theorem should hold because, in any finite partition of the integers, some part must have positive density.

Since any two distinct integers form a two-term arithmetic progression, the first nontrivial case of Erdős and Turán's conjecture is when k = 3. Define $r_3(N)$ to be the size of the largest subset of the first N integers containing no nontrivial arithmetic progressions, so that the k = 3 case of the conjecture is equivalent to $r_3(N) = o(N)$. This was first proven by ROTH (1953), who even produced an explicit bound for $r_3(N)$, using a variant of the circle method.

Theorem 0.1 (Rotн, 1953). We have

$$r_3(N) = O\left(\frac{N}{\log\log N}\right).$$

©Astérisque 438, SMF 2022

S. PELUSE

SZEMERÉDI (1975) proved Erdős and Turán's conjecture in full generality via a purely combinatorial argument in which he introduced his famous regularity lemma for graphs, now a fundamental tool in graph theory. There are now many proofs of Szemerédi's Theorem, most notably Furstenberg's proof using ergodic theory (FURSTENBERG, 1977), in which he introduced his famous correspondence principle and launched the field of ergodic Ramsey theory, and Gowers's proof of explicit quantitative bounds in Szemerédi's theorem (Gowers, 1998, 2001), which initiated the study of higher-order Fourier analysis.

We will, for the remainder of this exposition, mostly restrict our discussion to sets lacking three-term arithmetic progressions. It is now a central open problem in additive combinatorics to determine the best possible bounds in Roth's theorem, i.e., to determine the size of the largest subset of the first *N* integers containing no nontrivial three-term arithmetic progressions. This problem has catalyzed many important developments in additive and extremal combinatorics, spurring the invention of techniques that have had wide-ranging applications.

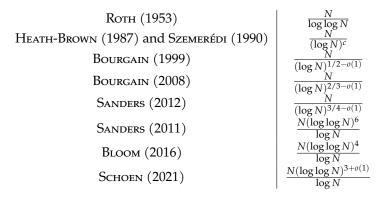
Beginning around the 1940's, Erdős repeatedly posed the conjecture that any subset *S* of the natural numbers satisfying

$$\sum_{n\in S}\frac{1}{n}=\infty$$

must contain arithmetic progressions of all lengths. It was also a very old, folklore conjecture that the primes contain arbitrarily long arithmetic progressions, and Erdős was interested in whether the primes (whose sum of reciprocals diverges) must contain arbitrarily long arithmetic progressions simply because they are sufficiently dense. This folklore conjecture is now known to be true thanks to celebrated work of GREEN and TAO (2008), who leveraged the pseudorandomness of the primes in their proof. Upper density and the divergence rate of $\sum_{n \in S} \frac{1}{n}$ are not quite equivalent notions of size, but, by partial summation, a bound of the quality $O_k\left(\frac{N}{(\log N)^{1+c}}\right)$, where c > 0, for the size of the largest subset of the first N integers containing no k-term arithmetic progressions would be sufficient to prove Erdős's conjecture. Over the past few decades, a sequence of works had improved Roth's bound right up to the $O\left(\frac{N}{\log N}\right)$ barrier. The table below summarizes these developments, where the second column lists bounds for the order of magnitude of $r_3(N)$ obtained by the authors in the first column.

548

ASTÉRISQUE 438



Here the *c* appearing in the second row is a small positive constant, the -o(1) in the exponent of log *N* in the third, fourth, and fifth rows hides bounded powers of log log *N* in the numerator, and the o(1) in the exponent of log log *N* in the last row hides a bounded power of log log log *N*.

Schoen's record upper bound for $r_3(N)$ appeared on the arXiv in May of 2020. Two months later, BLOOM and SISASK (2020) announced that they had finally broken through the $O\left(\frac{N}{\log N}\right)$ barrier in Roth's theorem, thus proving the first nontrivial case of Erdős's conjecture.

Theorem 0.2 (BLOOM and SISASK, 2020). *There exists an absolute constant* c > 0 *such that*

$$r_3(N) = O\left(\frac{N}{(\log N)^{1+c}}\right).$$

Therefore, any set *S* of natural numbers satisfying $\sum_{n \in S} \frac{1}{n} = \infty$ must contain a three-term arithmetic progression. Such sets include positive density subsets of the prime numbers, so that Theorem 0.2 also implies Green's Roth theorem in the primes (GREEN, 2005b).

We will now briefly discuss the known lower bounds for $r_3(N)$. By considering the integers whose ternary expansion contains no twos, it is easy to see that $r_3(N) = \Omega(N^{\log 2/\log 3})$. Salem and Spencer (1942) constructed subsets of the first N integers of density $\exp(-\log N/\log \log N)$ lacking three-term arithmetic progressions, showing that the true order of magnitude of $r_3(N)$ is larger than $N^{1-\varepsilon}$ for any fixed $\varepsilon > 0$. For this reason, sets free of three-term arithmetic progressions are sometimes called Salem–Spencer sets. A construction of Behrend (1946) shows that $r_3(N) = \Omega(N/\exp(C\sqrt{\log N}))$ for some absolute constant C > 0, which is still essentially the best known lower bound.

There is, then, the natural question of whether the true order of magnitude of $r_3(N)$ is closer to Behrend's lower bound or the upper bound of Bloom and Sisask. SCHOEN and SISASK (2016) have proven bounds of the form $O\left(N/\exp(C(\log N)^{1/7})\right)$

SOCIÉTÉ MATHÉMATIQUE DE FRANCE 2022

S. PELUSE

for subsets of the first *N* integers having no nontrivial solutions to the equation x + y + z = 3w. Since three-term arithmetic progressions are solutions to the equation x + y = 2z, it is reasonable to guess, by analogy, that $r_3(N)$ should also be on the order of $N / \exp(C(\log N)^c)$ for some absolute constants C, c > 0. Experts have, for a while, thought that a bound of this form is closer to the truth than, say, $\frac{N}{(\log N)^{100}}$, though it appears no one was brave enough to write down a conjecture. Bloom and Sisask have finally conjectured this in their paper, and they do not just reason by analogy–several of the steps of their proof are efficient enough to produce a bound of the form $O(N / \exp(C(\log N)^c))$.

When *G* is a finite abelian group of odd order, it is also natural to define $r_3(G)$ to be the size of the largest subset of *G* containing no nontrivial three-term arithmetic progressions, and to ask for upper and lower bounds on $r_3(G)$. Obtaining bounds for $r_3(\mathbf{Z}/M\mathbf{Z})$ as *M* tends to infinity is essentially equivalent to obtaining bounds in Roth's theorem in the integer setting. Another family of groups of great interest are the finite dimensional \mathbf{F}_3 -vector spaces. Subsets of \mathbf{F}_3^n lacking three-term arithmetic progressions are called *cap-sets*, and the problem of bounding $r_3(\mathbf{F}_3^n)$, known as the *cap-set problem*, has an old history. Nontrivial three-term arithmetic progressions are exactly the lines in \mathbf{F}_3^n , and, more generally, sets (in finite, real, or complex affine or projective space) with no-three-on-a-line are popular objects of study in discrete and combinatorial geometry.

BROWN and BUHLER (1982) were the first to prove $r_3(\mathbf{F}_3^n) = o(3^n)$. This fact, like $r_3(N) = o(N)$, is also a straightforward consequence of the *triangle removal lemma*, which states that, for every $\varepsilon > 0$, there exists a $\delta > 0$ such that any graph on M vertices containing δM^3 triangles can be made triangle-free by removing at most εM^2 edges. This was observed by FRANKL, GRAHAM, and RÖDL (1987), who then asked whether there exists a positive constant c < 3 such that $r_3(\mathbf{F}_3^n) = O(c^n)$. Alon and DUBINER (1993) also posed this question. By adapting Roth's argument to the setting of \mathbf{F}_3 -vector spaces, MESHULAM (1995) proved the first explicit bounds for the size of cap-sets.

Theorem 0.3 (MESHULAM, 1995). We have

$$r_3(\mathbf{F}_3^n) = O\left(\frac{3^n}{n}\right).$$

The quantity 3^n , which is the size of \mathbf{F}_3^n , is analogous to the length N of the interval $\{1, \ldots, N\}$ in Roth's theorem. Thus, Meshulam's result corresponds to a bound of the strength $O\left(\frac{N}{\log N}\right)$ in Roth's theorem.

The family of vector spaces $(\mathbf{F}_3^n)_{n=1}^{\infty}$ can serve as a useful testing ground for ideas and techniques to improve Roth's theorem in the integer setting, since many technical aspects are greatly simplified when working in \mathbf{F}_3^n . The surveys by GREEN (2005a) and

ASTÉRISQUE 438

Wolf (2015) give nice overviews of this philosophy. The setting of vector spaces over finite fields is often referred to in additive combinatorics as the "finite field model setting", and we will also use this terminology. In breakthrough work, BATEMAN and KATZ (2012) proved that $r_3(\mathbf{F}_3^n) = O\left(\frac{3^n}{n^{1+c}}\right)$ for some absolute constant c > 0, and their insights obtained in the finite field model setting were crucial in the work of BLOOM and SISASK (2020) in the integer setting.

Up until a few years ago, all quantitative improvements to the arguments of Roth and Meshulam were (increasingly more difficult and technical) refinements of Roth's original Fourier-analytic argument. In 2016, CROOT, LEV, and PACH (2017) introduced a new version of the polynomial method, which they used to prove that any subset of $(\mathbf{Z}/4\mathbf{Z})^n$ lacking three-term arithmetic progressions has cardinality at most $O(3.61^n)$, greatly improving upon the previous best bound of $O\left(\frac{4^n}{n(\log n)^c}\right)$ due to SANDERS (2009). Very shortly after, ELLENBERG and GIJSWIJT (2017) adapted the method of Croot, Lev, and Pach to prove a power-saving bound for the size of cap-sets, thus answering the question of Frankl, Graham, and Rödl.

Theorem 0.4 (ELLENBERG and GIJSWIJT, 2017). We have

 $r_3(\mathbf{F}_3^n) = O(2.756^n).$

The arguments of Croot–Lev–Pach and Ellenberg–Gijswijt are completely disjoint from the prior Fourier-analytic arguments, and constitute yet another instance of the polynomial method producing an elegant solution to a famous problem, joining (among other works) Dvir's solution of the finite field Kakeya problem (Dvir, 2009) and the work of Guth and Katz on the joints problem (Guth and Katz, 2010) and the Erdős distinct distances problem (Guth and Katz, 2015). EDEL (2004) has constructed cap-sets in \mathbf{F}_3^n of size $\Omega(2.217^n)$, so there is still an exponential gap between the best known upper and lower bounds for $r_3(\mathbf{F}_3^n)$.

In this exposition, we will survey the methods going into the two breakthrough results stated in Theorems 0.2 and 0.4. We will begin by introducing Roth's basic method in the finite field model and integer settings in Section 1, and then give an overview of most of the ingredients in Bloom and Sisask's argument in Section 2 before discussing their proof, with a focus on spectral boosting, in Section 3. We will then present a full proof of Theorem 0.4 in Section 4.

Acknowledgement. — I would like to thank Thomas Bloom, Jordan Ellenberg, Ben Green, Olof Sisask, Kannan Soundararajan, Avi Wigderson, and Nicolas Bourbaki for helpful comments on earlier drafts.

SOCIÉTÉ MATHÉMATIQUE DE FRANCE 2022