THEORY OF COMPUTING LIBRARY
GRADUATE SURVEYS 887 (2016), pp. 1–53
www.theoryofcomputing.org

Additive Combinatorics and its Applications in Theoretical Computer Science

Shachar Lovett[*]

Received October 1, 2013; Published August 21, 2016

Abstract: Additive combinatorics (or perhaps more accurately, arithmetic combinatorics) is a branch of mathematics which lies at the intersection of combinatorics, number theory, Fourier analysis and ergodic theory. It studies approximate notions of various algebraic structures, such as vector spaces or fields. In recent years, several connections between additive combinatorics and theoretical computer science have been discovered. Techniques and results in additive combinatorics were applied to problems in coding theory, property testing, hardness of approximation, computational complexity, communication complexity, randomness extraction and pseudo-randomness. The goal of this survey is to provide an introduction to additive combinatorics for students and researchers in theoretical computer science, to illustrate some of the exciting connections to classical problems in computer science, and to describe the many open problems that remain.

1 Introduction

Additive combinatorics (or perhaps more accurately, arithmetic combinatorics) is a branch of mathematics which lies at the intersection of combinatorics, number theory, Fourier analysis and ergodic theory. It

[*] Supported by NSF CAREER award 1350481.

ACM Classification: F.2.2, G.2.3

AMS Classification: 68Q17, 68Q25

Key words and phrases: additive combinatorics, theoretical computer science

DOI: 10.4086/toc.gs.2016.887

studies approximate notions of algebraic structures. As an illustrative example, consider the following problem. Let G be an Abelian group, and let A be a subset of G. The sumset of A is $A+A = \{a+a' : a,a' \in A\}$. It is easy to see that $|A+A| \geq |A|$ and that equality holds only when A is a subgroup of G, or a coset of a subgroup. A classic question studied in additive combinatorics is what is the structure of A when $A+A$ is not much larger than A. In particular, one would like to show that in such a case, A is in an "approximate subgroup" in some sense. For example, it could be that A is a dense subset of a subgroup.

In recent years, several connections between additive combinatorics and theoretical computer science have been discovered. Techniques and results in additive combinatorics were applied to problems in coding theory, property testing, hardness of approximation, computational complexity, communication complexity, randomness extraction and pseudo-randomness. In general, these advances occurred because additive combinatorics provided new tools to study the structures arising in various computational settings.

The goal of this survey is to provide an introduction to additive combinatorics for students and researchers in theoretical computer science. This is the main driving force behind the choice of topics covered, as well as the applications of them which are presented. By far, this is not a comprehensive survey. We chose to present proofs of the more basic results in order to give the flavour of the different techniques, and to refer to the original papers for the more advanced proofs. In this survey, we focus on three main topics: the structure of set addition, arithmetic progressions in sets, and the sum-product phenomena. For each, we cover basic results with detailed proofs, state more advanced results, and give several applications in computer science. Notably, an area which is not covered in this survey is higher-order Fourier analysis. This is an emerging field which greatly generalizes the classic theory of Fourier analysis, and which has deep connections to additive combinatorics. However, in order to keep this survey concise, we decided to defer an exposition of higher-order Fourier analysis and its applications in theoretical computer science to a future survey.

There are several other very useful resources on additive combinatorics, which readers may wish to consult:

- The book "Additive Combinatorics" by Tao and Vu [67] gives a detailed description of many results in additive combinatorics and their applications, mainly in number theory.

- A mini-course on additive combinatorics by Barak et al. [6] explores basic ideas in additive combinatorics and some of their applications in computer science.

- The survey "Finite field models in additive combinatorics" by Green [31].

- The survey "Selected Results in Additive Combinatorics: An Exposition" by Viola [69] covers the basic results related to set addition and their application in Samorodnitsky's theorem [57] on linearity testing for functions with multiple outputs.

- The survey "The polynomial Freiman–Ruzsa conjecture" by Green [32] explores the polynomial Freiman–Ruzsa conjecture, one of the central open problems in this area. A more specialized survey by the author [44] gives an exposition of a recent important result by Sanders [61] which gets close to proving this conjecture.

- The survey "Additive combinatorics and theoretical computer science" by Trevisan [68] covers in high level many of the recent advances in additive combinatorics, and discusses their relations to problems arising in theoretical computer science.

- The survey “Additive combinatorics: with a view towards computer science and cryptography–an exposition” by Bibak [12] covers a number of results in additive combinatorics, motivated by cryptographic applications.
- The survey “Additive combinatorics over finite fields: New results and applications” by Shparlinski [62] discusses recent results in additive combinatorics.

Acknowledgements. I thank the anonymous referees for a careful reading of this manuscript.

2 Set addition

Let G be an Abelian group, where a motivating example to have in mind is $G = \mathbb{F}^n$ (i. e., a vector space over a field). Let A be a finite subset of the group. The *sumset* of A is defined to be the set

$$2A = A + A = \{a + a' : a, a' \in A\}.$$

It is simple to see that $|2A| \geq |A|$. Equality holds only if A is either empty, or a subgroup of G, or a coset of a subgroup. Indeed, if $A \neq \emptyset$ then we can assume $0 \in A$ by shifting A (that is, replacing A by $A - a_0 = \{a - a_0 : a \in A\}$ for some $a_0 \in A$). This does not change the size of A or $2A$. Now, since $0 \in A$ we have $A \subseteq 2A$. Moreover, since by assumption $|2A| = |A|$ then in fact $2A = A$. That is, A is a nonempty finite subset closed under addition, and hence is a subgroup of G.

The focus of this chapter is on relaxations of this simple claim. We will consider various notions of *approximate subgroups* and how they relate to each other.

2.1 Ruzsa calculus

Ruzsa calculus is a set of basic inequalities between sizes of sets and their sumsets. Despite being basic, it is very useful. Let A, B be two subsets of an Abelian group G. Define $A + B = \{a + b : a \in A, b \in B\}$ and $A - B = \{a - b : a \in A, b \in B\}$ to be their sumset and difference set, respectively. We start with the Ruzsa triangle inequality, which is both simple and useful.

Claim 2.1 (Ruzsa triangle inequality)**.** *Let A, B, C be subsets of G. Then*

$$|A||B - C| \leq |A - B||A - C|.$$

Proof. The main idea is that any element $b - c \in B - C$ can be written in $|A|$ distinct ways as $b - c = (a - c) - (a - b)$. Formally, define a map $f : A \times (B - C) \to (A - B) \times (A - C)$ as follows: for any $x \in B - C$ fix a representation $x = b - c$ with $b \in B, c \in C$, and map $f(a, x) = (a - b, a - c)$. This map is injective, hence $|A||B - C| \leq |A - B||A - C|$. □

Definition 2.2 (Ruzsa distance)**.** The *Ruzsa distance* between sets A, B is defined as

$$d(A, B) = \log \frac{|A - B|}{|A|^{1/2}|B|^{1/2}}.$$

The Ruzsa distance is not formally a distance function, since $d(A,A) \neq 0$. However, it does satisfy the other requirements from a distance function: symmetry and triangle inequality.

Claim 2.3. *The Ruzsa distance is symmetric and obeys the triangle inequality.*

Proof. Symmetry holds since $|B-A| = |A-B|$. We need to prove that $d(A,C) \leq d(A,B) + d(B,C)$, which is equivalent to

$$|B||A-C| \leq |B-A||B-C|.$$

This follows from Claim 2.1 applied to B,A,C. □

Ruzsa distance can be used to show that various notions of "bounded growth" are related to each other. For example, the following claim (specialized to the case $A = B$) shows that if $|A+A| \leq K|A|$ then $|A-A| \leq K^2|A|$. We will see more general forms of such relations later.

Corollary 2.4. *Let A,B be subsets of G. Assume that $|A-B| \leq K|A|^{1/2}|B|^{1/2}$. Then $|A-A| \leq K^2|A|$.*

Proof.

$$\frac{|A-A|}{|A|} = \exp(d(A,A)) \leq \exp(d(A,B) + d(B,A)) = \frac{|A-B|^2}{|A||B|} \leq K^2.$$

□

2.2 The span of sets of small doubling

Let A be a subset of an Abelian group G. The *doubling constant* of A is $K = |A+A|/|A|$. We would like to understand the structure of sets with small doubling, and similarly the structure of sets for which $|A-A| \leq K|A|$. We already saw that $K = 1$ corresponds to subgroups of G. Hence, we might expect that small values of K correspond to sets which are close in some sense to a subgroup. The first question we would like to understand is what is the size of the smallest subgroup containing A. For example, when $G = \mathbb{F}^n$ is a vector space over a field $\mathbb{F}$ of prime order this is equivalent to the size of the linear subspace spanned by A.

We start by an argument of Laba [42] showing that when $|A-A| < (3/2)|A|$ the set A is close to a subgroup in a very strong sense: $A-A$ is already a subgroup. The constant $3/2$ is tight, as can be seen by taking $A = \{0,1\} \subset \mathbb{Z}$.

Lemma 2.5 (Laba)**.** *Let $A \subset G$ be a set such that $|A-A| < (3/2)|A|$. Then $A-A$ is a subgroup of G.*

Proof. We will show that for any $x \in A-A$ we have

$$|A \cap (A+x)| > |A|/2.$$

This implies that for any $x,y \in A-A$ we have that $(A+x) \cap (A+y)$ is nonempty. Indeed, if we shorthand $A_x = A \cap (A+x)$ then by the inclusion-exclusion principle,

$$|(A+x) \cap (A+y)| \geq |A_x \cap A_y| \geq |A_x| + |A_y| - |A_x \cup A_y| > |A|/2 + |A|/2 - |A| = 0.$$

Hence, there are $a_1, a_2 \in A$ such that $a_1 + x = a_2 + y$. This means that $x - y = a_2 - a_1 \in A - A$. Thus, $A - A$ is closed under taking differences and hence must be a subgroup. Now, let $x = a - a'$ where $a, a' \in A$. Then

$$|A \cap (A + x)| = |(A - a) \cap (A - a')|.$$

Since $A - a$, $A - a'$ are both subsets of $A - A$ of size $|A - a| = |A - a'| = |A|$, we have by the inclusion-exclusion principle that

$$|A \cap (A + x)| = |(A - a) \cap (A - a')| \geq |A - a| + |A - a'| - |A - A| > |A|/2.$$

□

The structure of A with general bounded doubling is unfortunately more complicated. In the special case of $G = \mathbb{R}^n$ Freiman [28] showed that sets of small doubling must be contained in a low dimensional affine subspace, by a relatively simple argument based on the convexity of Euclidean space. We will later see analogs of this result over other general Abelian groups, where the proofs are more complex.

Lemma 2.6 (Freiman)**.** *Let $A \subset \mathbb{R}^n$ with $|A + A| \leq K|A|$. Then A lies in an affine subspace of dimension at most $2K$.*

The dimension in the lemma is tight up to lower order terms, as can be seen by choosing A to be a set of $2K$ linearly independent vectors.

Proof. We will prove the following: if A has affine dimension d then

$$|A + A| \geq (d+1)|A| - \binom{d+1}{2}.$$

Since $|A| \geq d$ this implies that if $|A + A| \leq K|A|$ then $d \leq 2K - 1$. We will prove the claim by induction on $|A|$. If $A = 1$ then $|A + A| = 1, d = 0$ and claim follows. So, we assume from now on that $|A| > 1$. Let $M(A) = \{(a + a')/2 : a, a' \in A\}$ be the set of "mid-points" of A. Clearly, $|M(A)| = |A + A|$.

Let $C(A)$ be the convex hull of the points in A. That is, $C(A)$ is the minimal convex body containing A, which by assumption is a d-dimensional polytope. The vertices of $C(A)$ are the points $a \in A$ which cannot be obtained as a convex combination of the other points $A - \{a\}$. We say that two vertices a, a' of $C(A)$ are neighbors if the segment connecting them is a one-dimensional face of $C(A)$.

Let $a^* \in A$ be an arbitrary vertex of $C(A)$, and let $A' = A \setminus \{a^*\}$. There are two cases to consider:

(i) The affine dimension of A' is $d - 1$. In this case, the mid-points $(a + a^*)/2$ for all $a \in A$ are outside $C(A')$. Hence,

$$|M(A)| \geq |A| + |M(A')| \geq |A| + d|A'| - \binom{d}{2} = (d+1)|A| - d - \binom{d}{2} = (d+1)|A| - \binom{d+1}{2}.$$

(ii) The affine dimension of A' is d. Let $a_1, \ldots, a_t \in A'$ be the neighboring vertices to a^* in $C(A)$. Since $C(A)$ is d-dimensional we have $t \geq d$. The points a^* and $(a^* + a_i)/2$ for $1 \leq i \leq t$ are mid-points outside $C(A')$. Hence,

$$|M(A)| \geq (t+1) + |M(A')| \geq d + 1 + (d+1)|A'| - \binom{d+1}{2} = (d+1)|A| - \binom{d+1}{2}.$$

□

Ruzsa [55] established an analog of Freiman's theorem for arbitrary Abelian groups of bounded torsion. In the following, a group G has torsion $r \geq 1$ if $r \cdot g = 0$ for all $g \in G$.

Theorem 2.7 (Ruzsa)**.** *Let G be an Abelian group of torsion r. Let $A \subset G$ be a subset with $|A+A| \leq K|A|$. Then there exists a subgroup $H < G$ of size $|H| \leq K^2 r^{K^4} |A|$ such that $A \subset H$.*

Before proceeding to prove Theorem 2.7, let us first consider the parameters in it. Consider the following example. Let $G = \mathbb{F}_p^n$, a vector space over a finite field $\mathbb{F}_p$, which has torsion $r = p$. Let $U, V \subset \mathbb{F}_p^n$ be two subspaces with $U \cap V = \{0\}$ and set $A = U + \{v_1, \ldots, v_{2K}\}$ where $v_1, \ldots, v_{2K} \in V$ are linearly independent. Then $A + A = U + \{v_i + v_j : 1 \leq i \leq j \leq 2K\}$ and $|A+A|/|A| \approx K$. However, the size of the minimal subspace containing A is $p^{2K}|U| = (p^{2K}/2K)|A|$. Thus, an exponential dependency on K is unavoidable in the relation between the doubling constant and the size of the minimal subgroup containing the whole set. We will later see a conjecture (Marton's "Polynomial Freiman–Ruzsa conjecture") which speculates that a polynomial dependency on K is possible if the subspace is required to contain only a noticeable fraction of A, and not all of A like we require here. This polynomial dependency seems to be crucial for many applications in computer science.

In the current settings, the above example led to the following conjecture of Ruzsa on the optimal parameters for his theorem [55].

Conjecture 2.8 (Ruzsa)**.** *There exists an absolute constant $C \geq 2$ such that the following holds. For any Abelian group G of torsion r, and any subset $A \subset G$ with $|A+A| \leq K|A|$, the subgroup generated by A has order $\leq r^{CK}|A|$.*

A sequence of papers [23, 58, 34, 40, 25] established this conjecture for torsion $r = 2$ i. e., to the groups $G = \mathbb{F}_2^n$) with $C = 2$, and [26] extended it to any prime torsion, also with $C = 2$.

Theorem 2.9 ([26])**.** *Let p be a prime. Let $A \subset \mathbb{F}_p^n$ be a subset with $|A+A| \leq K|A|$. Then there exists a subspace $H \subset \mathbb{F}_p^n$ such that $A \subset H$ and $|H| \leq \frac{p^{2K-2}}{2K-1}|A|$.*

We will focus here on the proof of Theorem 2.7, as it is more general and allows us to introduce another important theorem: sets of small doubling don't grow too much even with repeated additions and subtractions. We will only use the following special case. The proof of it is deferred to Section 2.3 where we prove a more general result. In the following, recall that $2A = A + A$.

Theorem 2.10. *Let $A \subset G$. If $|2A| \leq K|A|$ then $|2A - 2A| \leq K^4|A|$.*

Proof of Theorem 2.7 assuming Theorem 2.10. Let $A \subset G$ be such that $|2A| \leq K|A|$. We may assume $0 \in A$ by possibly replacing A with $A - a$ for some $a \in A$. We will bound the size of the subgroup spanned by A.

We start by an approach known as "Ruzsa covering." Let $B = \{b_1, \ldots, b_m\} \subseteq 2A - A$ be a maximal collection of elements such that the sets $b_i - A$ are all disjoint. We will show that $\ell A - A \subset (k-1)B + A - A$ for all $\ell \geq 1$. The assumption that A has small doubling implies that $|B|$ is bounded, from which the theorem follows.

First, we bound the size of B. Since $b_i - A \subset 2A - 2A$ we have that

$$m \le |2A - 2A|/|A| \le K^4.$$

We first argue that $2A - A \subseteq B + A - A$. To see that, choose any $x \in 2A - A$. By construction there exists $b \in B$ such that $(x - A) \cap (b - A) \neq \emptyset$. That is, $x - a = b - a'$ for some $a, a' \in A$. Hence $x = b + a - a' \in B + A - A$. As a corollary, we get that for any $\ell \ge 1$,

$$\ell A - A \subseteq (\ell - 1)B + A - A.$$

The proof is by induction on ℓ:

$$\ell A - A = A + ((\ell - 1)A - A) \subseteq A + (\ell - 2)B + A - A \subseteq (\ell - 1)B + A - A.$$

Now, let $\langle A \rangle$ be the subgroup of G spanned by A, and $\langle B \rangle$ be the subgroup spanned by B. Then

$$\langle A \rangle = \bigcup_{\ell \ge 1} \ell A \subseteq \bigcup_{\ell \ge 1} (\ell A - A) \subseteq \bigcup_{\ell \ge 1} (\ell - 1)B + A - A = \langle B \rangle + A - A.$$

Hence we get that

$$|\langle A \rangle| \le |\langle B \rangle| \cdot |A - A| \le |\langle B \rangle| \cdot K^2 |A|,$$

where we applied Corollary 2.4 to bound $|A - A|$. To conclude, we need to bound the size of $\langle B \rangle$. As the group G has torsion r and $|B| \le K^4$ we have $|\langle B \rangle| \le r^{K^4}$ which concludes the proof. □

2.3 The growth of sets of small doubling

Assume that $|A + A|$ is not much larger than $|A|$. How large can be $|A + A + A|$? or $|A + A - A - A|$? The following theorem of Plünneke [47] which was re-discoverd by Ruzsa [54] gives a nearly complete answer. Define the ℓ-th iterated sumset of A as

$$\ell A = \{a_1 + \ldots + a_\ell : a_1, \ldots, a_\ell \in A\},$$

and more generally for $\ell, m \ge 1$ define

$$\ell A - mA = \{a_1 + \ldots + a_\ell - a_{\ell+1} - \ldots - a_{\ell+m} : a_1, \ldots, a_{\ell+m} \in A\}.$$

Theorem 2.11 (Plünneke–Ruzsa theorem)**.** *Let $A, B \subset G$ be sets of equal size $|A| = |B|$ such that $|A + B| \le K|A|$. Then $|\ell A - mA| \le K^{\ell+m}|A|$.*

Specializing to $B = A$ or $B = -A$, we obtain the following corollary.

Corollary 2.12. *If $|A + A| \le K|A|$ or $|A - A| \le K|A|$ then $|\ell A - mA| \le K^{\ell+m}|A|$.*

The original proof of Theorem 2.11 was based on graph theory and was quite involved. Recently, a much simpler proof was discovered by Petridis [46]. We present his proof below. The main technical step is the following lemma.

Lemma 2.13. *Let $A, B \subseteq G$ be sets of equal size $|A| = |B|$ with $|A+B| \le K|A|$. Let $B_0 \subseteq B$ be a nonempty set minimizing the ratio $K_0 = |A+B_0|/|B_0|$. Then for any set $C \subseteq G$,*

$$|A+B_0+C| \le K_0|B_0+C|.$$

Proof. We start with an important observation: by the minimality of K_0, for any set $B' \subseteq B$ we have $|A+B'| \ge K_0|B'|$. The proof now follows by induction on $|C|$. If $C = \{x\}$ then the lemma holds as

$$|A+B_0+x| = |A+B_0| = K_0|B_0| = K_0|B_0+x|.$$

If $|C| > 1$ then decompose $C = C' \cup \{x\}$. Let $B' \subseteq B_0$ be defined as

$$B' = \{b \in B_0 : A+b+x \subseteq A+B_0+C'\}.$$

Then, we can decompose $A+B_0+C$ as

$$A+B_0+C = (A+B_0+C') \cup ((A+B_0+x) \setminus (A+B'+x)).$$

This allows us to bound the size of $A+B_0+C$ inductively by

$$\begin{aligned} |A+B_0+C| &\le |A+B_0+C'| + |(A+B_0+x) \setminus (A+B'+x)| \\ &\le K_0|B_0+C'| + |A+B_0| - |A+B'| \\ &\le K_0(|B_0+C'| + |B_0| - |B'|), \end{aligned}$$

where we used the facts that $A+B'+x \subseteq A+B_0+x$ and the assumption on B_0. To conclude, we need to show that $|B_0+C'| + |B_0| - |B'| \le |B_0+C|$. Let $B'' \subseteq B_0$ be defined as

$$B'' = \{b \in B_0 : b+x \in B_0+C'\}.$$

Note that $B'' \subseteq B'$. We can decompose B_0+C as a disjoint union

$$B_0+C = (B_0+C') \cup ((B_0+x) \setminus (B''+x)).$$

Hence,

$$|B_0+C| = |B_0+C'| + |B_0| - |B''| \ge |B_0+C'| + |B_0| - |B'|$$

which is what we needed to show. □

Proof of Theorem 2.11. Let $B_0 \subseteq B$ be as in Lemma 2.13. By induction on ℓ we have that

$$|B_0+\ell A| \le K_0^{\ell}|B_0| \le K^{\ell}|B_0|.$$

By the Ruzsa triangle inequality (Claim 2.1) applied to $-B_0, \ell A, mA$ we have

$$|B_0||\ell A - mA| \le |B_0+\ell A||B_0+mA| \le K^{\ell+m}|B_0|^2$$

and hence

$$|\ell A - mA| \le K^{\ell+m}|B_0| \le K^{\ell+m}|A|.$$

□

2.4 Statistical set addition

Assume that A is a set where most sums a_1+a_2 lie in a small set, but not all of them. It might be the case that $A+A$ is much larger than A, as the following example shows. Take $A \subset \mathbb{F}_2^n$ as the union of a subspace V of dimension d (which has size $|V| = 2^d$) and a random subset of $\mathbb{F}_2^n$ of size 2^d. Then at least a $1/4$ of the sums a_1+a_2 for $a_1, a_2 \in A$ lie in V, but still with high probability $|A+A| \approx 2^d|A|$. However, A has a large subset (namely V) which has small doubling.

This example motivates the following question: if many sums in A lie in a small set, is it always the case that a large subset of A has a small doubling constant. The answer is yes, and this was first proved by Balog and Szemerédi [3] with poor quantitative bounds. Later, Gowers [30] found a simpler proof which also obtains much stronger quantitative bounds (improving exponential loss of parameters to a polynomial loss). This theorem is now known as the BSG (Balog-Szemerédi-Gowers) Theorem and is central in a large number of applications, both in mathematics and in computer science. We will present a variant of the proof due to Sudakov, Szemerédi and Vu [64]; the reader is also referred to an exposition of Viola [69] for a somewhat simplified proof over $\mathbb{F}_2^n$.

Theorem 2.14 (BSG Theorem [3, 30, 64])**.** *Let $A, B \subset G$ be sets of equal size $|A| = |B| = N$. Assume that there exists a set $C \subset G$ of size $|C| = cN$ such that*

$$\Pr_{a\in A, b\in B}[a+b \in C] \geq \varepsilon,$$

where $a \in A, b \in B$ are chosen uniformly and independently. Then there exist subsets $A' \subset A, B' \subset B$ of size $|A'|, |B'| \geq (\varepsilon^2/16)N$ such that $|A'+B'| \leq 2^{12}c^3(1/\varepsilon)^5 \cdot N$.

Note that in particular, we also have $|A'+A'| \leq \mathrm{poly}(c, 1/\varepsilon) \cdot N$ by Theorem 2.11. The proof of Theorem 2.14 is based on the following lemma in graph theory. It states that in any dense graph, there is a large subset of the vertices, such that for any pair of vertices in this large set there are many short paths between them.

Lemma 2.15 (Sudakov [64])**.** *Let $H = (A, B, E)$ be a bipartite graph with vertex sets A, B and edge set $E \subset A \times B$. Assume that $|A| = |B| = N$ and $|E| = \varepsilon N^2$. Then there exist $A' \subset A, B' \subset B$ of size $|A'|, |B'| \geq (\varepsilon^2/16)N$ such that for any $a \in A', b \in B'$ there are at least $2^{-12}\varepsilon^5 N^2$ paths of length 3 between a and b.*

We first prove Theorem 2.14 based on Lemma 2.15.

Proof of Theorem 2.14 assuming Lemma 2.15. Let H be the bipartite graph with vertex sets A, B and edge set $E = \{(a,b) : a+b \in C\}$. Applying Lemma 2.15 to H, let $A' \subset A, B' \subset B$ be the guaranteed subsets. We will upper bound $|A'+B'|$. For any $a \in A', b \in B'$, consider a path (a, b', a', b). Clearly,

$$y = a+b = (a+b') - (a'+b') + (a'+b) = x - x' + x'',$$

where $x = a+b', x' = a'+b', x'' = a'+b$ are elements of C, since they are all edges of the graph H. Moreover, any element $y \in A'+B'$ can be represented as $y = x - x' + x''$ for at least $2^{-12}\varepsilon^5 N^2$ ordered triples (x,x',x'') with $x,x',x'' \in C$. On the other hand, C has cardinality cN and hence there at c^3N^3 such triples in total. Hence,

$$|A'+B'| \le \frac{c^3N^3}{2^{-12}\varepsilon^5N^2} = 2^{12}c^3(1/\varepsilon)^5N.$$

□

We next prove Lemma 2.15. The main idea is the following simple but powerful observation called *dependent random choice*. In high level, it says that random neighbors of a random vertex in a graph have many common neighbors. In our context, let $v \in A$ be a randomly chosen vertex and let B' be the set of neighbors of v. The dependent random choice principle implies that most pairs of vertices in B' have many common neighbors. If we remove atypical vertices in B', which belong only to a few such pairs, we get a stronger property: for any $b \in B'$, for most $b' \in B'$ we have that b,b' have many common neighbors. We then choose A' to be the set of nodes with many neighbors in B'. Then, for any $a \in A', b \in B'$ there are many $b' \in B'$ which are neighbors of a, such that (b,b') have many common neighbors. This implies that there are many paths of length 3 between a and b.

Proof of Lemma 2.15. Let $H=(A,B,E)$ with $|A|=|B|=N$ and $|E|=\varepsilon N^2$. The average degree of a vertex in H is εN. We first delete all vertices from B of degree $\le (\varepsilon/2)N$. As we can delete at most $(\varepsilon/2)N^2$ edges this way, the resulting graph has $\ge (\varepsilon/2)N^2$ edges. For convenience we keep the same notation. That is, we assume $H=(A,B,E)$ with $|A|=N, N/2 \le |B| \le N$ and where any vertex in B has degree at least $(\varepsilon/2)N$.

Let $v \in A$ be a uniformly chosen vertex, and let $\Gamma(v) \subset B$ be the set of neighbours of v. We prove a few properties of $\Gamma(v)$. Let $X = |\Gamma(v)|$ be a random variable counting the number of neighbors of v. Its expected value is

$$\mathbb{E}[X] = \frac{\sum_{v\in A}|\Gamma(v)|}{|A|} = \frac{|E|}{|A|} \ge (\varepsilon/2)N.$$

We call a pair of vertices $b,b' \in B$ *bad* if the number of common neighbors of (b,b') is less than $(\varepsilon^3/128)N$. Let Y be a random variable counting the number of bad pairs which belong to $\Gamma(v)$. For any fixed bad pair (b,b'), the probability that $b,b' \in \Gamma(v)$ is equal to the probability that v is one of the common neighbors of b,b', hence

$$\Pr_v[b,b' \in \Gamma(v)] \le \varepsilon^3/128.$$

Since $|B| \le N$ there are at most $\binom{N}{2}$ pairs in total, and in particular bad pairs. Thus, by linearity of expectation,

$$\mathbb{E}[Y] \le (\varepsilon^3/128)\cdot\binom{N}{2} \le (\varepsilon^3/256)N^2.$$

Let $\tilde{B} \subset \Gamma(v)$ be the set of vertices $b \in \Gamma(v)$ which form a bad pair with at least $(\varepsilon^2/32)N$ other elements $b' \in \Gamma(v)$. Let $Z = |\tilde{B}|$ be a random variable counting the number of such vertices. Then

$$Z\cdot(\varepsilon^2/32)N \le 2Y,$$

where the factor 2 is due to the fact that a bad pair (b,b') can be counted twice. Hence

$$\mathbb{E}[Z] \le (64/\varepsilon^2 N) \cdot \mathbb{E}[Y] \le (\varepsilon/4)N.$$

We set $B' = \Gamma(v) \setminus \tilde{B}$. By linearity of expectation,

$$\mathbb{E}[|B'|] = \mathbb{E}[X] - \mathbb{E}[Z] \ge (\varepsilon/4)N.$$

Hence, there is a choice for $v \in A$ such that $|B'| \ge (\varepsilon/4)N$; and for any $b \in B'$ there are at most $(\varepsilon^2/32)N$ elements $b' \in B'$ such that (b,b') is a bad pair. Fix such B'.

Next, we define $A' = \{a \in A : |\Gamma(a) \cap B'| \ge (\varepsilon^2/16)N\}$. We first show that A' is not too small. The number of edges between A and B' is

$$|E(A,B')| \le |A'| \cdot |B'| + (\varepsilon^2/16)N \cdot |A \setminus A'| \le N|A'| + (\varepsilon^2/16)N^2.$$

On the other hand, any element $b \in B$ has degree at least $(\varepsilon/2)N$, hence

$$|E(A,B')| \ge (\varepsilon/2)N \cdot |B'| \ge (\varepsilon^2/8)N^2.$$

Combining the two estimates, we obtain that

$$|A'| \ge (\varepsilon^2/16)N^2.$$

Finally, we show that for any $a \in A', b \in B'$ there are many paths of length 3 connecting a and b. Indeed, there are at least $(\varepsilon^2/16)N$ neighbors b' of a in B'. Out of which, at most $(\varepsilon^2/32)N$ form a bad pair with b. Thus, there are $(\varepsilon^2/32)N$ choices for $b' \in \Gamma(a) \cap B'$ such that (b,b') is not a bad pair. That is, there are at least $(\varepsilon^3/128)N$ common neighbors a' of b,b'. These define a path of length 3 between a and b, namely (a,b',a',b). The number of these paths is hence at least

$$(\varepsilon^2/32)N \cdot (\varepsilon^3/128)N = 2^{-12}\varepsilon^5 N.$$

□

2.5 Linearity testing

The first application of additive combinatorics that we will see will be in property testing. Property testing asks whether specific properties of large objects can be efficiently detected by algorithms, which only access a small part of these objects. It was initiated by the work of Blum, Luby, and Rubinfeld [14] who observed that given a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, it is possible to inquire the value of f on a few random points, and accordingly probabilistically distinguish between the case that f is a linear function and the case that f has to be modified on at least a noticeable fraction of points to become a linear function. This test is now known as the BLR (Blum-Luby-Rubinfeld) test, and we will discuss it shortly.

Inspired by this observation, Rubinfeld and Sudan [53] defined the concept of property testing which is now a major area of research in theoretical computer science. Roughly speaking, to test a function for a property means to examine the value of the function on a few random points, and accordingly (probabilistically) distinguish between the case that the function has the property, and the case that the function needs to be significantly changed to have the property.

The original analysis of the BLR linearity test was combinatorial and gave non optimal bounds. We will present a tighter analysis by [9] based on Fourier analysis. We will first introduce some basic concepts in Fourier analysis, and then describe the BLR test and its analysis. We will then discuss an extension to linear maps $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ for $m > 1$, developed by Samorodnitsky [57], whose analysis relies on additive combinatorics.

2.5.1 Fourier analysis

Fourier analysis is a very useful framework to study additive properties of functions. Let G be a finite Abelian group. A character $\chi : G \to \mathbb{C}^*$ is a map which satisfies

$$\chi(g_1 g_2) = \chi(g_1)\chi(g_2) \qquad \forall g_1, g_2 \in G.$$

For example, if $G = \mathbb{Z}_2^n$ then its characters are

$$\chi_\alpha(x) = (-1)^{\alpha_1 x_1 + \ldots + \alpha_n x_n}, \qquad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_2^n.$$

More generally, any finite Abelian group is isomorphic to $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}$ for some $m_1, \ldots, m_n \geq 2$. Its characters are given by

$$\chi_\alpha(x) = \prod_{i=1}^{n} \omega_{m_i}^{\alpha_i x_i}, \qquad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n},$$

where $\omega_m = \exp(2\pi i/m)$ is a primitive m-th root of unity. If $\chi_1, \chi_2 : G \to \mathbb{C}^*$ are characters, then their product $\chi_1 \chi_2$ is also a character. Hence, the set of characters of G forms a group called the *dual group* of G, and is denoted by $\widehat{G}$. In the case of finite Abelian groups, $\widehat{G}$ is isomorphic to G. We will thus identify them, and consider the characters of G as $\{\chi_\alpha : \alpha \in G\}$.

There is a natural inner product defined on functions $f, g : G \to \mathbb{C}$, given by $\langle f, g \rangle = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$. The characters forms an orthonormal basis for functions $G \to \mathbb{C}$. That is, for any $\alpha, \beta \in G$,

$$\langle \chi_\alpha, \chi_\beta \rangle = \begin{cases} 1 & \text{if } \alpha = \beta \\ 0 & \text{if } \alpha \neq \beta \end{cases}.$$

In particular, note that as $\chi_0 \equiv 1$ we obtain that $\sum_{x \in G} \chi_\alpha(x) = 0$ for all $\alpha \neq 0$.

Any function $F : G \to \mathbb{C}$ can be decomposed as a (unique) linear combination of the characters. This is called the *Fourier expansion* of F,

$$F(x) = \sum_{\alpha \in G} \widehat{F}(\alpha) \chi_\alpha(x).$$

The *Fourier coefficients* of F are given by

$$\widehat{F}(\alpha) = \langle F, \chi_\alpha \rangle = \frac{1}{|G|} \sum_{x \in G} F(x) \overline{\chi_\alpha(x)}.$$

The orthogonality of the characters implies also the following identity, known as *Parseval's identity*,

$$\frac{1}{|G|}\sum_{x\in G}|F(x)|^2 = \sum_{\alpha\in G}|\widehat{F}(\alpha)|^2.$$

An especially useful case is when $F : G \to \{-1,1\}$, as then we have $\sum|\widehat{F}(\alpha)|^2 = 1$.

2.5.2 Testing linear functions

We now discuss the BLR linearity test. We focus on boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$, and note that the analysis can be extended to functions $f : \mathbb{F}_p^n \to \mathbb{F}_p$. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is linear if $f(x) = \sum a_i x_i$ for some $a_i \in \mathbb{F}_2$. The BLR test attempts to find whether an unknown boolean function is a linear function or far from linear, while making only a few (probabilistic) queries to the function.

The BLR test applied to a unknown boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is as follows. Choose randomly and uniformly $x,y \in \mathbb{F}_2^n$, query the values of $f(x), f(y), f(x+y)$, accept f if $f(x+y) = f(x)+f(y)$ and reject f if $f(x+y) \neq f(x)+f(y)$. Clearly, if f is a linear function then this probabilistic test always accepts f. What may be more surprising is that if f is far from all linear functions, in the sense that many values of f needs to be changed to make f a linear function, then the BLR test rejects f with a noticeable probability. Impressively, this is achieved while making only three queries to f.

First, we give some basic definitions. The distance between functions $f,g : \mathbb{F}_2^n \to \mathbb{F}_2$ is the fraction of elements in which they differ,

$$\mathrm{dist}(f,g) = \frac{1}{2^n}\left|\left\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\right\}\right|.$$

Let $\mathrm{Linear}_n = \{x \to \sum a_i x_i : a \in \mathbb{F}_2^n\}$ be the set of all linear functions $\mathbb{F}_2^n \to \mathbb{F}_2$. The distance of f from linear functions is the minimal fraction of points in f which needs to be changed to get some linear function,

$$\mathrm{dist}(f, \mathrm{Linear}_n) = \min_{\ell\in\mathrm{Linear}_n} \mathrm{dist}(f,\ell).$$

The following theorem analyzes the BLR test. We follow the analysis of [9].

Theorem 2.16 (BLR test analysis [14, 9]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. If f is linear then the BLR test always accepts f. If $\mathrm{dist}(f,\mathrm{Linear}_n) \geq \varepsilon$ then the BLR test rejects f with probability at least ε.*

Proof. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. If is obvious that if f is linear then the BLR test always accepts f. We will show that if $\mathrm{dist}(f,\mathrm{Linear}_n) = \varepsilon$ then the test rejects f with noticable probability. Let $F(x) = (-1)^{f(x)}$. The Fourier coefficients of F measure the distance of f from all linear functions. Specifically, let $\alpha \in \mathbb{F}_2^n$ and let $\ell(x) = \langle \alpha, x\rangle$ be a linear function. Then

$$\begin{aligned}\widehat{F}(\alpha) &= 2^{-n}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+\ell(x)}\\ &= 2^{-n}\left(|\{x : f(x) = \ell(x)\}| - |\{x : f(x) \neq \ell(x)\}|\right)\\ &= 1 - 2^{-n}\cdot 2|\{x : f(x) \neq \ell(x)\}| = 1 - 2\cdot\mathrm{dist}(f,\ell).\end{aligned}$$

In particular, if $\mathrm{dist}(f,\ell) \ge \varepsilon$ then $\widehat{F}(\alpha) \le 1-2\varepsilon$. We next use Fourier analysis to analyze the acceptance probability of the BLR test. Recall, the test accepts f if $f(x+y) = f(x)+f(y)$ where $x,y \in \mathbb{F}_2^n$ are uniformly chosen. Now,

$$\begin{aligned}\mathbb{E}_{x,y\in\mathbb{F}_2^n}[F(x+y)F(x)F(y)] &= \Pr[f(x+y)=f(x)+f(y)] - \Pr[f(x+y)\neq f(x)+f(y)]\\ &= 2\cdot\Pr[\text{BLR test accepts } f]-1.\end{aligned}$$

Taking the Fourier expansion of F, we get

$$\begin{aligned}\mathbb{E}[F(x+y)F(x)F(y)] &= \mathbb{E}_{x,y\in\mathbb{F}_2^n}\left[\sum_{\alpha\in\mathbb{F}_2^n}\widehat{F}(\alpha)\chi_\alpha(x)\cdot\sum_{\beta\in\mathbb{F}_2^n}\widehat{F}(\beta)\chi_\beta(x)\cdot\sum_{\gamma\in\mathbb{F}_2^n}\widehat{F}(\gamma)\chi_\gamma(x+y)\right]\\ &= \sum_{\alpha,\beta,\gamma\in\mathbb{F}_2^n}\widehat{F}(\alpha)\widehat{F}(\beta)\widehat{F}(\gamma)\cdot\mathbb{E}_{x,y}\left[\chi_\alpha(x)\chi_\beta(y)\chi_\gamma(x+y)\right]\\ &= \sum_{\alpha,\beta,\gamma\in\mathbb{F}_2^n}\widehat{F}(\alpha)\widehat{F}(\beta)\widehat{F}(\gamma)\cdot\mathbb{E}_{x}\left[\chi_{\alpha+\gamma}(x)\right]\cdot\mathbb{E}_{y}\left[\chi_{\beta+\gamma}(y)\right]\\ &= \sum_{\alpha\in\mathbb{F}_2^n}\widehat{F}(\alpha)^3,\end{aligned}$$

where the last equality follows because $\mathbb{E}_{x\in\mathbb{F}_2^n}[\chi_\alpha(x)] = 1$ if $\alpha = 0$, and is zero otherwise. Thus, we can express the acceptance probability of the BLR test as

$$\Pr[\text{BLR test accepts } f] = \frac{1}{2}\left(1+\sum_\alpha\widehat{F}(\alpha)^3\right).$$

We next bound the sum $\sum\widehat{F}(\alpha)^3$. Since we assume $\mathrm{dist}(f,\mathrm{Linear}_n) = \varepsilon$ we have that $\widehat{F}(\alpha) \le 1-2\varepsilon$ for all $\alpha \in G$. Also, by Parseval's identity, $\sum\widehat{F}(\alpha)^2 = 1$. Hence

$$\sum_\alpha\widehat{F}(\alpha)^3 \le (1-2\varepsilon)\sum_\alpha\widehat{F}(\alpha)^2 = 1-2\varepsilon,$$

and

$$\Pr[\text{BLR test accepts } f] \le 1-\varepsilon.$$

□

2.5.3 Testing linear maps

Consider now a more general scenario, where we are given a map $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ for some $m \ge 1$, and we want to test if f is a linear map or far from it. Here, we denote by $\mathrm{Linear}_{n,m} = \{x \to Ax : A \in \mathbb{F}_2^{m\times n}\}$ the set of linear maps, and the goal is to decide whether f is a linear map, or needs to be changed in a noticeable fraction of elements to become linear.

A natural extension of the BLR test seems reasonable: choose $x,y \in \mathbb{F}_2^n$ uniformly and accept f if $f(x+y) = f(x)+f(y)$. This test still always accepts linear maps. However, it is less clear how to analyze its behaviour on maps which are far from linear. The previous approach using Fourier analysis does not seem to generalize. A general technique, introduced by Alon et al. [2] and expanded by Kaufman and Sudan [38] can handle the case of high acceptance probabilities. Samorodnitsky[57] extended the analysis to low acceptance probabilities as well. We present his result, as its proof relies on additive combinatorics. For a survey on this result see also [69].

As we focus on the regime of low acceptance probabilities, it is more convenient to measure the *agreement* of functions, defined as

$$\mathrm{agree}(f,g) = 1-\mathrm{dist}(f,g) = 2^{-n}|\{x \in \mathbb{F}_2^n : f(x)=g(x)\}|.$$

The agreement of f with linear maps then equals

$$\mathrm{agree}(f,\mathrm{Linear}_{n,m}) = \max_{\ell \in \mathrm{Linear}_{n,m}} \mathrm{agree}(f,\ell).$$

The theorem below, due to Samorodnitsky [57], shows that the BLR test can distinguish maps which have some noticeable agreement with linear maps, from maps which have no agreement with linear maps.

Theorem 2.17 (Samorodnitsky)**.** *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a map, and consider the following test: choose $x,y \in \mathbb{F}_2^n$ independently and uniformly, query the values of $f(x), f(y), f(x+y)$, and accept f if*

$$f(x+y) = f(x)+f(y).$$

If the test accepts f with probability at least $\delta > 0$, then the agreement of f with linear functions is at least $\varepsilon(\delta) \geq \exp(-(1/\delta)^{O(1)})$.

The quantitative bounds in Theorem 2.17 are not sharp. A result of Sanders [61] improves the bound to $\varepsilon(\delta) \geq \exp(-\log(1/\delta)^{O(1)})$, e. g., a quasi-polynomial dependence between the acceptance probability and agreement with linear functions. A polynomial dependence is conjectured, and is equivalent to an important conjecture we will discuss soon, the polynomial Freiman–Ruzsa conjecture.

Proof. Assume that the test accepts f with probability at least δ. Let $A = \{(x, f(x)) : x \in \mathbb{F}_2^n\} \subset \mathbb{F}_2^{n+m}$ be the *graph* of f. Note that $|A| = 2^n$. Then, we know that

$$\Pr_{a,b \in A}[a+b \in A] = \Pr_{x,y \in \mathbb{F}_2^n}[(x+y, f(x)+f(y)) \in A] = \Pr_{x,y \in \mathbb{F}_2^n}[f(x+y) = f(x)+f(y)] \geq \delta.$$

Applying the Balog-Szemerédi-Gowers theorem (Theorem 2.14), we obtain a subset $A' \subset A$ of size $|A'| \geq \delta^{O(1)} \cdot 2^n$ such that $|A'+A'| \leq (1/\delta)^{O(1)}|A'|$. Applying Ruzsa span theorem (Theorem 2.7), we find that there exists a subspace $V \subset \mathbb{F}_2^{n+m}$ which contains A' such that $|V| \leq q|A'|$ where $q = \exp((1/\delta)^{O(1)})$. We will use the subspace V to extract a linear map $\ell : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $\mathrm{agree}(f,\ell) \geq \delta^{O(1)}/q$.

Let $U = \{x \in \mathbb{F}_2^n : \exists y \in \mathbb{F}_2^m, (x,y) \in V\}$ be the projection of V to its first n coordinates. Note that U is a subspace of $\mathbb{F}_2^n$ and that $|U| \geq |A'|$, since $(x, f(x)) \in V$ for all x such that $(x, f(x)) \in A'$. Let $x_1, \ldots, x_k \in \mathbb{F}_2^n$ be a basis of U for $k = \dim(U) \leq n$, and choose $y_1, \ldots, y_k \in \mathbb{F}_2^m$ such that $(x_i, y_i) \in V$. Let $\ell_1 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a linear map such that $\ell_1(x_i) = y_i$. Define the subspace

$$W = \{(x, \ell_1(x)) : x \in U\} \subset \mathbb{F}_2^{n+m}.$$

Then $W \subset V$, $|W| = |U|$. Moreover, V can be decomposed as a disjoint union of cosets of W,

$$V = \cup_{v \in V/W}(W + v).$$

As $A' \subset V$, there must exist $v \in V/W$ such that

$$A' \cap (W + v) \geq \frac{|W|}{|V|}|A'| \geq |A'|/q.$$

Hence, $f(x)$ has noticeable agreement with $\ell_1(x) + v$, as

$$|\{x \in \mathbb{F}_2^n : f(x) = \ell_1(x) + v\}| \geq |A' \cap (W + v)| \geq (\delta^{O(1)}/q) \cdot 2^n.$$

To obtain a genuinely linear map (instead of an affine map), let $\ell_2 : \mathbb{F}_2^n \to \mathbb{F}_2$ be a uniformly chosen linear function, and define $\ell(x) = \ell_1(x) + \ell_2(x)v$. For any nonzero $x \in \mathbb{F}_2^n$ such that $f(x) = \ell_1(x) + v$, we have that $\ell_2(x) = 1$ with probability $1/2$, in which case $f(x) = \ell(x)$. By linearity of expectation,

$$\mathbb{E}_{\ell_2}[\text{agree}(f, \ell)] \geq (1/2) \Pr_{x \in \mathbb{F}_2^n}[f(x) = \ell_1(x) + v] - 2^{-n} \geq \delta^{O(1)}/2q - 2^{-n}.$$

Hence, there must be a choice of ℓ_2 (and hence ℓ) obtaining the average. □

2.6 The polynomial Freiman–Ruzsa conjecture

The polynomial Freiman–Ruzsa conjecture is a conjecture on the structure of sets which have small doubling. Before stating the conjecture formally, it will be instructive to consider a few examples of sets of small doubling. We will focus for now on subsets of $\mathbb{F}_2^n$, and later we will comment on what changes in general Abelian groups.

Example 2.18. Let $V \subset \mathbb{F}_2^n$ be a subspace, $A \subset V$ a set of size $|A| \geq |V|/K$. Then $|A + A| \leq K|A|$. This example shows us that A could be a dense subset of a subspace.

Example 2.19. Let $U, V \subset \mathbb{F}_2^n$ be subspaces with $U \cap V = \{0\}$. Let $v_1, \ldots, v_K$ be linearly independent elements of V and consider $A = U + \{v_1, \ldots, v_K\}$. Then $|A + A| \leq K|A|$. However, the span of A has size $\approx 2^K|A|$.

The second example shows that we cannot hope for a polynomial dependency between the doubling constant of a set, and the size of its linear span. However, in this example, a large subset of A (namely U) does have a small linear span. This motivated the so-called "polynomial Freiman–Ruzsa conjecture," proposed in the 1980s by Katalin Marton[1]. In the following, $\langle A \rangle$ denotes the linear subspace spanned by a set A.

Conjecture 2.20 (Katalin Marton's "Polynomial Freiman–Ruzsa conjecture" in $\mathbb{F}_2^n$)**.** *There exists an absolute constant $c > 0$ such that the following holds. Let $A \subset \mathbb{F}_2^n$ be a set with $|A + A| \leq K|A|$. Then there exists a subset $A' \subset A$ of size $|A'| \geq K^{-c}|A|$ such that $|\langle A' \rangle| \leq |A|$.*

[1] Ruzsa credits Marton for the conjecture in [55] and in its 1993 DIMACS Tech. Report version, also linked in the bibliography. Marton's motivation came from the "two-help-one problem" in multi-user information theory, cf. [41]. The term "polynomial Freiman–Ruzsa conjecture" was coined by Green [**?**].

The Polynomial Freiman–Ruzsa conjecture is one of the central conjectures in additive combinatorics, as it speculates tight relations between two different notions of structure: a combinatorial notion, formalized as small doubling, and an algebraic notion, formalized as having a large intersection with a small-dimensional subspace. It turns out that this conjecture is very useful for applications in complexity theory. Moreover, it has a large number of equivalent versions. For example, it shows that in Theorem 2.17 the dependence of ε on δ can be improved to be polynomial. In fact, such a relation is equivalent to the polynomial Freiman–Ruzsa conjecture. We give a few equivalent formulations below; for a more complete list see [32].

Lemma 2.21. *Let $c_1, c_2, c_3, c_4, c_5 > 0$ be absolute constants. The following statements are equivalent:*

(1) If $A \subset \mathbb{F}_2^n$ has $|A+A| \le K|A|$ then there exists a subspace $V \subset \mathbb{F}_2^n$ of size $|V| \le |A|$ such that $|A \cap V| \ge K^{-c_1}|A|$.

(2) If $A \subset \mathbb{F}_2^n$ has $|A+A| \le K|A|$ then there exists a subspace $V \subset \mathbb{F}_2^n$ of size $|V| \le |A|$ and a set $X \subset \mathbb{F}_2^n$ of size $|X| \le K^{c_2}$ such that $A \subset V+X$.

(3) If $A \subset \mathbb{F}_2^n$ has $A+A \subset A+S$ where $|S| \le K$ then there exists a subspace $V \subset \mathbb{F}_2^n$ of size $|V| \le |A|$ and a set $X \subset \mathbb{F}_2^n$ of size $|X| \le K^{c_3}$ such that $A \subset V+X$.

(4) If $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has the property that $\Pr[f(x+y) = f(x)+f(y)] \ge 1/K$ then the agreement of f with linear maps is at least K^{-c_4} (e. g., a polynomial bound in Theorem 2.17).

(5) If $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has the property that $f(x+y)+f(x)+f(y) \in X$ for all $x, y \in \mathbb{F}_2^n$ where $|X| \le K$, then the agreement of f with linear maps is at least K^{-c_5}.

Proof. We sketch the high level ideas of the proof. For details, see [32].

(1)⇔(2): Clearly $(2) \Rightarrow (1)$. For the other direction, let $B = A \cap V$ such that $|V| \le |A|, |B| \ge K^{-c_1}|A|$. Let $X \subset A$ be maximal such that $B+x$ for $x \in X$ are all disjoint. Clearly, $|X| \le |A+A|/|B| \le K^{1+c_1}$. Also, for any $a \in A$, $(B+a) \cap (B+X) \neq \emptyset$. This implies that $A \subset B+B+X \subset V+X$.

(2)⇔(3). Clearly $(2) \Rightarrow (3)$. For the other direction, let A be such that $|A+A| \le K|A|$. As we saw in the proof of Theorem 2.7, there exists a set B of size $|B| \le K^4$ such that $4A \subset 2A+2B$. Applying (3) to the set $2A$, we obtain that $2A \subset V+X$ where $|V| \le K|A|, |X| \le K^{4c_3}$. The conclusion of (2) follows by partitioning V as the union of K cosets of a subspace of size at most $|A|$.

(2)⇒(4). Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and define $A = \{(x, f(x)) : x \in \mathbb{F}_2^n\}$. The set A satisfies that $\Pr_{a,a' \in A}[a+a' \in A] \ge 1/K$. Applying the BSG theorem (Theorem 2.14), we deduce that there exists a subset $A' \subset A$ of size $|A'| \ge K^{-O(1)}|A|$ such that $|A'+A'| \le K^{O(1)}|A|$. Applying (2) to A', there exists a subspace $V \subset \mathbb{F}_2^n$ and a set $X \subset \mathbb{F}_2^n$ such that $A' \subset V+X$ where $|V| \le |A'|$ and $|X| \le K^{O(1)}$. Following the proof of Theorem 2.17, this implies that there exists a linear function $\ell : \mathbb{F}_2^n \to \mathbb{F}_2^m$ such that $\Pr[f(x) = \ell(x)] \ge K^{-O(1)}$.

(4)⇒(1). Let $A \subset \mathbb{F}_2^n$ of size $2^{m-3} \le |A| \le 2^{m-2}$. Apply a random invertible linear transformation $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. The expected number of collisions is at most $|A|^2 2^{-m} \le |A|/2$, hence we can fix such a map with at most $|A|/2$ collisions. Deleting at most $|A|/2$ elements, we obtain a subset $A' \subset A$ for which there are no collisions. That is, we can write $a \in A'$ as $a = (x, f(x))$ with $x \in \mathbb{F}_2^m, f(x) \in \mathbb{F}_2^{n-m}$. Complete f by choosing $f(x)$ randomly for $x \notin A'$. We get that $\Pr[f(x) + f(y) = f(z) + f(w) | x + y = z + w] \ge K^{-O(1)}$. To get the exact condition in (4), we can for example make sure that x all belong to an affine subspace (say, first bit is 1), and then fix $f(x+y)$ to the majority value. Now, we deduce from (4) that f has a noticeable agreement with a linear function, which by simple manipulations show that A has a noticeable intersection with a subspace.

(5)⇔(3) Analogous.

□

The best known results, getting close to Conjecture 2.20, were achieved by Sanders [61]. We state below his result for $\mathbb{F}_2^n$; his result applies to general Abelian groups as well (with the exponent 4 replaced by 6). Interested readers may also refer to an exposition [44] of the proof over $\mathbb{F}_2^n$.

Theorem 2.22 (Sanders's "Quasi-polynomial Freiman–Ruzsa theorem"). *There exists an absolute constant $c > 0$ such that the following holds. Let $A \subset \mathbb{F}_2^n$ be a set with $|A+A| \le K|A|$. Then there exists a subset $A' \subset A$ of size $|A'| \le \exp(-c \cdot \log^4 K)|A|$ such that $|\langle A' \rangle| \le |A|$.*

We discuss briefly the extensions of Conjecture 2.20 to general Abelian groups. First, for groups of constant torsion (such as $\mathbb{F}_p^n$ for constant p) the conjecture extends as is, except that c is a function of p. However, for groups of large torsion (such as $\mathbb{R}$) there is another example which is worth noting.

Example 2.23. Let $B \subset \mathbb{R}^d$ be a ball of radius r and let $A = B \cap \mathbb{Z}^d$ be the integer points in B. If we fix d and let r be large enough, then $|A| \approx \mathrm{Vol}(B)$, the volume of B. Similarly, $|A+A| \approx \mathrm{Vol}(B+B) = 2^d|B|$. Hence, $|A+A| \approx 2^d|A|$.

The ball in the example can be replaced with any (nice enough) convex body. This example tells us that in groups of large torsion there is another example of structured sets with small doubling: integer points in convex bodies. For general Abelian groups, the structure of $\mathbb{Z}^d$ can be embedded in them via linear maps (that is, maps $\phi : \mathbb{Z}^d \to G$ for which $\phi(x+y) = \phi(x) + \phi(y)$). This is formulated by the following general version of the polynomial Freiman–Ruzsa conjecture.

Conjecture 2.24 (Polynomial Freiman–Ruzsa conjecture in general Abelian groups). *There exists an absolute constant $c > 0$ such that the following holds. Let G be an Abelian group, $A \subset G$ a set with $|A+A| \le K|A|$. Then there exist*

1. *A subgroup $H < G$;*

2. *A convex body $B \subset \mathbb{R}^d$ for $d \le c \cdot \log K$, whose integer points are $B \cap \mathbb{Z}^d$;*

3. *A linear map $\phi : \mathbb{Z}^d \to G$,*

Such that for the set $S = H + \phi(B \cap \mathbb{Z}^d)$ the following holds:

$$|S| \leq |A|, \qquad |A \cap S| \geq K^{-c}|A|.$$

For example, in the special case of $G = \mathbb{F}_p^n$ (where p could be large), Conjecture 2.24 has the following immediate corollary.

Corollary 2.25. *Let $A \subset \mathbb{F}_p^n$ be a set with $|A+A| \leq K|A|$. Then there exists a subset $A' \subset A$ of size $|A'| \geq p^{-O(\log K)}|A|$ such that $|\langle A' \rangle| \leq |A|$.*

Proof. Basically, the corollary holds since $|\phi(B \cap \mathbb{Z}^d)| \leq |\phi(\mathbb{Z}^d)| \leq p^d$. Formally, choose $A' = A \cap (H+b)$ for $b \in \phi(B \cap \mathbb{Z}^d)$ which maximizes $|A'|$. □

Another special case that is interesting is in characteristic zero, such as $\mathbb{R}^n$, since there exist no nontrivial finite subgroups. That is, we must take $H = \{0\}$ and the structure comes only from integer points in convex bodies. A weak version of this conjecture is that a large subset of A has a low dimension. This conjecture was explored in [20], motivated by applications in Lie groups.

Conjecture 2.26 (Weak polynomial Freiman–Ruzsa conjecture in characteristic zero)**.** *There exists an absolute constant $c > 0$ such that the following holds. Let $A \subset \mathbb{R}^n$ be a set with $|A+A| \leq K|A|$. Then there exist a subset $A' \subset A$ of size $|A'| \geq K^{-c}|A|$ such that* $\dim(A') \leq c \cdot \log(K)$.

3 Arithmetic progressions

3.1 Arithmetic progressions in large sets

A k-term arithmetic progression is a sequence $x, x+y, x+2y, \ldots, x+(k-1)y$ with $y \neq 0$. A basic question in number theory is the existence of arithmetic progressions in certain sets of numbers. One of the early results in this field is the Van der Waerden theorem [70] who showed that if the numbers $1, 2, \ldots, n$ are colored with a few colors, then one of the color sets must contain an arithmetic progression of any length, as long as n is large enough.

Theorem 3.1 (Van der Waerden's Theorem)**.** *Let $c, k \geq 1$ be constants, and let $n \geq n_0(c,k)$ be large enough. Then for any coloring of the integers $1, \ldots, n$ with c colors, there exist a k-term arithmetic progression which is monochromatic (that is, all its elements are assigned the same color).*

It turns out that in fact, as conjectured by Erdős and Turán, any set of integers of positive density must contain a long arithmetic progression. This was first proved by Roth [51, 52] for 3-term arithmetic progressions, and later generalized in Szemerédi's seminal paper [65] to k-term arithmetic progressions for any fixed $k \geq 3$.

Theorem 3.2 (Szemerédi's Theorem)**.** *Let $\varepsilon > 0, k \geq 1$ be constants, and let $n \geq n_0(\varepsilon, k)$ be large enough. Then any subset $A \subset \{1, \ldots, n\}$ of size $|A| \geq \varepsilon n$ contains a k-term arithmetic progression.*

Clearly, Theorem 3.1 follows immediately from Theorem 3.2 by setting $\varepsilon = 1/c$ and choosing A to be the largest color class. This completes the picture from a qualitative viewpoint when ε is a constant, but leaves open the problem of sub-constant ε. Otherwise put, for any fixed k and large n, what is the smallest size of a subset in $\{1,\dots,n\}$ which guarantees the existence of a k-term arithmetic progression. A famous problem of Erdős and Turán asks if any set A of natural numbers for which the reciprocals diverge contains an arbitrary long arithmetic progression.

Problem 3.3 (Erdős–Turán)**.** Let $A \subset \mathbb{N}$ be a set such that $\sum_{n\in A} \frac{1}{n} = \infty$. Does it follow that A contains an arithmetic progression of every length?

The quantitative behavior of Szemerédi's Theorem is not well understood. An affirmative answer to Problem 3.3 would imply that Theorem 3.2 holds for $\varepsilon = \Omega(1/\log n)$. It also implies that the prime numbers contain arbitrary long arithmetic progressions. The latter was proved in a breakthrough work of Green and Tao [33]. Getting back to quantitative bounds, the original argument of Roth showed in fact that any subset $A \subset \{1,\dots,n\}$ of size $n/\log\log(n)$ must contain a 3-term arithmetic progression. Further improvements due to several authors [35, 66, 15, 17, 60, 59, 13] improved this bound to $n/\log^{1-o(1)} n$. For the general case of $k > 3$, the original argument of Szemerédi gave a bound of $n/\log\cdots\log n$, where the log function is iterated a constant number of times (the constant depends on k).

We give below a proof for the simplest case of $k = 3$ case (Roth's theorem). We will present a simplified version due to Meshulam [45], who obtained similar results for groups of odd order. We will focus here on the simplest case, that of subsets of $\mathbb{F}_3^n$.

Theorem 3.4 (Meshulam)**.** *Let $A \subset \mathbb{F}_3^n$ be of size $|A| \ge c\cdot 3^n/n$ for an absolute constant $c > 0$. Then A contains a 3-term arithmetic progression. That is, there exist $x, y \in \mathbb{F}_3^n$ with $y \neq 0$ such that*

$$\{x, x+y, x+2y\} \subset A.$$

A set $A \subset \mathbb{F}_3^n$ which has no 3-term arithmetic progressions is called a *capset*. Equivalently, it is a set not containing any line. Theorem 3.4 showed that the maximal size of a capset is $|A| \le (c/n)\cdot 3^n$. More recently, Bateman and Katz [7] improved the bound to $|A| \le (c/n^{1+\varepsilon})\cdot 3^n$ for some small unspecified $\varepsilon > 0$. We do not know how tight these bounds are. A simple example for a capset is $A = \{0,1\}^n$ which has size $|A| = 2^n$. There are better examples, but they all have size $|A| \le (3-\varepsilon)^n$ for some $\varepsilon > 0$. Hence, there are large gaps between the known lower and upper bounds on the density of capsets.

3.1.1 Proof of Meshulam's theorem (Theorem 3.4)

The proof utilizes Fourier analysis over $\mathbb{F}_3^n$. We already introduced Fourier analysis in general Abelian groups in Section 2.5.2. Here, we just note that the characters of $\mathbb{F}_3^n$ are the functions $\chi_\alpha : \mathbb{F}_3^n \to \mathbb{C}^*$ for $\alpha \in \mathbb{F}_3^n$ defined as

$$\chi_\alpha(x) = \omega^{\langle \alpha, x\rangle}$$

where $\omega = \exp(2\pi/3)$ is a primite cubic root of unity.

Proof of Theorem 3.4. The proof is based on the following paradigm. Either the set A is "uniform" enough, in which case it behaves like a random set of the same density, and contains many 3-term arithmetic progressions; or otherwise it is "structured," and in which case we can increase its density by restricting it to a subspace, and iterate.

Let $\mu = |A|/3^n$ denote the density of A and let $1_A : \mathbb{F}_3^n \to \{0,1\}$ denote the indicator function of A. Note that $\widehat{1_A}(0) = \mu$. We introduce the notion of uniformity for a set.

Definition 3.5 (Uniformity)**.** The set A is ε-uniform if $|\widehat{1_A}(\alpha)| \le \varepsilon\mu$ for all $\alpha \neq 0$.

We first show that if A is uniform with a small enough ε, then it contains many 3-term arithmetic progressions. In fact, nearly as many as a random set of the same density (which with high probability is $\approx \mu^3 3^{2n}$).

Claim 3.6. *If A is ε-uniform with $\varepsilon < \mu^2$ then A contains at least $(\mu^3 - \mu\varepsilon^2 - 3^{-n}) \cdot 3^{2n}$ 3-term arithmetic progressions.*

Proof. Consider the expression

$$1_A(x)1_A(x+y)1_A(x+2y).$$

It is equal to one when $(x, x+y, x+2y)$ is a 3-term arithmetic progression or when $x \in A, y = 0$; and is equal to zero otherwise. Hence, the number of 3-term arithmetic progressions in A is equal to

$$\sum_{x,y\in\mathbb{F}_3^n, y\neq 0} 1_A(x)1_A(x+y)1_A(x+2y) \ge \sum_{x,y\in\mathbb{F}_3^n} 1_A(x)1_A(x+y)1_A(x+2y) - 3^n.$$

In order to compute the sum, consider its Fourier expansion

$$\begin{aligned} 1_A(x)1_A(x+y)1_A(x+2y) &= \sum_{\alpha,\beta,\gamma\in\mathbb{F}_3^n} \widehat{1_A}(\alpha)\widehat{1_A}(\beta)\widehat{1_A}(\gamma)\omega^{\langle\alpha,x\rangle+\langle\beta,x+y\rangle+\langle\gamma,x+2y\rangle} \\ &= \sum_{\alpha,\beta,\gamma\in\mathbb{F}_3^n} \widehat{1_A}(\alpha)\widehat{1_A}(\beta)\widehat{1_A}(\gamma)\omega^{\langle\alpha+\beta+\gamma,x\rangle+\langle\beta+2\gamma,y\rangle}. \end{aligned}$$

Consider the sum over $x, y \in \mathbb{F}_3^n$. The orthogonality of the Fourier coefficients implies that for $a \in \mathbb{F}_{3^n}$, $\sum_{x\in\mathbb{F}_3^n} \omega^{\langle a,x\rangle} = 3^n\langle\chi_a, \chi_0\rangle = 3^n 1_{a=0}$. Hence, summing $\omega^{\langle\alpha+\beta+\gamma,x\rangle+\langle\beta+2\gamma,y\rangle}$ over $x, y \in \mathbb{F}_3^n$ evaluates to zero unless $\alpha+\beta+\gamma = 0, \beta+2\gamma = 0$ (which implies $\alpha = \beta = \gamma$), in which case it evaluates to 3^{2n}. Thus, we may simplify

$$\sum_{x,y\in\mathbb{F}_3^n} 1_A(x)1_A(x+y)1_A(x+2y) = 3^{2n} \sum_{\alpha\in\mathbb{F}_3^n} \widehat{1_A}(\alpha)^3.$$

We now apply the assumption that A is ε-uniform. We have $\widehat{1_A}(0) = \mu$ and by the Parseval identity

$$\left|\sum_{\alpha\in\mathbb{F}_3^n,\alpha\neq 0} \widehat{1_A}(\alpha)^3\right| \le \varepsilon\mu \sum_{\alpha\in\mathbb{F}_3^n,\alpha\neq 0} |\widehat{1_A}(\alpha)|^2 \le \varepsilon\mu \sum_{\alpha\in\mathbb{F}_3^n} |\widehat{1_A}(\alpha)|^2 = \varepsilon\mu \cdot 3^{-n} \sum_{x\in\mathbb{F}_3^n} 1_A(x)^2 = \varepsilon\mu^2.$$

Hence

$$\sum_{x,y\in\mathbb{F}_3^n} 1_A(x)1_A(x+y)1_A(x+2y) \ge 3^{2n}(\mu^3 - \mu\varepsilon^2)$$

and the number of 3-term arithmetic progressions in A is at least $3^{2n}(\mu^3 - \mu\varepsilon^2) - 3^n$. □

Assume that A does not contain any 3-term arithmetic progression. Claim 3.6 implies that A cannot be ε-uniform for $\varepsilon = \mu^2/2$, say. So, A must have a noticeable Fourier coefficient. That is, there exists $\alpha \in \mathbb{F}_3^n$, $\alpha \neq 0$ such that $|\widehat{1_A}(\alpha)| \geq \mu^2/2$. We will show that this implies that we can increase the density of A by restricting it to an affine subspace. Define $H_v = \{x \in \mathbb{F}_3^n : \langle \alpha, x \rangle = v\}$ for $v \in \mathbb{F}_3$ to be the affine subspaces of co-dimension one orthogonal to α.

Claim 3.7. *Let A be a set of size $|A| = \mu 3^n$. Assume there exist $\alpha \neq 0$ such that $|\widehat{1_A}(\alpha)| \geq \sigma$. Then there exists $v \in \mathbb{F}_3$ such that*

$$\frac{|A \cap H_v|}{|H_v|} \geq \mu + \sigma/6.$$

Proof. Let $\mu_v = |A \cap H_v|/3^{n-1}$ be the density of $A \cap H_v$ in H_v and let $\Delta_v = \mu_v - \mu$. We need to prove that $\Delta_v \geq \sigma/6$ for some $v \in \mathbb{F}_3$. Clearly, $\Delta_0 + \Delta_1 + \Delta_2 = 0$. By definition

$$\widehat{1_A}(\alpha) = \mu_0 + \omega\mu_1 + \omega^2\mu_2 = \Delta_0 + \omega\Delta_1 + \omega^2\Delta_2$$

where we used the fact that $1 + \omega + \omega^2 = 0$. Hence, since $|\widehat{1_A}(\alpha)| \geq \sigma$ such must exist u such that $|\Delta_u| \geq \sigma/3$. If $\Delta_u \geq \sigma/3$ then we are done; otherwise, since $\Delta_0 + \Delta_1 + \Delta_2 = 0$ there must exist $v \in \mathbb{F}_3 \setminus \{u\}$ such that $\Delta_v \geq \sigma/6$. □

We now conclude the proof by induction. Let $c > 0$ be a large enough constant and let $A \subset \mathbb{F}_3^n$ be a set without 3-term arithmetic progressions of density $\mu = c/n$. We proved that there exist a co-dimension one affine subspace H_v such that

$$\frac{|A \cap H_v|}{|H_v|} \geq \frac{c}{n} + \frac{c^2}{12n^2}.$$

The set $A \cap H_v$ is also a set without 3-term arithmetic progressions in $n-1$ dimensions. By choosing c large enough ($c > 24$ suffices) we have that

$$\frac{c}{n} + \frac{c^2}{12n^2} \geq \frac{c}{n-1}.$$

We can now apply the argument inductively to $A \cap H_v$. The argument must fail for some $n > 1$ since $c > 1$ and we cannot have sets of density greater than 1. Thus, A must contain a 3-term arithmetic progression. □

3.2 Sets without arithmetic progressions

We next focus on constructions of large sets without arithmetic progressions. As we mentioned, for subsets of $\mathbb{F}_3^n$ the best constructions have exponentially small density. If we turn our attention to subsets of the integers, much better constructions are known. We present below a construction due to Behrend [8] from 1946, which has only been marginally improved since.

Theorem 3.8 (Behrend)**.** *There exist a set $A \subset \{1, \dots, n\}$ which contains no 3-term arithmetic progressions of size $|A| \geq n \cdot 2^{-O(\sqrt{\log n})}$.*

Theorem 3.8 was generalized by Rankin [48] who gave a construction of a set $A \subset \{1,\ldots,n\}$ which contains no k-term arithmetic progression of size $|A| = n \cdot 2^{-O((\log n)^{1/(k-1)})}$.

Before moving to the proof, we note that in some applications it is easier to assume we are given a subset $A \subset \mathbb{Z}_n$ without any 3-term arithmetic progressions. That is, we allow the arithmetic progression to be taken modulo n. A simple solution is to choose $A \subset \{1,\ldots,n/3\}$ based on Theorem 3.8, that is without any 3-term arithmetic progressions over the integers. It is straightforward to verify that such a set, when viewed as a subset of $\mathbb{Z}_n$, cannot have 3-term arithmetic progressions modulo n.

Proof of Theorem 3.8. We start with the following basic observation: a sphere in $\mathbb{R}^d$ does not contain any 3 points on a line. In order to discretize this, define

$$B = \left\{ x \in \{0,\ldots,m-1\}^d : \sum x_i^2 = r \right\}.$$

Choosing a value of $0 \le r \le (m-1)^2 d$ which maximizes $|B|$ gives

$$|B| \ge \frac{m^d}{m^2 d}.$$

Since B is a subset of the sphere of radius $r^{1/2}$, it implies that B does not contain any 3-term arithmetic progression (and in fact no three points on a line). In order to construct a subset of integers, we construct a map from $\mathbb{Z}^d$ to $\mathbb{Z}$ which preserves the property of having no 3-term arithmetic progression. Such a map is called a *Freiman homomorphism*, and is widely used tool in additive combinatorics. Define a map $\varphi : \{0,\ldots,m-1\}^d \to \mathbb{Z}$ by

$$\varphi(x) = \sum_{i=1}^{d} x_i \cdot (2m)^{i-1}.$$

We take $A = \{\varphi(x) : x \in B\}$ and show that A contains no 3-term arithmetic progressions. Assume to the contrary that there exist $x,y,z \in \{0,\ldots,m-1\}^d$ such that $\varphi(x), \varphi(y), \varphi(z)$ form a 3-term arithmetic progression. We will show that this implies that x,y,z also form a 3-term arithmetic progression, which is impossible by the construction of B.

Now, if $\varphi(x), \varphi(y), \varphi(z)$ form a 3-term arithmetic progression then $\varphi(x) + \varphi(z) = 2\varphi(y)$, which implies

$$S = \sum_{i=1}^{d} (x_i + z_i - 2y_i) \cdot (2m)^{i-1} = 0.$$

By construction we have that $|x_i + z_i - 2y_i| < 2m$. Hence, since $S \mod 2m = 0$ we must have that $x_1 + z_1 - 2y_1 = 0$. Since $(S/2m) \mod 2m = 0$ we must have that $x_2 + z_2 - 2y_2 = 0$, and so on. That is, $x + z = 2y$, i. e., x,y,z form an arithmetic progression. Finally, we optimize parameters. Set

$$n = \max(A) \le \sum_{i=1}^{d} (m-1) \cdot (2m)^{i-1} \le (m-1) \cdot \frac{(2m)^d - 1}{2m-1} \le (2m)^d.$$

Furthermore we have

$$|A| \ge \frac{m^d}{m^2 d} \ge \frac{n}{2^d m^2 d}.$$

Setting $2m = 2^{\sqrt{\log n}}$ and $d = \sqrt{\log n}$ so that $(2m)^d = n$, we get that

$$|A| \geq n \cdot 2^{-3\sqrt{\log n}(1+o(1))}.$$

□

3.3 Graphs with many disjoint triangles

We give a simple and beautiful application of the existence of large sets without arithmetic progressions. We use them to construct graphs on n vertices with $n^{2-o(1)}$ edge-disjoint triangles, and no other triangles. Clearly, the number of edge-disjoint triangles is bounded by $\binom{n}{2}$, the number of edges, which is less than n^2, hence up to the $o(1)$ term this is the best possible. Formally, we prove the following theorem.

Theorem 3.9 (Graph with many edge-disjoint triangles)**.** *For every n, there exists a graph on n vertices with $n^2 \cdot 2^{-O(\sqrt{\log n})}$ edge-disjoint triangles, and no other triangles.*

Let p be a prime and let $A \subset \mathbb{Z}_p$ be a set without any 3-term arithmetic progressions modulo p. We will construct a graph G on $n = 3p$ vertices with $p|A|$ edge disjoint triangles, and no other triangles (for other values of n add isolated vertices to the graph). Choosing A as guaranteed by Theorem 3.8, the theorem follows.

Now, define $G = (V,E)$ to be the desired graph with $|V| = 3p$. We partition the vertex set to three sets of size p each, and label the vertices x_i, y_i, z_i for $i \in \mathbb{Z}_p$. We set the edges to be

$$E = \{(x_i, y_{i+a}) : i \in \mathbb{Z}_p, a \in A\} \cup \{(y_i, z_{i+a}) : i \in \mathbb{Z}_p, a \in A\} \cup \{(x_i, z_{i+2a}) : i \in \mathbb{Z}_p, a \in A\}.$$

Clearly, the graph $G = (V,E)$ contains $p|A|$ triangles (x_i, y_{i+a}, z_{i+2a}) for $i \in \mathbb{Z}_p, a \in A$. By construction, these triangles are edge-disjoint. What we need to show is that this accounts for all the triangles in the graph G.

Claim 3.10. *If (x_i, y_j, z_k) is a triangle in G then $j = i + a, k = i + 2a$ for some $a \in A$.*

Proof. We have $j = i + a, k = j + b, k = i + 2c$ for $a, b, c \in A$. Substituting gives

$$i + a + b = i + 2c,$$

which implies that a, c, b form an arithmetic progression. Since A contains no non-trivial arithmetic progressions, this can only hold if $a = b = c$. □

An application of Theorem 3.9 is to provide lower bounds in graph property testing. A "graph property" is a property of graphs which does not depend on the labeling of the vertices. Equivalently, it is a family of graphs closed under isomorphisms. Examples include bipartite graphs, 3-colorable graphs, and graphs which contain an hamiltonian cycle. A graph property can be *tested* if there is a randomized algorithm, which queries adjacency of only a small (ideally constant) number of pairs of vertices of a graph, and accepts the graph with if it has a given property, and rejects it with high probability if it is far from all graphs with the property. There is a large body of work on graph property testing, which is out of scope for us. We refer the interested reader to the survey [29] and the references cited there.

More related to our context, consider the property that a graph is *triangle-free* (has no triangles). One of the first applications of the Szemerédi regularity lemma [65] was the following beautiful theorem of Ruzsa and Szemerédi [56]. They showed that if a graph G contains only $o(n^3)$ triangles, then one can make G triangle-free by removing $o(n^2)$ edges. More quantitatively, if G contains only δn^3 triangles, then one can make G triangle-free by removing εn^2 edges, where $\varepsilon = \varepsilon(\delta)$. In the language of property testing, one can test whether a graph G is triangle free or ε-far from being triangle free, by randomly choosing $O(1/\delta)$ potential triangles, and checking if they are contained in the graph. Note that this is a randomized algorithm which queries at most $O(1/\delta)$ edges of G. An interesting question is what is the dependence between δ and ε. The bound obtained in [56] was horrible: $1/\delta$ is a tower of powers of two of height polynomial in $1/\varepsilon$. This was recently improved by Fox [27] to a tower of height logarithmic in $1/\varepsilon$. Still, one may ask whether a much better bound is possible, ideally δ polynomial in ε. Unfortunately, the following result of Alon [1] shows that a super-polynomial dependency is necessary.

Theorem 3.11 (Alon)**.** *For any $\varepsilon > 0$ and n large enough, there exists a graph on n vertices which is ε-far from triangle free (e. g., at least εn^2 edges needs to be removed to make it triangle-free), but that contains only δn^3 triangles for $\delta = \varepsilon^{O(\log 1/\varepsilon)}$.*

Proof. Consider the graph G constructed in Theorem 3.9. It contains εn^2 edge-disjoint triangles for $\varepsilon = 2^{-O(\sqrt{\log n})}$, and no other triangles. It is $(\varepsilon/3)$-far from being triangle-free, as one edge from each triangle needs to be removed, but contains at most $n^2 = \varepsilon^{O(\log 1/\varepsilon)} n^3$ triangles in total. □

One can generalize Theorem 3.9 from triangles to larger cliques. We state a result of Dell and van Melkebeek [22] which has a surprising application in computational complexity (described in the next section).

Theorem 3.12 (Dell–van Melkebeek: Graph with many edge-disjoint s-cliques)**.** *Let $s, t \geq s^2$ be large enough parameters. There exists a graph G on $n = O(s \cdot t^{1/2+o(1)})$ vertices such that*

1. *G contains t edge-disjoint cliques of size s.*

2. *G contains no other cliques of size s.*

Moreover, there exists a deterministic algorithm computing the graph as a function of s, t, which runs in time polynomial in s, t.

We note that the parameters are tight, up to the $o(1)$ factor: each clique of size s contains $\binom{s}{2}$ edges, and hence t edge-disjoint cliques of size s contain $t\binom{s}{2}$ edges. Hence, the graph must have at least $\Omega(s\sqrt{t})$ vertices.

Proof. Let $p \approx t^{1/2+o(1)}$ be a prime. Let $A \subset \mathbb{Z}_p$ be a set without 3-term arithmetic progressions given by Theorem 3.8, and assume that $|A| = p^{1-o(1)} \geq \sqrt{t}$. Define the graph $G = (V, E)$ as follows: $V = [s] \times \mathbb{Z}_p$. For any $a \in A, b \in \mathbb{Z}_p$ define the set of vertices

$$K_{a,b} = \{(i, ai + b) : i \in [s]\},$$

and let E be the union of cliques on $K_{a,b}$ for all $a \in A, b \in \mathbb{Z}_p$. Note that this is a generalization of the construction in Theorem 3.9 where we had $s = 3$. We observe a few properties of G:

(i) The graph G has $|V| = s \cdot p = O(s \cdot t^{1/2+o(1)})$ vertices.

(ii) The graph G is s-partite with parts $V_i = \{(i,c) : c \in \mathbb{Z}_p\}$ for $1 \le i \le s$.

(iii) The graph G has $p|A| \ge t$ edge-disjoint cliques $K_{a,b}$ of size s each.

We need to show that any clique K of size s is one of $K_{a,b}$. Let $K = \{(i,h(i)) : i \in [s]\}$ be a clique. We need to show that $h(i) = ai + b$ for some $a \in A, b \in \mathbb{Z}_p$.

Consider vertices in three consecutive parts $v_0 = (i,h(i)), v_1 = (i+1,h(i+1)), v_2 = (i+2,h(i+2))$. By construction we have

- The vertices v_0, v_1 lie on the line $(x, a_1x + b_1)$. In particular, $h(i+1) - h(i) = a_1$.
- The vertices v_1, v_2 lie on the line $(x, a_2x + b_2)$. In particular, $h(i+2) - h(i+1) = a_2$.
- The vertices v_0, v_2 lie on the line $(x, a_3x + b_3)$. In particular, $h(i+2) - h(i) = 2a_3$.

We thus get that $a_1 + a_2 = 2a_3$, or equivalently that a_1, a_3, a_2 forms a 3-term arithmetic progression. Since A has no nontrivial 3-term arithmetic progressions this could only hold if $a_1 = a_2 = a_3$. Hence also $b_1 = b_2 = b_3$. Now, since this holds for any 3 consecutive points in the clique, it must hold for all points in the clique. □

3.4 Impossibility of compression of NP-hard languages

We present a complexity theoretic application of Theorem 3.12 due to Dell and van Melkebeek [22]. They show that under reasonable complexity assumptions, instances of NP-hard problems cannot be non-trivially compressed by poly-time algorithms. Here, we focus on the clique problem, and note that similar results can be obtained for other NP-hard problems.

The clique problem takes as input an undirected graph G and a parameter k, and asks whether G contains a clique of size k.

$$\text{CLIQUE} = \{(G,k) : G \text{ is a graph containing a clique of size } k\}.$$

The CLIQUE problem is a classical NP-hard problem [21, 43, 37] and the best algorithms for it run in exponential time. Instead, we study a different question: can the input be efficiently compressed while preserving the information of whether it is in CLIQUE or not. If the graph G has n vertices then the input can be specified using $O(n^2)$ bits. Clearly, if one allows exponential time (or non-deterministic polynomial time) then this can be done by simply solving the CLIQUE problem. However, what we show is that deterministic polynomial time algorithms cannot compress an instance (G,k) to length $n^{2-\varepsilon}$ bits for any $\varepsilon > 0$.

Theorem 3.13 ([22]). *Let $\varepsilon > 0$. Assume there exists a deterministic polynomial time algorithm $\mathcal{A}$ which takes as input an instance (G,k), where G is a graph on n vertices and $1 \le k \le n$, and outputs $w = \mathcal{A}(G,k)$ such that*

1. *Given w it is possible to determine whether $(G,k) \in$ CLIQUE or not (information theoretically, not necessarily efficiently).*

2. *The length of w is at most $O(n^{2-\varepsilon})$.*

Then coNP $\subset$ NP/poly.

The complexity class NP/poly is a non-uniform version of NP. For the reader who is not versed in the complexity zoo, let us explain it briefly. The class NP is the class of problems with short proofs. For example, the statement that a CNF formula is satisfiable has a short proof, namely an assignment to the variables that satisfy the formula. It is believed that the complement language, namely unsatisfiable formulas, do not have short proofs. The containment coNP $\subset$ NP/poly means that there are short proofs for a formula being unsatisfiable, if one is allowed to give a short nonuniform advice which depends only on the number of inputs.

We also note (without proof) that Theorem 3.13 can be used to show that other NP-hard problems cannot be compressed. For example, it can be used to show that under the same assumptions, 3-CNF formulas cannot be compressed in deterministic polynomial time to witnesses of length $O(n^{3-\varepsilon})$.

We prove Theorem 3.13 in the remainder of this section. We assume the existence of a compression algorithm given in Theorem 3.13. Fix for the remainder of the proof an NP-complete language L, where we choose 3-SAT for convenience. Let $s = O(n^3)$ denote the size of 3-CNF formulas (i. e., the number of clauses). For $t = \mathrm{poly}(s)$ large enough to be determined later, we define the language $\mathrm{OR}(t,s)$ to be the language given by disjunction of t formulas of size s each.

$$\mathrm{OR}(t) = \{(\varphi_1,\ldots,\varphi_t) : \varphi_1,\ldots,\varphi_t \text{ are 3-CNF formulas with } sclauseseach \\ \text{and at least one of } \varphi_1,\ldots,\varphi_t \text{ is satisfiable}\}.$$

We first follow a standard reduction from 3-SAT to the clique problem on s-partite graphs. In the following we consider s-partite graphs $G = (V,E)$, with each part of size 3. That is, $V = V_1 \cup \ldots \cup V_s$, $|V_1| = \ldots = |V_s| = 3$ and $E \subset \cup_{i \neq j} V_i \times V_j$.

Claim 3.14. *Let φ be a 3-CNF formula with s clauses. Then there exist an s-partite graph G_φ, with each part of size 3, such that φ is satisfiable if and only if G_φ has a clique of size s. Moreover, G_φ can be constructed in deterministic polynomial time.*

Proof. Let $\varphi(x) = C_1 \wedge \ldots \wedge C_s$ where each C_i is a disjunction of three literals. Construct the graph $G_\varphi = (V,E)$ where $V = V_1 \cup \ldots \cup V_s$, $|V_1| = \ldots = |V_s| = 3$, and the i-th vertex in V_a is connected to the j-th vertex in V_b if the i-th literal in C_a and the j-th literal in C_b are not contradicting (i. e., they are not a variable and its negation). Then G_φ has a clique of size s if and only if φ is satisfiable. □

We will show that assuming the compression algorithm, for large enough t an instance of $\mathrm{OR}(t)$ can be compressed to at most t bits. We then show that this type of compression implies that $L \in$ coNP/poly, and hence NP $\subset$ coNP/poly or equivalently coNP $\subset$ NP/poly.

Lemma 3.15 (Compression of $\mathrm{OR}(t)$)**.** *Let s be large enough and let $t \geq s^{6/\varepsilon}$. Assuming the conditions of Theorem 3.13 there exists a deterministic polynomial time compression algorithm $\mathcal{A}'$, that given a collection of t 3-CNF formulas of size s each, produces a witness $w = \mathcal{A}'(\varphi_1,\ldots,\varphi_t)$ such that*

1. *Given w it is possible to determine whether at least one of $\varphi_1,\ldots,\varphi_t$ is satisfiable (information theoretically, not necessarily efficiently).*

2. *The length of w is at most t.*

Proof. Let $G = (V,E)$ be a graph on $n = O(s \cdot t^{1/2+o(1)})$ vertices with t edge-disjoint cliques $K_1,\dots,K_t$ of size s, and no other cliques of size s, guaranteed by Theorem 3.12. Define a graph $G' = (V',E')$ as follows. Its vertex set is $V' = V \times \{1,2,3\}$. For each $1 \le i \le t$, identify the vertices of $K_i \times \{1,2,3\}$ with the vertices of G_{φ_i} and set the edges accordingly (crucially, this uses the fact that $K_1,\dots,K_t$ are edge disjoint edge-disjoint). Then, G' contains a clique of size s if and only if at least one of $\varphi_1,\dots,\varphi_t$ is satisfiable.

The graph G' can be built in deterministic polynomial time. Hence, if we run the assumed compression algorithm we get a witness $w = \mathcal{A}(G')$ as required. The length of w is bounded by

$$n^{2-\varepsilon} \le (s \cdot t^{1/2+o(1)})^{2-\varepsilon} \le t^{\varepsilon/3} \cdot t^{1-\varepsilon/2+o(1)} \le t^{1-\varepsilon/6+o(1)} < t$$

for large enough values of t. □

We finalize the proof by showing that compression of $\mathrm{OR}(t)$ implies that the basic language L defining it (in our case, 3-SAT instances of size s) is in $\mathrm{coNP/poly}$.

Lemma 3.16. *Let $L \subset \{0,1\}^*$ be a language, $t = t(n)$ be polynomially bounded, and let*

$$\mathrm{OR}_L(t) = \{(x_1,\dots,x_t) : x_1,\dots,x_t \in \{0,1\}^n \text{ and at least one of } x_1,\dots,x_t \text{ is in } L\}.$$

Assume that for large enough n, there exists a deterministic polynomial time compression algorithm $\mathcal{A}$ such that $w = \mathcal{A}(x_1,\dots,x_t)$ allows to determine whether $(x_1,\dots,x_t) \in \mathrm{OR}_L(t)$, and the length of w is at most $t(n)$. Then $L \in \mathrm{coNP/poly}$.

Proof. Fix n and let $U = L^c \cap \{0,1\}^n$. Given $x \in U$ we will construct a proof that $x \in U$ of size $\mathrm{poly}(n)$ which can be verified deterministically in polynomial time. This will prove that $L^c \in \mathrm{NP/poly}$, which is equivalent to $L \in \mathrm{coNP/poly}$.

Let $W = \{w : w = \mathcal{A}(x_1,\dots,x_t), x_1,\dots,x_t \in U\}$ be the set of witnesses for inputs of length n not in $\mathrm{OR}_L(t)$. The basic idea is the following: if we are given as advice some $w \in W$, and moreover it happens to be that $\mathcal{A}(x,x_2,\dots,x_t) = w$ for some $x_2,\dots,x_t \in \{0,1\}^n$, then it must be the case that $x \in U$. This can be verified by the deterministic algorithm $\mathcal{A}$ given the advice w and $x_2,\dots,x_t$.

Concretely, we will show that there exists a small list of advice strings $w_1,\dots,w_n \in W$ such that the following holds. For any $x \in U$, there exist $x_1,\dots,x_t \in \{0,1\}^n$ such that

1. $\mathcal{A}(x_1,\dots,x_t) = w_i$ for some $1 \le i \le n$.
2. $x = x_j$ for some $1 \le j \le t$.

Then, given $w_1,\dots,w_n$ as a common advice for all inputs on length n, the proof that $x \in U$ will be the appropriate list $(x_1,\dots,x_t)$. Clearly, this proof can be verified deterministically given the common advice.

We construct the sequence $w_1,\dots,w_n$ in a greedy manner. Let $U_1 = U$. Since $W \subset \{0,1\}^t$ we have that $|W| \le 2^t$. Hence, there must exist a "popular" witness $w_1 \in W$ that many tuples $(x_1,\dots,x_t) \in (U_1)^t$ are compressed to. That is, we can choose w_1 so that the set

$$A_1 = \{(x_1,\dots,x_t) \in (U_1)^t : \mathcal{A}(x_1,\dots,x_t) = w_1\}$$

has size $|A_1| \geq |U_1|^t/|W| \geq 2^{nt-t}$. We say that an element $x \in U$ is *covered* by w_1 if there exist $(x_1,\ldots,x_t) \in U^t$ such that $x = x_i$ for some $1 \leq i \leq t$ and $\mathcal{A}(x_1,\ldots,x_t) = w_1$. Define the set of elements covered by w_1 to be

$$B_1 = \{x \in U_1 : \exists (x_1,\ldots,x_t) \in A_1, x = x_i \text{ for some } 1 \leq i \leq t\}.$$

Note that $A_1 \subset (B_1)^t$. Hence $|B_1| \geq |U_1|/2$. Now, if x happens to be in B_1 then we are done: we prove that $x \in B_1$ by giving the appropriate sequence $(x_1,\ldots,x_t)$ as proof. Let $U_2 = U_1 \setminus B_1$ be the remaining potential inputs, with $|U_2| \leq |U_1|/2$.

Following the same arguments with U_1 replaced with U_2, there exist a "popular" witness $w_2 \in W$ such that the set

$$A_2 = \{(x_1,\ldots,x_t) \in (U_2)^t : \mathcal{A}(x_1,\ldots,x_t) = w_2\}$$

has size $|A_2| \geq |U_2|^t/2^t$. The set of elements in U_2 covered by w_2 is

$$B_2 = \{x \in U_2 : \exists (x_1,\ldots,x_t) \in A_2, x = x_i \text{ for some } 1 \leq i \leq t\}.$$

Again, $A_2 \subset (B_2)^t$ and hence $|B_2| \geq |U_2|/2$. If x happens to be in B_2 then we are done as before. Continuing in this fashion, we get a sequence $w_1, w_2, \ldots \in W$ where each one halves the potential inputs not already covered. As $|U| \leq 2^n$ this process halts after at most n steps. □

Theorem 3.13 follows by combining Lemma 3.15 and Lemma 3.16.

4 Sum-product phenomena

Let A be a set of numbers. Recall that $A+A = \{a+a' : a,a' \in A\}$ is its sumset, and let $A \cdot A = \{aa' : a,a' \in A\}$ denote its productset. In general, if $|A| = n$ then $n \leq |A+A|, |A \cdot A| \leq n^2$. Consider the following two examples. If A is an arithmetic progression, say $A = \{1,2,3,\ldots,n\}$, then $|A+A| = O(n)$ and $|A \cdot A| = \Omega(n^2)$. If A is a geometric progression, say $A = \{1,2,4,8,\ldots,2^n\}$, then $|A \cdot A| = O(n)$ and $|A+A| = \Omega(n^2)$. Is it possible that both $|A+A|, |A \cdot A|$ are small, of size $O(n)$? or is it true that whenever the sumset is small, the productset is large, and vice versa? Results of this type are called "sum-product theorems" and have a multitude of applications in number theory, discrete geometry and complexity. We will present two results of this type in different domains: when A is a set of real numbers, and when A is a subset of a finite field. We refer the reader also to a mini course on additive combinatorics [6] for exposition of the different applications of sum-product theorems.

4.1 Sum-product theorems over the reals

We start by considering the case where A is a subset of real numbers. Erdős and Szemerédi [24] shows that either the sumset or the productset of A is polynomially larger than A.

Theorem 4.1 ([24]). *For any set A of real numbers, either $|A+A| \geq c|A|^{1+\varepsilon}$ or $|A \cdot A| \geq c|A|^{1+\varepsilon}$, where $c, \varepsilon > 0$ are absolute constants.*

In fact, in the same paper they conjecture that one of $|A+A|, |A \cdot A|$ should be close to maximal.

Conjecture 4.2 ([24]). *For any $\varepsilon > 0$ and large enough set of real numbers A,*

$$\max(|A+A|, |A \cdot A|) \geq |A|^{2-\varepsilon}.$$

Despite much research, Conjecture 4.2 remains open. The best known result is by Solymosi [63] who showed that $\max(|A+A|, |A \cdot A|) \geq |A|^{4/3-o(1)}$. Another related recent result is by Iosevich et al. [36] who showed that $|A \cdot A + A \cdot A| \geq |A|^{2-o(1)}$. This is tight (up to the $o(1)$ factor), as can be seen for example by taking A to be a geometric progression.

We prove Theorem 4.1 in the remainder of this section. The proof will rely on the ordering of the real numbers. We will later see more algebraic proofs in the context of finite fields, which do not rely on this. We first establish a lemma, which proves the result in the special case where all the numbers are bounded between m and $2m$ for some value m.

Lemma 4.3. *Let A be a set of real numbers between m and $2m$. Then*

$$\max(|A+A|, |A \cdot A|) \geq c|A|^{1+\varepsilon},$$

where $c, \varepsilon > 0$ are absolute constants.

Proof of Lemma 4.3. Let $a_1 < \ldots < a_N$ be the elements of A. Partition A to $N^{7/8}$ segments of length $s = N^{1/8}$ each, $A_i = \{a_{is}, \ldots, a_{is+s-1}\}$. The diameter of A_i is $\max(A_i) - \min(A_i)$. Let $B = A_{i^*}$ be the set of the smallest diameter. We claim that if $i - j > 10$ then $A_i + B, A_j + B$ are disjoint, and $A_i \cdot B, A_j \cdot B$ are disjoint. To see that, let $a \in A_i, a' \in A_j, b, b' \in B$ and let $a = a' + x, b = b' + y$. By assumption, $x \geq 9 \cdot \mathrm{diam}(B) \geq 9|y|$. Clearly, it cannot be that $a + b = a' + b'$. Assume that $ab = a'b'$. Then $(a' + x)b = a'(b - y)$ which implies $x/y = -a'/b$. But $|x/y| \geq 9$ and $1/2 \leq a'/b \leq 2$ since the elements of A are between m and $2m$.

Thus, we can bound

$$|A+A| + |A \cdot A| \geq \sum_i |A_{10i} + B| + |A_{10i} \cdot B|.$$

Let $I = \{i : |A_i + B|, |A_i \cdot B| \leq s^{1+\alpha}\}$ for $\alpha > 0$ to be chosen later ($\alpha < 1/3$ suffices). We will shortly show that $|I| \leq s^4 = N^{1/2}$ which is much smaller than the number of sets A_{10i} which is $(1/10) \cdot N^{7/8}$. Hence, for most sets A_i, $|A_i + B| + |A_i \cdot B| \geq s^{1+\alpha} = N^{1/8 \cdot (1+\alpha)}$ and we deduce that

$$|A+A| + |A \cdot A| \geq (N^{7/8}/10 - N^{1/2}) \cdot N^{1/8 \cdot (1+\alpha)} \geq (1/20) \cdot N^{1+\alpha/8}.$$

To conclude the proof, we bound $|I|$. Fix $i \in I$ so that $|A_i + B|, |A_i \cdot B| \leq s^{1+\alpha}$. We will show that there exist $b_1, b_2, b_3, b_4 \in B$ such that

$$\frac{(b_1 - b_2)b_4}{b_3 - b_4} \in A_i.$$

As there are $|B|^4 = s^4$ choices for b_1, b_2, b_3, b_4, this shows that $|I| \leq s^4$.

In order to show this, consider the s^2 sums $a + b$ for $a \in A_i, b \in B$. By assumption, there are at most $s^{1+\alpha}$ distinct possible sums. Hence, there is a sum σ such that

$$a_j + b_j = \sigma$$

for at least $s^{1-\alpha}$ different pairs $a_j \in A_i, b_j \in B$. Consider now the $s^{2-2\alpha}$ products $a_j b_k$, where $a_j + b_j = a_k + b_k = \sigma$. As they take at most $s^{1+\alpha}$ different values, if $\alpha < 1/3$ then there is a pair which takes the same product. This means we can find $a_1, a_2 \in A_i, b_1, b_2, b_3, b_4 \in B$ such that

$$a_1 + b_1 = a_2 + b_2, \quad a_1 b_3 = a_2 b_4.$$

Solving for a_1 gives that $a_1 = (b_1 - b_2) b_4 / (b_3 - b_4)$. □

Proof of Theorem 4.1 given Lemma 4.3. Let $|A| = N$. We can assume, without loss of generality, that all the elements in A are positive (by possibly reducing $|A|$ by a factor of two). Let $A_i = \{a \in A : 2^i < a \leq 2^{i+1}\}$. Note that $|A_i + A_i|$ and $|A_j + A_j|$ are disjoint for any $i \neq j$: any element in $A_i + A_i$ is in $(2^{i+1}, 2^{i+2}]$ and any element in $A_j + A_j$ is in $(2^{j+1}, 2^{j+2}]$. Similarly $|A_i \cdot A_i|$ and $|A_j \cdot A_j|$ are disjoint for $i \neq j$. Let $I = \{i : 0 < |A_i| < N^{1/4}\}$. We consider two cases.

(i) Assume first that $\sum_{i \in I} |A_i| < N/2$. Then by removing these elements (and reducing $|A|$ by a factor of two) we can assume that if A_i is not empty then $|A_i| \geq N^{1/4}$. Applying Lemma 4.3, we get that for any non-empty set A_i,

$$|A_i + A_i| + |A_i \cdot A_i| \geq c|A_i|^{1+\varepsilon} \geq c|A_i| N^{\varepsilon/4}$$

and

$$|A + A| + |A \cdot A| \geq \sum_i |A_i + A_i| + |A_i \cdot A_i| \geq c N^{\varepsilon/4} \sum |A_i| = c N^{1+\varepsilon/4}.$$

(ii) Otherwise, we must have that $|I| \geq (1/2) \cdot N^{3/4}$. Let $I' \subset I$ be such that $|i - j| \geq 2$ for all distinct $i, j \in I'$, where $|I'| \geq (1/4) \cdot N^{3/4}$. Fix arbitrary $a_i \in A_i$ for $i \in I'$. Then, the pairwise sums $a_i + a_j$ for distinct $i, j \in I'$ are all disjoint. To see that, assume that $a_i + a_j = a_k + a_\ell$ where i, j, k, ℓ are distinct. If say $i > \max(j, k, \ell)$ then $a_i > 2^i$ while $a_k + a_\ell \leq 2^{i-1} + 2^{i-3} < 2^i$. Hence, we get that

$$|A + A| \geq \binom{|I'|}{2} \geq c \cdot N^{3/2}.$$

□

4.2 Sum-product theorems over finite fields

We consider here now the sum-product problem over finite fields. Let $\mathbb{F}$ be a finite field. There is another source of examples of finite fields, coming fromsubfields. Specifically, if $\mathbb{K}$ is a subfield of $\mathbb{F}$ then $\mathbb{K} + \mathbb{K} = \mathbb{K} \cdot \mathbb{K} = \mathbb{K}$. Hence, we will restrict our attention to fields without nontrivial subfields, namely prime finite fields $\mathbb{F} = \mathbb{F}_p$. We note that results can be extended to non-prime fields if care is given to exclude subfields (or sets close to subfields). Bourgain, Katz and Tao [19], Konyagin [39] and Bourgain, Glibichuk and Konyagin [18] proved a sum-product theorem over prime finite fields. We will later see applications of this theorem for the construction of extractors in complexity theory.

Theorem 4.4 ([19, 39, 18]). *For any $\alpha > 0$ there exist $\varepsilon > 0$ such that the following holds. For any prime p, and any set $A \subset \mathbb{F}_p$ of size $|A| \le p^{1-\alpha}$,*

$$\max(|A+A|, |A \cdot A|) \ge |A|^{1+\varepsilon}.$$

Note that one cannot hope for a bound of $|A|^{2-o(1)}$ here, as $|A+A|, |A \cdot A| \le p$. For simplicity lets fix $\alpha = 0.1$ for the remainder of the proof. We first show that if we iterate sums and products enough times, then sets mush grow. Concretely, in Lemma 4.5 we show that for any set $A \subset \mathbb{F}_p$ of size $|A| \le p^{0.9}$ we have $|R(A)| \ge |A|^{1.01}$, where

$$R(A) = (A-A)\cdot(A-A) + (A-A)\cdot A + (A-A+A\cdot A - A\cdot A)\cdot A.$$

Next, in Lemma 4.6 we show that if $|A+A|, |A \cdot A| \le |A|^{1+\varepsilon}$ then for any polynomial expression (an expression like $R(\cdot)$ above, composed of fixed number of additions, subtractions and multiplications applied to a set), there exists a subset $B \subset A$ which doesn't grow much under R, that is

$$|R(B)| \le |B|^{1+O(\varepsilon)}.$$

Applying Lemma 4.5 to B yields that ε is lower bounds by an absolute constant (which depends on α). We now formally state the lemmas.

Lemma 4.5. *Let $A \subset \mathbb{F}_p$ of size $|A| \le p^{0.9}$. Then $|R(A)| \ge |A|^{1.01}$ where*

$$R(A) = (A-A)\cdot(A-A) + (A-A)\cdot A + (A-A+A\cdot A - A\cdot A)\cdot A.$$

Lemma 4.6. *Let $A \subset \mathbb{F}_p$ be such that $|A+A|, |A \cdot A| \le |A|^{1+\varepsilon}$. For any polynomial expression $R(\cdot)$ there exists a subset $B \subset A$ such that*

$$|R(B)| \le |B|^{1+c\varepsilon}.$$

Here, $c = c(R)$ is a constant which depends only on the polynomial expression $R(\cdot)$.

We first describe how the proof of Theorem 4.4 follows from Lemma 4.5 and Lemma 4.6, and then proceed to prove the two lemmas.

proof of Theorem 4.4. Let $A \subset \mathbb{F}_p$ be of size $|A| \le p^{0.9}$ such that $|A+A|, |A \cdot A| \le |A|^{1+\varepsilon}$. Let $R(\cdot)$ be the polynomial expression in Lemma 4.5. By Lemma 4.6 there exists a subset $B \subset A$ such that $|R(B)| \le |B|^{1+c\varepsilon}$, where $c = c(R)$. But by Lemma 4.5 applied to B, $|R(B)| \ge |B|^{1.01}$. Hence $\varepsilon \ge 1/100c$. □

4.2.1 Proof of Lemma 4.5

Consider the set of $\lambda \in \mathbb{F}_p$ for which $|A + \lambda A| < |A|^2$. That is, there exist $a_1, a_2, a_3, a_4 \in A$ with $a_1 \ne a_3, a_2 \ne a_4$ such that

$$a_1 + \lambda a_2 = a_3 + \lambda a_4,$$

or equivalently

$$\lambda = \frac{a_3 - a_1}{a_2 - a_4}.$$

Let $A' = (A-A) \setminus \{0\}$ and let $B = A'/A' = \{a'_1/a'_2 : a'_1, a'_2 \in A'\}$ be the set of such λ. We consider two cases, whether $B = \mathbb{F}_p$ or $B \neq \mathbb{F}_p$. Assume first that $B = \mathbb{F}_p$. Set $R_0(A) = (A-A)(A-A)$. Applying the Ruzsa triangle inequality (Claim 2.1) to the multiplicative group $\mathbb{F}_p^*$, we obtain that

$$\frac{|A'/A'|}{|A'|} \leq \left(\frac{|A' \cdot A'|}{|A'|}\right)^2$$

and hence

$$|R_0(A)| \geq |A' \cdot A'| \geq \left(\frac{|B|}{|A'|}\right)^{1/2} |A'| = p^{1/2}|A'|^{1/2} \geq p^{1/2}|A|^{1/2} \geq |A|^{21/20},$$

where we used the assumption that $|A| \leq p^{0.9}$.

Otherwise, assume that $B \neq \mathbb{F}_p$. Fix a nonzero $a \in A$. There must exist $\lambda \in B$ such that $\lambda + a \notin B$, where we use the fact that the additive group of $\mathbb{F}_p$ is generated by any nonzero element. Then

$$|A + (\lambda + a)A| = |A|^2.$$

Let $\lambda = (a_3 - a_1)/(a_2 - a_4)$, then

$$|(a_2 - a_4)A + (a_3 - a_1 + aa_2 - aa_4)A| = |A|^2.$$

Hence

$$R_1(A) = (A-A) \cdot A + (A - A + A \cdot A - A \cdot A) \cdot A$$

satisfies $|R_1(A)| \geq |A|^2$. Taking $R(A) = R_0(A) + R_1(A)$ we obtain a polynomial expression which grows polynomially.

4.2.2 Proof of Lemma 4.6

We will need the following lemma.

Lemma 4.7. *Let A be a subset of an Abelian group such that $|A+A| \leq K|A|$. Then there exists $B \subset A$ of size $|B| \geq K^{-O(1)}|A|$ such that any $b_1 - b_2 \in B - B$ can be written as*

$$b_1 - b_2 = \sum_{i=1}^{12} a_i, \qquad a_i \in A \cup -A$$

in at least $K^{-O(1)}|A|^{11}$ distinct ways; and any $b_1 + b_2 \in B + B$ can be written as

$$b_1 + b_2 = \sum_{i=1}^{12} a_i, \qquad a_i \in A \cup -A$$

in at least $K^{-O(1)}|A|^{11}$ distinct ways.

Proof. We will prove the lemma for $B-B$, the proof for $B+B$ is similar. Let $N=|A|$. Following the same idea of the proof of the BSG Theorem (Theorem 2.14), let $C\subset A+A$ be the set of elements which can be written as $c=a_1+a_2$ with $a_1,a_2\in A$ in at least $N/2K$ distinct ways. As $|A+A|\le K|A|$ we have $|C|\ge N/2K$. Let H be the bipartite graph with vertex sets A,A and edges $E=\{(a_1,a_2):a_1+a_2\in C\}$. Applying Lemma 2.15 to H, let $B,B'\subset A$, $|B|,|B'|\ge K^{-O(1)}N$ be sets such that for any $b\in B,b'\in B'$ there are at least $K^{-O(1)}N^2$ paths of length three (b,a,a',b') between b,b'. This means that we can write

$$b+b'=(b+a)-(a+a')+(a'+b')=c_1-c_2+c_3$$

with $c_1,c_2,c_3\in C$ in at least $K^{-O(1)}N^2$ distinct ways. As any element $c\in C$ can be written as $c=a+a'$ in at least $N/2K$ distinct ways, we can write

$$b+b'=\sum_{i=1}^{6}a_i,\qquad a_i\in A\cup -A$$

in at least $K^{-O(1)}N^5$ distinct ways. To conclude, express any $b_1-b_2\in B-B$ as $(b_1+b')-(b_2+b')$ over all choices of b', which gives that we can express

$$b_1-b_2=\sum_{i=1}^{12}a_i,\qquad a_i\in A\cup -A$$

in at least $K^{-O(1)}N^{11}$ distinct ways. □

In order to prove Lemma 4.6, we will show by induction that polynomial expressions do not grow. In the following, for a subset $B\subset\mathbb{F}_p$ let $B^s=\{b_1\cdots b_s:b_i\in B\}$, $B^{-1}=\{b^{-1}:b\in B,b\neq 0\}$ and shorthand $B^{-s}=(B^{-1})^s$.

Lemma 4.8. *For any integers $t,s\ge 1$ there exists a constant $c=c(t,s)>0$ such that the following holds. If $|A+A|,|A\cdot A|\le|A|^{1+\varepsilon}$ then there exists $B\subset A$ of size $|B|\ge|A|^{1-c\varepsilon}$ such that*

$$|(B^t-B^t)\cdot B^s\cdot B^{-s}|\le|B|^{1+c\varepsilon}.$$

Lemma 4.6 follows from Lemma 4.8, since for $s=0$ we have $|B^t-B^t|\le|B|^{1+c\varepsilon}$, and by the the Plünneke–Ruzsa theorem (Theorem 2.11) this implies that also $|tB^t-tB^t|\le|B|^{1+c'\varepsilon}$ for $c'=2tc$. Hence, for any polynomial expression $R(\cdot)$, if we choose t large enough we can express $R(B)$ as the sum or difference of at most t monomials of degree t, hence $|R(B)|\le|B|^{1+c(R)\cdot\varepsilon}$. We now prove Lemma 4.8.

Proof. We will prove the lemma by induction on t. The base case is $t=1$. Let $B\subset A$ be the set guaranteed by Lemma 4.7, where $|B|\ge|A|^{1-O(\varepsilon)}$. Any $b_1-b_2\in B-B$ can be written as

$$b_1-b_2=\sum_{i=1}^{12}a_i,\qquad a_i\in A\cup -A$$

in at least $|A|^{11-O(\varepsilon)}$ distinct ways. Multiplying by an arbitrary element of B^sB^{-s}, we get that any element $x\in(B-B)B^sB^{-s}$ can be written as

$$x=\sum_{i=1}^{12}x_i,\qquad x_i\in\pm A^{s+1}A^{-s}$$

in at least $|A|^{11-O(\varepsilon)}$ distinct ways. Since $|A \cdot A| \le |A|^{1+\varepsilon}$, by the Plünneke–Ruzsa theorem (Theorem 2.11) we have $|A^{s+1}A^{-s}| \le |A|^{1+(2s+1)\varepsilon} = |A|^{1+O(\varepsilon s)}$. Hence the number of choices for $x_1, \dots, x_{12}$ is at most $|A|^{12+O(\varepsilon s)}$, and hence

$$|(B-B) \cdot B^s B^{-s}| \le \frac{|A|^{12+O(\varepsilon s)}}{|A|^{11-O(\varepsilon)}} = |A|^{1+O(\varepsilon s)} \le |B|^{1+O(\varepsilon s)}.$$

Hence, we proved the lemma for $t=1$ with $c(1,s) = O(s)$.

We proceed to prove the inductive case. We assume we proved the lemma for t, ℓ for all $\ell \ge 0$; and we will prove it for $t+1, s$. Let $\ell = \ell(t,s)$ be large enough (to be determined later) and assume we already constructed a set $B \subset A$ of size $|B| \ge |A|^{1-c\varepsilon}$ such that

$$|(B^t - B^t) \cdot B^\ell B^{-\ell}| \le |B|^{1+c\varepsilon},$$

where $c = c(t,\ell)$. In particular, $|B \cdot B| \le |B|^{1+c\varepsilon}$. Apply Lemma 4.7 to the multiplicative group of $\mathbb{F}_p$ to get a subset $C \subset B$ of size $|C| \ge |B|^{1-O(c\varepsilon)}$, such that any $x \in C \cdot C$ can be written as

$$x = \prod_{i=1}^{12} b_i, \qquad b_i \in B \cup B^{-1}$$

in at least $|B|^{11-O(c\varepsilon)}$ distinct ways. Furthermore, lets assume (without loss of generality, losing only constant factors) that in all these $b_1, \dots, b_m \in B$ and $B_{m+1}, \dots, B_{12} \in B^{-1}$ for some $m \ge 1$. Multiplying this expression by an arbitrary element of C^{t-1}, we can write any element in $x \in C^{t+1}$ as

$$x = \prod_{i=1}^{12} b_i, \qquad b_1 \in B^t, b_2, \dots, b_m \in B, b_{m+1}, \dots, b_{12} \in B^{-1}$$

in at least $|B|^{11-O(c\varepsilon)}$ distinct ways.

Fix now $x, y \in C^{t+1}$ and a representation $x = x_1 \dots x_{12}$. We will enumerate over representations $y = y_1 \dots y_{12}$, with $x_1, y_1 \in B^t$, $x_i, y_i \in B$ for $i = 2, \dots, m$ and $x_i, y_i \in B^{-1}$ for $i = m+1, \dots, 12$. We have

$$\begin{aligned} x - y &= x_1 x_2 \dots x_{12} - y_1 y_2 \dots y_{12} \\ &= (x_1 - y_1) x_2 x_3 \dots x_{12} \\ &+ y_1 (x_2 - y_2) x_3 \dots x_{12} \\ &+ \dots \\ &+ y_1 y_2 \dots y_{11} (x_{12} - y_{12}) \end{aligned}$$

The first term is contained in $(B^t - B^t) B^{m-1} B^{-(12-m)}$, the next $m-1$ terms are contained in $B^t(B - B)B^{m-2}B^{-(12-m)}$, and the last $12-m$ terms are contained in $B^t(B^{-1} - B^{-1})B^{m-1}B^{-(11-m)}$. To get a unified expression, note that $B^{-1} - B^{-1} \subset (B-B)B^{-2}$, and hence all 12 terms are contained in $(B^t - B^t)B^{t+12}B^{-12}$. If we multiply the expression by an arbitrary element of $B^s B^{-s}$, then any term would be contained in $(B^t - B^t)B^\ell B^{-\ell}$ for $\ell = t+s+12$. In particular, any element of $(C^{t+1} - C^{t+1})C^s C^{-s}$ is expressable in $|B|^{11-O(c\varepsilon)}$ distinct ways as the sum of 12 terms, each coming from a set of size $|B|^{1+c\varepsilon}$. Hence

$$|(C^{t+1} - C^{t+1}) \cdot C^s C^{-s}| \le \frac{|B|^{12+O(c\varepsilon)}}{|B|^{11-O(c\varepsilon)}} \le |B|^{1+O(c\varepsilon)} \le |C|^{1+O(c\varepsilon)}.$$

Hence, we proved the inductive case with $c(t+1,s) = O(c(t, t+s+12))$. □

4.3 Extractors

Extractors are deterministic functions which can "extract" pure randomness from "weak" random sources. There are various notions of extractors, and here we will focus on extractors for independent sources. First, we need some notion of entropy which measures the amount of randomness in a random variable or a distribution. There are several potential notions. Let X be a random variable with a finite support. We define

- The *Erdős-Renyi entropy* of X is the log of its collision probability, given by $H_2(X) = -\log \Pr[X_1 = X_2]$ where X_1, X_2 are i.i.d copies of X.
- The *Shannon entropy* of X is $H(X) = -\sum_x \Pr[X = x] \log \Pr[X = x]$.
- The *min-entropy* of X is $H_\infty(X) = -\log(\max_x \Pr[X = x])$.

For example, if X is uniform on a set of size N, then it has entropy $\log N$ in all the above notions of entropy. Hence, we think of a random variable with entropy k as a source which hides k bits of randomness. Moreover, note that $H_2(X), H(X) \geq H_\infty(X)$. Here, we focus on min-entropy, and note that the results we present below can be extended to other notions of entropy, with appropriate modifications. We will typically have random variables X supported on $\{0,1\}^n$. If $H_\infty(X) = \delta n + o(n)$ for some constant δ and large n, we say that X has *min-entropy rate* δ.

We start with the following claim, which would allow us to restrict our attention to distributions which are uniform over sets.

Claim 4.9. *Let X be a random variable with $H_\infty(X) \geq k$ for some integer $k \geq 1$. Then X is the convex combination of uniform distributions on sets of support size 2^k. That is, there exist sets $A_1, A_2, \ldots$ each of size 2^k, and probabilities $p_1, p_2, \ldots$ with $\sum p_i = 1$, such that if $X_i \in A_i$ are chosen uniformly then*

$$\Pr[X = x] = \sum p_i \Pr[X_i = x].$$

Proof. Let $x_1, \ldots, x_N$ be the elements in the support of X, let $q_i = \Pr[X = x_i]$, and assume that $2^{-k} \geq q_1 \geq \ldots \geq q_N > 0$. If $N = 2^k$ we are done, so assume $N > 2^k$. Define $A_1 = \{x_1, \ldots, x_{2^k}\}$, let $p = 2^k q_{2^k+1} > 0$ and define a random variable Y by

$$\Pr[X = x] = p 2^{-k} \cdot 1_{x \in A_1} + (1-p) \Pr[Y = x].$$

We have that Y is well defined and that $H_\infty(Y) \geq k$. Indeed, if $i \leq 2^k$ then $\Pr[Y = x_i] = (q_i - p2^{-k})/(1-p) \leq 2^{-k}$, and if $i > 2^k$ then $\Pr[Y = x_i] = q_i/(1-p) \leq 2^{-k}$ by our choice of p. Hence, we can apply the claim to Y. One can verify that the process converges to the required solution. □

A *two-source extractor* is a deterministic function which takes as input two independent inputs, each with some nontrivial amount of min-entropy, and outputs a bit which is close to uniform (or even more than one bit, but here we will stick with the simplest notions). We will assume throughout that the inputs are random variables taking values in $\{0,1\}^n$.

Definition 4.10 (Two-source extractor)**.** A function $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is an (n,k,ε) two-source extractor if, for any two independent random variables X,Y taking values in $\{0,1\}^n$ with $H_\infty(X), H_\infty(Y) \geq k$, we have

$$1/2-\varepsilon \leq \Pr[E(X,Y)=0] \leq 1/2+\varepsilon.$$

Claim 4.9 shows that it suffices to verify the conditions for X,Y uniform over sets of size 2^k. This suggests an alternative view on two-source extractors, as an extension of the more familiar notion of bipartite Ramsey graphs (also called *dispersers* in the computer science literature). In the following, we denote bipartite graphs by $H=(U,V,E)$ where U,V are the vertex sets and $E \subset U \times V$ is the edge set. For subsets $A \subset U, B \subset V$ we denote by $E(A,B)=E \cap (A \times B)$ the induced edges between A and B.

Definition 4.11 (Bipartite Ramsey graph)**.** A bipartite graph $H=(U,V,E)$ with is an (n,k) bipartite Ramsey graph if $|U|=|V|=2^n$, and H contains no $(2^k,2^k)$ complete set and no $(2^k,2^k)$ independent set. That is, for all subsets $A \subset U, B \subset V$ of size $|A|=|B|=2^k$, we have

$$1 \leq |E(A,B)| \leq |A||B|-1.$$

Definition 4.12 (Two-source extractor)**.** A bipartite graph $H=(U,V,E)$ is an (n,k,ε) two-source extractor if $|U|=|V|=2^n$, and all the $(2^k,2^k)$ induced subgraphs of H are nearly balanced. That is, for all subsets $A \subset U, B \subset V$ of size $|A|=|B|=2^k$, we have

$$(1/2-\varepsilon)|A||B| \leq |E(A,B)| \leq (1/2+\varepsilon)|A||B|.$$

Note that the two definitions of (n,k,ε) two-source extractors coincide. Both Ramsey graphs and two-source extractors have been extensively studied in the graph theory and computational complexity communities. A simple probabilistic argument shows that a random graph is a bipartite Ramsey graph, and a two-source extractor, for any fixed ε and $k=O(\log n)$. A major line of research is to match these existential results by explicit constructions. We start by describing a simple construction, based on inner product in $\mathbb{F}_2^n$, which attains min-entropy rate $\delta=1/2$.

4.3.1 The Hadamard two-source extractor

Consider the following bipartite graph $H=(U,V,E)$. Identify $U=V=\mathbb{F}_2^n$ and take $E=\{(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : \langle u,v \rangle = 0\}$. This graph is called the inner-product graph, or the Hadamard two-source extractor. When we consider it as a function, we will denote by it by $E_{\text{Had}} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. We will show that it is indeed a two-source extractor for min-entropy rate $1/2$. First, we show the simpler claim that it is a bipartite Ramsey graph for min-entropy rate $1/2$.

Claim 4.13. *Let $A,B \subset \mathbb{F}_2^n$ be sets such that $|A||B| > 2^n$. Then $\{\langle a,b \rangle : a \in A, b \in B\} = \{0,1\}$. In particular, E_{Had} is an (n,k) bipartite Ramsey graph for $k=n/2+1$.*

Proof. Let $A,B \subset \mathbb{F}_2^n$ be sets with $|A||B|>2^n$. Let V_A,V_B be the minimal affine subspaces containing A,B, respectively. Note that as $|A||B|>2^n$ we have $\dim(V_A)+\dim(V_B) \geq n+1$, and hence they cannot be orthogonal to each other. Hence it cannot be that $\langle a,b \rangle = 0$ for all $a \in A, b \in B$, as then the same would hold for all $a \in V_A, b \in V_B$. A similar argument shows that it cannot be that $\langle a,b \rangle = 1$ for all $a \in A, b \in B$. □

Note that the bound $k = n/2$ is tight, as if A is a subspace of dimension $n/2$ and B is the orthogonal subspace, then A, B is a clique. We next show that H is in fact a two-source extractor for roughly the same parameters.

Lemma 4.14. *Fix $\varepsilon > 0$. Let $A, B \subset \mathbb{F}_2^n$ be sets such that $|A||B| \geq (1/\varepsilon)^3 \cdot 2^n$. Then*

$$(1/2-\varepsilon)|A||B| \leq |E(A,B)| \leq (1/2+\varepsilon)|A||B|.$$

In particular, E_{Had} is a (n,k,ε) two-source extractor for $k = n/2 + 3\log(1/\varepsilon)$.

Proof. We will prove the equivalent statement

$$\left|\mathbb{E}_{a\in A, b\in B}[(-1)^{\langle a,b\rangle}]\right| \leq 2\varepsilon,$$

where $a \in A, b \in B$ are uniform and independent. Define

$$S = \left\{\alpha \in \mathbb{F}_2^n : \left|\mathbb{E}_{b\in B}[(-1)^{\langle \alpha,b\rangle}]\right| \geq \varepsilon\right\}.$$

We will soon show that $|S| \leq \varepsilon|A|$, and hence

$$\left|\mathbb{E}_{a\in A, b\in B}[(-1)^{\langle a,b\rangle}]\right| \leq \frac{1}{|A|}\left(|S| + \sum_{a\in A\setminus S}\left|\mathbb{E}_{b\in B}[(-1)^{\langle a,b\rangle}]\right|\right) \leq 2\varepsilon.$$

In order to bound S, define the function $\varphi_B : \mathbb{F}_2^n \to \mathbb{R}$ by $\varphi_B(x) = \frac{2^n}{|B|}1_B(x)$, and note that its Fourier coefficients are exactly

$$\widehat{\varphi_B}(\alpha) = \mathbb{E}_{x\in\mathbb{F}_2^n}[\varphi_B(x)(-1)^{\langle\alpha,x\rangle}] = \mathbb{E}_{b\in B}[(-1)^{\langle\alpha,b\rangle}].$$

Hence,

$$S = \{\alpha \in \mathbb{F}_2^n : |\widehat{\varphi_B}(\alpha)| \geq \varepsilon\}.$$

By Parseval's identity, we know that

$$\sum_{\alpha\in\mathbb{F}_2^n}|\widehat{\varphi_B}(\alpha)|^2 = 2^{-n}\sum_{x\in\mathbb{F}_2^n}|\varphi_B(x)|^2 = \frac{2^n}{|B|}.$$

In particular, as $|\widehat{\varphi_B}(\alpha)| \geq \varepsilon$ for all $\alpha \in S$, we can bound

$$|S| \leq (1/\varepsilon^2)\cdot\frac{2^n}{|B|} \leq \varepsilon|A|.$$

□

4.3.2 Extractors for several independent sources

Finding explicit constructions of two-source extractors which attain min-entropy rate $\delta < 1/2$ turns out to be a difficult challenge. As a first step, we show a result of Barak, Impagliazzo and Wigderson [4] that attains this if we allow more than two independent sources. The construction and the proof are based on the sum-product theorem over finite fields (Theorem 4.4). We start with the definition of multi-source extractors, which is an immediate generalization of the definition of two-source extractors.

Definition 4.15 (Multi-source extractors). A function $E : (\{0,1\}^n)^\ell \to \{0,1\}$ is an (n,k,ε) ℓ-source extractor, if for any ℓ independent random variables $X_1,\dots,X_\ell$ supported on $\{0,1\}^n$ with $H_\infty(X_1),\dots,H_\infty(X_\ell) \geq k$, we have

$$1/2-\varepsilon \leq \Pr[E(X_1,\dots,X_\ell)=0] \leq 1/2+\varepsilon.$$

Let us recall the sum-product theorem (Thereom 4.4): if $A \subset \mathbb{F}_p$, $|A| \leq p^{0.9}$, then $\max(|A+A|,|A\cdot A|) \geq |A|^{1+\varepsilon}$ for some absolute constant $\varepsilon > 0$ (which depends only on the choice of 0.9). In particular,

$$|A\cdot A+A\cdot A| \geq |A|^{1+\varepsilon}.$$

Let $A' = A\cdot A+A\cdot A$. We can apply the sum-product theorem to A'. Either $|A'| \geq p^{0.9}$, or else

$$|A'\cdot A'+A'\cdot A'| \geq |A'|^{1+\varepsilon} \geq |A|^{1+2\varepsilon}.$$

We can continue in this fashion, until the size of the resulting set exceeds $p^{0.9}$. This is summarized in the following claim. Here, by ℓA^ℓ we mean the sum of ℓ copies of $A^\ell = A\cdots A$.

Claim 4.16. *For any $\delta > 0$ there exist $\ell = \ell(\delta)$ such that the following holds. For any $A \subset \mathbb{F}_p$ be of size $|A| \geq p^\delta$ it holds that*

$$|\ell A^\ell| \geq p^{0.9}.$$

Proof. Let $A_0 = A$ and define inductively $A_{i+1} = A_i\cdot A_i + A_i\cdot A_i$. Note that $A_i \subset 2^i A^{2^i}$. By the previous arguments, either $|A_i| \geq p^{0.9}$ or else $|A_{i+1}| \geq |A_i|^{1+\varepsilon}$. Hence after $O(\log(1/\delta))$ steps the process must stop, and we have $\ell = (1/\delta)^{O(1)}$. □

Barak et al. [4] prove a statistical analog of Claim 4.16. Analogously to the $\{0,1\}^n$, we say that a random variable Y taking values in $\mathbb{F}_p$ has min-entropy rate δ if $\min_x \Pr[Y=y] \leq p^{-\delta}$. The statistical distance between two random variables Y,Y' is $\frac{1}{2}\sum_y |\Pr[Y=y]-\Pr[Y'=y]|$. We say that a random variable Y is statistically ε-close to min-entropy rate 0.9, if there exists a random variable Y' with min-entropy 0.9 which has statistical distance at most ε from Y.

Theorem 4.17 ([4]). *For any $\delta,\varepsilon > 0$ there exist $\ell = \ell(\delta,\varepsilon)$ such that the following holds. There exists a polynomial expression $R : \mathbb{F}_p^\ell \to \mathbb{F}_p$, such that, for any independent random variables $Y_1,\dots,Y_\ell \in \mathbb{F}_p$, each with min-entropy rate at least δ, the random variable*

$$R(Y_1,\dots,Y_\ell)$$

is statistically ε-close to min-entropy rate 0.9.

The final multi-source extractor is constructed by a combination of the above result with the Hadamard two-source extractor. Formally, it requires to first translate the inputs from $\{0,1\}^n$ to $\mathbb{F}_p$, apply Theorem 4.17 twice, translate back to bits, and then apply the Hadamard two-source extractor.

Theorem 4.18 ([4])**.** *Fix $\delta,\varepsilon > 0$ and let $\ell = \ell(\delta,\varepsilon/3)$ be as given in Theorem 4.17. Define an (2ℓ)-source extractor $E : (\{0,1\}^n)^{2\ell} \to \{0,1\}$ as follows.*

1. *Let $X_1,\ldots,X_{2\ell} \in \{0,1\}^n$ denote the inputs.*
2. *Let p be prime such that $2^n < p < 2^{n+1}$, and let $\varphi : \{0,1\}^n \to \mathbb{F}_p$ be any injective map.*
3. *Let $Y_1 = R(\varphi(X_1),\ldots,\varphi(X_\ell))$ and $Y_2 = R(\varphi(X_{\ell+1}),\ldots,\varphi(X_{2\ell}))$.*
4. *Let $\psi : \mathbb{F}_p \to \{0,1\}^{n+1}$ be any injective map.*
5. *Let E_{Had} be the two-source Hadamard extractor defined over $\mathbb{F}_2^{n+1}$. Output $E_{\mathrm{Had}}(\phi(Y_1),\psi(Y_2))$.*

Then E is an (n,k,ε) (2ℓ)-source extractor with $k = (\delta + o(1))n$.

Proof. The random variables $\varphi(X_i)$ take values in $\mathbb{F}_p$, are independent and have min-entropy rate $\delta + o(1)$. Hence by Theorem 4.17 each random variables Y_i is statistically $(\varepsilon/3)$-close to a random variable Y_i' which has min-entropy rate 0.9, and the same holds for $\psi(Y_i')$. Applying the Hadamard two-source extractor to $\psi(Y_1'),\psi(Y_2')$, we obtain a bit such that $\Pr[E_{\mathrm{Had}}(\psi(Y_1'),\psi(Y_2')) = 0] = 1/2 + o(1)$. Hence also $\Pr[E_{\mathrm{Had}}(\psi(Y_1),\psi(Y_2)) = 0] = 1/2 \pm \varepsilon$. □

4.3.3 Bourgain's two-source extractor

The Hadamard two-source extractor fails for sources with min-entropy rate below $1/2$. The reason is that one can take X uniform over a subspace of $\mathbb{F}_2^n$ of dimension $n/2$, and Y uniform over the orthogonal subspace. Then both X,Y have min-entropy rate $1/2$ but $\langle X,Y\rangle = 0$ with probability one. However, this is a pathological example, and typically we do not expect such highly structured sources. If we can encode the source as an "unstructured" source, then perhaps we would be able to achieve a two-source extractor for a lower min-entropy rate. This is the idea behind the two-source extractor of Bourgain [16], which works for sources with min-entropy rate of $1/2 - \varepsilon_0$ for some small unspecified constant $\varepsilon_0 > 0$. It is a challenging open problem to find explicit constructions which still work for lower rates. We also refer the reader to an excellent exposition of Bourgain's result by Rao [49].

As a first step, we show that if the sources grow with addition, then one can achieve a better min-entropy rate. We recall that it is sufficient to consider random variables which are uniform over sets. For a set A, define the collision probability of its k-iterated sum as

$$\mathrm{CP}_k(A) = \Pr_{a_1,\ldots,a_k,a_1',\ldots,a_k' \in A}[a_1 + \ldots + a_k = a_1' + \ldots + a_k'],$$

We have $\mathrm{CP}_1(A) = |A|^{-1}$ and $\mathrm{CP}_{k+1}(A) < \mathrm{CP}_k(A)$ for all k. The following lemma shows that if $\mathrm{CP}_k(A)\mathrm{CP}_k(B) \ll 2^{-n}$ for some fixed k, then the Hadamard extractor works successfully for the sets A,B. Moreover, note that when $A \subset \mathbb{F}_2^n$ is a subspace, then $\mathrm{CP}_k(A) = 1/|A|$ for any $k \geq 1$, and hence we still have the barrier of A,B being orthogonal subspaces.

Lemma 4.19. *Fix $k \ge 1$. Let $A,B \subset \mathbb{F}_2^n$ be sets such that $\mathrm{CP}_k(A)\mathrm{CP}_k(B) \le \varepsilon^{c(k)}2^{-n}$, where $c(k)$ is a constant depending only on k. Then*

$$\left|\mathbb{E}_{a\in A,b\in B}[(-1)^{\langle a,b\rangle}]\right| \le \varepsilon.$$

Proof. We will prove the lemma for $k = 2$, the proof of the general case is similar. The main idea is to apply "repeated squaring" to simplify the expressions. First, we note that by the Cauchy-Schwarz inequality,

$$\left(\mathbb{E}_{a\in A,b\in B}[(-1)^{\langle a,b\rangle}]\right)^2 \le \mathbb{E}_{a\in A}\left(\mathbb{E}_{b\in B}[(-1)^{\langle a,b\rangle}]\right)^2 = \mathbb{E}_{a\in A,b,b'\in B}[(-1)^{\langle a,b+b'\rangle}].$$

Applying the Cauchy-Schwarz inequality again gives that

$$\left(\mathbb{E}_{a\in A,b\in B}[(-1)^{\langle a,b\rangle}]\right)^4 \le \mathbb{E}_{a,a'\in A,b,b'\in B}[(-1)^{\langle a+a',b+b'\rangle}].$$

Hence, it suffices to bound $\mathbb{E}_{a,a'\in A,b,b'\in B}[(-1)^{\langle a+a',b+b'\rangle}]$. Note that $\mathrm{CP}_2(A)$ is the collision probability for the random variable $a+a'$, and similarly $\mathrm{CP}_2(B)$ for $b+b'$. We will see that these can replace the role that $|A|,|B|$ took in the analysis of the Hadamard extractor. Define

$$S = \left\{\alpha \in \mathbb{F}_2^n : \left|\mathbb{E}_{b,b'\in B}[(-1)^{\langle \alpha,b+b'\rangle}]\right| \ge \varepsilon\right\}.$$

We will show that $\Pr_{a,a'\in A}[a+a' \in S] \le \varepsilon$. As before, this will show that

$$\mathbb{E}_{a,a'\in A,b,b'\in B}[(-1)^{\langle a+a',b+b'\rangle}] \le \Pr[a+a' \in S] + \sum_{x\notin S}\Pr[a+a'=x]\left|\mathbb{E}_{b,b'\in B}[(-1)^{\langle x,b+b'\rangle}]\right| \le 2\varepsilon.$$

Define $\varphi(x) = 2^n \cdot \Pr_{b,b'\in B}[b+b'=x]$. Then $\widehat{\varphi}(\alpha) = \mathbb{E}_{b,b'\in B}[(-1)^{\langle \alpha,b+b'\rangle}]$ and hence $S = \{\alpha : |\widehat{\varphi(\alpha)}| \ge \varepsilon\}$. We bound

$$|S|\varepsilon^2 \le \sum_{\alpha\in\mathbb{F}_2^n} |\widehat{\varphi(\alpha)}|^2 = \mathbb{E}_{x\in\mathbb{F}_2^n}[\varphi(x)^2] = 2^n \sum_{x\in\mathbb{F}_2^n}\Pr_{b,b'\in B}[b+b'=x]^2 = 2^n\cdot\mathrm{CP}_2(B).$$

Hence by assumption $|S| \le \varepsilon^{O(1)}\cdot\mathrm{CP}_2(A)^{-1}$. On the other hand, we have

$$\Pr_{a,a'\in A}[a+a'\in S]^2 = (\sum_{x\in S}\Pr_{a,a'\in A}[a+a'=x])^2 \le |S|\sum_{x\in S}\Pr_{a,a'\in A}[a+a'=x]^2 \le |S|\cdot\mathrm{CP}_2(A).$$

Putting these together we conclude that

$$\Pr_{a,a'\in A}[a+a'\in S] \le (|S|\cdot\mathrm{CP}_2(A))^{1/2} \le \varepsilon^{O(1)}.$$

□

So, we get that the only sets A,B for which the Hadamard extractor fails are those that do not grow under addition. The next idea is to build an encoding function which would make all large enough sets grow nontrivially under addition. Assume we had a function $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ with the following property: for any set $A \subset \mathbb{F}_2^n$ of size $|A| \geq 2^{\delta n}$, we have that

$$\mathrm{CP}_k(f(A)) \leq \varepsilon^{c(k)} 2^{-m/2}$$

for some $k \geq 1$. Then, if we define

$$E(X,Y) = \langle f(X), f(Y) \rangle$$

we would get a two-source extractor for min-entropy rate δ.

Note that equivalently, if we view this extractor as a bipartite graph, then it is a subgraph of the graph corresponding to the Hadamard extractor over $\mathbb{F}_2^m$. That is, it is a bipartite graph of the form (U,V,E) where $|U| = |V| = 2^n$, $U,V \subset \{0,1\}^m$, and $E = \{(u,v) : \langle u,v \rangle = 0\}$.

The only remaining question is how to construct such an encoding function f. This is where the sum-product theorem will come into play. First, for technical reasons we will need to generalize the construction of the Hadamard extractor to fields of odd characteristics. The following Lemma is a generalization of Lemma 4.19. For a proof see [49].

Lemma 4.20. *Let $\mathbb{F}_p$ be a prime finite field. Define $E:\mathbb{F}_p^n \times \mathbb{F}_p^n \to \{0,1\}$ as*

$$E(x,y) = \langle x,y \rangle \mod 2.$$

If X,Y are independent random variables, taking values in $\mathbb{F}_p^n$, such that $\mathrm{CP}_k(A)\mathrm{CP}_k(B) \leq \varepsilon^{c(k)} p^{-n}$, then

$$\left| \Pr[E(X,Y)=0] - 1/2 \right| \leq \varepsilon + O(1/p).$$

The construction we will present will be for a large prime p and $n = 2$. We note that similar constructions for small p, large n can be attained using the sum-product theorem for non-prime fields (which we did not present, and will not discuss here). So, fix a large prime p and consider the map $f:\mathbb{F}_p \to \mathbb{F}_p^2$ defined as

$$f(x) = (x, x^2).$$

Let $A \subset \mathbb{F}_p$ be mapped to $f(A) \subset \mathbb{F}_p^2$. Consider first $f(A)+f(A)$. For any $x,y \in \mathbb{F}_p$, the number of solutions for $(a+b, a^2+b^2) = (x,y)$ is at most two, hence $|f(A)+f(A)| \geq |A|^2/2$. For the same reason, $\mathrm{CP}_2(f(A)) \leq 2|A|^{-2}$. It might seem like we gained in the collision probability, but the universe size has also grown from p to p^2, hence the min-entropy rate of A in $\mathbb{F}_p$ is the same as that of $f(A)$ in $\mathbb{F}_p^2$ (that is: if $|A| = p^\alpha$ then $|f(A)+f(A)| \approx (p^2)^\alpha$). The actual advantage will come once we consider the collision probability of the sum of three copies of $f(A)$.

Lemma 4.21. *There exist an absolute constant $\varepsilon_0 > 0$ such that the following holds. If $A \subset \mathbb{F}_p$ has size $|A| \geq p^{1/2-\varepsilon_0}$ then $\mathrm{CP}_3(f(A)) \leq p^{-(1+\varepsilon_0)}$.*

We are now in business. Combining Lemma 4.21 with Lemma 4.20, we get the following corollary.

Corollary 4.22. *Let $\mathbb{F}_p$ be a large enough prime field. Define $E_{\mathrm{Bou}} : \mathbb{F}_p \times \mathbb{F}_p \to \{0,1\}$ as*

$$E_{\mathrm{Bou}}(x,y) = (xy + x^2y^2) \mod 2.$$

Then, if $X,Y \subset \mathbb{F}_p$ are random variables of min-entropy rate $\geq 1/2 - \varepsilon_0$, then

$$|\Pr[E_{\mathrm{Bou}}(X,Y) = 0] - 1/2| \leq p^{-O(\varepsilon_0)}.$$

We are left with proving Lemma 4.21. Surprisingly perhaps, its proof relies on the intersection pattern of lines and points in $\mathbb{F}_p^2$. Let $P \subset \mathbb{F}_p^2$ be a set of points in $\mathbb{F}_p^2$. A line in $\mathbb{F}_p^2$ is a set of the form $\ell_{a,b} = \{(x, ax+b) : x \in \mathbb{F}_p\}$. Let $\mathcal{L}$ denote the set of all lines, $|\mathcal{L}| = p^2$. Let $L \subset \mathcal{L}$ be a subset of the lines. We denote the set of intersections of P and L by

$$I(P,L) = \{(x,\ell) \in P \times L : x \in L\}.$$

A trivial upper bound is $|I(P,L)| \leq |P||L| \leq p^4$. A slightly less trivial upper bound, utilizing the fact that any two points lie on at most one line, is that $|I(P,L)| \leq |P|^{1/2}|L| \leq p^3$.

Claim 4.23. $I(P,L) \leq |P|^{1/2}|L|$.

Proof. We have $I(P,L) = \sum_{x \in P, \ell \in L} 1_{x \in \ell}$. Hence by the Cauchy-Schwarz inequality,

$$I(P,L)^2 \leq \left(\sum_{x \in P, \ell \in L} 1_{x \in \ell} \right)^2 \leq |L| \sum_{\ell \in L} \left(\sum_{x \in P} 1_{x \in \ell} \right)^2 = |L| \sum_{x,x' \in P} \sum_{\ell \in L} 1_{x,x' \in \ell} \leq |L||P|^2.$$

□

A similar claim, using the fact that two lines intersect in at most one point, gives the dual bound $|I(P,L)| \leq |P||L|^{1/2}$. These bounds are in general tight, as if one takes $P = \mathbb{F}_p^2$ the set of all points and $L = \mathcal{L}$ the set of all lines, then $|P| = |L| = p^2$ and $|I(P,L)| = p^3$. However, the next theorem shows is that the bound is tight only in such extreme cases.

Theorem 4.24 ([19, 39, 18])**.** *For any $\alpha > 0$ there exist $\varepsilon > 0$ such that the following holds. If* $\max(|P|,|L|) = M \leq p^{2-\alpha}$ *then* $|I(P,L)| \leq M^{3/2-\varepsilon}$.

The sum-product Theorem 4.4 follows from Theorem 4.24. To see this, let $A \subset \mathbb{F}_p$ be a set of size $|A| \leq p^{0.9}$. For simplicity, we assume $0 \notin A$. Define the following sets of points and lines

$$P = (A \cdot A) \times (A + A), \qquad L = \{\ell_{a^{-1},b} : a \in A, b \in A\}.$$

Any line $\ell_{a^{-1},b} \in L$ can be equivalently written as

$$\ell_{a^{-1},b} = \{(x, a^{-1}x + b) : x \in \mathbb{F}_p\} = \{(ax, x+b) : x \in \mathbb{F}_p\}.$$

Hence, whenever $x \in A$ we have $(ax, x+b) \in P$ and hence

$$|I(P,L)| \geq |L||A| = |A|^3.$$

Let $M = \max(|P|,|L|) = |A \cdot A||A+A|$. If $M \ge p^{1.9}$ then we are done, as this implies that $\max(|A \cdot A|, |A+A|) \ge p^{0.95} \ge |A|^{1.05}$. Otherwise, apply Theorem 4.24 with $\alpha = 0.1$. There exists $\varepsilon > 0$ for which $|I(P,L)| \le M^{3/2-\varepsilon}$, or equivalently

$$|A \cdot A|\ |A+A| \ge (|A|^3)^{1/(3/2-\varepsilon)} = |A|^{2+\Omega(\varepsilon)},$$

which implies that $\max(|A \cdot A|, |A+A|) \ge |A|^{1+\Omega(\varepsilon)}$. One can also deduce Theorem 4.24 from Theorem 4.4, but this is more complicated, and we refer the interested readers to the original papers [19, 39, 18] for the details.

Finally, we show how Lemma 4.21 follows from Theorem 4.24.

Proof of Lemma 4.21. An element of $f(A)+f(A)+f(A)$ is of the form

$$(a+b+c, a^2+b^2+c^2)$$

with $a,b,c \in A$. For $x,y \in \mathbb{F}_p$ let

$$N(x,y) = \{(a,b,c) \in A^3 : (a+b+c, a^2+b^2+c^2) = (x,y)\}.$$

We have

$$\mathrm{CP}_3(f(A)) = \sum_{x,y \in \mathbb{F}_p} \Pr_{a,b,c \in A}[(a+b+c, a^2+b^2+c^2) = (x,y)]^2 = |A|^{-6} \sum_{x,y \in \mathbb{F}_p} N(x,y)^2.$$

Let us first build some intuition. Our goal is to show that $\mathrm{CP}_3(f(A)) \ll p^{-1}$. A trivial upper bound is $N(x,y) \le 2|A|$, since for every fixed c, there are at most two solutions for $(a+b+c, a^2+b^2+c^2) = (x,y)$. Moreover, since $\sum N(x,y) = |A|^3$ this implies the bound $\mathrm{CP}_3(f(A)) \le O(|A|^{-2})$, which would require $|A| \gg p^{1/2}$, corresponding to min-entropy rate $1/2$. However, we are interested in beating this, namely in sets of size $|A| \ge p^{1/2-\varepsilon}$ for some $\varepsilon > 0$. This should not be surprising, as so far we did not apply any sum-product or point-line incidence machinery.

Formally, for $\delta > 0$ to be defined later, define the set of points to be

$$P = \{(x,y) \in \mathbb{F}_p^2 : N(x,y) \ge |A|^{1-\delta}\}.$$

Since $\sum N(x,y) = |A|^3$ we have $|P| \le |A|^{2+\delta}$. If $(a+b+c, a^2+b^2+c^2) = (x,y)$ then $(a+b+c, ab+ac+bc) = (x, (y-x^2)/2)$. We define the set of lines to be

$$\begin{aligned} L &= \left\{\ell_{a+b, ab-(a+b)^2} : a,b \in A\right\} \\ &= \left\{\{(x, (a+b)x + ab - (a+b)^2) : x \in \mathbb{F}_p\} : a,b \in A\right\} \\ &= \left\{\{(a+b+x, ab+(a+b)x) : x \in \mathbb{F}_p\} \quad : a,b \in A\right\}. \end{aligned}$$

With this definition, $N(x,y)$ counts the number of lines in L which pass through $(x,(y-x^2)/2)$. By our assumption, any point in P lies on at least $|A|^{1-\delta}$ lines, hence

$$|I(P,L)| \ge |P| \cdot |A|^{1-\delta}.$$

We next will apply Theorem 4.24. Let $M = \max(|P|,|L|) \le |A|^{2+\delta}$. Note that as we may assume $|A| \le p^{1/2}$ we have $M \le p^{1+\delta/2}$, which is in the allowed regime for any $\delta < 2$. More concretely, if we choose $\delta < 1$ (say) then $M \le p^{3/2}$, and there exists an absolute constant $\varepsilon > 0$ (independent of δ !) such that

$$|I(P,L)| \le M^{3/2-\varepsilon}.$$

Rearranging,

$$|P| \le |A|^{(2+\delta)(3/2-\varepsilon)-(1-\delta)} = |A|^{2-2\varepsilon+O(\delta)}.$$

Choosing $\delta > 0$ small enough, we have

$$|P| \le |A|^{2-\varepsilon}.$$

That is, for nearly all points x,y we have $N(x,y) \le |A|^{1-\delta}$. We next apply this to derive an improved bound on $\mathrm{CP}_3(f(A))$.

$$\begin{aligned}|A|^6 \cdot \mathrm{CP}_3(f(A)) &= \sum_{(x,y)\in P} N(x,y)^2 + \sum_{(x,y)\notin P} N(x,y)^2\\ &\le |P| \cdot \max_{(x,y)\in P} N(x,y)^2 + \sum_{(x,y)\notin P} N(x,y) \cdot \max_{(x,y)\notin P} N(x,y)\\ &\le |P| \cdot (2|A|)^2 + |A|^3 \cdot |A|^{1-\delta}\\ &\le 4|A|^{4-\varepsilon} + |A|^{4-\delta}.\end{aligned}$$

By possibly replacing δ with $\min(\varepsilon,\delta)$, we get that

$$\mathrm{CP}_3(f(A)) \le O(|A|^{-(2+\delta)}).$$

One can now verify that the lemma follows with $\varepsilon_0 = \delta/12$. □

4.4 Approximate duality

We present here another approach to the construction of two-source extractors, based on an approximate notion of orthogonal subspaces, called *approximate duality*. It was introduced by Ben-Sasson and Ron-Zewi [50] who used it to show that a family of potential constructions of bipartite Ramsey graphs must also be two-source extractors. Later works used the notion of approximate duality to give an improvement on the known upper bounds for the log-rank conjecture in communication complexity [10] and to prove lower bounds on certain families of locally decodable codes [11].

Let $A,B \subset \mathbb{F}^n$ be two subsets of a vector space. The sets A,B are called approximate dual if a noticeable fraction of the pairs $(a,b) \in A \times B$ are orthogonal under the standard inner product on $\mathbb{F}^n$. If the sets A,B were random and $|\mathbb{F}| = p$ we would expect $1/p$ fraction of the pairs to be orthogonal; hence, any larger fraction is considered noticeable.

Definition 4.25 (Approximate duality)**.** Sets $A,B \subset \mathbb{F}^n$ are ε-approximately dual if

$$\left|\left\{(a,b) \in A \times B : \langle a,b\rangle = 0\right\}\right| \ge \left(\frac{1}{|\mathbb{F}|} + \varepsilon\right)|A||B|.$$

The value 0 is chosen for convenience; with the price of increasing the dimension by one, it can be changed to any other field element $z \in \mathbb{F}$ by replacing A with $A \times \{1\}$ and B with $B \times \{z\}$. We also note that in characteristic zero, for example in $\mathbb{R}^n$, the definition corresponds to having an ε-fraction of orthogonal vectors. The approximate duality conjecture speculates that any two large approximate dual sets must contain large subsets which are dual (orthogonal) to each other.

Conjecture 4.26 (Approximate duality conjecture [50])**.** *For any $\varepsilon > 0$ there exists a constant $c = c(\varepsilon) > 0$ such that the following holds. Let $A, B \subset \mathbb{F}^n$ be ε-approximately dual sets. Then there exist subsets $A' \subset A, B' \subset B$ such that*

$$\langle a, b \rangle = 0 \qquad \forall a \in A', b \in B'$$

and

$$\frac{|A|}{|A'|}, \frac{|B|}{|B'|} \leq 2^{c\sqrt{n}}.$$

The bound $|A|/|A'|, |B|/|B'| \leq 2^{c\sqrt{n}}$ might seem unnatural. However, it is the best possible as can be seen by the following example. In the following, the *support* of a vector $x \in \mathbb{F}^n$ is the set of its nonzero coordinates.

Example 4.27. Let $A \subset \mathbb{F}^n$ be the set of all $\{0,1\}^n$ vectors which have support of size at most $0.1\sqrt{n}$. Set $B = A$. The probability that a randomly chosen pair of vectors $a \in A, b \in B$ have disjoint supports is at least 0.9, in which case $\langle a, b \rangle = 0$. Hence, A, B are ε-approximately dual for $\varepsilon = 0.9 - 1/|F| \geq 0.4$. On the other hand, it can be verified that the largest orthogonal subsets $A' \subset A, B' \subset B$ are given by

$$A' = \{x \in A : x_1 = \cdots = x_{n/2} = 0\}, \quad B' = \{x \in B : x_{n/2+1} = \cdots = x_n = 0\}$$

and $|A|/|A'| = |B|/|B'| \geq \exp(c\sqrt{n})$ for some constant $c > 0$.

The approximate duality conjecture was introduced by [50], who used it to construct two-source extractors from constructions of bipartite Ramsey graphs which are subgraphs of the inner-product graph (i. e., the Hadamard extractor).

Theorem 4.28 ([50])**.** *Let $H = (U, V, E)$ be a graph with vertex sets $U, V \subset \mathbb{F}_2^n$ and edge set $E = \{(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : \langle u, v \rangle = 0\}$. Assume that H is an (n, k) bipartite Ramsey graph. Then, assuming the approximate duality conjecture (Conjecture 4.26), it is also an (n, k', ε) two-source extractor for $k' = k + c(\varepsilon)\sqrt{n}$. In particular, if $k = \delta n$ then $k' = (\delta + o(1))n$.*

Proof. Assume towards contradiction that H is not an (n, k', ε) two-source extractor. Then, there exist subsets $A \subset U, B \subset V$ of size $|A|, |B| \geq 2^{k'}$ such that

$$\left| E(A, B) - \frac{1}{2}|A||B| \right| \geq \varepsilon |A||B|.$$

Consider first the case that $|E(A, B)| \geq (1/2 + \varepsilon)|A||B|$. We apply the approximate duality conjecture and deduce that there exist subsets $A' \subset A, B' \subset B$ which are orthogonal and $|A|/|A'|, |B|/|B'| \leq 2^{c\sqrt{n}}$ where $c = c(\varepsilon)$. This means that $|E(A', B')| = 0$ and by assumption this can only happen if $|A'| < 2^k$ or $|B'| < 2^k$. Hence, we have $k' < k + c\sqrt{n}$. The case that $|E(A, B)| \leq (1/2 - \varepsilon)|A||B|$ is handled analogously by considering the complement graph. □

There are explicit constructions of bipartite Ramsey graphs for any constant min-entropy (and in fact also for sub-constant) [5]. Unfortunately, these constructions are not subgraphs of the inner-product graph, and hence Theorem 4.28 cannot apply to them.

We next turn to investigate the approximate duality conjecture (Conjecture 4.26). The best result to date is by [10] who proved that a weak version of the approximate duality conjecture in $\mathbb{F}_2^n$ holds assuming the polynomial Freiman–Ruzsa conjecture in $\mathbb{F}_2^n$. It was generalized to groups of constant torsion in [11] who used it to prove lower bounds for certain families of locally decodable codes. We do not know if the approximate duality conjecture is equivalent to the polynomial Freiman–Ruzsa conjecture, or if one of them follows from the other. In [50] it was shown that certain weak variants of the two conjectures are equivalent.

For simplicity, from now on we focus on the approximate duality conjecture in $\mathbb{F}_2^n$. First, we state a very weak version of Conjecture 4.26 which is known to hold unconditionally, when most pairs are orthogonal.

Theorem 4.29 ([50])**.** *Let $A,B \subset \mathbb{F}_2^n$ be sets which are $(1-\varepsilon)$-approximately dual. Then there exist subsets $A' \subset A, B' \subset B$ such that*

$$\langle a,b\rangle = c \qquad \forall a \in A', b \in B'$$

for some $c \in \mathbb{F}_2$, where

$$\frac{|A|}{|A'|}, \frac{|B|}{|B'|} \le 2^{\delta n}$$

for $\delta = O(\varepsilon \log(1/\varepsilon))$.

Proof. By assumption we know that $\Pr_{a\in A, b\in B}[\langle a,b\rangle = 1] \le \varepsilon$. Let

$$A_0 = \{a \in A : \Pr_{b\in B}[\langle a,b\rangle = 1] \le 2\varepsilon\}.$$

By the Markov inequality we have that $|A_0| \ge |A|/2$. Let $d = \dim(A_0)$ and fix $a_1,\ldots,a_d \in A_0$ linearly independent. For each $b \in B$ define $w(b)$ to be

$$w(b) = \{i \in [d] : \langle a_i,b\rangle = 1\}.$$

We have that $\mathbb{E}_{b\in B}[w(b)] = \sum_{i=1}^d \Pr[\langle a_i,b\rangle = 1] \le 2\varepsilon d$. Hence, if we define

$$B_0 = \{b \in B : w(b) \le 4\varepsilon d\}$$

then again by the Markov inequality we have $|B_0| \ge |B|/2$. Now, the main observation is that the number of distinct inner product patterns $(\langle a_i,b\rangle)_{i\in[d]}$ for $b \in B_0$ is bounded by $\binom{d}{\le 4\varepsilon d} \le 2^{\delta d}$ for $\delta = O(\varepsilon \log(1/\varepsilon))$. Thus, we can find $c_1,\ldots,c_d \in \mathbb{F}_2$ such that for

$$B' = \{b \in B_0 : \langle a_i,b\rangle = c_i \; \forall i \in [d]\}$$

we have $|B'| \ge |B_0| 2^{-\delta d}$. Note that since $a_1,\ldots,a_d$ span A_0, we have that for any $a \in A_0$, the inner products $\langle a,b\rangle$ for all $b \in B'$ are all equal. Let

$$A' = \{a \in A_0 : \langle a,b\rangle = c \; \forall b \in B'\}$$

where $c \in \mathbb{F}_2$ is chosen to maximize $|A'| \ge |A_0|/2$. The theorem follows. □

A serious shortcoming of Theorem 4.29 is that it applies only to sets which are already nearly orthogonal, and moreover, it loses an exponential factor. The following result improves both of these. However, it assumes the polynomial Freiman–Ruzsa conjecture.

Theorem 4.30 ([10])**.** *Let $A,B \subset \mathbb{F}_2^n$ be sets which are ε-approximately dual. Assuming the polynomial Freiman–Ruzsa conjecture in $\mathbb{F}_2^n$ (Conjecture 2.20), there exist subsets $A' \subset A, B' \subset B$ such that*

$$\langle a,b\rangle = c \qquad \forall a \in A', b \in B'$$

for some $c \in \mathbb{F}_2$, where

$$\frac{|A|}{|A'|}, \frac{|B|}{|B'|} \le 2^{cn/\log n}$$

where $c = c(\varepsilon)$.

References

[1] NOGA ALON: Testing subgraphs in large graphs. *Random Structures and Algorithms*, 21(3-4):359–370, 2002. Preliminary version in FOCS'01. [doi:10.1002/rsa.10056] 25

[2] NOGA ALON, TALI KAUFMAN, MICHAEL KRIVELEVICH, SIMON LITSYN, AND DANA RON: Testing Reed-Muller codes. *IEEE Trans. Inform. Theory*, 51(11):4032–4039, 2005. Preliminary version in RANDOM'03. [doi:10.1109/TIT.2005.856958] 15

[3] ANTAL BALOG AND ENDRE SZEMERÉDI: A statistical theorem of set addition. *Combinatorica*, 14(3):263–268, 1994. [doi:10.1007/BF01212974] 9

[4] BOAZ BARAK, RUSSELL IMPAGLIAZZO, AND AVI WIGDERSON: Extracting randomness using few independent sources. *SIAM J. Comput.*, 36(4):1095–1118, 2006. Preliminary version in FOCS'04. [doi:10.1137/S0097539705447141] 39, 40

[5] BOAZ BARAK, ANUP RAO, RONEN SHALTIEL, AND AVI WIGDERSON: 2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction. In *Proc. 38th STOC*, pp. 671–680. ACM Press, 2006. [doi:10.1145/1132516.1132611] 47

[6] BOAZ BARAK, LUCA TREVISAN, AND AVI WIGDERSON: A mini-course on additive combinatorics, 2007. Available at course website. 2, 29

[7] MICHAEL BATEMAN AND NETS KATZ: New bounds on cap sets. *J. Amer. Math. Soc.*, 25(2):585–613, 2012. [doi:10.1090/S0894-0347-2011-00725-X, arXiv:1101.5851] 20

[8] FELIX A. BEHREND: On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. U.S.A.*, 32(12):331–332, 1946. Available at PMC. 22

[9] MIHIR BELLARE, DON COPPERSMITH, JOHAN HÅSTAD, MARCOS KIWI, AND MADHU SUDAN: Linearity testing over characteristic two. *IEEE Trans. Inform. Theory*, 42(6):1781–1795, 1996. Preliminary version in FOCS'95. [doi:10.1109/18.556674] 12, 13

[10] ELI BEN-SASSON, SHACHAR LOVETT, AND NOGA RON-ZEWI: An additive combinatorics approach relating rank to communication complexity. *J. ACM*, 61(4):22:1–22:18, 2014. Preliminary versions in FOCS'12 and ECCC. [doi:10.1145/2629598] 45, 47, 48

[11] ABHISHEK BHOWMICK, ZEEV DVIR, AND SHACHAR LOVETT: New bounds for matching vector families. *SIAM J. Comput.*, 43(5):1654–1683, 2014. Preliminary versions in STOC'13 and ECCC. [doi:10.1137/130932296] 45, 47

[12] KHODAKHAST BIBAK: Additive combinatorics with a view towards computer science and cryptography – an exposition. In *Number Theory and Related Fields*, volume 43, pp. 99–128. Springer, 2013. [doi:10.1007/978-1-4614-6642-0_4, arXiv:1108.3790] 3

[13] THOMAS F. BLOOM: Translation invariant equations and the method of Sanders. *Bull. London Math. Soc.*, 44(5):1050–1067, 2012. [doi:10.1112/blms/bds045, arXiv:1107.1110] 20

[14] MANUEL BLUM, MICHAEL LUBY, AND RONITT RUBINFELD: Self-testing/correcting with applications to numerical problems. *J. Comput. System Sci.*, 47(3):549–595, 1993. Preliminary version in STOC'90. [doi:10.1016/0022-0000(93)90044-W] 11, 13

[15] JEAN BOURGAIN: On triples in arithmetic progression. *Geom. Funct. Anal.*, 9(5):968–984, 1999. [doi:10.1007/s000390050105] 20

[16] JEAN BOURGAIN: More on the sum-product phenomenon in prime fields and its applictaions. *Internat. J. Number Theory*, 1(1):1–32, 2005. [doi:10.1142/S1793042105000108] 40

[17] JEAN BOURGAIN: Roth's theorem on progressions revisited. *Journal d'Analyse Mathématique*, 104(1):155–192, 2008. [doi:10.1007/s11854-008-0020-x] 20

[18] JEAN BOURGAIN, ALEKSEI A. GLIBICHUK, AND SERGEI VLADIMIROVICH KONYAGIN: Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc.*, 73(2):380–398, 2006. [doi:10.1112/S0024610706022721] 31, 32, 43, 44

[19] JEAN BOURGAIN, NETS KATZ, AND TERENCE TAO: A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004. [doi:10.1007/s00039-004-0451-1, arXiv:math/0301343] 31, 32, 43, 44

[20] MEI-CHU CHANG: Some consequences of the polynomial Freiman–Ruzsa conjecture. *C. R. Acad. Sci. Paris Ser. I Math.*, 347(11-12):583–588, 2009. [doi:10.1016/j.crma.2009.04.006] 19

[21] STEPHEN A. COOK: The complexity of theorem-proving procedures. In *Proc. 3rd STOC*, pp. 151–158. ACM Press, 1971. [doi:10.1145/800157.805047] 26

[22] HOLGER DELL AND DIETER VAN MELKEBEEK: Satisfiability allows no nontrivial sparsification unless the polynomial-time hierarchy collapses. *J. ACM*, 61(4):23:1–23:27, 2014. Preliminary version in STOC'10. [doi:10.1145/2629620] 25, 26

[23] JEAN-MARC DESHOUILLERS, FRANÇOIS HENNECART, AND ALAIN PLAGNE: On small sumsets in $(\mathbb{Z}/2\mathbb{Z})^n$. *Combinatorica*, 24(1):53–68, 2004. [doi:10.1007/s00493-004-0004-0] 6

[24] PAUL ERDŐS AND ENDRE SZEMERÉDI: On sums and products of integers. *Studies in Pure Math.*, pp. 213–218, 1983. [doi:10.1007/978-3-0348-5438-2_19] 29, 30

[25] CHAIM EVEN-ZOHAR: On sums of generating sets in $\mathbb{Z}_2^n$. *Combin. Probab. Comput.*, 21(6):916–941, 2012. [doi:10.1017/S0963548312000351, arXiv:1108.4902] 6

[26] CHAIM EVEN-ZOHAR AND SHACHAR LOVETT: The Freiman–Ruzsa theorem over finite fields. *J. Combinat. Theory, Ser. A*, 125:333–341, 2014. Preliminary verion in ECCC. [doi:10.1016/j.jcta.2014.03.011, arXiv:1212.5738] 6

[27] JACOB FOX: A new proof of the graph removal lemma. *Ann. of Math.*, 174(1):561–579, 2011. [doi:10.4007/annals.2011.174.1.17, arXiv:1006.1300] 25

[28] GREGORY ABELEVICH FREIMAN: *Foundations of a structural theory of set addition*. Volume 37. Amer. Math. Soc., 1973. 5

[29] ODED GOLDREICH: Introduction to testing graph properties. In *Property Testing*, volume 6390 of *LNCS*, pp. 105–141. Springer, 2010. [doi:10.1007/978-3-642-16367-8_7] 24

[30] WILLIAM TIMOTHY GOWERS: A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001. [doi:10.1007/s00039-001-0332-9] 9

[31] BEN GREEN: Finite field models in additive combinatorics. *Surveys in Combinatorics*, pp. 1–28, 2005. [doi:10.1017/CBO9780511734885.002, arXiv:math/0409420] 2

[32] BEN GREEN: The polynomial Freiman-Ruzsa conjecture, 2005. Available at author's website. 2, 17

[33] BEN GREEN AND TERENCE TAO: The primes contain arbitrarily long arithmetic progressions. *Ann. of Math.*, 167(2):481–547, 2008. [doi:10.4007/annals.2008.167.481, arXiv:math/0404188] 20

[34] BEN GREEN AND TERENCE TAO: Freiman's theorem in finite fields via extremal set theory. *Combin. Probab. Comput.*, 18(3):335–355, 2009. [doi:10.1017/S0963548309009821, arXiv:math/0703668] 6

[35] DAVID RODNEY HEATH-BROWN: Integer sets containing no arithmetic progressions. *J. London Math. Soc.*, s2-35(3):385–394, 1987. [doi:10.1112/jlms/s2-35.3.385] 20

[36] ALEX IOSEVICH, OLIVER ROCHE-NEWTON, AND MISHA RUDNEV: On an application of Guth-Katz theorem. *Math. Res. Lett.*, 18(4):691–697, 2011. [doi:10.4310/MRL.2011.v18.n4.a8, arXiv:1103.1354] 30

[37] RICHARD M. KARP: Reducibility among combinatorial problems. In RAYMOND E. MILLER AND JAMES W. THATCHER, editors, *Complexity of Computer Computations*, The IBM Research Symposia Series, pp. 85–103. Springer, 1972. [doi:10.1007/978-1-4684-2001-2_9] 26

[38] TALI KAUFMAN AND MADHU SUDAN: Algebraic property testing: the role of invariance. In *Proc. 40th STOC*, pp. 403–412. ACM Press, 2008. [doi:10.1145/1374376.1374434] 15

[39] SERGEI VLADIMIROVICH KONYAGIN: A sum-product estimate in fields of prime order, 2003. [arXiv:math/0304217] 31, 32, 43, 44

[40] SERGEI VLADIMIROVICH KONYAGIN: On the Freiman theorem in finite fields. *Math. Notes*, 84(3):435–438, 2008. [doi:10.1134/S0001434608090137] 6

[41] JÁNOS KÖRNER AND KATALIN MARTON: How to encode the modulo-two sum of binary sources. *IEEE Trans. Inform. Theory*, 25(2):219–221, 1979. Available from IEEE. 16

[42] IZABELLA ŁABA: Fuglede's conjecture for a union of two intervals. *Proc. Amer. Math. Soc.*, 129(10):2965–2972, 2001. [doi:10.1090/S0002-9939-01-06035-X, arXiv:math/0002067] 4

[43] LEONID A. LEVIN: Universal sequential search problems. *Problems of Information Transmission*, 9(3):115–116, 1973. Available at Mathnet. 26

[44] SHACHAR LOVETT: *An exposition of Sanders' quasi-polynomial Freiman-Ruzsa theorem*. Number 6 in Graduate Surveys. Theory of Computing Library, 2015. Preliminary version in ECCC. [doi:10.4086/toc.gs.2015.006] 2, 18

[45] ROY MESHULAM: On subsets of finite abelian groups with no 3-term arithmetic progressions. *J. Combinat. Theory, Ser. A*, 71(1):168–172, 1995. [doi:10.1016/0097-3165(95)90024-1] 20

[46] GIORGIS PETRIDIS: New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012. [doi:10.1007/s00493-012-2818-5, arXiv:1101.3507] 7

[47] HELMUT PLÜNNEKE: Eigenschaften und Abschätzungen von Wirkungsfunktionen. *Gesellschaft für Mathematik und Datenverarbeitung*, 1969. 7

[48] ROBERT ALEXANDER RANKIN: Sets of integers containing not more than a given number of terms in arithmetical progression. *Proc. Royal Soc. Edinburgh. Sec. A. Math. Phys. Sci.*, 65(4):332–344, 1961. [doi:10.1017/S0080454100017726] 23

[49] ANUP RAO: An exposition of Bourgain's 2-source extractor. *Electronic Colloquium on Computational Complexity (ECCC)*, 14(34), 2007. Available at ECCC. 40, 42

[50] NOGA RON-ZEWI AND ELI BEN-SASSON: From affine to two-source extractors via approximate duality. *SIAM J. Comput.*, 44(6):1670–1697, 2015. Preliminary versions in STOC'11 and ECCC. [doi:10.1137/12089003X] 45, 46, 47

[51] KLAUS ROTH: Sur quelques ensembles d'entiers. *C. R. Acad. Sci. Paris Ser. I Math.*, 234:388–390, 1952. 19

[52] KLAUS ROTH: On certain sets of integers. *J. London Math. Soc.*, s1-28(1):104–109, 1953. [doi:10.1112/jlms/s1-28.1.104] 19

[53] RONITT RUBINFELD AND MADHU SUDAN: Robust characterizations of polynomials and their applications to program testing. *SIAM J. Comput.*, 25(2):252–271, 1996. [doi:10.1137/S0097539793255151] 11

[54] IMRE Z. RUZSA: Arithmetical progressions and the number of sums. *Periodica Math. Hung.*, 25(1):105–111, 1992. [doi:10.1007/BF02454387] 7

[55] IMRE Z. RUZSA: An analog of Freiman's theorem in groups. *Structure Theory of Set-Addition. Astérisque*, 258:323–326, 1999. Available at author's website. Virtually identical version available as DIMACS TR 93-77, 1993 from CiteSeer. 6, 16

[56] IMRE Z. RUZSA AND ENDRE SZEMERÉDI: Triple systems with no six points carrying three triangles. In *Coll. Math. Soc. J. Bolyai*, volume 18, pp. 939–945. Bolyai Soc. and North-Holland, 1978. 25

[57] ALEX SAMORODNITSKY: Low-degree tests at large distances. In *Proc. 39th STOC*, pp. 506–515. ACM Press, 2007. [doi:10.1145/1250790.1250864, arXiv:math/0604353] 2, 12, 15

[58] TOM SANDERS: A note on Freiman's theorem in vector spaces. *Combin. Probab. Comput.*, 17(2):297–305, 2008. [doi:10.1017/S0963548307008644, arXiv:math/0605523] 6

[59] TOM SANDERS: On Roth's theorem on progressions. *Ann. of Math.*, 174(1):619–636, 2011. [doi:10.4007/annals.2011.174.1.20, arXiv:1011.0104] 20

[60] TOM SANDERS: On certain other sets of integers. *Journal d'Analyse Mathématique*, 116(1):53–82, 2012. [doi:10.1007/s11854-012-0003-9, arXiv:1007.5444] 20

[61] TOM SANDERS: On the Bogolyubov-Ruzsa lemma. *Analysis and PDE*, 5(3):627–655, 2012. [doi:10.2140/apde.2012.5.627, arXiv:1011.0107] 2, 15, 18

[62] IGOR E. SHPARLINSKI: Additive combinatorics over finite fields: New results and applications. In *Finite Fields and Their Applications: Character Sums and Polynomials*, volume 11 of *Radon Series on Computational and Applied Mathematics*, pp. 233–272. De Gruyter, 2013. 3

[63] JÓZSEF SOLYMOSI: Bounding multiplicative energy by the sumset. *Advances in Math.*, 222(2):402–408, 2009. [doi:10.1016/j.aim.2009.04.006, arXiv:0806.1040] 30

[64] BENNY SUDAKOV, ENDRE SZEMERÉDI, AND VAN H. VU: On a question of Erdős and Moser. *Duke Math. J.*, 129(1):129–155, 2005. [doi:10.1215/S0012-7094-04-12915-X] 9

[65] ENDRE SZEMERÉDI: On sets of integers containing no k elements in arithmetic progression. *Acta Arithmetica*, 27(1):199–245, 1975. Available at PLDML. 19, 25

[66] ENDRE SZEMERÉDI: Integer sets containing no arithmetic progressions. *Acta Math. Hung.*, 56(1):155–158, 1990. [doi:10.1007/BF01903717] 20

[67] TERENCE TAO AND VAN H. VU: *Additive Combinatorics*. Volume 13. Cambridge Univ. Press, 2006. 2

[68] LUCA TREVISAN: Additive combinatorics and theoretical computer science. *ACM SIGACT News*, 40(2):50–66, 2009. [doi:10.1145/1556154.1556170] 2

[69] EMANUELE VIOLA: *Selected Results in Additive Combinatorics: An Exposition*. Number 3 in Graduate Surveys. Theory of Computing Library, 2011. [doi:10.4086/toc.gs.2011.003] 2, 9, 15

[70] BARTEL LEENDERT VAN DER WAERDEN: Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wisk.*, 15:212–216, 1927. 19

AUTHOR

Shachar Lovett
assistant professor
University of California, San Diego
slovett@cse.ucsd.edu
http://cseweb.ucsd.edu/~slovett

ABOUT THE AUTHOR

SHACHAR LOVETT graduated from the Weizmann Institute of Science in 2010; his advisors were Omer Reingold and Ran Raz. He was a member of the the Institute for Advanced Study, School of Mathematics, between 2010-2012. Since then, he has been a faculty member at the University of California, San Diego. He is interested in the role that structure and randomness play in computation and mathematics, and in particular in computational complexity, coding theory, pseudo-randomness and algebraic constructions.