THEORY OF COMPUTING LIBRARY
GRADUATE SURVEYS 6 (2015), pp. 1–14
www.theoryofcomputing.org

An Exposition of Sanders' Quasi-Polynomial Freiman-Ruzsa Theorem

Shachar Lovett*

Received August 1, 2013; Published July 29, 2015

Abstract: The polynomial Freiman-Ruzsa conjecture is one of the most important conjectures in additive combinatorics. It asserts that one can switch between combinatorial and algebraic notions of approximate subgroups with only a polynomial loss in the underlying parameters. This conjecture has also found several applications in theoretical computer science. Recently, Tom Sanders proved a weaker version of the conjecture, with a quasi-polynomial loss in parameters. The aim of this note is to make his proof accessible to the theoretical computer science community, and in particular to readers who are less familiar with additive combinatorics.

ACM Classification: G.2.1

AMS Classification: 05E40

Key words and phrases: additive combinatorics, Fourier analysis

1 Introduction

Let A be a finite subset of an abelian group G. Its sumset $A+A$ is defined as $A+A = \{a_1+a_2 : a_1, a_2 \in A\}$. It is straightforward to see that $|A+A| = |A|$ if and only if A is a subgroup of G, or a coset of a subgroup. Thus, one may think of subsets A for which $|A+A| \approx |A|$ as an approximate version of a subgroup. To make this precise, if $|A+A| \le K|A|$ we say that A has *doubling* K and study the structure of sets of small doubling. For the sake of simplicity of exposition, we focus in this note on the group $G = \mathbb{F}_2^n$. However, we note that many of the results discussed here can be extended to vector spaces over larger fields, general abelian groups, and sometimes even to non-abelian groups.

*Supported by NSF CAREER award 1350481.

 DOI: 10.4086/toc.gs.2015.006

Ruzsa [19], following previous work of Freiman [9] who studied similar problems over the integers, showed that sets of small doubling must be contained in subspaces of small dimension. These bounds were later improved in a series of works [11, 21, 12, 13, 8]. In the following we denote by $\mathrm{Span}(A)$ the linear subspace spanned by A.

Theorem 1.1 (Freiman-Ruzsa Theorem in $\mathbb{F}_2^n$)**.** *Let $A \subseteq \mathbb{F}_2^n$ be a set such that $|A+A| \le K|A|$. Then $|\mathrm{Span}(A)| \le O(2^{2K}/K) \cdot |A|$.*

This bound is sharp, as can be seen from the following example. Let $A = \mathbb{F}_2^m \times \{e_1, \dots, e_n\} \subset \mathbb{F}_2^{m+n}$. Then

$$|A| = 2^m n, \qquad K = \frac{|A+A|}{|A|} = \frac{1}{n}\left(\binom{n}{2}+1\right) \approx \frac{n}{2} \quad \text{and} \quad |\mathrm{Span}(A)| = 2^{n+m} \approx \left(\frac{2^{2K}}{K}\right)|A|.$$

This shows that the ratio between $|\mathrm{Span}(A)|$ and $|A|$ must depend exponentially on the doubling of A. However, the above example suggests that maybe a refined question, relating the ratio between the span and the size of large subsets of A, might have better dependence on the doubling of A. This is captured by the Polynomial Freiman-Ruzsa conjecture (PFR).

Conjecture 1.2 (Polynomial Freiman-Ruzsa conjecture in $\mathbb{F}_2^n$)**.** *Let $A \subset \mathbb{F}_2^n$ be a set such that $|A+A| \le K|A|$. Then there exists a subset $A' \subset A$ of size $|A'| \ge K^{-c}|A|$ such that $|\mathrm{Span}(A')| \le K^c|A|$, where $c > 0$ is an absolute constant.*

The PFR conjecture plays a central role in additive combinatorics. The main reason is that it allows one to switch between a combinatorial notion of approximate vector space (that of having small doubling) and an algebraic notion (that of having small linear span) with only a polynomial loss in the parameters. It has many equivalent formulations, we refer the interested reader to a survey of Green [10] which lists many of them. Also, Green and Tao [12] and independently the author [14] showed the PFR conjecture is equivalent to a polynomial bound for the inverse Gowers U^3-norm.

The PFR conjecture has already found several diverse applications in computer science as well:

1. Samorodnitsky [20] gave an analysis of linearity testing for maps $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$. If one assumes the PFR conjecture, his result improves to only suffer a polynomial loss in the parameters.

2. Ben-Sasson and Zewi [18] used the PFR conjecture to construct two-source extractors from affine extractors.

3. Ben-Sasson, Zewi and the author [3] used it to get the first sublinear bounds on the deterministic communication complexity of functions in terms of the rank of their associated matrix.

4. Bhowmick, Dvir and the author [4] used it to give super-polynomial lower bounds on the block size of locally decodable codes arising from matching vector families.

5. Aggarwal, Dodis and the author [1] used it to construct non-malleable codes in the split state model, with polynomial size block length. In fact, they use Sanders' theorem (Theorem 1.3) to obtain an unconditional result.

The aim of this note is to give a detailed exposition of the following breakthrough result of Sanders [22], who proved a weaker version of the Freiman-Ruzsa conjecture with a quasi-polynomial loss in parameters. As noted before, his result extends to more general abelian groups, but we focus on $\mathbb{F}_2^n$ for simplicity of exposition.

Theorem 1.3 (Quasi-polynomial Freiman-Ruzsa theorem [22])**.** *Let $A \subset \mathbb{F}_2^n$ be a set such that $|A+A| \le K|A|$. Then there exists a subset $A' \subseteq A$ of size $|A'| \ge K^{-O(\log^3 K)}|A|$ such that $|\operatorname{Span}(A')| \le |A|$.*

In terms of its impact on applications, Theorem 1.3 implies a quasi-polynomial loss of parameters in Samorodnitsky's result [20] which implies similar bounds for the Gowers U^3 norm. However, currently it seems to be insufficient for the other applications discussed above [18, 3, 4], mainly because they require structural result for very large doubling constants. As mentioned, the result of Aggarwal et al. [1] already uses Sanders' theorem.

Returning to Sanders' result, he in fact proved an even stronger result. For $t \ge 1$ let

$$tA = \{a_1 + \cdots + a_t : a_1, \ldots, a_t \in A\}$$

denote the t-sumset of A.

Theorem 1.4 (Quasi-polynomial Bogolyubov-Ruzsa theorem [22])**.** *Let $A \subset \mathbb{F}_2^n$ be a set such that $|A+A| \le K|A|$. Then there exists a linear subspace $V \subset 4A$ such that $|V| \ge K^{-O(\log^3 K)}|A|$.*

As we show below, the deduction of Theorem 1.3 from Theorem 1.4 is standard given some basic tools and results in additive combinatorics. Given Theorem 1.4, one may conjecture a polynomial version of it, which would in particular imply in a similar way the polynomial Freiman-Ruzsa conjecture.

Conjecture 1.5 (Polynomial Bogolyubov-Ruzsa conjecture)**.** *Let $A \subset \mathbb{F}_2^n$ be a set such that $|A+A| \le K|A|$. Then there exists a linear subspace $V \subset tA$ such that $|V| \ge K^{-c}|A|$, where $t \ge 1, c > 0$ are absolute constants.*

We note that it is not clear whether Conjecture 1.5 is indeed strictly stronger than Conjecture 1.2, or whether one can deduce it assuming Conjecture 1.2.

General abelian groups. We now discuss briefly the how the polynomial Freiman-Ruzsa conjecture (Conjecture 1.2) and Sanders' result (specifically, Theorem 1.4) can be extended to general abelian groups.

Extending the polynomial Freiman-Ruzsa conjecture to groups of the form $G = \mathbb{F}_p^n$ for fixed p is straightforward. However, for groups of high (or infinite) torsion, stating the conjecture becomes more technical. This is because there is another type of structure which implies low doubling: integer points in a low-dimensional convex body. To be specific, if $B \subset \mathbb{R}^d$ is a centrally symmetric convex body, then the set $B \cap \mathbb{Z}^d$ has doubling bounded by an exponential in d. Hence, in general groups, one must account for both types of structure which imply low doubling—subgroups and integer points in convex bodies.

Conjecture 1.6 (Polynomial Freiman-Ruzsa conjecture, general abelian groups)**.** *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* $d \leq c \cdot \log K$*, whose integer points are* $B \cap \mathbb{Z}^d$*; and*

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:*

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

where $c > 0$ *is an absolute constant.*

To extend Sanders' result to a general abelian group G, we need to define the notion of a generalized arithmetic progression (GAP). A d-dimensional GAP is a set $P \subset G$ of the form

$$P = \left\{ g_0 + \sum_{i=1}^{d} x_i g_i : 1 \leq x_i \leq a_i \right\},$$

with $g_0, g_1, \ldots, g_d \in G$ and $a_i \in \mathbb{N}$. It is said to be proper if $|P| = \prod_{i=1}^{d} a_i$, that is all the elements are distinct.

Theorem 1.7 (Quasi-polynomial Bogolyubov-Ruzsa theorem, general abelian groups [22])**.** *Let* G *be an abelian group,* $A \subset G$ *a set such that* $|A + A| \leq K|A|$*. Then there exists a subgroup* $H < G$ *and a* $d(K)$*-dimensional proper generalized arithmetic progression* P*, such that* $|P + H| \geq \exp(-h(K))|A|$ *and*

$$P + H \subset 4A.$$

One can take $d(K) = O(\log^6 K)$ *and* $h(K) = O(\log^6 K \cdot \log\log K)$*.*

Further reading. This exposition is focused on the proof of Sanders' theorem. For readers who are interested in more aspects of additive combinatorics, and in particular applications in theoretical computer science, there are other surveys and books which may be of interest. These include the book "Additive Combinatorics" by Tao and Vu [23]; a mini-course on additive combinatorics by Barak et al. [2]; a survey covering selected results in additive combinatorics by Viola [25]; a survey on additive combinatorics and theoretical computer science by Trevisan [24]; a survey with a focus on applications in cryptography by Bibak [5]; and a survey on additive combinatorics and its applications in computer science by the author [15].

1.1 Proof overview

We first show, using standard techniques in additive combinatorics, that

1. Theorem 1.3 follows from Theorem 1.4, and

2. it suffices to prove Theorem 1.4 for "large sets" $A \subset \mathbb{F}_2^n$ for which $|A| \geq K^{-1} \cdot 2^n$.

Explicitly, these reductions use a theorem of Ruzsa which bounds the size of $|tA|$ for sets of small doubling, and the notion of a Freiman homomorphism.

We can thus assume from that point on the stronger condition $|A| \geq K^{-1} \cdot 2^n$, where our goal is to find a large subspace in $4A$. We first show that there exists a large set $X \subset \mathbb{F}_2^n$ such that $tX \subset 4A$ for $t = O(\log K)$. In fact, we will show a stronger property. For any $x_1, \ldots, x_t \in X$,

$$\Pr_{a_1,a_2 \in A}[a_1 + a_2 + x_1 + \cdots + x_t \in 2A] \geq 0.9\,. \tag{1.1}$$

This utilizes an argument of Croot and Sisask [7]. The set X allows us to find a large vector space V such that $V \subset 4A$, by choosing V to be the subspace orthogonal to the large Fourier coefficients of X. The proof of this is achieved by applying (1.1) to randomly chosen $x_1, \ldots, x_t \in X$ and appealing to standard Fourier arguments and Chang's lemma.

Paper organization. We give some preliminaries in Section 2. We establish the two reductions in Section 3. We prove the existence of the set X in Section 4. We conclude with the Fourier argument in Section 5.

2 Preliminaries

Norms. Let $f : \mathbb{F}_2^n \to \mathbb{R}$ be a function. For $1 \leq p \leq \infty$, its ℓ_p norm is defined as

$$\|f\|_p = \left(\mathbb{E}_{x \in \mathbb{F}_2^n}[|f(x)|^p]\right)^{1/p}.$$

Let $f, g : \mathbb{F}_2^n \to \mathbb{R}$ be functions. Their inner product is defined as

$$\langle f, g \rangle = \mathbb{E}_{x \in \mathbb{F}_2^n}[f(x)g(x)]\,.$$

For $1 \leq p, q \leq \infty$ such that $1/p + 1/q = 1$, the Hölder inequality states that $|\langle f, g \rangle| \leq \|f\|_p \|g\|_q$.

Fourier analysis. Let $f : \mathbb{F}_2^n \to \mathbb{R}$ be a function. Its Fourier coefficients are

$$\widehat{f}(\alpha) = \mathbb{E}_{x \in \mathbb{F}_2^n}\left[f(x)(-1)^{\langle x, \alpha \rangle}\right]$$

where $\alpha \in \mathbb{F}_2^n$. A function is determined by its Fourier coefficients by the inversion formula,

$$f(x) = \sum_{\alpha \in \mathbb{F}_2^n} f(x)(-1)^{\langle x, \alpha \rangle}\,.$$

Parseval's identity asserts that $\|f\|_2^2 = \sum_{\alpha \in \mathbb{F}_2^n} \widehat{f}(\alpha)^2$. For functions $f, g : \mathbb{F}_2^n \to \mathbb{R}$ their inner product is

$$\langle f, g \rangle = \mathbb{E}_{x \in \mathbb{F}_2^n}[f(x)g(x)]$$

and their convolution $f * g : \mathbb{F}_2^n \to \mathbb{R}$ is defined as

$$(f * g)(x) = \mathbb{E}_{y \in \mathbb{F}_2^n}[f(y)g(x+y)]\,.$$

Note that in $\mathbb{F}_2^n$ addition and subtraction are the same. The Fourier coefficients of the convolution obey

$$\widehat{f * g}(\alpha) = \widehat{f}(\alpha)\widehat{g}(\alpha)\,.$$

3 Reductions

We show in this section that

1. Theorem 1.3 follows from Theorem 1.4, and

2. it suffices to prove Theorem 1.4 for "large sets" $A \subset \mathbb{F}_2^n$ for which $|A| \geq K^{-1} \cdot 2^n$.

Note that the condition $|A| \geq K^{-1} \cdot 2^n$ is stronger than the assumption of small doubling, as any such set A satisfies $|A+A| \leq 2^n \leq K|A|$.

3.1 Reduction 1: Theorem 1.3 follows from Theorem 1.4

We first show how Theorem 1.3 follows from Theorem 1.4. This requires the following theorem of Plünnecke [17] and Ruzsa [19], stating that if A has small doubling then tA cannot be too large.

Theorem 3.1 ([17, 19]). *Let $A \subset \mathbb{F}_2^n$ be a set such that $|A+A| \leq K|A|$. Then for any $t \geq 1$ we have that $|tA| \leq K^t|A|$.*

Let $A \subset \mathbb{F}_2^n$ be a set such that $|A+A| \leq K|A|$. Theorem 1.4 asserts that there exists a linear subspace $V \subset 4A$ of size $|V| \geq \delta|A|$ where $\delta = K^{-O(\log^3 K)}$. Let $S \subset A$ be maximal such that the elements of S fall in different cosets of V; that is, $s+s' \notin V$ for all distinct $s, s' \in S$. Note that $|S| \leq K^5/\delta$, as

$$|S||V| = |S+V| = |A+V| \leq |A+4A| = |5A| \leq K^5|A|,$$

where the last inequality follows from Theorem 3.1. Let $A' = A \cap (V+s)$ where $s \in S$ is chosen to maximize $|A'|$. We have that $|A'| \geq |A|/|S| = K^{-O(\log^3 K)}|A|$, and that

$$|\operatorname{Span}(A')| \leq |\operatorname{Span}(V+s)| \leq 2|V| \leq 2K^5|A'|.$$

3.2 Reduction 2: It is sufficient to prove Theorem 1.4 for large sets

We next show it suffices to prove Theorem 1.4 for large sets. This requires the notion of a *Freiman homomorphism*. Let $A \subset \mathbb{F}_2^n$. A linear map $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is said to be a Freiman homomorphism of A of order t if ϕ is injective on tA. That is, for any $a_1, \dots, a_t, b_1, \dots, b_t \in A$,

$$\phi(a_1) + \cdots + \phi(a_t) = \phi(b_1) + \cdots + \phi(b_t) \quad \Rightarrow \quad a_1 + \cdots + a_t = b_1 + \cdots + b_t.$$

We note that the standard definition of Freiman homomorphisms do not require the map to be linear, but here we restrict our attention to linear Freiman homomorphism. The following claim is very useful.

Claim 3.2 ([9]). *Let $A \subset \mathbb{F}_2^n$. Fix $t \geq 1$, and let $m = m(t)$ be minimal such that a linear Freiman homomorphism $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^m$ of A of order t exists. Then $\phi(2tA) = \mathbb{F}_2^m$.*

Proof. First note that since for $m = n$ the identity map is a linear Freiman homomorphism of all orders, m is well-defined. Assume to the contrary of the claim that $\phi(2tA) \subsetneq \mathbb{F}_2^m$, and let x be an element in $\mathbb{F}_2^m \setminus \phi(2tA)$. Let $\psi : \mathbb{F}_2^m \to \mathbb{F}_2^{m-1}$ be a surjective linear map which sends x to zero, and define $\phi' = \psi \circ \phi$. We claim that ϕ' is also a linear Freiman homomorphism of A of order t, which contradicts the minimality of m. To establish the claim, we need to show that ϕ' is injective on tA. If this is not the case, then there exist distinct $a, b \in tA$ such that $\phi'(a) = \phi'(b)$, that is $\psi(\phi(a)) = \psi(\phi(b))$. Now, by definition of ψ this can only occur if $\phi(a) = \phi(b)$ or $\phi(a) = \phi(b) + x$. The first case is ruled out since we assumed ϕ is injective on tA, hence by the linearity of ϕ we have that $x = \phi(a+b) \in \phi(2tA)$, violating our initial assumption. $\square$

We now show it suffices to prove Theorem 1.4 for large sets. We will assume throughout that $0 \in A$, which can be assumed without loss of generality by replacing A with $A + a$ for some $a \in A$. Let $A \subseteq \mathbb{F}_2^n$ be such that $|A + A| \leq K|A|$. Let $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a minimal linear Freiman homomorphism of A of order 12 and define $A' = \phi(A)$. We note that by the assumption that $0 \in A$, we have that ϕ is injective on tA for all $t \leq 12$.

We first note that A' also has doubling K, since $|A'| = |A|$ and $|A' + A'| = |A + A|$ because by assumption ϕ is injective on both A and $2A$. This implies that A' is large in $\mathbb{F}_2^m$ since

$$|\mathbb{F}_2^m| = |24A'| \leq K^{24}|A'|\,,$$

where the equality follows from Claim 3.2 and the inequality from Theorem 3.1. We can thus apply to A' the assumed Theorem 1.4. The theorem asserts the existence of a linear subspace $V' \subset 4A'$ of size $V' \geq \delta|A'|$ where $\delta = \exp(-O(\log^4(K^{24})))$. Since ϕ is injective on $12A$ we can define a local inverse $\phi^{-1} : 12A' \to 12A$. In particular, set $V = \phi^{-1}(V') \subset 4A$. We will show that V is also a linear subspace, thus establishing the theorem for A.

We will use the fact that the property of being a linear subspace can be verified by local tests. Specifically, we need to show that for any $x, y \in V$ we have that $x + y \in V$. Let $x' = \phi(x), y' = \phi(y)$. Then $x', y' \in V'$ and hence $z' = x' + y' \in V'$ since V' is a linear subspace. Let $z = \phi^{-1}(z') \in V$. We need to show that $x + y = z$. Note that $x + y + z \in 12A$ since $x, y, z \in V \subset 4A$. However, $\phi(x + y + z) = x' + y' + z' = 0$ and since ϕ is injective on $12A$ and since $0 \in 12A$ is mapped by ϕ to zero, we must have that $x + y + z = 0$.

4 Existence of a large near-invariant set

We establish the following lemma in this section.

Lemma 4.1. *Let $A \subset \mathbb{F}_2^n$ be such that $|A| \geq K^{-1} \cdot 2^n$. Set $t = O(\log K)$. Then there exists $X \subset \mathbb{F}_2^n$ of size $|X| \geq K^{-O(\log^3(K))} \cdot 2^n$ such that for any $x_1, \ldots, x_t \in X$,*

$$\Pr_{a_1, a_2 \in A}[a_1 + a_2 + x_1 + \cdots + x_t \in 2A] \geq 0.9\,.$$

The lemma can be interpreted as follows: it is clear that $\Pr_{a_1, a_2 \in A}[a_1 + a_2 \in 2A] = 1$. The lemma shows that this is approximately true for many shifts of $2A$ as well; and furthermore, that these shifts are iterated sums of a large sets.

We first fix some notations. For a set $A \subset \mathbb{F}_2^n$ let $\mathbf{1}_A : \mathbb{F}_2^n \to \{0,1\}$ denote the indicator function for A, and $\varphi_A(x) = (2^n/|A|)\mathbf{1}_A(x)$ denote the normalized indicator for which $\mathbb{E}_{x\in\mathbb{F}_2^n}[\varphi_A(x)] = 1$. Note that $(\varphi_A * f)(x) = \mathbb{E}_{a\in A}[f(x+a)]$ is a "smoothing" of the function f by averaging over random shifts chosen from a set A. For an element $x \in X$ we shorthand $\varphi_x = \varphi_{\{x\}}$ and note that $(\varphi_x * f)(y) = f(x+y)$ is a shift of f by x. In these notations, for any $x \in \mathbb{F}_2^n$ we have that

$$\Pr_{a_1,a_2\in A}[a_1+a_2+x \in 2A] = \langle \varphi_x * \varphi_A * \varphi_A, \mathbf{1}_{2A}\rangle = \langle \varphi_x * \varphi_A * \mathbf{1}_{2A}, \varphi_A\rangle \,. \tag{4.1}$$

Note that for $x = 0$,

$$\langle \varphi_A * \mathbf{1}_{2A}, \varphi_A\rangle = \Pr_{a_1,a_2\in A}[a_1+a_2 \in 2A] = 1\,. \tag{4.2}$$

We will show that there exists a large set $X \subset \mathbb{F}_2^n$ so that for all $x \in tX$, $\varphi_x * \varphi_A * \mathbf{1}_{2A} \approx \varphi_A * \mathbf{1}_{2A}$. In particular, this shows that (4.1) $\approx$ (4.2) and implies Lemma 4.1. In order to do so, we will use the following lemma of Croot and Sisask [7] which we reprove below. The lemma shows that if we take a bounded function f and smooth it by a random shift from a large set A, then the resulting function will be nearly invariant to many shifts.

Lemma 4.2. *Let $A \subset \mathbb{F}_2^n$ be a set such that $|A| \ge K^{-1}\cdot 2^n$. Let $f : \mathbb{F}_2^n \to [0,1]$ be a function. Let $p \ge 1$ and $\varepsilon > 0$ be parameters. Then there exists a set $X \subset \mathbb{F}_2^n$ of size $|X| \ge K^{-O(p/\varepsilon^2)}\cdot 2^n$ such that for any $x \in X$,*

$$\|\varphi_x * \varphi_A * f - \varphi_A * f\|_p \le \varepsilon\,.$$

We first show how Lemma 4.1 follows from Lemma 4.2. Set

$$f = \mathbf{1}_{2A}, \quad p = \log K, \quad t = O(\log K), \quad \varepsilon = 1/(20t) = \Omega(1/\log K)$$

in Lemma 4.2 so that $|X| \ge K^{-O(\log^3(K))}\cdot 2^n$ as claimed. We first claim that for any $x \in tX$ we have that

$$\|\varphi_x * \varphi_A * \mathbf{1}_{2A} - \varphi_A * \mathbf{1}_{2A}\|_p \le t\varepsilon\,. \tag{4.3}$$

In order to establish (4.3) let $x = x_1 + \cdots + x_t$ where $x_1,\dots,x_t \in X$ and expand it as a telescopic sum. Then

$$\begin{aligned}\|\varphi_{x_1+\cdots+x_t} * \varphi_A * \mathbf{1}_{2A} - \varphi_A * \mathbf{1}_{2A}\|_p &\le \sum_{i=1}^{t} \|\varphi_{x_1+\cdots+x_i} * \varphi_A * \mathbf{1}_{2A} - \varphi_{x_1+\cdots+x_{i-1}} * \varphi_A * \mathbf{1}_{2A}\|_p \\ &= \sum_{i=1}^{t} \|\varphi_{x_i} * \varphi_A * \mathbf{1}_{2A} - \varphi_A * \mathbf{1}_{2A}\|_p \le t\varepsilon\,,\end{aligned}$$

where we used the fact that the ℓ_p norm is invariant under shifts, that is $\|\varphi_x * g\|_p = \|g\|_p$ for all elements $x \in \mathbb{F}_2^n$ and functions $g : \mathbb{F}_2^n \to \mathbb{R}$. By our setting of $\varepsilon = 1/(20t)$, we have that for all $x \in tX$

$$\|\varphi_x * \varphi_A * \mathbf{1}_{2A} - \varphi_A * \mathbf{1}_{2A}\|_p \le t\varepsilon \le 1/20\,. \tag{4.4}$$

We next apply the Hölder inequality. We have that

$$|\langle \varphi_x * \varphi_A * \mathbf{1}_{2A} - \varphi_A * \mathbf{1}_{2A}, \varphi_A\rangle| \le \|\varphi_x * \varphi_A * \mathbf{1}_{2A} - \varphi_A * \mathbf{1}_{2A}\|_p \|\varphi_A\|_q \tag{4.5}$$

where $q = p/(p-1)$ is the dual of p. By the choice of $p = \log K$ we have that

$$\|\varphi_A\|_q = (2^n/|A|)^{1-1/q} \le K^{1/(\log K - 1)} \le 2\,. \tag{4.6}$$

Combining (4.1), (4.2), (4.5) and (4.6) we conclude that for any $x \in tX$,

$$\begin{aligned}\Pr_{a_1,a_2 \in A}[a_1 + a_2 + x \in 2A] &= \langle \varphi_x * \varphi_A * \mathbf{1}_{2A}, \varphi_A \rangle \\ &= 1 - \langle \varphi_A * \mathbf{1}_{2A} - \varphi_x * \varphi_A * \mathbf{1}_{2A}, \varphi_A \rangle \ge 0.9 \end{aligned} \tag{4.7}$$

which concludes the proof of Lemma 4.1. We now move to prove Lemma 4.2. The proof will use the Marcinkiewicz–Zygmund inequality [16], which is a generalization of the classical Khintchine inequality.

Theorem 4.3 (Marcinkiewicz–Zygmund inequality)**.** *For any $p \ge 1$, let $X_1, \ldots, X_\ell$ be independent, mean zero random variables with $\mathbb{E}|X_i|^p < \infty$. Then*

$$\mathbb{E}\left[|X_1 + \cdots + X_\ell|^p\right] \le (Cp)^{p/2} \cdot \mathbb{E}\left[\left(|X_1|^2 + \cdots + |X_\ell|^2\right)^{p/2}\right],$$

where $C > 0$ is an absolute constant.

We will actually only need the following corollary for bounded random variables.

Corollary 4.4. *Let $X_1, \ldots, X_\ell$ be independent, mean zero random variables with $|X_i| \le 1$. Then for any $p \ge 1$,*

$$\mathbb{E}\left[\left|\frac{1}{\ell}(X_1 + \cdots + X_\ell)\right|^p\right] \le (Cp/\ell)^{p/2}.$$

We now turn to prove Lemma 4.2.

Proof of Lemma 4.2. Let $A \subset \mathbb{F}_2^n$ be a set of size $|A| \ge K^{-1} \cdot 2^n$ and let $f : \mathbb{F}_2^n \to [0,1]$ be a function. For ℓ to be determined later, let $a_1, \ldots, a_\ell$ be uniformly and independently chosen elements from A. We first claim if ℓ is chosen large enough, then $\varphi_A * f$ can be approximated by

$$\frac{1}{\ell}\sum_{i=1}^{\ell} \varphi_{a_i} * f\,.$$

That is, we approximate the "smoothing" of f with random shifts chosen from the set A, with a new average which is only over the shifts from the empirical sample $a_1, \ldots, a_\ell$. Explicitly, we will show that for $\ell = O(p/\varepsilon^2)$ we have that

$$\Pr_{a_1,\ldots,a_\ell \in A}\left[\left\|\varphi_A * f - \frac{1}{\ell}\sum_{i=1}^{\ell} \varphi_{a_i} * f\right\|_p \le \varepsilon/2\right] \ge 1/2\,. \tag{4.8}$$

In order to show (4.8), we will establish that

$$\mathbb{E}_{a_1,\ldots,a_\ell \in A}\left[\left\|\varphi_A * f - \frac{1}{\ell}\sum_{i=1}^{\ell} \varphi_{a_i} * f\right\|_p^p\right] \le (Cp/\ell)^{p/2}, \tag{4.9}$$

where $C > 0$ is an absolute constant, and then apply Markov's inequality. Now, (4.9) follows from Corollary 4.4. Define $X_i = \varphi_A * f - \varphi_{a_i} * f$ so that $X_i(x) = \mathbb{E}_{a\in A}[f(x+a)] - f(x+a_i)$. Then

$$\left\|\varphi_A * f - \frac{1}{\ell}\sum_{i=1}^{\ell}\varphi_{a_i} * f\right\|_p^p = \mathbb{E}_{x\in\mathbb{F}_2^n}\left[\left|\frac{1}{\ell}(X_1(x)+\cdots+X_\ell(x))\right|^p\right],$$

and the claim follows by averaging over $a_1,\ldots,a_\ell$ and applying Corollary 4.4.

Let $S(A) \subset (\mathbb{F}_2^n)^\ell$ denote the set of $(a_1,\ldots,a_\ell)$ for which

$$\left\|\varphi_A * f - \frac{1}{\ell}\sum_{i=1}^{\ell}\varphi_{a_i} * f\right\|_p \le \varepsilon/2\,.$$

We have just shown that by our choice of ℓ, at least half the sequences $(\alpha_1,\ldots,\alpha_\ell)\in A^\ell$ have this property. Hence

$$|S(A)| \ge 0.5|A|^\ell \ge 0.5K^{-\ell}\cdot 2^{n\ell}\,. \tag{4.10}$$

Applying the same argument to any shift $A+x$ of A we deduce that $|S(A+x)| \ge 0.5K^{-\ell}\cdot 2^{n\ell}$ as well (alternatively, this can be deduced from the fact that $S(A+x) = \{(a_1+x,\ldots,a_\ell+x) : (a_1,\ldots,a_\ell)\in A\}$). Hence, by an averaging argument there must exist a subset $X' \subset \mathbb{F}_2^n$ of size $|X'| \ge 0.5K^{-\ell}\cdot 2^n$ and a sequence $(a_1,\ldots,a_\ell)\in(\mathbb{F}_2^n)^\ell$ such that $(a_1,\ldots,a_\ell)\in S(A+x)$ for all $x\in X'$. But then we get that for all $x',x''\in X'$ we have that

$$\left\|\varphi_{A+x'} * f - \varphi_{A+x''} * f\right\|_p \le \left\|\varphi_{A+x'} * f - \frac{1}{\ell}\sum_{i=1}^{\ell}\varphi_{a_i} * f\right\|_p + \left\|\varphi_{A+x''} * f - \frac{1}{\ell}\sum_{i=1}^{\ell}\varphi_{a_i} * f\right\|_p \le \varepsilon\,.$$

Let $x'\in X'$ be arbitrary and set $X = X'+x'$. We conclude that for any $x\in X$,

$$\left\|\varphi_{A+x} * f - \varphi_A * f\right\|_p = \left\|\varphi_{A+x+x'} * f - \varphi_{A+x'} * f\right\|_p \le \varepsilon\,. \qquad \square$$

5 A Fourier-analytic argument

Let $A\subset\mathbb{F}_2^n$ be a set such that $|A|\ge K^{-1}\cdot 2^n$. We showed in Lemma 4.1 that there exists a set $X\subset\mathbb{F}_2^n$ of size $|X|\ge K^{-O(\log^3 K)}\cdot 2^n$ such that for any $x\in tX$, where $t = O(\log K)$, we have that

$$\Pr_{a_1,a_2\in A}[a_1+a_2+x\in 2A] \ge 0.9\,. \tag{5.1}$$

We now show that the linear subspace $V\subset\mathbb{F}_2^n$ which is orthogonal to the large Fourier coefficients of X is contained in $4A$. In order to show that, we apply (5.1) for $x = x_1+\cdots+x_t$ where $x_1,\ldots,x_t\in X$ are chosen uniformly, and deduce that

$$\Pr_{\substack{a_1,a_2\in A,\\ x_1,\ldots,x_t\in X}}[a_1+a_2+x_1+\cdots+x_t\in 2A] \ge 0.9\,. \tag{5.2}$$

For a set $X \subset \mathbb{F}_2^n$ we adopt the shorthand $\widehat{X}(\alpha)$ to stand for the Fourier coefficients of φ_X,

$$\widehat{X}(\alpha) = \widehat{\varphi_X}(\alpha) = \mathbb{E}_{x\in X}[(-1)^{\langle \alpha,x\rangle}] .$$

Note that $\widehat{X}(0) = 1$. The spectrum of a set X is the set of its large Fourier coefficients. Explicitly, its γ-spectrum for $0 < \gamma < 1$ is defined as

$$\mathrm{Spec}_\gamma(X) = \{\alpha \in \mathbb{F}_2^n : |\widehat{X}(\alpha)| \geq \gamma\}.$$

Parseval's identity allows one to bound

$$|\,\mathrm{Spec}_\gamma(X)| \leq \frac{2^n}{|X|}\cdot(1/\gamma)^2 \quad \text{which implies} \quad \dim(\mathrm{Spec}_\gamma(X)) \leq \frac{2^n}{|X|}\cdot(1/\gamma)^2 .$$

A better bound on the dimension of $\mathrm{Spec}_\gamma(X)$ is given by Chang's theorem [6].

Theorem 5.1 (Chang [6])**.** *Let $X \subseteq \mathbb{F}_2^n$. Then*

$$\dim(\mathrm{Spec}_\gamma(X)) \leq 8\log(2^n/|X|)\cdot(1/\gamma)^2 .$$

Define the vector space $V \subseteq \mathbb{F}_2^n$ as the orthogonal space to $\mathrm{Spec}_{1/2}(X)$.

$$V = \mathrm{Spec}_{1/2}(X)^\perp = \{v \in \mathbb{F}_2^n : \langle v,\alpha\rangle = 0\ \forall \alpha \in \mathrm{Spec}_{1/2}(X)\} .$$

Theorem 5.1 implies that $|V| \geq (|X|/2^n)^{32}\cdot 2^n = K^{-O(\log^3 K)}\cdot 2^n$. We next show that $V \subset 4A$. We will do so by showing that

$$\Pr[a_1+a_2+x_1+\cdots+x_t+v \in 2A] \approx \Pr[a_1+a_2+x_1+\cdots+x_t \in 2A] \geq 0.9 ,$$

where $a_1,a_2 \in A$, $x_1,\ldots,x_t \in X$ and $v \in V$ are chosen uniformly. This in particular implies that

$$\Pr[a_1+a_2+x_1+\cdots+x_t+v \in 2A] \geq 0.8 .$$

Hence, there exists a a fixed $b = a_1+a_2+x_1+\cdots+x_t$ such that $|V\cap(2A+b)| \geq 0.8|V|$. Consequently $V \subset 4A$ as every element $v \in V$ can be written in $|V|/2$ disjoint ways as $v = v_1+v_2$ where $v_1,v_2 \in V$, and at least for one of these it must hold that $v_1,v_2 \in 2A+b$ and hence $v = v_1+v_2 \in 4A$.

To conclude the proof, it remains to show that

$$|\Pr[a_1+a_2+x_1+\cdots+x_t+v \in 2A] - \Pr[a_1+a_2+x_1+\cdots+x_t \in 2A]| \leq 0.1 ,$$

where again $a_1,a_2 \in A$, $x_1,\ldots,x_t \in X$ and $v \in V$ are chosen uniformly. We now apply Fourier analysis. We can rewrite

$$\Pr_{\substack{a_1,a_2\in A,\\ x_1,\ldots,x_t\in X}}[a_1+a_2+x_1+\cdots+x_t \in 2A] = \sum_{\alpha\in\mathbb{F}_2^n} \widehat{A}(\alpha)^2\widehat{X}(\alpha)^t\,\widehat{1_{2A}}(\alpha) \tag{5.3}$$

and

$$\Pr_{\substack{a_1,a_2\in A,\\ x_1,\ldots,x_t\in X, v\in V}}[a_1+a_2+x_1+\cdots+x_t+v\in 2A]=\sum_{\alpha\in\mathbb{F}_2^n}\widehat{A}(\alpha)^2\widehat{X}(\alpha)^t\widehat{V}(\alpha)\widehat{1_{2A}}(\alpha)\,. \tag{5.4}$$

The Fourier coefficients of V are simple to describe since it is a linear subspace. We have that $\widehat{V}(\alpha)=1$ if $\alpha\in V^{\perp}$ and that $\widehat{V}(\alpha)=0$ otherwise. Thus

$$\begin{aligned}\Pr[a_1+a_2+x_1+\cdots+x_t\in 2A]-\Pr[a_1+a_2+x_1+\cdots+x_t+v\in 2A]\\ =\sum_{\alpha\notin V^{\perp}}\widehat{A}(\alpha)^2\widehat{X}(\alpha)^t\widehat{1_{2A}}(\alpha)\,.\end{aligned} \tag{5.5}$$

We now bound (5.5). By the definition of V, we have that if $\alpha\notin V^{\perp}$ then $\alpha\notin\mathrm{Spec}_{1/2}(X)$, and hence

$$|\widehat{X}(\alpha)|^t\le 2^{-t}\,.$$

Moreover, $|\widehat{1_{2A}}(\alpha)|\le 1$ and

$$\sum_{\alpha\notin V^{\perp}}\widehat{A}(\alpha)^2\le\sum_{\alpha\in\mathbb{F}_2^n}\widehat{A}(\alpha)^2=\mathbb{E}_{x\in\mathbb{F}_2^n}[\varphi_A(x)^2]=K\,.$$

Thus we conclude since

$$\big|\Pr[a_1+a_2+x_1+\cdots+x_t\in 2A]-\Pr[a_1+a_2+x_1+\cdots+x_t+v\in 2A]\big|\le 2^{-t}K\le 0.1$$

by choosing $t=\log(10K)$.

6 Acknowledgements

I thank Eli Ben-Sasson, Zeev Dvir, Hamed Hatami, Amir Shpilka, Avi Wigderson, Noga Zewi and David Zuckerman for the encouragement to write this exposition and for useful comments and suggestions on an earlier version of this note, and the anonymous reviewers for many helpful suggestions.

References

[1] DIVESH AGGARWAL, YEVGENIY DODIS, AND SHACHAR LOVETT: Non-malleable codes from additive combinatorics. In *Proc. 46th STOC*, pp. 774 – 783. ACM Press, 2014. Available at ACM DL. Preliminary version in ECCC. [doi:10.1145/2591796.2591804] 2, 3

[2] BOAZ BARAK, LUCA TREVISAN, AND AVI WIGDERSON: A mini-course on additive combinatorics, 2007. Available at Alan Frieze's webpage. 4

[3] ELI BEN-SASSON, SHACHAR LOVETT, AND NOGA RON-ZEWI: An additive combinatorics approach relating rank to communication complexity. *J. ACM*, 61(4):22, 2014. Preliminary version in FOCS'12. [doi:10.1145/2629598] 2, 3

[4] ABHISHEK BHOWMICK, ZEEV DVIR, AND SHACHAR LOVETT: New bounds for matching vector families. In *Proc. 45th STOC*, pp. 823–832. ACM Press, 2013. [doi:10.1145/2488608.2488713] 2, 3

[5] 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. Preliminary version in arXiv. [doi:10.1007/978-1-4614-6642-0_4] 4

[6] MEI-CHU CHANG: A polynomial bound in Freiman's theorem. *Duke Math. J.*, 113(3):399–419, 2002. Available at Project Euclid. 11

[7] ERNIE CROOT AND OLOF SISASK: A probabilistic technique for finding almost-periods of convolutions. *Geom. Funct. Anal.*, 20(6):1367–1396, 2010. [doi:10.1007/s00039-010-0101-8] 5, 8

[8] CHAIM EVEN-ZOHAR: On sums of generating sets in $\mathbb{Z}_2^n$. *Combin. Probab. Comput.*, 21(6):916–941, 2012. Preliminary version in CoRR. [doi:10.1017/S0963548312000351] 2

[9] GREGORY A. FREIMAN: *Foundations of a structural theory of set addition*. Volume 37 of *Translations of Mathematical Monographs*. Amer. Math. Soc., 1973. 2, 6

[10] BEN GREEN: The polynomial Freiman-Ruzsa conjecture, 2005. Available at Open Problems in Mathematics. 2

[11] BEN GREEN AND IMRE Z. RUZSA: Sets with small sumset and rectification. *Bull. Lond. Math. Soc.*, 38(1):43–52, 2006. Preliminary version in arXiv. 2

[12] 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] 2

[13] SERGEY V. KONYAGIN: On the Freiman theorem in finite fields. *Math. Notes*, 84(3-4):435–438, 2008. [doi:10.1134/S0001434608090137] 2

[14] SHACHAR LOVETT: Equivalence of polynomial conjectures in additive combinatorics. *Combinatorica*, 32(5):607–618, 2012. Preliminary version in ECCC. [doi:10.1007/s00493-012-2714-z] 2

[15] SHACHAR LOVETT: Additive combinatorics and its applications in theoretical computer science (draft). Available at author's website, 2013. 4

[16] JÓZEF MARCINKIEWICZ AND ANTONI ZYGMUND: Sur les fonctions indépendantes. *Func. Math.*, 29, 1937. Available from the Polish Virtual Library of Science. 9

[17] HELMUT PLÜNNECKE: *Eigenschaften und Abschätzungen von Wirkungsfunktionen*. Gesellschaft für Mathematik und Datenverarbeitung, 1969. 6

[18] NOGA RON-ZEWI AND ELI BEN-SASSON: From affine to two-source extractors via approximate duality. In *Proc. 43rd STOC*, pp. 177–186. ACM Press, 2011. Preliminary version in ECCC. [doi:10.1145/1993636.1993661] 2, 3

[19] IMRE Z. RUZSA: An analog of Freiman's theorem in groups. *Structure Theory of Set-Addition. Astérisque*, 258:323–326, 1999. 2, 6

[20] ALEX SAMORODNITSKY: Low-degree tests at large distances. In *Proc. 39th STOC*, pp. 506–515. ACM Press, 2007. Preliminary version in ECCC. [doi:10.1145/1250790.1250864] 2, 3

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

[22] TOM SANDERS: On the Bogolyubov-Ruzsa lemma. *Analysis & PDE*, 5(3):627–655, 2012. [doi:10.2140/apde.2012.5.627] 3, 4

[23] TERENCE TAO AND VAN H. VU: *Additive Combinatorics*. Cambridge Univ. Press, 2006. 4

[24] LUCA TREVISAN: Guest column: additive combinatorics and theoretical computer science. *ACM SIGACT News*, 40(2):50–66, 2009. [doi:10.1145/1556154.1556170] 4

[25] EMANUELE VIOLA: Selected results in additive combinatorics: An exposition. *Theory of Computing Library, Graduate Surveys*, 3:1–15, 2011. [doi:10.4086/toc.gs.2011.003] 4

AUTHOR

Shachar Lovett
assistant professor
University of California, San Diego
slovett@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 has a broad interest in theoretical computer science and mathematics. In particular, he is interested in computational complexity, randomness and pseudo-randomness, algebraic constructions, coding theory, discrete mathematics and additive combinatorics.