On the Structure of Sets with Few Three-Term Arithmetic Progressions

Ernie Croot *

Georgia Institute of Technology
School of Mathematics
103 Skiles
Atlanta, Ga 30332

ecroot@math.gatech.edu

Submitted: Jun 19, 2009; Accepted: Aug 17, 2010; Published: Sep 22, 2010
Mathematics Subject Classification: 11B25, 11B30 (primary), 11N30 (secondary)

Abstract

Fix a prime $p \geqslant 3$, and a real number $0 < \alpha \leqslant 1$. Let $S \subset \mathbb{F}_p^n$ be any set with the least number of solutions to $x + y = 2z$ (note that this means that x, z, y is an arithmetic progression), subject to the constraint that $|S| \geqslant \alpha p^n$. What can one say about the structure of such sets S? In this paper we show that they are "essentially" the union of a small number of cosets of some large-dimensional subspace of $\mathbb{F}_p^n$.

1 Introduction

Of central importance to the subject of additive combinatorics is that of determining when a subset of the integers $\{1, ..., N\}$ contains a k-term arithmetic progression. This subject has a long history (see [9, ch. 10-11]). In this paper we consider a specific problem in this area, posed by B. Green [1]. Before we state this problem, we require some notation:

Given a function $f : \mathbb{F}_p^n \to [0, 1]$, where $\mathbb{F}_p^n$ denotes the vector space of dimension n over $\mathbb{F}_p$, define

$$\mathbb{E}(f) \ = \ p^{-n} \sum_{m \in \mathbb{F}_p^n} f(m).$$

Define

$$\Lambda_3(f) \ = \ p^{-2n} \sum_{m,d} f(m) f(m+d) f(m+2d).$$

In the case where f is an indicator function for some set $S \subseteq \mathbb{F}_p^n$, we have that $\Lambda_3(f)$ is the normalized count of the number of three-term arithmetic progressions $m, m+d, m+2d \in S$.

*Supported by NSA grant and NSF grant DMS-1001111.

Note that $\Lambda_3(f) > 0$, unless $\mathbb{E}(f) = 0$, because of the contribution of trivial progressions where $d = 0$.

Green's problem is as follows:

Problem. Given $0 < \alpha \leqslant 1$, suppose $S \subseteq \mathbb{F}_p$ satisfies $|S| \geqslant \alpha p$, and has the least number of three-term arithmetic progressions. What is $\Lambda_3(S)$?

It seems that the only hope of answering a question like this is to understand the structure of these sets S, as Green and Sisask did in [5] for values of α near to 1.[1] In this paper we address the analogous problem in $\mathbb{F}_p^n$, where p is held fixed, and n tends to infinity. In some ways this context is simpler to work with than the $\mathbb{F}_p$ one, and it is now standard practice to first work out problems in $\mathbb{F}_p^n$. See Green [4] for a discussion of this philosophy.

The results we prove are not of a type that would allow us to deduce $\Lambda_3(S)$, but they do reveal that these sets S are very highly structured. With some work, such results can perhaps be deduced from the work of Green [3], which makes use of regularity lemma ideas (resulting in bounds that only work for densities $\alpha \gg 1/\log_*(n)$), but our theorems below are proved using basic harmonic analysis, and give bounds that hold for densities $\alpha \gg 1/\log n$ (see the remark after Theorem 1 and also Corollary 1).

We will first introduce a definition which will make the theorems below a little easier to state.

Definition. We say that a subset $S \subseteq \mathbb{F}_p^n$ is a *critical set* if $\Lambda_3(S)$ is minimal among all sets of size at least $|S|$; that is, if $|T| \geqslant |S|$, then $\Lambda_3(T) \geqslant \Lambda_3(S)$.

Also, we introduce here a certain function Δ which will make many of our main theorems below easier to state:

$$\Delta \;=\; \Delta(\epsilon, p) \;:=\; (\epsilon^5/2^{11}p^2)p^{-12/\epsilon}, \tag{1}$$

Theorem 1 *Fix a characteristic $p \geqslant 3$ prime. Suppose that $n > n_0(p)$, that S is a critical set of $\mathbb{F}_p^n$, and that $c_p/\log n \leqslant \epsilon \leqslant 1$ (where c_p depends only on p).*

Then, there exists a subspace

$$W \;\leqslant\; \mathbb{F}_p^n,\; \dim(W) \;\geqslant\; n - \Delta^{-2} \tag{2}$$

and a set A, such that

$$|S \;\Delta\; (A + W)| \;\leqslant\; 2\epsilon p^n.^2$$

[1] Actually, they considered the analogous problem of determining the *maximal* number of three-term progressions in a set of a given density; however, through an application of Lemma 3 below this can be turned into a question about the *minimal* number of three-term progressions.

[2] The notation $B\Delta C$ means the symmetric difference between B and C.

Remark. Note that the conclusion is non-trivial when $|S| = \alpha p^n$, where $\alpha > 2\epsilon$.

The conclusion of this theorem is telling us that, roughly, S is a union of a small number of cosets of some large-dimensional subspace W. An immediate corollary of this theorem, which is perhaps helpful for understanding what it says, is given as follows:

Corollary 1 *Fix a characteristic p prime, and a real number $0 < \alpha \leqslant 1$. Let S be a subset of $\mathbb{F}_p^n$ with $\Lambda_3(S)$ minimal, subject to the constraint*

$$|S| \geqslant \alpha p^n.$$

Then, there exists a subgroup (or subspace)

$$W \leqslant \mathbb{F}_p^n, \ \dim(W) = n - o(n),$$

and a set A, such that

$$|S \ \Delta \ (A + W)| = o(p^n).$$

In fact we get this conclusion when α is allowed to depend on n; indeed, the conclusion holds if $\alpha^{-1} = o(\log n)$.

Our second theorem is a slighly more abstract version of Theorem 1, where instead of sets S, we have a function $f : \mathbb{F}_p^n \to [0,1]$. We have not bothered to optimize the conclusion of the theorem (to the same extent as we did Theorem 1) given the method of proof, though much more can certainly be proved:

Theorem 2 *Fix a characteristic $p \geqslant 3$ prime, a density $0 < \alpha \leqslant 1$, and any function $\xi(n) < n/2$ (for $n \geqslant 3$) that tends arbitrarily slowly to infinity with n. Suppose that*

$$f : \mathbb{F}_p^n \to [0,1]$$

is such that $\Lambda_3(f)$ is minimal, subject to the constraint that

$$\mathbb{E}(f) \geqslant \alpha.$$

Then, there exists a subspace

$$W \leqslant \mathbb{F}_p^n, \ \dim(W) \geqslant n - \xi(n),$$

such that f is approximately an indicator function on cosets of W, in the following sense: There is a function

$$h : \mathbb{F}_p^n \to \{0,1\},$$

which is constant on cosets of W (which means $h(a) = h(a+w)$ for all $w \in W$), such that

$$\mathbb{E}(|f(m) - h(m)|) \ll 1/(\log \xi(n))^{1/2}.$$

It would seem that Theorem 1 is a corollary of some refined version of Theorem 2. This may be the case, but in later sections we will prove a third theorem (Theorem 4), from which we will deduce both Theorem 1 and Theorem 2.

An important point worth making, before we proceed with the proofs, is what more we would like our theorems above to say. We state this in the form of a conjecture.

Conjecture. Fix $p \geqslant 3$ prime, and $0 < \alpha \leqslant 1$. There exists an integer $m \geqslant 1$ such that the following holds for n sufficiently large: Suppose $f : \mathbb{F}_p^n \to [0,1]$ minimizes $\Lambda_3(f)$, subject to the constraint $\mathbb{E}(f) \geqslant \alpha$. Then, there exists a subspace W of codimension m (dimension $n-m$) such that f is constant on cosets of W.

One sees that this conjecture somewhat resembles Theorem 2 above, but is different in two important ways: First, the codimension m is fixed once p and α are decided – it does not grow as $n \to \infty$ or $\epsilon \to 0$; second, the conclusion says that g is *exactly* constant on cosets of W, rather than only approximately constant on cosets of W. This conjecture appears to be rather difficult to prove, and would require new ideas, perhaps in addition to the ones in the present paper.

2 Proofs

2.1 Additional Notation

We will require a little more notation: First, given a set $S \subseteq \mathbb{F}_p^n$, through an abuse of notation we will define $S(x)$ to be the indicator function for the set S; that is,

$$S(x) \ := \ 1_S(x) \ = \ \begin{cases} 1, & \text{if } x \in S; \\ 0, & \text{if } x \notin S. \end{cases}$$

Given any three subsets $U, V, W \subseteq \mathbb{F}_p^n$, define

$$T_3(f|U,V,W) \ = \ \textstyle\sum_{m \in U, m+d \in V, m+2d \in W} f(m) f(m+d) f(m+2d).$$

We note that this implies $T_3(1|U,U,U)$ is the number of three-term progressions belonging to a set U. If we omit U, V, W, it is understood that $U = V = W = \mathbb{F}_p^n$; further, given a set S, we let $T_3(S)$ denote the number of triples $(m, m+d, m+2d) \in S^3$.

Given a vector $v \in \mathbb{F}_p^n$, we will write

$$v \ = \ (v_1, ..., v_n)$$

to mean that

$$v \ = \ v_1 e_1 + \cdots + v_n e_n,$$

where $e_1, ..., e_n$ is the standard basis for $\mathbb{F}_p^n$. Given another such vector $w = (w_1, ..., w_n)$, we will define the dot-product

$$v \cdot w \ = \ v_1 w_1 + \cdots + v_n w_n \ \in \ \mathbb{F}_p.$$

As in the case of $\mathbb{R}$ and $\mathbb{C}$ vector spaces we will have for a subspace $W \subseteq \mathbb{F}_p^n$ that

$$\dim(W) + \dim(W^\perp) \;=\; n. \tag{3}$$

To see this, first note that $\dim(W^\perp)$ is the rank of the right-nullspace of the $\mathbb{F}_p$-matrix whose rows are any $\dim(W)$ basis vectors for W. Then, from the rank-nullity theorem (rank+nullity= n) for matrices, which still holds in $\mathbb{F}_p$ as it does in $\mathbb{R}$, along with the fact that the matrix has rank $\dim(W)$, we have that (3) now follows.

We also note that from the involution $(W^\perp)^\perp = W$, we have that $W^\perp$ determines W uniquely. To prove this involution, first observe that $(W^\perp)^\perp$ has the same dimension as W from (3). And so, it suffices to show $W \subseteq (W^\perp)^\perp$, which follows tautologically from the definition of the orthogonal complement of a subspace.

Given $f : \mathbb{F}_p^n \to \mathbb{C}$, we will define the Fourier transform of f at $a \in \mathbb{F}_p^n$ by

$$\hat{f}(a) \;=\; \textstyle\sum_m f(m) e^{2\pi i a \cdot m/p}.$$

(Note: We think of the $a \cdot m$ as an element of $\mathbb{Z}$ through the obvious embedding $\mathbb{F}_p \to \{0, 1, 2, ..., p-1\} \subset \mathbb{Z}$.)

A key theorem that we will need is Parseval's identity. Before we state it, we define the L^2 norm of a function $f : \mathbb{F}_p^n \to \mathbb{C}$ to be

$$\|f\|_2 \;=\; \left(p^{-n} \textstyle\sum_m |f(m)|^2\right)^{1/2}.$$

Theorem 3 (Parseval's Identity) *Suppose that $f : \mathbb{F}_p^n \to \mathbb{C}$. Then,*

$$\|\hat{f}\|_2^2 \;=\; p^n \|f\|_2^2.$$

Given functions

$$f, g \;:\; \mathbb{F}_p^n \;\to\; \mathbb{C},$$

we define the convolution

$$(f * g)(m) \;:=\; \textstyle\sum_t f(t) g(m-t).$$

We then have that

$$\widehat{(f * g)}(a) \;=\; \hat{f}(a)\hat{g}(a).$$

Given a subspace W of $\mathbb{F}_p^n$, and given a function

$$f \;:\; \mathbb{F}_p^n \;\to\; [0, 1],$$

we define the "W-smoothed version of f" as follows:

$$f_W(m) \;=\; \frac{1}{|W|}(f * W)(m) \;=\; \frac{1}{|W|} \textstyle\sum_{w \in W} f(m + w).$$

This function has a number of properties: First, we note that $f_W(m)$ is constant on cosets of W, in the sense that

$$\text{for all } w \in W,\ f_W(m) \ = \ f_W(m+w).$$

Thus, it makes sense to write

$$f_W(m+W) \ := \ f_W(m).$$

We also have that

$$\mathbb{E}(f_W) \ = \ \mathbb{E}(f). \tag{4}$$

And finally, the Fourier transforms $\hat{f}$ and $\hat{f}_W$ are related via

$$\hat{f}_W(x) \ = \ \begin{cases} \hat{f}(x), & \text{if } x \in W^{\perp}; \\ 0, & \text{if } x \notin W^{\perp}. \end{cases} \tag{5}$$

2.2 Theorem 4 and Lemma 1

Theorems 1 and 2 are corollaries of Theorem 4 and Lemma 1 listed below. Before we state them, let $m(\delta, \mathbb{F}_p^n)$ denote the minimal possible $\Lambda_3(f)$ out of all $f : \mathbb{F}_p^n \to [0,1]$ with $\mathbb{E}f = \delta$.

Theorem 4 *Fix a prime $p \geqslant 3$ and $0 < \epsilon \leqslant 1$, and assume that*

$$n \ > \ \Delta^{-2} + \frac{\log(4p/\epsilon)}{\log p}. \tag{6}$$

Suppose that $f \ : \ \mathbb{F}_p^n \ \to \ [0,1]$ is almost minimal in Λ_3 in the sense that

$$\Lambda_3(f) \ \leqslant \ m(\mathbb{E}f, \mathbb{F}_p^n) + \Delta.$$

Then, there is a subspace W of codimension at most Δ^{-2} such that

$$\mathbb{E}(|f(m) - f_W(m)|) \ \leqslant \ \epsilon.$$

Lemma 1 *The following holds for n sufficiently large: Suppose that $f \ : \ \mathbb{F}_p^n \ \to \ [0,1]$. Then, there exists an indicator function $g \ : \ \mathbb{F}_p^n \ \to \ \{0,1\}$, such that*

$$\mathbb{E}(g) \ \geqslant \ \mathbb{E}(f), \ \ |\Lambda_3(g) \ - \ \Lambda_3(f)| \ \leqslant \ p^{-n/3}, \tag{7}$$

and such that for every subspace W of codimension at most $n/4$ we have that for every $m \in \mathbb{F}_p^n$,

$$|g_W(m) \ - \ f_W(m)| \ < \ p^{-n/12}. \tag{8}$$

2.3 Proof of Lemma 1

In order to prove this lemma we will need to use a theorem of Hoeffding (see [6] or [7, Theorem 5.7])

Proposition 1 *Suppose that $z_1, ..., z_r$ are independent real random variables with $|z_i| \leqslant 1$. Let $\mu = \mathbb{E}(z_1 + \cdots + z_r)$, and let $\Sigma = z_1 + \cdots + z_r$. Then,*

$$\mathbb{P}(|\Sigma - \mu| > rt) \ \leqslant \ 2\exp(-rt^2/2).$$

Proof of the Lemma. The proof of this lemma is standard: Given f as in the theorem above, let g_0 be a random function from $\mathbb{F}_p^n$ to $\{0,1\}$ (which can be thought of as a sequence of random variables $g_0(a_1), ..., g_0(a_{p^n})$, where $a_1, ..., a_{p^n}$ run through the elements of our vector space), where $g_0(m) = 1$ with probability $f(m)$, and equals 0 with probability $1 - f(m)$; moreover, $g_0(m)$ is independent of all the other $g_0(m')$. Then, one can easily show that with probability $1 - o(1)$,

$$\left|p^{-n}\textstyle\sum_m g_0(m) \ - \ \mathbb{E}(f)\right|, \ |\Lambda_3(g_0) - \Lambda_3(f)| \ < \ p^{-n/3}/2. \tag{9}$$

2.3.1 Comment about the second inequality

Both of these can be proved using Chebyshev's inequality, though the second one here requires a little explaining: First, let

$$\Lambda_3'(f) \ := \ p^{-2n}\textstyle\sum_{n,d\in\mathbb{F}_p^n, d\neq 0} f(n)f(n+d)f(n+2d).$$

Note that for $f : \mathbb{F}_p^n \to [0,1]$, $\Lambda'(f)$ differs from $\Lambda(f)$ by an amount at most p^{-n}, so that it suffices to show that $|\Lambda_3'(g_0) - \Lambda_3'(f)| < p^{-n/3}/2 - p^{-n}$ holds with probability $1 - o(1)$.

We can treat $\Lambda_3'(g_0) - \Lambda_3'(f)$ as a sum of the random variables

$$z_{x,d} \ := \ p^{-2n}(g_0(x)g_0(x+d)g_0(x+2d) - f(x)f(x+d)f(x+2d)),$$

so that

$$\Lambda_3'(g_0) - \Lambda_3'(f) = \textstyle\sum_{x,d\in\mathbb{F}_p^n, d\neq 0} z_{x,d}.$$

Although these random variables are not independent, they almost are. Note first that if $d \neq 0$, then $\mathbb{E}z_{x,d} = 0$, so that

$$\begin{aligned}\mathrm{Var}(\Lambda_3'(g_0) - \Lambda_3'(f)) &= \mathbb{E}((\textstyle\sum_{x,d\in\mathbb{F}_p^n, d\neq 0} z_{x,d})^2) \\ &= \textstyle\sum_{x_1,d_1,x_2,d_2\in\mathbb{F}_p^n; d_1,d_2\neq 0} \mathbb{E}(z_{x_1,d_1}z_{x_2,d_2}).\end{aligned}$$

Now, so long as $\{x_1, x_1+d_1, x_1+2d_1\}$ and $\{x_2, x_2+d_2, x_2+2d_2\}$ are disjoint we will have z_{x_1,d_1} and z_{x_2,d_2} are independent, meaning that

$$\mathbb{E}(z_{x_1,d_1}z_{x_2,d_2}) \ = \ \mathbb{E}(z_{x_1,d_1})\mathbb{E}(z_{x_2,d_2}) \ = \ 0;$$

and otherwise, if we do not have independence, we at least will have an upper bound of p^{-4n} on $\mathbb{E}(z_{x_1,d_1}z_{x_2,d_2})$. Now, for each variable $z_{x,d}$ there can be at most $O(p^n)$ other variables dependent on $z_{x,d}$; and so,

$$\mathrm{Var}(\Lambda_3'(g_0) - \Lambda_3'(f)) \ \leqslant \ p^{-4n}p^{2n}O(p^n) \ \ll \ p^{-n}.$$

Clearly, then, by Chebyshev's inequality that $\mathbb{P}(|X-\mu| \geqslant t\sigma) \leqslant 1/t^2$ for any $t > 0$, where X is a random variable having mean μ and variance σ^2, we have that

$$\mathbb{P}(|\Lambda_3'(g_0) - \Lambda_3'(f)| > p^{-n/3}/2 - p^{-n}) \ \ll \ p^{-n}/(p^{-n/3})^2 \ < \ p^{-n/3};$$

and likewise for Λ_3 in place of Λ_3'.

2.3.2 Continuation of the proof of Lemma 1

We furthermore claim that with probability $1 - o(1)$ the following holds: For every subspace W of codimension at most $n/4$, and every $m \in \mathbb{F}_p^n$,

$$|(g_0)_W(m) \ - \ f_W(m)| \ \leqslant \ p^{-n/3}/2. \tag{10}$$

This can be seen as follows: For a fixed W, and fixed $m \in \mathbb{F}_p^n$, we need an upper bound on the probability that

$$|(g_0)_W(m) - f_W(m)| \ > \ p^{-n/3}/2.$$

This is the same as

$$|\Sigma| \ > \ p^{-n/3}|W|/2,$$

where

$$\Sigma \ = \ \textstyle\sum_{w\in W} z_w(m), \text{ where } z_w(m) \ = \ g_0(m+w) - f(m+w).$$

Note that all the $z_w(m)$ are independent and satisfy $|z_w(m)| \leqslant 1$ and $\mathbb{E}(z_w(m)) = 0$. So, from Proposition 1 we deduce that

$$\mathbb{P}(|\Sigma| > |W|p^{-n/3}/2) \ \leqslant \ 2\exp(-|W|p^{-2n/3}/8).$$

Now, since the number of such subspaces W is at most the number of sequences of $n/4$ possible basis vectors for $W^\perp$ (see section 2.1 for discussion on how $W^\perp$ uniquely determines W), which is at most $p^{n^2/4}$, we deduce that the probability that there exists a subspace W of codimension at most $n/4$ satisfying

$$|(g_0)_W(m) - f_W(m)| \ > \ p^{-n/3}/2$$

is

$$\leqslant \ 2p^{n^2/4}\exp(-p^{-2n/3}|W|/8) \ \leqslant \ 2p^{n^2/4}\exp(-p^{-2n/3}p^{3n/4}/8) \ = \ o(1/p^n).$$

The probability that this holds for some $m \in \mathbb{F}_p^n$ is therefore $o(1)$. Thus, (10) holds for all such W and $m \in \mathbb{F}_p^n$ with probability $1 - o(1)$.

We deduce now that there is an instantiation of g_0, call it g_1, such that both (9) and (10) hold for all W of codimension at most $n/4$ and all $m \in \mathbb{F}_p^n$. Then, by reassigning at most $p^{2n/3}/2$ places m where $g_1(m) = 0$ to the value 1, we arrive at a function g satisfying (7) and (8) upon noting that each alteration of $g_1(m)$ from 0 to 1 affects $\Lambda_3(g_1)$ by an amount at most p^{-n}. Since changing at most $p^{2n/3}/2$ values affects $\Lambda_3(g_1)$ by an amount at most $p^{-n/3}/2$, and changes $(g_1)_W(m)$ by an amount at most $|W|^{-1}p^{2n/3}/2 \leqslant p^{-n/12}/2$, we have that g satisfies the properties claimed by the lemma. ■

Proof of Theorem 1. To prove Theorem 1, we begin by letting f be the indicator function for the set S.

Now suppose that

$$\mathbb{E}(|f(m) - f_W(m)|) \leqslant \epsilon, \tag{11}$$

for some subspace W of codimension at most Δ^{-2}. Let $h(m)$ be $f_W(m)$ rounded to the nearest integer. Clearly, $h(m)$ is constant on cosets of W, and from the fact that

$$|h(m) - f_W(m)| \leqslant |f(m) - f_W(m)|,$$

we deduce that

$$\begin{aligned}\mathbb{E}(|f(m) - h(m)|) &\leqslant \mathbb{E}(|h(m) - f_W(m)|) + \mathbb{E}(|f(m) - f_W(m)|)\\ &\leqslant 2\mathbb{E}(|f(m) - f_W(m)|)\\ &\leqslant 2\epsilon.\end{aligned}$$

But since h is constant on cosets of W, and only assumes the values 0 or 1, we deduce that h is the indicator function for some set of the form $A + W$. Thus, we deduce

$$|S \,\Delta\, (A + W)| \leqslant 2\epsilon p^n,$$

where W has dimension at least $n - \Delta^{-2}$. This then proves Theorem 1 under the assumption (11).

Next, suppose that

$$\mathbb{E}(|f(m) - f_W(m)|) > \epsilon. \tag{12}$$

for every subspace W of codimension at most Δ^{-2}. Then, from the contrapositive of Theorem 4, we have that

$$\Lambda_3(f) > m(\mathbb{E}(f), \mathbb{F}_p^n) + \Delta.$$

Let $h : \mathbb{F}_p^n \to [0, 1]$ be any function satisfying

$$\mathbb{E}(h) = \mathbb{E}(f), \text{ and } \Lambda_3(h) = m(\mathbb{E}(f), \mathbb{F}_p^n),$$

Then, applying Lemma 1 (using $f = h$) we find there exists $g : \mathbb{F}_p^n \to \{0, 1\}$ satisfying

$$\mathbb{E}(g) \geqslant \mathbb{E}(h) = \mathbb{E}(f);$$

and,

$$\Lambda_3(g) \leqslant \Lambda_3(h) + p^{-n/3} < \Lambda_3(f) - \Delta + p^{-n/3}.$$

If we let S' be the set for which g is an indicator function, then one sees that S' has fewer three-term arithmetic progressions than does S, while $|S'| \geqslant |S|$, provided that

$$\Delta \ > \ p^{-n/3}.$$

Working through the definition of Δ in (1) we find that this holds provided that

$$\epsilon \ \gg_p \ 1/n. \tag{13}$$

This inequality is certainly is true, since we have assumed $\epsilon \geqslant c_p/\log n$.

We now arrive at a contradiction, since we have assumed our set S has the minimal number of three-term arithmetic progressions among all sets at least αp^n elements, and yet S' has even fewer. ■

Proof of Theorem 2. Let

$$g(m) \ : \ \mathbb{F}_p^n \ \rightarrow \ \{0,1\},$$

where $g(m)$ is as given in Lemma 1. Note that this implies that

$$\mathbb{E}(g) \ \geqslant \ \mathbb{E}(f), \ \Lambda_3(g) \ \leqslant \ \Lambda_3(f) + p^{-n/3},$$

and that for any subspace W of codimension at most $n/4$,

$$|g_W(m) \ - \ f_W(m)| \ \leqslant \ p^{-n/12}. \tag{14}$$

Let $\epsilon > 0$ be such that

$$\Delta^{-2} \ = \ \xi(n) \ < \ n/2. \tag{15}$$

Note that this implies

$$1/\log \xi(n) \ \ll \ \epsilon \ \ll \ 1/\log \xi(n),$$

and Δ will then satisfy the inequality (6), which will be important when we go to apply Theorem 4.

Suppose that there exists a subspace W of codimension at most Δ^{-2} such that

$$\mathbb{E}(|g(m) - g_W(m)|) \ \leqslant \ \epsilon. \tag{16}$$

Then, if we let $h(m)$ equal $f_W(m)$ rounded to the nearest integer, we will have that $h(m)$ is constant on cosets of W; and, we will have from (14) that

$$\begin{aligned} \mathbb{E}(|h(m) - f_W(m)|) \ &\leqslant \ \mathbb{E}(|g(m) - f_W(m)|) \\ &\leqslant \ \mathbb{E}(|g(m) - g_W(m)|) + p^{-n/12} \\ &\leqslant \ \epsilon + p^{-n/12}. \end{aligned} \tag{17}$$

Let V be any complementary subspace of W, so

$$\mathbb{F}_p^n \ = \ V \oplus W.$$

From (17) we know that at most

$$(\epsilon^{1/2} + \epsilon^{-1/2}p^{-n/12})|V|$$

vectors $v \in V$ satisfy

$$|h(v) - f_W(v)| \ > \ \epsilon^{1/2}.$$

Let $V' \subseteq V$ be those $v \in V$ satisfying the reverse inequality

$$|h(v) - f_W(v)| \ \leqslant \ \epsilon^{1/2}.$$

Suppose $v \in V'$ and $h(v) = 0$. Then, $f_W(v) \leqslant \epsilon^{1/2}$, and we have

$$\textstyle\sum_{m \in v+W} |f(m) - h(m)| \ = \ |W| f_W(v) \ \leqslant \ |W|\epsilon^{1/2}. \tag{18}$$

On the other hand, if $v \in V'$ and $h(v) = 1$, then $f_W(v) \geqslant 1 - \epsilon^{1/2}$, and so

$$\textstyle\sum_{m \in v+W} |f(m) - h(m)| \ = \ |W|(1 - f_W(v)) \ \leqslant \ |W|\epsilon^{1/2}. \tag{19}$$

Combining (18) with (19) we deduce that

$$\begin{aligned} \mathbb{E}(|f(m) - h(m)|) \ &\leqslant \ \epsilon^{1/2} + (|V| - |V'|)|V|^{-1} \\ &\leqslant \ 2\epsilon^{1/2} + \epsilon^{-1/2}p^{-n/12} \\ &\ll \ 1/(\log \xi(n))^{1/2}. \end{aligned} \tag{20}$$

Our theorem is now proved in this case (assuming there exists a subspace W satisfying (16)).

To complete the proof, we will assume that there are no subspaces of codimension at most Δ^{-2} satisfying (16). We deduce from the contrapositive of Theorem 4 (using $f = g$ in that case) that

$$\Lambda_3(g) \ > \ m(\mathbb{E}(g), \mathbb{F}_p^n) + \Delta \ \geqslant \ \Lambda_3(f) + \Delta \ \geqslant \ \Lambda_3(g) - p^{-n/3} + \Delta.$$

This is a contradiction provided

$$\Delta \ \geqslant \ p^{-n/3},$$

which it is, by (15). Our theorem is now proved. ■

3 Proof of Theorem 4

We will prove the contrapositive; so, we begin by assuming $f : \mathbb{F}_p^n \to [0, 1]$ has the property that for every subspace W of codimension at most Δ^{-2},

$$\mathbb{E}(|f(m) - f_W(m)|) \ > \ \epsilon. \tag{21}$$

And then we will show that

$$\Lambda_3(f) \ > \ m(\mathbb{E}f, \mathbb{F}_p^n) + \Delta. \tag{22}$$

As is well-known (see [9, Proposition 10.11]; note the difference in normalizations, and how this leads to the factor p^{-3n} in our formula),

$$\Lambda_3(f) \ = \ p^{-3n} \textstyle\sum_{a \in \mathbb{F}_p^n} \hat{f}(a)^2 \hat{f}(-2a).$$

If we let A denote the set of all $a \in \mathbb{F}_p^n$ where

$$|\hat{f}(a)| \ > \ \Delta p^n,$$

then we clearly have

$$\Lambda_3(f) \ = \ p^{-3n} \textstyle\sum_{a \in A} \hat{f}(a)^2 \hat{f}(-2a) \ + \ \mathcal{E}, \tag{23}$$

where, by Parseval,

$$|\mathcal{E}| \ \leqslant \ \Delta p^{-n} \|\hat{f}\|_2^2 \ \leqslant \ \Delta. \tag{24}$$

A simple application of Parseval's identity also shows that $|A|$ is small: We have

$$|A| \Delta^2 p^{2n} \ < \ p^n \|\hat{f}\|_2^2 \ \leqslant \ p^{2n},$$

which implies

$$|A| \ < \ \Delta^{-2}.$$

Let V be the subspace of $\mathbb{F}_p^n$ generated by the elements of A, and then let $W = V^\perp$. In general, we will not have that $\mathbb{F}_p^n = V \oplus W$, but that does not matter for the argument that follows.

From (5) and (23) (along with the fact that $(V^\perp)^\perp = V$, as discussed in section 2.1), we deduce that

$$\begin{aligned} \Lambda_3(f_W) &= p^{-3n} \textstyle\sum_{a \in A} \hat{f}_W(a)^2 \hat{f}_W(-2a) + p^{-3n} \sum_{\mathbb{F}_p^n \setminus A} \hat{f}_W(a)^2 \hat{f}_W(-2a) \\ &= p^{-3n} \textstyle\sum_{a \in A} \hat{f}(a)^2 \hat{f}(-2a) + \mathcal{E}' \\ &= \Lambda_3(f) + \mathcal{E}' - \mathcal{E}, \end{aligned} \tag{25}$$

where

$$\mathcal{E}' \ = \ p^{-3n} \textstyle\sum_{\mathbb{F}_p^n \setminus A} \hat{f}_W(a)^2 \hat{f}_W(-2a).$$

Now, by (5) again we find (by similar ideas as used in (24)) that

$$|\mathcal{E}' - \mathcal{E}| \ \leqslant \ p^{-3n} \sum_{a \in \mathbb{F}_p^n \setminus A} |\hat{f}(a)^2 \hat{f}(-2a)| \ \leqslant \ \Delta p^{-n} \|f\|_2^2 \ \leqslant \ \Delta.$$

Substituting this in to (25), we deduce that

$$\Lambda_3(f_W) \leqslant \Lambda_3(f) + \Delta. \tag{26}$$

Since W is an additive subgroup of $\mathbb{F}_p^n$, we can write $\mathbb{F}_p^n$ as a union of its cosets, and for these cosets we will use the standard representation given by

$$u + W, \text{ where } v \in U,$$

where U is any complementary subspace of W, satisfying

$$\mathbb{F}_p^n = U \oplus W.$$

This representation has the following important property.

Lemma 2 *Suppose that $h : \mathbb{F}_p^n \to [0,1]$. Then,*

$$T_3(h) = \sum_{\substack{u_1,u_2,u_3 \in U \\ u_1+u_3=2u_2}} T_3(h|u_1+W, u_2+W, u_3+W).$$

Proof. The lemma will follow if we can just show that $u_1+w_1, u_2+w_2, u_3+w_3$, $u_1, u_2, u_3 \in V$ and $w_1, w_2, w_3 \in W$, are in arithmetic progression implies u_1, u_2, u_3 are in arithmetic progression: If

$$(u_1 + w_1) + (u_3 + w_3) = 2(u_2 + w_2),$$

then

$$u_1 + u_3 - 2u_2 = -w_1 - w_3 + 2w_2.$$

Now, as $U \cap W = \{0\}$, we deduce that

$$u_1 + u_3 - 2u_2 = 0,$$

whence u_1, u_2, u_3 are in arithmetic progression. ■

Now let

$$U' := \{u \in U : f_W(u+W) \in [\epsilon/4, 1-\epsilon/4]\}; \tag{27}$$

that is, these cosets are all the places where f_W is not "too close" to being an indicator function.

3.1 Construction of the Function g

To construct the function g with the properties claimed by our Theorem, we start with the following standard lemma (see [2, Lemma 5]).

Lemma 3 *Suppose $h_1 : \mathbb{F}_p^n \to [0,1]$, let $\beta = \mathbb{E}(h_1)$, and let $h_2(n) = 1 - h_1(n)$. Then,*

$$\Lambda_3(h_1) + \Lambda_3(h_2) = 1 - 3\beta + 3\beta^2.$$

Now, let ℓ be the unique integer satisfying

$$4/\epsilon \leqslant p^\ell < 4p/\epsilon,$$

and let S be any subspace of W of codimension ℓ relative to W (that is, $\dim(S) = \dim(W) - \ell$). We note that such subspaces S exist to choose from, as W has dimension at least ℓ once n is sufficiently large, by virtue of the bound (6), along with the fact that W has codimension at most Δ^{-2}.

Let T be the set complement of S relative to W, and set

$$\beta = \frac{|T|}{|W|} = \frac{|W| - |S|}{|W|} = 1 - p^{-\ell} \geqslant 1 - \epsilon/4,$$

which is the density of T relative to W. Then, from the above lemma, we deduce that

$$T_3(S) + T_3(T) = (1 - 3\beta + 3\beta^2)|W|^2.$$

$T_3(S)$ clearly equals $(1-\beta)^2|W|^2$, because given any pair of elements $m, m+d \in S$, since S is a subspace we also must have $m + 2d \in S$; and, note that there are $(1-\beta)^2|W|^2$ ordered pairs $m, m+d$ in S. Thus, we deduce

$$T_3(T) = (2\beta^2 - \beta)|W|^2.$$

We now define the function $g : \mathbb{F}_p^n \to [0,1]$ as follows: Given $u \in U, w \in W$, we let

$$g(u+w) = \begin{cases} f_W(u), & \text{if } u \notin U'; \\ \beta^{-1}T(w)f_W(u), & \text{if } u \in U'. \end{cases}$$

It is easy to show that

$$\mathbb{E}(g) = \mathbb{E}(f_W) = \mathbb{E}(f).$$

We also observe, from Lemma 2, that

$$T_3(g) = \sum_{\substack{u_1,u_2,u_3 \in U \\ u_1+u_3=2u_2}} T_3(g|u_1+W, u_2+W, u_3+W).$$

This sum has eight types of terms, according to whether each of u_1, u_2, u_3 lie in U' or not.

First, consider the case where all of

$$u_1, u_2, u_3 \in U'. \tag{28}$$

In this case we have

$$\begin{aligned} T_3(g|u_1+W, u_2+W, u_3+W) &= \beta^{-3} f_W(u_1)f_W(u_2)f_W(u_3)T_3(T) \\ &= f_W(u_1)f_W(u_2)f_W(u_3)|W|^2(2\beta^{-1} - \beta^{-2}) \\ &\leqslant f_W(u_1)f_W(u_2)f_W(u_3)|W|^2(1 - p^{-2\ell}) \\ &< f_W(u_1)f_W(u_2)f_W(u_3)|W|^2(1 - \epsilon^2/16p^2). \end{aligned}$$

This last inequality follows from the fact that

$$p^\ell \ < \ 4p/\epsilon.$$

Now, as

$$T_3(f_W|u_1+W,u_2+W,u_3+W) \ = \ f_W(u_1)f_W(u_2)f_W(u_3)|W|^2,$$

we deduce that if (28) holds, then

$$T_3(g|u_1+W,u_2+W,u_3+W) \ < \ T_3(f_W|u_1+W,u_2+W,u_3+W)(1-\epsilon^2/16p^2).$$

On the other hand, if any of u_1,u_2,u_3 fail to lie in U', then we will get that

$$T_3(g|u_1+W,u_2+W,u_3+W) \ = \ T_3(f_W|u_1+W,u_2+W,u_3+W).$$

To see this, consider all the cases where u_1 fails to lie in U'. In this case, we clearly have

$$\begin{aligned} T_3(g|u_1+W,u_2+W,u_3+W) &= \textstyle\sum_{m_1\in u_2+W,m_2\in u_3+W} f_W(u_1)g(m_1)g(m_2) \\ &= f_W(u_1)(|W|^2 f_W(u_2)f_W(u_3)) \\ &= T_3(f_W|u_1+W,u_2+W,u_3+W). \end{aligned}$$

The cases where u_2 or u_3 fail to lie in U' are identical to this one.

Putting together the above observations we deduce that

$$\begin{aligned} T_3(g) &< T_3(f_W) - (\epsilon^2/16p^2)\textstyle\sum_{\substack{u_1,u_2,u_3\in U' \\ u_1+u_3=2u_2}} T_3(f_W|u_1+W,u_2+W,u_3+W) \\ &\leqslant T_3(f_W) - (\epsilon^5/1024p^2)|W|^2 T_3(U'). \end{aligned} \tag{29}$$

This last inequality follows from the fact that $f_W(u) \geqslant \epsilon/4$ for $u \in U'$.

3.2 A Lower Bound for $|U'|$

In order to give a lower bound for $T_3(U')$, we will first need a lower bound for $|U'|$.

We begin by noting that if u belongs to U, but not U', then either $f_W(u) < \epsilon/4$ or $f_W(u) > 1-\epsilon/4$. Suppose the former holds. Then, we have

$$\begin{aligned} \textstyle\sum_{m\in u+W}|f(m)-f_W(m)| \ \leqslant \ |W|f_W(u) + \sum_{m\in u+W} f(m) &= 2|W|f_W(u) \\ &< \epsilon|W|/2. \end{aligned} \tag{30}$$

On the other hand, if $f_W(u) > 1-\epsilon/4$, then we have

$$\begin{aligned} \textstyle\sum_{m\in u+W}|f(m)-f_W(m)| &\leqslant \textstyle\sum_{m\in u+W}(1-f(m)) + \sum_{m\in u+W}(1-f_W(m)) \\ &= 2|W| - 2|W|f_W(u) \\ &< \epsilon|W|/2. \end{aligned} \tag{31}$$

Putting together (30) and (31) we deduce that

$$\sum_{u\in U\setminus U'}\sum_{m\in u+W}|f(m)-f_W(m)| \ < \epsilon|W||U|/2.$$

We also have the trivial upper bound

$$\sum_{u\in U'}\sum_{m\in u+W}|f(m)-f_W(m)| \ \leqslant \ |W||U'|.$$

Adding these together and dividing by $|W||U|$ gives

$$|U|^{-1}(|U'|+\epsilon|U|/2) \ > \ \mathbb{E}(|f(m)-f_W(m)|) \ > \ \epsilon.$$

(The second inequality is our assumption (21).) It follows that

$$|U'| \ > \ \epsilon|U|/2. \tag{32}$$

3.3 Conclusion of the proof

Using our lower bound for $|U'|$, we will need the following theorem from [9, 10.17] (specialized to our problem) to obtain a lower bound for $T_3(U')$:

Theorem 5 *Suppose that $S \subseteq U \subseteq \mathbb{F}_p^n$ satisfies $|S| = \alpha|U|$, where U is a subspace. Then,*

$$T_3(S) \ \geqslant \ p^{-6/\alpha}|U|^2.$$

From Theorem 5 and (32) we deduce that

$$T_3(U') \ \geqslant \ p^{-12/\epsilon}|U|^2.$$

Combining this with (29), we deduce that

$$T_3(g) \ < \ T_3(f_W) - 2\Delta p^{2n}.$$

This, along with (26) implies

$$\Lambda_3(g) \ < \ \Lambda_3(f_W) - 2\Delta \ \leqslant \ \Lambda_3(f) - \Delta,$$

which proves (22), and therefore the theorem.

Acknowledgements

I would like to thank the anonymous referee for the numerous suggestions, which have led to a great improvement in the paper's readability.

References

[1] *Some Problems in Additive Combinatorics, AIM ARCC Workshop*, compiled by E. Croot and S. Lev.

[2] E. Croot, *The minimal number of three-term progressions modulo a prime converges to a limit*, Canad. Math. Bull **51** (2008), 47-56.

[3] B. Green, *A Szemerédi-type Regularity Lemma in Abelian Groups*, GAFA **15** (2005), 340-376.

[4] ————, *Finite field models in additive combinatorics*, Surveys in Combinatorics, Vol. 327, London Math. Soc. Lecture Notes.

[5] B. Green and O. Sisask, *On the maximal number of three-term arithmetic progressions in subsets of* $\mathbb{Z}/p\mathbb{Z}$, Bull. London Math. Soc. **40** (2008), 945-955.

[6] W. Hoeffding, *Probability Inequalities for Sums of Independent Random Variables*, J. Amer. Statist. Assoc. **58** (1963), 13-30.

[7] C. McDiarmid, *On the Method of Bounded Differences*, London Math. Soc. Lecture Note Ser. 14, Cambridge Univ. Press, Cambridge, 1989.

[8] R. Meshulam, *On subsets of finite abelian groups with no 3-term arithmetic progressions*, J. Comb. Theory Ser. A. **71** (1995), 168-172.

[9] T. Tao and V. Vu, *Additive Combinatorics*, (CUP, 2006).

[10] P. Varnavides, *On Certain Sets of Positive Density*, J. London Math. Soc. **34** (1959), 358-360.