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

Ernie Croot

October 16, 2018

1 Introduction

Given a function $f : \mathbb{F}_p^n \rightarrow [0, 1]$, and a subset $W \subseteq \mathbb{F}_p^n$, we define

$$E(f|W) = |W|^{-1} \sum_{m \in W} f(m).$$

If no set $W$ is given, then we just assume $W = \mathbb{F}_p^n$, and then we get

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

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 $m, m + d, m + 2d \in S$. Note that $\Lambda_3(f) \geq 0$, unless $E(f) = 0$, because of the contribution of trivial progressions where $d = 0$.

Of central importance to the subject of additive combinatorics is the problem of determining when a subset of the integers $\{1, \ldots, N\}$ contains a $k$-term arithmetic progression. This subject has a long history, and we will not mention it here; however, the specific problem in this area which motivated our paper, and which is due to B. Green [1], is as follows:

**Problem.** Given $0 < \alpha \leq 1$, suppose $S \subseteq \mathbb{F}_p$ satisfies $|S| \geq \alpha p$, 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 $S$. In this paper we address the analogous problem in $\mathbb{F}_p^n$, where $p$ and $\alpha$ are held fixed, while $n$ tends to infinity. 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. Such results can perhaps be deduced from the work of B. Green [2], which makes use of the Szemerédi regularity lemma, but our theorems below are proved using basic harmonic analysis.

**Theorem 1** Let $0 < \alpha \leq 1$. Suppose that $S$ is a subset of $\mathbb{F}_p^n$, such that $\Lambda_3(S)$ is minimal, subject to the constraint

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

Then, there exists a subgroup (or subspace)

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

such that $S$ is approximately a union of $p^{o(n)}$ cosets of $W$; more precisely, there is a set $A$ of size $p^{o(n)}$ such that

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

Our second theorem is a slightly more abstract version of this one, where instead of sets $S$, we have a function $f : \mathbb{F}_p^n \to [0, 1]$.

**Theorem 2** Let $0 < \alpha \leq 1$. Suppose that

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

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

$$\mathbb{E}(f) \geq \alpha > 0.$$  

Then, there exists a subgroup $W \subseteq \mathbb{F}_p^n$ of dimension $n - o(n)$, 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

$$\mathbb{E}(|f(m) - h(m)|) = o(1).$$

---

1The notation $B \Delta C$ means the symmetric difference between $B$ and $C$.  

2
It would seem that Theorem 1 is a corollary of Theorem 2; however, with a little thought one sees this is not the case. Nonetheless, we will prove a third theorem, from which we will deduce both Theorem 1 and Theorem 2.

2 Proofs

2.1 Additional Notation

We will require a little more notation.

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

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

We note that this implies $T_3(1|U, U, U)$ is the number of three-term progressions belonging to a set $U$.

Given a subspace $W$ of $\mathbb{F}_p^n$, and given a function $f : \mathbb{F}_p^n \to [0, 1]$, we define

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

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

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

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

Finally, if $V$ is the orthogonal complement of $W$ (with respect to the standard basis), then

if $v \in V$, then $\hat{f}_W(v) = \hat{f}(a)$; and, if $v \notin V$, then $\hat{f}_W(v) = 0$.

We will also define the $L^2$ norm of a function $f : \mathbb{F}_p^n \to \mathbb{C}$ to be

$$||f||_2 = \left( p^{-n} \sum_m |f(m)|^2 \right)^{1/2}.$$
2.2 Theorem 3, and Proofs of Theorems 1 and 2

Theorems 1 and 2 are corollaries of the following theorem:

**Theorem 3** Let \( \epsilon > 0 \), and suppose that \( f : \mathbb{F}_{p^n} \to [0,1] \) has the following property: For every subspace \( W \) of \( \mathbb{F}_{p^n} \) of codimension at most \( \Delta^{-2} \), where

\[
\Delta = (\epsilon^6/2^{13}p^2) \exp(-16\epsilon^{-1}c_p \log p),
\]

where \( c_p \) is a certain constant appearing in Theorem 4 below, suppose that

\[
\mathbb{E}(|f(m) - f_W(m)|) > \epsilon.
\]

Then, there exists a function

\[
g : \mathbb{F}_{p^n} \to [0,1]
\]

such that

\[
\mathbb{E}(g) = \mathbb{E}(f), \text{ and } \Lambda_3(g) < \Lambda_3(f) - \Delta.
\]

**Comment.** Using the Lemma 1 below we can deduce the stronger conclusion that there exists

\[
g : \mathbb{F}_{p^n} \to \{0,1\}
\]

(so, \( g \) is an indicator function) such that

\[
\mathbb{E}(g) \geq \mathbb{E}(f), \text{ and } \Lambda_3(g) < \Lambda_3(f) - \Delta + O(p^{-n/3}). \tag{3}
\]

**Lemma 1** Suppose that \( j : \mathbb{F}_{p^n} \to [0,1] \). There exists an indicator function \( j_2 : \mathbb{F}_{p^n} \to \{0,1\} \), such that

\[
\mathbb{E}(j_2) \geq \mathbb{E}(j), \Lambda_3(j_2) = \Lambda_3(j) + O(p^{-n/3}),
\]

and such that for every subspace \( W \) of codimension at most \( n^{1/2} \) we have\(^2\) that for every \( m \in \mathbb{F}_{p^n} \),

\[
(j_2)_W(m) = j_W(m) + O(1/n).
\]

\(^2\)The codimension \( n^{1/2} \) condition can be improved; however, it is good enough for our purposes, and it is larger than \( \Delta^{-2} \), where \( \epsilon = 1/\log \log n \), as will appear in later applications.
In order to prove this lemma we will need to use a theorem of Hoeffding (see [3] or [4, Theorem 5.7])

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

$$P(|\Sigma - \mu| > rt) \leq 2 \exp(-rt^2/2).$$

**Proof of the Lemma.** The proof of this lemma is standard: Given $j$ as in the theorem above, let $j_0$ be a random function from $F_p^n$ to $\{0, 1\}$, where $j_0(m) = 1$ with probability $j(m)$, and equals 0 with probability $1 - j(m)$; moreover, $j_0(m)$ is independent of all the other $j_0(m')$. Then, one can easily show that with probability $1 - o(1)$,

$$p^{-n} \sum_m j_0(m) = \mathbb{E}(j) + O(p^{-n/3}), \quad \text{and} \quad \Lambda_3(j_0) = \Lambda_3(j) + O(p^{-n/3}). \quad (4)$$

Furthermore, we claim that with probability $1 - o(1)$ we will have that for any subspace $W$ of codimension at most $n^{1/2}$,

$$(j_0)_W(m) = j_W(m) + O(1/n). \quad (5)$$

This can be seen as follows: For a fixed $W$ we need an upper bound on the probability that

$$|(j_0)_W(m) - j_W(m)| > 1/n.$$

This is the same as showing

$$|\Sigma| > |W|/n,$$

where

$$\Sigma = \sum_{w \in W} z_w(m), \quad \text{where} \quad z_w(m) = j_0(m + w) - j(m + w).$$

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

$$P(|\Sigma| > |W|/n) \leq 2 \exp(-|W|/2n^2).$$

Now, since the number of such subspaces $W$ is at most the number of sequences of $n^{1/2}$ possible basis vectors, which is $O(p^{n^{3/2}})$, we deduce that
the probability that there exists a subspace $W$ of codimension at most $n^{1/2}$ satisfying

$$\left| (j_0)_W(m) - j_W(m) \right| > 1/n$$

is $O(p^{3/2} \exp(-|W|/2n^2)) = o(1)$. Thus, (5) holds for all such $W$ with probability $1 - o(1)$ (in fact, the explicit constant in the $O(1)$ can be taken to be 1 once $n$ is sufficiently large).

We deduce now that there is an instantiation of $j_0$, call it $j_1$, such that both (4) and (5) hold. Then, by reassigning at most $O(p^{2n/3})$ places $m$ where $j_1(m) = 0$ to the value 1, or from the value 0 to the value 1, we arrive at a function $j_2$ having the claimed properties of the lemma.

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

$$\epsilon = \frac{1}{\log \log n}.$$

Now suppose that

$$\mathbb{E}( |f(m) - f_W(m)| ) \leq \epsilon,$$  \hspace{1cm} (6)

for some subspace $W$ of codimension at most $\Delta^{-2}$. 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

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

we deduce that

$$\mathbb{E}( |f(m) - h(m)| ) \leq \mathbb{E}( |h(m) - f_W(m)| ) + \mathbb{E}( |f(m) - f_W(m)| ) \leq 2\mathbb{E}( |f(m) - f_W(m)| ) \leq 2\epsilon.$$

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

$$|S \Delta A + W| \leq 2\epsilon p^n,$$
where \( W \) has dimension \( n - o(n) \). This then proves Theorem 1 under the assumption (6).

Next, suppose that
\[
E(|f(m) - f_W(m)|) > \epsilon.
\]
(7)
for every subspace \( W \) of codimension at most \( \Delta^{-2} \). Then, from the comment following Theorem 3 there exists an indicator function \( g \) satisfying (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 \( E(S') \geq E(S) \). This is a contradiction, and thus the theorem is proved.

Proof of Theorem 2
Let \( j(m) = f(m) \), and then let
\[
\ell(m) = j_2(m) : \mathbb{F}_p^n \to \{0, 1\},
\]
where \( j_2(m) \) is as given in Lemma 1. Note that this implies that
\[
E(\ell) \geq E(f), \quad \Lambda_3(\ell) = \Lambda_3(f) + O(p^{-n/3}),
\]
and that for any subspace \( W \) of codimension at most \( n^{1/2} \),
\[
\ell_W(m) = f_W(m) + O(1/n).
\]
(8)

Next let
\[
\epsilon = \frac{1}{\log \log n},
\]
and suppose that there exists a subspace \( W \) of codimension at most \( \Delta^{-2} \) such that
\[
E(|\ell(m) - \ell_W(m)|) \leq \epsilon.
\]
(9)
Then, if we let \( h(m) \) equal \( f_W(m) \) rounded to the nearest integer, we will have from (8) that
\[
E(|h(m) - f_W(m)|) \leq E(|\ell(m) - f_W(m)|)
\]
\[
\leq E(|\ell(m) - \ell_W(m)|) + O(1/n)
\]
\[
\leq \epsilon + O(1/n).
\]
(10)
Let $V$ be the orthogonal complement of $W$. From (10) we know that at most
$$(\epsilon^{1/2} + O(\epsilon^{-1/2}/n))|V|$$
values $v \in V$ satisfy
$$|h(v) - f_W(v)| \geq \epsilon^{1/2}.$$ 

Let $V' \subseteq V$ be those $v \in V$ satisfying the reverse inequality
$$|h(v) - f_W(v)| < \epsilon^{1/2}.$$ 

Suppose $v \in V'$ and $h(v) = 0$. Then, $f_W(v) < \epsilon^{1/2}$, and we have
$$\sum_{m \in v + W}|f(m) - h(m)| = |W|f_W(v) < |W|\epsilon^{1/2}. \quad (11)$$ 
On the other hand, if $v \in V'$ and $h(v) = 1$, then $f_W(v) > 1 - \epsilon^{1/2}$, and so
$$\sum_{m \in v + W}|f(m) - h(m)| = |W|(1 - f_W(v)) < |W|\epsilon^{1/2}. \quad (12)$$ 

Combining (11) with (12) we deduce that
$$\mathbb{E}(|f(m) - h(m)|) \leq \epsilon^{1/2} + (|V| - |V'|)|V|^{-1} \leq 2\epsilon^{1/2} + O(\epsilon^{-1/2}/n). \quad (13)$$ 

Our theorem is now proved in this case (assuming there exists a subspace $W$ satisfying (9)).

To complete the proof, we will assume that there are no subspaces of codimension at most $\Delta^{-2}$ satisfying (9). Since $\ell$ then satisfies the hypotheses of Theorem 3, we deduce from Theorem 3 that there exists a function $g : \mathbb{F}_p^n \to [0, 1]$ such that
$$\mathbb{E}(g) = \mathbb{E}(\ell) \geq \mathbb{E}(f) \geq \alpha,$$
and
$$\Lambda_3(g) < \Lambda_3(\ell) - \Delta = \Lambda_3(f) - \Delta + O(p^{-n/3}).$$ 
This then contradicts the fact that $\Lambda_3(f)$ was minimal, given $\mathbb{E}(f) \geq \alpha$. Our theorem is now proved. 

\[\blacksquare\]
3 Proof of Theorem 3

Let $\Delta$ be as in the statement of Theorem 3.

As is well-known,

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

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

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

where

$$|E| \leq \Delta p^{-n} ||\hat{f}||_2^2 \leq \Delta. \quad (15)$$

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

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

which implies

$$|A| \leq \Delta^{-2}. \quad (16)$$

Let $V$ be the additive subgroup of $\mathbb{F}_{p^n}$ generated by the elements of $A$, and let $W$ be the orthogonal complement of $V$; that is,

$$W = \{ w \in \mathbb{F}_{p^n} : \text{for every } v \in V, \ w \cdot v = 0 \}. \quad (14)$$

From (14), (15), and (2) we deduce that

$$\Lambda_3(f_W) \leq \Lambda_3(f) + \Delta. \quad (16)$$

Since $W$ is an additive subgroup of $\mathbb{F}_{p^n}$, we will use the standard representation for the cosets of $W$, given by

$$v + W, \text{ where } v \in V.$$
Lemma 2 Suppose that $h : \mathbb{F}_p^n \to [0, 1]$. Then,

$$T_3(h) = \sum_{v_1, v_2, v_3 \in V} T_3(h|v_1 + W, v_2 + W, v_3 + W).$$

Proof. The lemma will follow if we can just show that $v_1 + w_1, v_2 + w_2, v_3 + w_3,$
$v_1, v_2, v_3 \in V$ and $w_1, w_2, w_3 \in W$, are in arithmetic progression implies
$v_1, v_2, v_3$ are in arithmetic progression: If

$$(v_1 + w_1) + (v_3 + w_3) = 2(v_2 + w_2),$$

then

$$v_1 + v_3 - 2v_2 = -w_1 - w_3 + 2w_2.$$ 

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

$$v_1 + v_3 - 2v_2 = 0,$$

whence $v_1, v_2, v_3$ are in arithmetic progression. ■

Now let

$$V' := \{v \in V : f_W(v + W) \in [\epsilon/4, 1 - \epsilon/4]\}; \quad (17)$$

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 lemma:

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

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

Proof. We first realize that for $a \neq 0$, $\hat{h}_1(a) = -\hat{h}_2(a)$. Thus,

$$\Lambda_3(h_1) + \Lambda_3(h_2) = p^{-3n}\sum_a (\hat{h}_1(a)^2\hat{h}_1(-2a) + \hat{h}_2(a)^2\hat{h}_2(-2a))$$

$$= p^{-3n}(\hat{h}_1(0)^3 + \hat{h}_2(0)^3)$$

$$= \beta^3 + (1 - \beta)^3.$$. ■
Now, let $\ell$ be the unique integer satisfying
\[4/\epsilon \leq p^\ell < 4p/\epsilon,\]
and let $S$ be any subspace of $W$ of codimension $\ell$. Let $T$ be the complement of $S$ relative to $W$ (not orthogonal complement, as we have used earlier), and set
\[\beta = \frac{|T|}{|W|} = \frac{|W| - |S|}{|W|} = 1 - p^{-\ell} \geq 1 - \epsilon/4,\]
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 also have that if $b_1 + W, b_2 + W, b_3 + W$ are cosets that are in arithmetic progression, in the sense that there is a triple $m, m + d, m + 2d$, belonging to $b_1 + W, b_2 + W, b_3 + W$, respectively, then
\[T_3(1b_1 + T, b_2 + T, b_3 + T) = (2\beta^2 - \beta)|W|^2.\]

We now define the function $g : \mathbb{F}_p^n \to [0, 1]$ as follows: Given $v \in V, w \in W$, we have
\[g(v + w) = \begin{cases} f_W(v), & \text{if } v \notin V'; \\ \beta^{-1}T(w)f_W(v), & \text{if } v \in V'. \end{cases}\]

It is easy to see that
\[\mathbb{E}(g) = \mathbb{E}(f_W) = \mathbb{E}(f);\]

We also observe, from Lemma 2, that
\[T_3(g) = \sum_{v_1, v_2, v_3 \in V} T_3(g|v_1 + W, v_2 + W, v_3 + W).\]
This sum has eight types of terms, according to whether each of $v_1, v_2, v_3$ lie in $V'$ or not.

First, consider the case where all of

$$v_1, v_2, v_3 \in V'. \quad (18)$$

In this case we have

$$T_3(g|v_1 + W, v_2 + W, v_3 + W) = \beta^{-3} f_W(v_1) f_W(v_2) f_W(v_3) T_3(T)$$

$$= f_W(v_1) f_W(v_2) f_W(v_3) |W|^2 (2\beta^{-1} - \beta^{-2})$$

$$\leq f_W(v_1) f_W(v_2) f_W(v_3) |W|^2 (1 - p^{-2\ell})$$

$$< f_W(v_1) f_W(v_2) f_W(v_3) |W|^2 (1 - \epsilon^2/16p^2).$$

This last inequality follows from the fact that

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

Now, as

$$T_3(f_W|v_1 + W, v_2 + W, v_3 + W) = f_W(v_1) f_W(v_2) f_W(v_3) |W|^2,$$

we deduce that if (18) holds, then

$$T_3(g|v_1 + W, v_2 + W, v_3 + W) \leq T_3(f_W|v_1 + W, v_2 + W, v_3 + W)(1 - \epsilon^2/16p^2).$$

On the other hand, if any of $v_1, v_2, v_3$ fail to lie in $V'$, then we will get that

$$T_3(g|v_1 + W, v_2 + W, v_3 + W) = T_3(f_W|v_1 + W, v_2 + W, v_3 + W).$$

To see this, consider all the cases where $v_1$ fails to lie in $V'$. In this case, we clearly have

$$T_3(g|v_1 + W, v_2 + W, v_3 + W) = \sum_{m_1 \in_{v_1 + W}, m_2 \in_{v_3 + W}} f_W(v_1) g(m_1) g(m_2)$$

$$= f_W(v_1) |W|^2 f_W(v_2) f_W(v_3)$$

$$= T_3(f_W|v_1 + W, v_2 + W, v_3 + W).$$

The cases where $v_2$ or $v_3$ fail to lie in $V'$ are identical to this one.

Putting together the above observations we deduce that

$$T_3(g) \leq T_3(f_W) - (\epsilon^2/16p^2) \sum_{v_1, v_2, v_3 \in V'} T_3(f_W|v_1 + W, v_2 + W, v_3 + W)$$

$$\leq T_3(f_W) - (\epsilon^2/1024p^2)|W|^2 T_3(V'). \quad (19)$$

This last inequality follows from the fact that $f_W(v) \geq \epsilon/4$ for $v \in V'$.
3.2 A Lower Bound for $|V'|$

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

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

$$\sum_{m \in v + W} |f(m) - f_W(m)| \leq |W|f_W(v) + \sum_{m \in v + W} f(m) = 2|W|f_W(v) < \epsilon|W|/2. \quad (20)$$

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

$$\sum_{m \in v + W} |f(m) - f_W(m)| \leq \sum_{m \in v + V} (1 - f(m)) + \sum_{m \in v + W} (1 - f_W(m)) = 2|W| - 2|W|f_W(v) < \epsilon|W|/2. \quad (21)$$

Putting together (20) and (21) we deduce that

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

We also have the trivial upper bound

$$\sum_{v \in V'} \sum_{m \in v + W} |f(m) - f_W(m)| \leq |W||V'|.$$  

Thus,

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

(The second inequality is one of the hypotheses of the Theorem.) It follows that

$$|V'| > \frac{\epsilon|V|}{2(1 - \epsilon/2)} > \epsilon|V|/2. \quad (22)$$

3.3 Some Results of Meshulam and Varnavides

Using our lower bound for $|V'|$, we will need the following result of Meshulam [5] to obtain a lower bound for $T_3(V')$:

**Theorem 4** Suppose that $S \subseteq \mathbb{F}_p^n$ satisfies $|S| \geq c_p p^n/n$, where $c_p > 0$ is a certain constant depending only on $p$. Then, $S$ contains a non-trivial three-term arithmetic progression.
If we combine this with an idea of Varnavides [3], we get the following theorem.

**Theorem 5** Suppose that $S \subseteq \mathbb{F}_{p^n}$ satisfies $|S| = \alpha p^n$. Then,

$$\Lambda_3(S) \geq (\alpha/2) \exp(-8\alpha^{-1}c_p \log p).$$

**Proof of the Theorem.** From Meshulam’s theorem we know that if $U \subseteq \mathbb{F}_{p^m}$ satisfies $E(U) \geq \alpha/2$, and $m = \lceil 2c_p/\alpha \rceil$, then $U$ contains a three-term arithmetic progression.

Let $\mathcal{V}$ denote the sets of all additive subgroups of $\mathbb{F}_{p^n}$ of size $p^m$. For our proof we will need to establish some facts about $\mathcal{V}$: First, observe that any sequence of $m$ linearly independent vectors in $\mathbb{F}_{p^n}$ determines a subgroup in $\mathcal{V}$; however, each subgroup has many corresponding sequences of $m$ vectors, though each subgroup has the same number of sequences. Now, it is easy to see that the number of sequences of $m$ linearly independent vectors in $\mathbb{F}_{p^n}$ is

$$(p^n - 1)(p^n - p) \cdots (p^n - p^{m-1}) = \epsilon_1 p^{mn}, \text{ where } 1/2 < \epsilon_1 < 1;$$

and, given a subgroup in $\mathcal{V}$ (which can also be thought of as an $\mathbb{F}_p$ vector subspace of dimension $m$), there are

$$(p^m - 1)(p^m - p) \cdots (p^m - p^{m-1}) = \epsilon_2 p^{m^2}, \text{ where } 1/2 < \epsilon_2 \leq \epsilon_1 < 1,$$

sequences of $m$ linearly independent vectors in $\mathbb{F}_{p^n}$ that span this subgroup. So,

$$|\mathcal{V}| = \epsilon_3 p^{m(n-m)}, \text{ where } 1 \leq \epsilon_3 < 2.$$  

Next, suppose that $a \in \mathbb{F}_{p^n}$. We will need to know how many subgroups in $\mathcal{V}$ contain $a$: Any such subgroup (subspace) can be written as $\text{span}(a) + Z$, where $\dim(Z) = m-1$, and $Z \subseteq \text{span}(a)^\perp$. Thus, $Z$ is any $m-1$ dimensional subspace of an $n-1$ dimensional space; and so, from our bounds on $|\mathcal{V}|$, we deduce that there are $\epsilon_4 p^{(m-1)(n-m)}$, $1/2 < \epsilon_4 < 1$, possibilities for $Z$, which implies that there are

$$\epsilon_4 p^{(m-1)(n-m)} = \epsilon_5 |\mathcal{V}| p^{m-n}, \text{ where } 1/2 < \epsilon_5 \leq 1,$$

subspaces of $\mathbb{F}_{p^n}$ of dimension $m$ that contain $a$.

Now, given an arithmetic progression $a, a + d, a + 2d$, we note that the progression lies in a coset $b + A$ of an additive subgroup $A$ if and only if
$a \in b + A$ and $d \in A$. Thus, if we define $T'_3(X)$ to be the number of non-trivial three-term arithmetic progressions belonging to a set $X$, then the sum of the number of non-trivial arithmetic progressions lying in $(b + A) \cap S$, over all $A \in \mathcal{V}$, and $b \in A^\perp$ equals

\[
\sum_{A \in \mathcal{V}} \sum_{b \in A^\perp} T'_3((b + A) \cap S) = \sum_{a,a+d,a+2d \in S} \sum_{d \in A} \sum_{b \in A^\perp} 1 \leq |\mathcal{V}| \alpha p^n T'_3(S).
\]

We now give a lower bound on this first double sum over $A$ and $b$: We begin with

\[
|\mathcal{V}| \sum_{A \in \mathcal{V}} \sum_{b \in A^\perp} |(b + A) \cap S| = |\mathcal{V}||S|,
\]

which can be seen by noting that each $s \in S$ lies in exactly one coset $b + A$ of each subgroup $A \in \mathcal{V}$. Now consider all the cosets $b + A$, $A \in \mathcal{V}$, such that

\[
|(b + A) \cap S| \geq \alpha |A|/2.
\]

We claim that there are more than $|\mathcal{V}| p^{n-\alpha}/2$ such cosets. To see this, suppose there are fewer than this many cosets. Then, the left-most quantity in (24) is at most

\[
(|\mathcal{V}| p^{n-\alpha}/2)p^m + (|\mathcal{V}| p^{n-m})(\alpha |A|/2) < |\mathcal{V}| \alpha p^n = |\mathcal{V}||S|,
\]

which would contradict (24).

Thus, there are indeed more than $|\mathcal{V}| p^{n-m} \alpha/2$ cosets satisfying (25). For each such coset $b + A$, since

\[
|A| = p^m = p^{\lceil 2cp/\alpha \rceil},
\]

we deduce that $T'_3((b + A) \cap S) \geq 1$; and so,

\[
\sum_{A \in \mathcal{V}} \sum_{b \in A^\perp} T'_3((b + A) \cap S) \geq |\mathcal{V}| p^{n-m} \alpha/2.
\]

Combining this with (23) we deduce that

\[
T'_3(S) \geq p^{2n-2m} \alpha/2 \geq p^{2n}(\alpha/2) \exp(-8 \alpha^{-1} c_p \log p).
\]

This clearly implies the theorem.
3.4 Resumption of the Proof

From Theorem 5 and (22) we deduce that

\[ T_3(V') \geq (\epsilon/4) \exp(-16\epsilon^{-1}c_p \log p)|V|^{2}. \]

Combining this with (19), we deduce that

\[ T_3(g) \leq T_3(f_W) - 2\Delta p^{2n}. \]

This, along with (16) implies

\[ \Lambda_3(g) \leq \Lambda_3(f_W) - 2\Delta \leq \Lambda_3(f) - \Delta, \]

which proves the theorem.

References

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

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

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

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

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

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