On the Decay of the Fourier Transform and Three Term Arithmetic Progressions

Ernie Croot
Georgia Institute of Technology
School of Mathematics
267 Skiles
Atlanta, GA 30332
ecroot@math.gatech.edu

Submitted: August 21, 2006; Accepted: April 21, 2007; Published: June 13, 2007

Abstract

In this paper we prove a basic theorem which says that if the tail of the spectral L^2 norm of a function $f : \mathbb{F}_{p^n} \to [0,1]$ is sufficiently small (i.e. the function f is "sufficiently smooth"), then there are lots of arithmetic progressions $m, m+d, m+2d$ where

$$f(m)f(m+d)f(m+2d) \ > \ 0.$$

If f were an indicator function for some set S, then this would be saying that S has many three-term arithmetic progressions.

In principle this theorem can be applied to sets having very low density, where $|S|$ is around $p^{n(1-\gamma)}$ for some small $\gamma > 0$.

Furthermore, we show that if $g : \mathbb{F}_{p^n} \to [0,1]$ is majorized by f, and $\mathbb{E}(g)$ is not too "small", then in fact there are lots of progressions $m, m+d, m+2d$ where $f(m)g(m+d)f(m+2d) > 0$.

1 Introduction

Suppose that p is a prime number, and $n \geq 1$ is an integer. Let $\mathbb{F}$ denote the finite field $\mathbb{F}_{p^n}$ and set $F = |\mathbb{F}|$. Suppose that

$$f \ : \ \mathbb{F} \ \to \ [0,1].$$

We will use the expectation operator, defined to be

$$\mathbb{E}(f) \ := \ F^{-1}\sum_m f(m).$$

For an $a \in \mathbb{F}$ we will denote the Fourier transform of f at a as follows

$$\hat{f}(a) \ = \ \sum_m f(m)\omega^{a\cdot m},$$

where $\omega = e^{2\pi i/p}$, and where $a \cdot m$ denotes the dot product of a and m with respect to the standard $\mathbb{F}_p$ basis for $\mathbb{F}$.

Write $\mathbb{F} = \{a_1, ..., a_F\}$, where the a_i are ordered so that

$$|\hat{f}(a_1)| \ \geq \ |\hat{f}(a_2)| \ \geq \ \cdots \ \geq \ |\hat{f}(a_F)|.$$

For convenience we set $f_i = \hat{f}(a_i)$; and thus,

$$|f_1| \ \geq \ \cdots \ \geq \ |f_F|.$$

We also define

$$\sigma_i \ = \ \sum_{i<j\leq F}|f_j|^2,$$

which is the tail of the spectral L^2 norm of $\hat{f}$.

As a consequence of Parseval we have that if $\mathbb{E}(f) = \beta$, then

- For all $i = 1, ..., F$, $\sigma_i \leq \beta F^2$.
- Given $\varepsilon \in (0, 1]$, the number of indices $i = 1, ..., F$ such that $|f_i| \geq \varepsilon F$ is at most $\beta\varepsilon^{-2}$.

There are certain functions which have a lot fewer "large" Fourier coefficients as predicted by this second application of Parseval; for example, suppose that S is a subset of $\mathbb{F}$ having βF elements, and set

$$f(m) \ = \ \frac{1}{|S|}(S * S)(m).$$

Then, $f(m)$ is supported on the elements of $S + S$, and clearly takes on values in $[0, 1]$; also, $\mathbb{E}(f) = \beta$. Now, if

$$|\hat{f}(a)| \ = \ \frac{|\hat{S}(a)|^2}{|S|} \ \geq \ \varepsilon F,$$

then

$$|\hat{S}(a)|^2 \ \geq \ \varepsilon\beta F^2;$$

and, by Parseval one can easily show that the number of $a \in \mathbb{F}$ with this property is at most ε^{-1}, which is better than the $\beta\varepsilon^{-2}$ claimed after the second bullet above (at least for fixed β and small enough ε). Furthermore, the σ_i satisfy a sharper inequality than just $\sigma_i \ \leq \ \beta F^2$. In fact, if i is chosen so that $|f_i| \leq \varepsilon F$, then we will have

$$\sigma_i \ \leq \ \frac{|\hat{S}(a_i)|^2}{|S|^2}\sum_{i \leq j \leq F}|\hat{S}(a_j)|^2 \ \leq \ \varepsilon F^2.$$

If we were to take f to be something like

$$f(m) \ = \ \frac{1}{|S|^2}(S * S * S)(m),$$

we would get even sharper inequalities.

The main theorem of our paper will show that functions like f above must always be rich in three-term arithmetic progressions in a certain sense (at least if f is smooth enough – in fact, we will require f to be even smoother than the two examples above); actually, it will show even more – it will show that there are lots of such three-term progressions that pass through dense subsets where f is positive.

Two motivations for the results in the present paper are: First, Roth iteration, the primary Fourier-analytic method for proving that sets have three-term arithmetic progressions, does not work when the underlying set (or set-like function $f : \mathbb{F}_{p^n} \to [0, 1]$) has very low density, because only n iterations can be used, which in turn limits the method to densities $\geq c/n$, where $c = c(p) > 0$. In order to prove stronger theorems using Fourier methods, then, one needs to branch out with new approaches – the present paper does not use Roth iteration to prove its results. Second, although there are certain isolated results on "smooth functions" or "smooth sets", which say, for example, that sumsets $A + A$ have arithmetic progressions (see, for example, [1], [3], [7], and [8]), as well as results which say that dense subsets of random or pseudorandom sets (which are a type of smooth function, since they have only one large Fourier coefficient; though, they are not smooth in the sense that we use in the present paper) have arithmetic progressions (see [5] and [4]), there is no general theory that tells one when such sets have arithmetic progressions based purely on the decay properties of their Fourier transforms.

Rather than starting with the statement of this theorem, we will begin by stating one of its corollaries that is easy to parse. First, we introduce some more notation: Given $f_1, f_2, f_3 : \mathbb{F} \to \mathbb{C}$, define

$$\begin{aligned} \Lambda_3(f_1, f_2, f_3) \ &= \ \mathbb{E}_{m,d}(f_1(m)f_2(m + d)f_3(m + 2d)) \\ &= \ F^{-2}\sum_{m,d} f_1(m)f_2(m + d)f_3(m + 2d). \end{aligned}$$

If all three of our functions f_1, f_2, f_3 are the same function f, then we use the abbreviated notation

$$\Lambda_3(f) \ := \ \Lambda_3(f, f, f).$$

We note that the trivial progressions m, m, m provide the trivial lower bound

$$\Lambda_3(f) \ \geq \ \mathbb{E}(f)^3 F^{-1}.$$

We also define the usual norms (and quasinorms for $t < 1$)

$$||f||_t \ = \ \left(\sum_a |f(a)|^t\right)^{1/t}.$$

The corollary alluded to above is as follows.

Corollary 1 *Suppose $f, g : \mathbb{F} \to [0,1]$, and that*

$$\text{For all } m \in \mathbb{F}, \ f(m) \ \geq \ g(m) \ \geq \ 0; \text{ and, } \mathbb{E}(f) \ \geq \ \mathbb{E}(g) \ \geq \ F^{-\theta}.$$

Then, if

$$||\hat{f}||_{1/3} \ < \ F^{1+\gamma},$$

we will have that

$$\Lambda_3(f,g,f), \ \Lambda_3(g,f,f) \ \geq \ 10^{-10} p^{-10} F^{-12\theta - 4\gamma}.$$

Remark 1. It is possible to prove a similar results for quasinorms higher than 1/3; however, our method will not give good results for quasinorms 1/2 or higher.

Remark 2. An example of a function f where this theorem gives non-trivial results is as follows: First, let S be a subset of $\mathbb{F}$ having $F^{99/100}$ elements. Then, define

$$f(m) \ = \ |S|^{-6}(S * S * S * S * S * S * S)(m)$$

Note that $f : \mathbb{F} \to [0,1]$, $\mathbb{E}(f) = \mathbb{E}(S)$, and f is supported on the sumset $S+S+S+S+S+S+S$. Now,

$$|\hat{f}(a)| \ = \ |S|^{-6} |\hat{S}(a)|^7;$$

and, using Parseval, we find that the number of places a where

$$|\hat{S}(a)| \ \geq \ 2^{-j} F$$

is bounded from above by $F^{-1/100} 2^{2j}$. Thus,

$$\begin{aligned} ||\hat{f}||_{1/3} \quad &\leq \quad |S|^{-6} \left(\sum_{j=0}^{\infty} 2^{-7j/3} F^{7/3} (F^{-1/100} 2^{2j})\right)^3 \\ &\ll \quad F^{1+3/100}. \end{aligned}$$

Applying Corollary 1, it is easy to see that there are lots of m and $d \neq 0$ such that

$$f(m) f(m+d) f(m+2d) \ > \ 0.$$

Of course, it is fairly easy to prove non-trivial lower bounds for $\Lambda_3(f)$ without using this corollary (see [2]); however, the ideas in the corollary that give these lower bounds are different from these other methods (in the Fourier setting the ideas in [2] amount to forcing the Fourier transform $\hat{f}(a)$ to be a non-negative real number at all places a; this is quite different from the ideas that lead to the proof of the above corollary).

Remark 3. One way in which this corollary is different from others in the theory of arithmetic progressions (e.g. [6]), is that it produces lower bounds for $\Lambda_3(f)$ for when $\mathbb{E}(f)$ is quite small. However, note that the condition that $||\hat{f}||_{1/3}$ is "small" is a very strong requirement, only satisfied by certain special "smooth" functions, whereas Meshulam's result [6] holds for arbitrary general functions f where $\mathbb{E}(f) \geq c_p/n$.

The main theorem from which the above corollary follows is:

Theorem 1 *Suppose that* $f, g : \mathbb{F} \to [0,1]$ *satisfy*

$$f(m) \geq g(m) \geq 0, \text{ and } \mathbb{E}(f) \geq \mathbb{E}(g) \geq \max(F^{-\theta}, 8p^{-1/2}k^{-1}),$$

and

$$\sigma_k \leq \delta^2 F^2,$$

for some $k \geq 1$. *Then,*

$$\Lambda_3(f,g,f),\ \Lambda_3(g,f,f) \geq p^{-2}\binom{k}{2}^{-1} F^{-4\theta}/128 - 9\delta F^{-2\theta}/8.$$

Remark 4. One way that one can see how this theorem is much stronger than the above corollary is as follows: Say we start with f such that $||\hat{f}||_{1/3}$ is small enough so that the corollary implies there are lots of m, d such that $f(m)g(m+d)f(m+2d) > 0$. Now suppose we change the value of $f(m)$ at just one place m; then, $||\hat{f}||_{1/3}$ may no longer be all that small, and the corollary will give only a trivial lower bound for $\Lambda_3(f,g,f)$; however, in a lot of cases, the change to just one (or in fact many) value of $f(m)$ has little affect on the value of σ_k, and so has little affect on the conclusion given by the above theorem.

It would be good if we could have $m, m+d, m+2d$ all three belong to certain special *dense* subsets of $\mathbb{F}$ (subsets A of $\mathbb{F}$ such that $\mathbb{E}(f(m)A(m)) > c > 0$); however, this appears to be a very difficult and delicate problem to solve, and would require new ideas in addition to the ones in this paper.

We close the introduction of this paper with the following conjecture, which is motivated by the above theorem. We keep the conjecture intentionally vague:

Conjecture. Suppose $f : \mathbb{F} \to [0,1]$, and $\mathbb{E}(f) \geq F^{-\theta}$. Let $k = k(\varepsilon)$ denote the number of places $a \in \mathbb{F}$ where $|\hat{f}(a)| > \varepsilon F$. Then, one can obtain a non-trivial bound for $\Lambda_3(f)$ purely in terms of ε, k, and θ. Basically, what we are asking is a bound of the type appearing in the above theorem, except that it should not depend on the tail of the spectral L^2 norm of $\hat{f}$ – it should only depend on basic information about the large Fourier coefficients; and, it should give good results when there are only very few large Fourier coefficients.

2 Proof of Theorem 1 and its corollary

2.1 Proof of Corollary 1

We first note that from the bound

$$||\hat{f}||_{1/3} < F^{1+\gamma},$$

we deduce

$$|f_j| < \frac{F^{1+\gamma}}{j^3}.$$

From this it follows that

$$\sigma_k < F^{2+2\gamma}\textstyle\sum_{j \geq k+1} j^{-6} < F^{2+2\gamma}\displaystyle\int_k^\infty x^{-6}dx = \frac{F^{2+2\gamma}}{5k^5}.$$

Thus,

$$\sigma_k < \delta^2 F^2, \text{ for } \delta = (2k^{5/2})^{-1}F^{\gamma}.$$

From Theorem 1 we deduce that

$$\begin{aligned}\Lambda_3(f,g,f) &> p^{-2}\binom{k}{2}^{-1} F^{-4\theta}/128 - 9k^{-5/2}F^{-2\theta+\gamma}/16. \\ &\geq p^{-2}k^{-2}F^{-4\theta}/64 - 9k^{-5/2}F^{-2\theta+\gamma}/16.\end{aligned}$$

The value of k which maximizes this last quantity is

$$k = 2025p^4F^{4\theta+2\gamma},$$

and it produces the lower bound

$$\Lambda_3(f,g,f) \geq 10^{-10}p^{-10}F^{-12\theta-4\gamma}.$$

■

2.2 Notations and preliminary lemmas

Let

$$A \ = \ \{a_1, ..., a_k\}.$$

denote the set of places corresponding to $f_1, ..., f_k$; that is,

$$f_i \ = \ \hat{f}(a_i).$$

Note that because we can have $|f_i| = |f_j|$, the set A is not well defined; nonetheless, for the purposes of our proof all we need is that $f_1, ..., f_k$ correspond to *any* set of k largest Fourier coefficients of f. Also, let

$$B \ := \ A - A \ = \ \{a - b \ : \ a, b \in A\}.$$

We seek a subspace W of $\mathbb{F}$ such that

• At least a quarter of the translates $t \in \mathbb{F}$ (actually, we only need consider $t \in W^{\perp}$) satisfy

$$\sum_{m \in t+W} g(m) \ \geq \ \mathbb{E}(g)|W|/2. \tag{1}$$

• If V denotes the orthogonal complement of W, then there are no non-zero elements of B that lie in V; that is,

$$B \cap V = \{0\}. \tag{2}$$

What this would imply is that all the cosets $a + V$, $a \in A$, are distinct.

• We want W to have small dimension.

We will show that there is a subspace W satisfying the first two bullets above, where $|W| = p^{n'}$ (so, n' is the dimension of W), where

$$1 + (\log p)^{-1} \log \binom{k}{2} \ \leq \ n' \ < \ 2 + (\log p)^{-1} \log \binom{k}{2}.$$

To this end, we let S denote the set of all subspaces of $\mathbb{F}$ having this dimension n'.

We begin with a lemma.

Lemma 1 *If we pick a subpace $W \in S$ at random (using uniform measures), we will have that if $V = W^{\perp}$, then*

$$B \ \cap \ V \ = \ \{0\}.$$

holds with probability at least $1/2$.

Proof of the Lemma. Given a random subspace V of codimension n' (chosen with the uniform measure), the probability that some fixed element $b \in B$, $b \neq 0$, lies in V will be

$$\frac{|V| - 1}{F - 1} = \frac{p^{n-n'} - 1}{p^n - 1}.$$

This follows because 0 lies in every subspace, and if we eliminate it, we are left with $F - 1$ elements in our field; and, each non-zero element of the field is just as likely to be in a random subspace V as any other element – since there are $|V| - 1$ non-zero elements of V, this gives the probability $(|V| - 1)/(F - 1)$.

Thus, since there are at most $\binom{k}{2}$ pairs $\{b, -b\} \subseteq B$ (which is all we need to consider, since $b \in V$ if and only if $-b \in V$), the probability that no $b \in B$, $b \neq 0$, lies in V is at least

$$1 \ - \ \binom{k}{2} \frac{p^{n-n'} - 1}{p^n - 1} \ > \ 1 \ - \ \binom{k}{2} p^{-n'}.$$

This last quantity exceeds $1/2$ whenever

$$n' \ \geq \ 1 + (\log p)^{-1} \log \binom{k}{2}.$$

■

This Lemma 1 is what allows us to produce subspaces V satisfying (2); however, the following lemma will be needed to get (1) to hold:

Lemma 2 *If*

$$\mathbb{E}(g) \ > \ 8p^{-1/2}k^{-1},$$

then if $t \in \mathbb{F}$ and $W \in S$ are chosen independently at random using uniform measures, we will have that (1) holds with probability exceeding 3/4.

Proof of the Lemma. The proof of this corollary is via Chebychev's inequality: Suppose we select $t \in \mathbb{F}$ and $W \in S$ independently at random using uniform measures. Define the random variable

$$X \ := \ \sum_{m \in t+W} g(m).$$

To prove our corollary it suffices to show that

$$\mathrm{Prob}(|X - |W|\mathbb{E}(g)| \ > \ |W|\mathbb{E}(g)/2) \ < \ 1/4.$$

To prove this using Chebychev, we first consider

$$\mathbb{E}(X^2) \ = \ |S|^{-1}F^{-1}\sum_{t \in \mathbb{F}}\sum_{W \in S}\left(\sum_{m \in t+W} g(m)\right)^2.$$

On expanding out this square, we are left to estimate

$$\sum_{m_1,m_2 \in \mathbb{F}} g(m_1)g(m_2)\sum_{\substack{(t,W) \in \mathbb{F} \times S \\ m_1,m_2 \in t+W}} 1.$$

It is easy to see that this equals

$$\sum_{m_1,m_2 \in \mathbb{F}} g(m_1)g(m_2)\sum_{\substack{W \in S \\ m_1 - m_2 \in W}}\sum_{\substack{t \in \mathbb{F} \\ m_1 - t \in W}} 1.$$

(Note that in this final inner sum we get that if $m_1 - t \in W$, then $m_2 - t \in W$ as well, because $m_1 - m_2 \in W$.) Clearly, given W and m_1, there are $|W|$ choices for $t \in \mathbb{F}$ such that $m_1 - t \in W$; and so, the sum is

$$\sum_{m_1,m_2 \in \mathbb{F}} g(m_1)g(m_2)\sum_{\substack{W \in S \\ m_1 - m_2 \in W}} |W|.$$

To bound this from above, we consider the case where $m_1 = m_2$ seperate from the case $m_1 \neq m_2$: The contribution of all m_1, m_2 where $m_1 = m_2$ is

$$\sum_{m \in \mathbb{F}} g(m)^2|S||W| \ \leq \ F|S||W| \ = \ |S|p^{n+n'}.$$

The contribution of all unequal pairs m_1, m_2 is at most

$$\begin{aligned}\sum_{m_1,m_2 \in \mathbb{F}} g(m_1)g(m_2)|S||W|\frac{|W|-1}{F-1} &\leq |S|p^{2n'-n}\sum_{m_1,m_2 \in F} g(m_1)g(m_2) \\ &= |S|p^{2n'+n}\mathbb{E}(g)^2.\end{aligned}$$

So, we deduce that

$$\begin{aligned}\mathbb{E}(X^2) &\leq |S|^{-1}F^{-1}\left(|S|p^{2n'+n}\mathbb{E}(g)^2 + |S|p^{n'+n}\right) \\ &= p^{2n'}\mathbb{E}(g)^2 + p^{n'}.\end{aligned}$$

We also have that

$$\begin{aligned}\mathbb{E}(X) &= |S|^{-1}F^{-1}\sum_{W \in S}\sum_{t \in \mathbb{F}}\sum_{m \in t+W} g(m) \\ &= |S|^{-1}F^{-1}\sum_{m \in \mathbb{F}} g(m)\sum_{W \in S}\sum_{\substack{t \in \mathbb{F} \\ m \in t+W}} 1 \\ &= |S|^{-1}F^{-1}\sum_{m \in \mathbb{F}} g(m)\sum_{W \in S}|W| \\ &= p^{n'}\mathbb{E}(g).\end{aligned}$$

So, we deduce that

$$\mathrm{Var}(X) \ = \ \mathbb{E}(X^2) - \mathbb{E}(X)^2 \ \leq \ p^{n'}.$$

Chebychev's inequality then gives that

$$\mathbb{P}(|X - \mathbb{E}(X)| > \mathbb{E}(X)/2) \ \leq \ \frac{4\mathrm{Var}(X)}{p^{2n'}\mathbb{E}(g)^2} \ \leq \ \frac{4}{p^{n'}\mathbb{E}(g)^2} \ < \ \frac{1}{4},$$

provided

$$\mathbb{E}(g)^2 \ > \ 64p^{-1}k^{-2} \ > \ 16p^{-1}\binom{k}{2}^{-1} \ \geq \ 16p^{-n'}.$$

■

A corollary of both Lemmas 1 and 2 is as follows:

Corollary 2 *Suppose that*

$$\mathbb{E}(g) \ > \ 8p^{-1/2}k^{-1}.$$

Then, there exists a subspace $W \in S$ such that

- *Equation (2) holds for $V = W^{\perp}$; and,*
- *At least $F/4$ of the translates $t \in \mathbb{F}$ satisfy (1).*

Proof of the Corollary. Suppose we select $(t, W) \in \mathbb{F} \times S$ at random using the uniform measure. Let E_1 be the event that (2) holds for $V = W^{\perp}$, and let E_2 be the event that (1) holds. Then,

$$\mathbb{P}(E_2 \mid E_1) \ = \ \frac{\mathbb{P}(E_1, E_2)}{\mathbb{P}(E_1)} \ \geq \ \mathbb{P}(E_1) + \mathbb{P}(E_2) - 1.$$

By Lemma 1 we have $\mathbb{P}(E_1) \geq 1/2$, and by Lemma 2 we have $\mathbb{P}(E_2) > 3/4$; and so,

$$\mathbb{P}(E_2 \mid E_1) \ > \ 1/4.$$

It follows that some $W \in S$ has the property that (2) holds and that (1) holds for at least $F/4$ translates $t \in \mathbb{F}$. ■

2.3 Construction of the subspace V and the coset $t + W$

Let W be one of the subspaces described by Corollary 2. Then, suppose $t \in \mathbb{F}$, and define $\alpha := \alpha_t : \mathbb{F} \to \{0, 1\}$ to be the indicator function for the coset $t + W$; that is,

$$\alpha(m) \ = \ \begin{cases} 1, & \text{if } m \in t + W; \\ 0, & \text{if } m \notin t + W. \end{cases}$$

If we let $V = W^{\perp}$, then the Fourier transform of α is given by

$$\hat{\alpha}(a) \ = \ \begin{cases} |W|\omega^{a \cdot t}, & \text{if } a \in V; \\ 0, & \text{if } a \notin V. \end{cases}$$

Let

$$h(m) \ = \ (f\alpha * V)(m) \ = \ \textstyle\sum_{a+b=m}(f\alpha)(a)V(b) \ = \ \sum_{b \in V}(f\alpha)(m-b),$$

where $V(b)$ denotes the indicator function for V. If $w \notin W$, then $\hat{h}(w) = 0$ (because $\hat{V}(w) = 0$ in that case); however, if $w \in W$, then the Fourier transform of h is given by

$$\begin{aligned} \hat{h}(w) &= \widehat{(f\alpha)}(w)\hat{V}(w) \\ &= \frac{1}{F}(\hat{f} * \hat{\alpha})(w)\hat{V}(w) \\ &= \frac{|V|}{F}\textstyle\sum_{u_1+u_2=w}\hat{f}(u_1)\hat{\alpha}(u_2) \\ &= \frac{|V| \cdot |W|}{F}\textstyle\sum_{u_2 \in V}\hat{f}(w-u_2)\omega^{u_2 \cdot t} \\ &= \textstyle\sum_{v \in V}\hat{f}(w+v)\omega^{-v \cdot t}. \end{aligned} \tag{3}$$

We will now show that there is a choice for $t \in \mathbb{F}$ which guarantees that the large Fourier spectrum of $h(m)$ is 'close' to that of $f(m + t)$: First, split W into the union of the sets W_1 and W_2, where W_1 is the set of all $w \in W$ such that the coset $w + V$ contains some element of A (which must be unique); W_2 is the remaining elements of W. We use the notations $v(x)$ and $w(x)$ to denote the unique pair of elements of V and W, respectively, such that

$$x \ = \ v(x) + w(x).$$

Note that if $x \in A$, then $w(x) \in W_1$.

We seek $t \in \mathbb{F}$ such that the following three things all hold:

- We have that
$$\sum_{a\in A}|\hat{h}(w(a)) \ - \ \omega^{-v(a)\cdot t}\hat{f}(a)|^2 \ \leq \ 4\delta^2F^2. \tag{4}$$
- We have that
$$\sum_{w\in W_2}|\hat{h}(w)|^2 \ \leq \ 4\delta^2F^2. \tag{5}$$
- Finally, we want that
$$\sum_{m\in t+W}g(m) \ \geq \ \mathbb{E}(g)|W|/2. \tag{6}$$

One condition guaranteeing the first two bullets is

$$\sum_{a\in A}|\hat{h}(w(a)) - \omega^{-v(a)\cdot t}\hat{f}(a)|^2 \ + \ \sum_{w\in W_2}|\hat{h}(w)|^2 \ \leq \ 4\delta^2F^2. \tag{7}$$

From our formula (3) we get that if we sum the first sum in (7) over $t \in V$, we get

$$\begin{aligned}
&\sum_{t\in V}\sum_{a\in A}|\hat{h}(w(a)) - \omega^{-v(a)\cdot t}\hat{f}(a)|^2 \\
&\quad = \ \sum_{a\in A}\sum_{t\in V}\left|\sum_{\substack{v\in V\\ v\neq v(a)}}\hat{f}(v+w(a))\omega^{-v\cdot t}\right|^2 \\
&\quad = \ \sum_{a\in A}\sum_{\substack{v_1,v_2\in V\\ v_1,v_2\neq v(a)}}\sum_{t\in V}\hat{f}(v_1+w(a))\overline{\hat{f}(v_2+w(a))}\omega^{-(v_1-v_2)\cdot t} \\
&\quad = \ |V|\sum_{a\in A}\sum_{\substack{v\in V\\ v\neq v(a)}}|\hat{f}(v+w(a))|^2.
\end{aligned} \tag{8}$$

If we sum the second sum in (7) over $t \in V$, we get

$$\begin{aligned}
&\sum_{w\in W_2}\sum_{v_1,v_2\in V}\sum_{t\in V}\hat{f}(v_1+w)\overline{\hat{f}(v_2+w)}\omega^{-(v_1-v_2)\cdot t} \\
&\quad = \ |V|\sum_{w\in W_2}\sum_{v\in V}|\hat{f}(v+w)|^2.
\end{aligned} \tag{9}$$

The quantities in (8) and (9) sum to

$$|V|\sum_{\substack{a\in\mathbb{F}\\ a\notin A}}|\hat{f}(a)|^2 \ = \ |V|\sigma_k. \tag{10}$$

Since the left-hand-side of (7) is invariant under translating t by any element of W, we deduce that if we extend the sum of the left-hand-side of (7) from all $t \in V$ to all $t \in \mathbb{F}$, this sum is bounded from above by $F\sigma_k$ (instead of $|V|\sigma_k$ as in (10)).

Now, if we let T denote the set of $t \in \mathbb{F}$ for which (1) holds, then we note that $|T| \geq F/4$; and, the sum over all $t \in T \subseteq \mathbb{F}$ of the left-hand-side of (7) is bounded from above by the sum over all $t \in F$, which is $F\sigma_k$. It follows by simple averaging that there exists $t \in T$ such that

$$\sum_{a\in A}|\hat{h}(w(a)) - \omega^{-v(a)\cdot t}\hat{f}(a)|^2 \ + \ \sum_{w\in W_2}|\hat{h}(w)|^2 \ \leq \ \frac{F\sigma_k}{T} \ \leq \ 4\sigma_k;$$

and so, for this $t \in T$ we will have that both (4) and (5) hold; and, trivially, (6) holds by virtue of the fact that $t \in T$.

2.4 An $m \in t + W$, $g(m) \geq 0$ is a midpoint of many arithmetic progressions

Now select $m \in t + W$ such that

$$g(m) \ \geq \ \mathbb{E}(g)/2.$$

(By (1) it is obvious such m exists.) We will show that

$$\sum_d f(m-d)g(m)f(m+d) \ \text{ is large.}$$

To do this we just need to show that

$$\sum_d f(m-d)f(m+d) \text{ is large.}$$

Expressing this in terms of Fourier transforms, we find that it equals

$$F^{-1}\sum_a \hat{f}(a)^2\omega^{-2a\cdot m} \;=\; F^{-1}\sum_{a\in A}\hat{f}(a)^2\omega^{-2a\cdot m} \;+\; E, \tag{11}$$

where the error E satisfies

$$|E| \;\le\; F^{-1}\sum_{j=k+1}^{F} f_j^2 \;=\; F^{-1}\sigma_k \;\le\; \delta^2 F.$$

We now compare the final sum in (11) with the following:

$$F^{-1}\sum_{a\in A}\hat{h}(w(a))^2\omega^{2v(a)\cdot t-2a\cdot m}. \tag{12}$$

From the Cauchy-Schwarz inequality, we find that these two sums (12) and the final sum in (11) differ by at most

$$F^{-1}\left(\sum_{a\in A}|\hat{h}(w(a))-\hat{f}(a)\omega^{-v(a)\cdot t}|^2\right)^{1/2}\left(\sum_{a\in A}|\hat{h}(w(a))+\hat{f}(a)\omega^{-v(a)\cdot t}|^2\right)^{1/2}.$$

Using (4) and Parseval we find that this is at most

$$F^{-1}(2\delta F)(2F) \;=\; 4\delta F.$$

Next, observe that since $m \in t+W$, we have that

$$a\cdot m \;=\; v(a)\cdot m + w(a)\cdot m \;=\; v(a)\cdot t + w(a)\cdot m;$$

and so, the sum in (12) equals

$$F^{-1}\sum_{a\in A}\hat{h}(w(a))^2\omega^{-2w(a)\cdot m}.$$

We wish to extend this to a sum over all the elements of $\mathbb{F}$, and to do this we use the error estimate (5) to deduce that this sum equals

$$F^{-1}\sum_b \hat{h}(b)^2\omega^{-2b\cdot m} \;+\; E', \tag{13}$$

where

$$|E'| \;\le\; F^{-1}\sum_{w\in W_2}|\hat{h}(w)|^2 \;\le\; 4\delta^2 F.$$

Now, we can interpret the sum in (13) purely in terms of combinatorial properties of h: The sum equals

$$\sum_d h(m-d)h(m+d).$$

Using the fact that h is translation-invariant by elements of V, we find that the sum is at least

$$\begin{aligned}\sum_{d\in V}h(m-d)h(m+d) \;=\; h(m)^2\sum_{d\in V}1 \quad &\ge \quad h(m)^2|V| \\ &= \quad f(m)^2|V|.\end{aligned}$$

This last equality holds since h and f are equal on the coset $t+W$.

Putting together all our estimates, we find that

$$\begin{aligned}\sum_d f(m-d)f(m+d) \quad &\ge \quad f(m)^2|V| \;-\; 4\delta^2 F \;-\; 4\delta F \;-\; \delta^2 F \\ &\ge \quad g(m)^2|V| \;-\; 9\delta F \\ &\ge \quad \mathbb{E}(g)^2|V|/4 \;-\; 9\delta F.\end{aligned}$$

2.5 From one midpoint to many

We can repeat the argument in the previous subsection many times for different values of m. The idea is to reassign $g(m)$ to 0, to produce the new function

$$g_2(x) \ := \ \begin{cases} g(x), & \text{if } x \neq m; \\ 0, & \text{if } x = m. \end{cases}$$

Then, we find a different m_2 where $g_2(m_2) \geq \mathbb{E}(g_2)/2$, and where

$$\textstyle\sum_d f(m_2 - d)f(m_2 + d) \ \geq \ \mathbb{E}(g_2)^2|V|/4 - 9\delta F.$$

Thus, we will produce a sequence of functions $g_1 := g, g_2, g_3, ..., g_r$, and a sequence of numbers $m_2, m_3, ..., m_r$ where $r \geq \mathbb{E}(g)F/2$, each $\mathbb{E}(g_i) \geq \mathbb{E}(g)/2$, and $g_i(m_i) \geq \mathbb{E}(g_i)/2 \geq \mathbb{E}(g)/4$. We can conclude from this that

$$\begin{aligned} \Lambda_3(f,g,f) &\geq F^{-2}\textstyle\sum_{i=1}^{r}(\mathbb{E}(g_i)^2 p^{n-n'}/4 - 9\delta F)(\mathbb{E}(g)/4) \\ &\geq F^{-2}(\mathbb{E}(g)F/2)(\mathbb{E}(g)/4)(\mathbb{E}(g)^2 p^{n-n'}/16 - 9\delta F) \\ &= \mathbb{E}(g)^4(128p^{n'})^{-1} - 9\delta\mathbb{E}(g)^2/8 \\ &\geq p^{-2}\binom{k}{2}^{-1} F^{-4\theta}/128 - 9\delta F^{-2\theta}/8. \end{aligned}$$

The proof for $\Lambda_3(g,f,f)$ is nearly identical; the only difference is that in this case we need to bound

$$F^{-1}\textstyle\sum_a \hat{f}(a)\hat{f}(-2a)\omega^{a\cdot m}, \tag{14}$$

instead of

$$F^{-1}\textstyle\sum_a \hat{f}(a)^2\omega^{-2a\cdot m}. \tag{15}$$

The methods we apply above work equally well for (14) as they do for (15). ■

References

[1] J. Bourgain, *On Arithmetic Progressions in Sums of Sets of Integers*, A Tribute to Paul Erdős, 105-109, Cambridge Univ. Press, 1990.

[2] E. Croot, I. Ruzsa and T. Schoen, *Arithmetic Progressions in Sparse Sumsets*, To appear in INTEGERS conference procceedings.

[3] B. Green, *Arithmetic Progressions in Sumsets*, Geom. Funct. Anal. **12** (2002), 584-597.

[4] B. Green and T. Tao, *The Primes Contain Arbitrarily Long Arithmetic Progressions*, to appear in Ann. of Math.

[5] M. Hamel and I. Laba, *Arithmetic Structures in Random Sets*, preprint on the ARXIVES.

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

[7] T. Sanders, *Additive Structures in Sumsets*, preprint on ARXIVES.

[8] ————————, *Three Term Arithmetic Progressions in Sumsets*, preprint on ARXIVES.