

# NOTES ON THE POLYNOMIAL FREIMAN-RUZSA CONJECTURE

BEN GREEN

ABSTRACT. Let  $G$  be an abelian group. The Polynomial Freiman-Ruzsa conjecture (PFR) concerns the structure of sets  $A \subseteq G$  for which  $|A + A| \leq K|A|$ . These notes provide proofs for the statements made in §10 of [8], and as such constitute a reasonably detailed discussion of the PFR in the case  $G = \mathbb{F}_2^n$ .

Although the purpose of these notes is to furnish proofs for the statements in §10 of [8], they are reasonably self-contained. For further context see the article [8] itself. A great deal of the material in this section was communicated to me in person by Imre Ruzsa, and is reproduced here with his kind permission.

## 1. TOOLS

In this section we assemble a number of tools which are nowadays regarded as part of the standard armoury of an additive combinatorialist. The forthcoming book [18] will serve as a compendium for these and much more besides.

Let us briefly recall some notation concerning sumsets. Suppose that  $G$  is an abelian group and that  $A, B \subseteq G$ . Then we write

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

More generally if  $k, l$  are any two non-negative integers then we set

$$kA - lB := \{a_1 + \cdots + a_k - b_1 - \cdots - b_l \mid a_i \in A, b_j \in B\}.$$

If  $|A| = n$  and if  $|A + A| \leq K|A|$ , where  $K$  is “small” relative to  $n$ , then we say that  $A$  has small doubling. We call the ratio  $|A + A|/|A|$  the *doubling constant* of  $A$ .

The first tool is an inequality of Plünnecke [13], a new proof of which was found by Ruzsa [16]. Expositions of the proof may also be found in [12] or [9].

**Proposition 1.1** (Plünnecke’s inequalities). *Suppose that  $A$  and  $B$  are subsets of some abelian group  $G$ , and that  $|A + B| \leq K|A|$ . Then for any non-negative integers  $k, l$  we have*

$$|kB - lB| \leq K^{k+l}|A|.$$

The second tool is a simple but surprisingly powerful covering lemma of Ruzsa.

**Lemma 1.2** (Ruzsa). *Let  $S, T$  be subsets of an abelian group such that  $|S + T| \leq K'|S|$ . Then there is a set  $X \subseteq T$ ,  $|X| \leq K'$ , such that  $T \subseteq S - S + X$ .*

*Proof.* Pick a maximal set  $X \subseteq T$  such that the sets  $S + x$ ,  $x \in X$ , are pairwise disjoint. Since  $\bigcup_{x \in X} (S + x) \subseteq S + T$ , we have  $|S||X| \leq K'|S|$ , which implies that  $|X| \leq K'$ . Now suppose that  $t \in T$ . By maximality we there must be some  $x \in X$  such that  $(S + t) \cap (S + x) \neq \emptyset$ , which means that  $t \in S - S + x$ .  $\square$

---

The author is a Fellow of Trinity College, Cambridge.

The next proposition is due, in qualitative form, to Balog and Szemerédi [1]. The version below is due to Gowers [6, Proposition 12]. Somewhat better dependencies between the constants are now known (see for example [4]).

**Proposition 1.3** (Balog–Gowers–Szemerédi). *Let  $A$  be a subset of an abelian group. Suppose that  $|A| = n$ , and that there are at least  $cn^3$  quadruples  $(a_1, a_2, a_3, a_4) \in A^4$  such that  $a_1 + a_2 = a_3 + a_4$ . Then there is a set  $A' \subseteq A$  with  $|A'| \geq 2^{-19}c^{12}n$  and  $|A' - A'| \leq 2^{57}c^{-36}|A'|$ .*

## 2. THE POLYNOMIAL FREIMAN-RUZSA CONJECTURE

Write  $\mathbb{F}_2^\infty$  for the vector space of countable dimension over the finite field  $\mathbb{F}_2$ . Let  $A \subseteq \mathbb{F}_2^\infty$  have doubling at most  $K$ , meaning that we have the inequality  $|A + A| \leq K|A|$ . What can be said about the structure of  $A$ ?

It is hard to think of any examples of sets  $A$  with this property other than cosets of subspaces, and large subsets of them. In fact, these are the only such examples as was shown by Imre Ruzsa [14]. This is the finite field analogue of a celebrated theorem of Freiman [5]. The best known bounds for a result of this type are due to Ruzsa and the author [11]:

**Theorem 2.1** (Freiman’s theorem in  $\mathbb{F}_2^\infty$ ). *Let  $A \subseteq \mathbb{F}_2^\infty$  be a finite set with  $|A + A| \leq K|A|$ . Then  $A$  is contained within a coset of some subgroup  $H \leq \mathbb{F}_2^\infty$  with  $|H| \leq K^2 2^{2K^2-2}|A|$ .*

A version of this result, with somewhat weaker bounds, will be a consequence of Proposition 2.2 below (which is also due to Imre Ruzsa).

Theorem 2.1 gives, in a weak sense, a complete description of sets with small doubling. We showed that if  $|A + A| \leq K|A|$  then  $A$  is contained in a coset of a subspace of size at most  $K^2 2^{2K^2-2}|A|$ ; conversely, if  $A$  has this property then it is clear that  $|A + A| \leq K^2 2^{2K^2-2}|A|$ . It would be of great interest to have a structure theorem which does not result in exponential losses in  $K$  of this sort. Perhaps one can even arrange things so that one has a result of the form

$$\text{doubling constant } K \implies \text{structure} \implies \text{doubling constant } K',$$

where  $K'$  is *polynomial* in  $K$ .

It is easy to see that such a structure theorem would have to take a form somewhat different from Theorem 2.1. Indeed if one takes  $A \subseteq \mathbb{F}_2^\infty$  to be a subspace  $H$  together with  $K$  points  $x_1, \dots, x_K$  such that  $\text{Span}(x_1, \dots, x_K) \cap H = \{0\}$  then it is clear that  $|A + A| \leq K|A|$ , but that the smallest coset-of-a-subspace containing  $A$  has size roughly  $2^K|A|$ .

Ruzsa [14] reports that Katalin Marton has suggested that one should be looking for a covering of  $A$  by a small number  $C_1(K)$  of cosets of some rather smaller subspace of size  $C_2(K)|A|$ . I agree with this, and it is to some extent believable that  $C_1(K)$  and  $C_2(K)$  can be polynomial in  $K$ . This is what I shall call the Polynomial Freiman-Ruzsa conjecture (PFR) – it will be introduced in more detail later.

Imre Ruzsa indicated to me a large part of the following proposition giving a number of statements equivalent to such a structure theorem.

**Proposition 2.2** (Ruzsa). *The following five statements are equivalent.*

- (1) *If  $A \subseteq \mathbb{F}_2^\infty$  has  $|A + A| \leq K|A|$ , then there is  $A' \subseteq A$ ,  $|A'| \geq |A|/C_1(K)$ , which is contained in a coset of some subspace of size at most  $C_2(K)|A|$ .*
- (2) *If  $A \subseteq \mathbb{F}_2^\infty$  has  $|A + A| \leq K|A|$ , then  $A$  may be covered by at most  $C_3(K)$  cosets of some subspace of size at most  $C_4(K)|A|$ .*
- (3) *If  $A \subseteq \mathbb{F}_2^\infty$  has  $|A + A| \leq K|A|$ , and if additionally there is a set  $B$ ,  $|B| \leq K$ , such that  $A + B = A + A$ , then  $A$  may be covered by at most  $C_5(K)$  cosets of some subspace of size at most  $C_6(K)|A|$ .*
- (4) *Suppose that  $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^\infty$  is a function with the property that*

$$|\{f(x) + f(y) - f(x + y) : x, y \in \mathbb{F}_2^m\}| \leq K.$$

*Then  $f$  may be written as  $g + h$ , where  $g$  is linear and  $|\text{Im}(h)| \leq C_7(K)$ .*

- (5) *Suppose that  $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^\infty$  is a function with the property that for at least  $2^{3m}/K$  of the quadruples  $(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^m$  with  $x_1 + x_2 = x_3 + x_4$  we have  $f(x_1) + f(x_2) = f(x_3) + f(x_4)$ . Then there is an affine linear function  $g : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^\infty$  such that  $f(x) = g(x)$  for at least  $2^m/C_8(K)$  values of  $x$ .*

Furthermore if  $C_i(K)$  is bounded by a polynomial in  $K$  for all  $i \in I$ , where  $I$  is any of the sets  $\{1, 2\}$ ,  $\{3, 4\}$ ,  $\{5, 6\}$ ,  $\{7\}$ ,  $\{8\}$  then in fact  $C_i(K)$  is bounded by a polynomial in  $K$  for all  $i$ .

*Remarks.* Statement (4) is perhaps the most elegant and natural one here. Observe also that (4) is rather easy with the bound  $C_7(K) = 2^K$ . Thus Proposition 2.2 implies a weak version of Theorem 2.1. It is the possibility of polynomial bounds for  $C_i(K)$  that is the most interesting feature of this proposition. Let us call this the PFR conjecture:

**Conjecture 2.3** (Polynomial Freiman-Ruzsa conjecture for  $\mathbb{F}_2^n$ ). *The function  $C_7(K)$  (and hence all of the other functions  $C_i(K)$ ,  $i = 1, \dots, 8$ ), can be taken to be polynomial in  $K$ .*

Ruzsa was probably the first to actually dare to conjecture this, and he certainly states such a conjecture explicitly in [17]. Such matters are also touched upon (in the  $\mathbb{Z}$ -setting) in [2, 7].

The next section is devoted to the proof of Proposition 2.2. We do not purport to have done this in the most efficient manner.

### 3. PROOF OF PROPOSITION 2.2

(1)  $\Leftrightarrow$  (2). It is easy to see that (2)  $\Rightarrow$  (1). To go in the opposite direction, suppose that  $A \subseteq \mathbb{F}_2^\infty$  has  $|A + A| \leq K|A|$ . Using (1), we may pass to a subset  $A' \subseteq A$  with  $|A'| \geq |A|/C_1(K)$  and such that  $A'$  is contained in a coset of a hyperplane of size at most  $C_2(K)|A|$ . Apply Lemma 1.2 with  $S = A'$ ,  $T = A$  and  $K' = KC_1(K)$ . We get a set  $X$ ,  $|X| \leq KC_1(K)$ , such that  $A \subseteq A' - A' + X$ . This immediately implies (2) with  $C_3(K) \leq KC_1(K)$  and  $C_4(K) = C_2(K)$ .

(2)  $\Leftrightarrow$  (3). It is trivial that (2)  $\Rightarrow$  (3). To proceed in the opposite direction, we apply (3) to the set  $D = A - A$ . By Proposition 1.1, we have  $|D + D| = |2A - 2A| \leq K^4|A| \leq$

$K^4|D|$ . We claim that there is a set  $B$ ,  $|B| \leq K^8$ , such that  $D + B = D + D$ . To see this, apply Lemma 1.2 with  $S = A$ ,  $T = 2A - A$  and  $K' = K^4$  (this is a permissible choice by another application of Proposition 1.1). We get a set  $X$ ,  $|X| \leq K^4$ , such that  $2A - A \subseteq X + (A - A)$ , which implies that  $2A - 2A \subseteq X + (A - 2A) \subseteq X - X + (A - A)$ . This proves the claim, with  $B = X - X$ . Now apply (3) with to get that  $D$ , and hence  $A$ , may be covered by at most  $C_5(K^8)$  cosets of some subspace of size at most  $C_6(K^8)|D| \leq K^2 C_6(K^8)|A|$ .

(4)  $\Rightarrow$  (3). Suppose that we have a set  $A \subseteq \mathbb{F}_2^\infty$  with  $|A + A| \leq K|A|$ , together with a set  $B$ ,  $|B| \leq K$ , such that  $A + A \subseteq A + B$ . Let  $H_0$  be a minimal subspace such that the projection  $\pi : A \rightarrow H_0$  is one-to-one. Then  $\pi(A + A) = \pi(A - A) = H_0$  (or else we could find a smaller subspace). We define a map  $f : H_0 \rightarrow \mathbb{F}_2^\infty$  as follows. Put some fixed ordering on  $b$ , and for each  $x \in H_0$  pick the minimal  $b \in B$  such that  $x = \pi(a + b)$  for some  $a \in A$ , and set  $f(x) = a$ .

We claim that  $|\{f(x) + f(y) - f(x + y) : x, y \in H_0\}| \leq K^7$ . To see this, write  $x = \pi(a_1 + b_1)$ ,  $y = \pi(a_2 + b_2)$  and  $x + y = \pi(a_3 + b_3)$ . Then

$$f(x) + f(y) - f(x + y) = a_1 + a_2 - a_3. \quad (3.1)$$

Now we may pick  $a_4 \in A$ ,  $b_4 \in B$  such that  $a_1 + a_2 = a_4 + b_4$  and then  $a_5 \in A$ ,  $b_5 \in B$  such that  $a_3 + a_4 = a_5 + b_5$ . Summing gives

$$a_1 + a_2 - a_3 = a_5 + b_4 + b_5, \quad (3.2)$$

whence (since  $\pi$  is linear and we are in characteristic two)

$$\pi(a_5) = \pi(b_1 + b_2 + b_3 + b_4 + b_5).$$

Since  $\pi$  is one-to-one on  $A$ , the number of possible values of  $a_5$  is thus at most  $K^5$ . From (3.2), we see that there are at most  $K^7$  possible values of  $a_1 + a_2 - a_3$  which, in view of (3.1), implies our claim.

Now (4) implies that  $f = g + h$ , where  $g : H_0 \rightarrow \mathbb{F}_2^\infty$  is linear and  $|\text{Im}(h)| \leq C_7(K^7)$ . Statement (3) follows immediately with  $H = g(H_0)$ , and with  $C_5(K) \leq C_7(K^7)$ ,  $C_6(K) \leq K$ .

(1)  $\Rightarrow$  (5). Suppose that  $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^\infty$  is a function with the property we are interested in, viz. that for at least  $2^{3m}/K$  of the quadruples  $(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^m$  with  $x_1 + x_2 = x_3 + x_4$  we have  $f(x_1) + f(x_2) = f(x_3) + f(x_4)$ . Consider the graph  $\Gamma = \{(x, f(x)) : x \in \mathbb{F}_2^m\}$  of  $f$ . The set  $\Gamma \subseteq \mathbb{F}_2^m \times \mathbb{F}_2^\infty$  has cardinality  $N = 2^m$ , and the number of solutions to the equation  $t_1 + t_2 = t_3 + t_4$  with  $t_i \in \Gamma$  is at least  $N^3/K$ .

It follows from Proposition 1.3 that there is  $\Gamma' \subseteq \Gamma$ ,  $|\Gamma'| \geq 2^{-19}K^{-12}N$ , such that  $|\Gamma' - \Gamma'| \leq 2^{57}K^{36}|\Gamma'|$ . Applying (2), we see that  $\Gamma'$  may be covered by  $l = C_3(2^{57}K^{36})$  cosets  $H + x_1, \dots, H + x_l$  of some subspace  $H \subseteq \mathbb{F}_2^m \times \mathbb{F}_2^\infty$ ,  $|H| \leq C_4(2^{57}K^{36})N$ . By increasing  $l$  to  $C_9(K) := C_3(2^{57}K^{36})C_4(2^{57}K^{36})$  if necessary, we may assume that the projection  $\pi$  of  $H$  onto the first factor  $\mathbb{F}_2^m$  is an isomorphism. By the pigeonhole principle, there is some  $i$  such that  $|\Gamma' \cap (H + x_i)| \geq |\Gamma'|/C_9(K) \geq 2^{-19}K^{-12}N/C_9(K)$ . Write  $\Gamma'' = \Gamma' \cap (H + x_i)$ , and set  $E = \pi(\Gamma'')$ . It is clear that  $f|_E$  is affine linear. This confirms (5), with  $C_8(K) = 2^{19}K^{12}C_9(K)$ .

(5)  $\Rightarrow$  (4). Set  $N = 2^n$ . Suppose that  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^\infty$  is a map such that  $|B| \leq K$ , where  $B := \{f(x) + f(y) - f(x + y) : x, y \in \mathbb{F}_2^n\}$ . A simple application of the Cauchy-Schwarz inequality confirms that there are at least  $N^3/K$  quadruples  $(x_1, x_2, x_3, x_4)$

with  $x_1 + x_2 = x_3 + x_4$  and  $f(x_1) + f(x_2) = f(x_3) + f(x_4)$ . Thus there is a set  $E \subseteq \mathbb{F}_2^n$ ,  $|E| \geq N/C_8(K)$ , such that  $f|_E$  is affine linear. Write  $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^\infty$  for the extension of this affine linear function to all of  $\mathbb{F}_2^n$ .

Now Lemma 1.2 applies to show that there is a set  $T$ ,  $|T| \leq C_8(K)$ , such that  $T + E - E = \mathbb{F}_2^n$ . However it is easy to confirm that

$$f(t + e_1 - e_2) = f(e_1) - f(e_2) + f(t) + b_1 - b_2 = g(t + e_1 - e_2) + f(t) - g(t) + g(0) + b_1 - b_2$$

for some  $b_1, b_2 \in B$ . Thus  $|\text{Im}(f - g)| \leq |T|^2|B|^2 \leq C_8(K)^2 K^2$ . This concludes the proof.  $\square$

*Remark.* The equivalence of (1) – (4) could be shown without recourse to Proposition 1.3.

#### 4. SUBPLÜNNECKARITY

Recall, from §1, the statement of Plünnecke's inequality. The reader may observe that (1) of Proposition 2.2 implies a much stronger bound for some large subset  $A' \subseteq A$ , for large  $s, t$ , at least if there is a good bound on  $C_2(K)$ . We may call such an  $A'$  *subplünnecke*. Nets Katz asked me to formulate a converse, that is to say a principle to the effect that  $A$  being subplünnecke implies that  $A$  is very economically contained in some coset of a subspace. The following result is my best effort so far in this direction:

**Proposition 4.1.** *Let  $A \subseteq \mathbb{F}_2^\infty$ , and suppose that there is a constant  $B$  such that  $|tA| \leq t^B|A|$  for all  $t \geq B \log B$ . Then  $A$  is contained in a union of  $2^{CB \log B}$  cosets of some subspace having size at most  $|A|$ .*

The proof of this proposition is a variant of Chang's proof of Freiman's theorem [3], which is itself based on Ruzsa's argument [15]. We will make use of the Fourier transform. Recall that by fixing a basis  $(e_1, \dots, e_n)$  for  $\mathbb{F}_2^n$  one may identify the characters on  $\mathbb{F}_2^n$  with the group itself. Indeed if  $\xi \in \mathbb{F}_2^n$  then the map  $x \mapsto (-1)^{\xi^T x}$  is a character, and we may define the Fourier transform

$$\widehat{f}(\xi) := \sum_{x \in \mathbb{F}_2^n} f(x) (-1)^{\xi^T x}.$$

If  $A \subseteq \mathbb{F}_2^n$  is a set then we write  $\widehat{A}$  for the Fourier transform of the characteristic function of  $A$ . See [8, §2] for more details.

The following very useful lemma of Chang says that if  $A \subseteq \mathbb{F}_2^n$  then the set of points  $\xi$  at which  $\widehat{A}(\xi)$  is large has considerable structure.

**Lemma 4.2** (Chang). *Let  $A \subseteq \mathbb{F}_2^n$  have cardinality  $\alpha N$ , let  $\rho \in (0, 1)$  be a real number and let  $\Lambda$  be the set of all  $\xi$  for which  $|\widehat{A}(\xi)| \geq \rho|A|$ . Then  $\Lambda$  is contained in a subspace of dimension at most  $8\rho^{-2} \log(1/\alpha)$ .*

*Remark.* Chang [3] derived this result using an inequality of Rudin. See also [9]. In the finite field case an alternative (though morally very similar) proof may be given using an inequality of Beckner (see [10]).

In order to prove Proposition 4.1 we also need the notion of a *Freiman isomorphism*. Suppose that  $A$  and  $B$  are subsets of abelian groups and that  $\phi : A \rightarrow B$  is a map. Let

$k$  be a positive integer. We say that  $\phi$  is a Freiman  $k$ -homomorphism if whenever

$$a_1 + \cdots + a_k = a'_1 + \cdots + a'_k$$

we have

$$\phi(a_1) + \cdots + \phi(a_k) = \phi(a'_1) + \cdots + \phi(a'_k).$$

If  $\phi$  has an inverse which is also a Freiman  $k$ -homomorphism then we say that  $\phi$  is a Freiman  $k$ -isomorphism. In this case we write  $A \cong_k B$ .

**Lemma 4.3.** *Let  $A \subseteq \mathbb{F}_2^\infty$ , and suppose that  $|kA| \leq k^B|A|$ . Then  $A$  is Freiman  $k$ -isomorphic to a subset of  $\mathbb{F}_2^n$ , where  $2^n \leq k^{4B}|A|$ .*

*Proof.* Take a minimal  $n$  such that there is a set  $S \subseteq \mathbb{F}_2^n$  with  $S \cong_k A$ . For any  $x \in \mathbb{F}_2^n$  there is a linear projection  $\pi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^{n-1}$  with  $\ker(\pi) = \langle x \rangle$ . Any such projection induces a Freiman homomorphism (of any order) on  $S$ . Thus, by minimality,  $\pi|_S$  does not have an inverse which is also a Freiman  $k$ -homomorphism. This means that there are  $s_1, \dots, s_k, s'_1, \dots, s'_k \in S$  with

$$s_1 + \cdots + s_k \neq s'_1 + \cdots + s'_k$$

but

$$\phi(s_1) + \cdots + \phi(s_k) = \phi(s'_1) + \cdots + \phi(s'_k).$$

By our choice of  $\pi$ , this implies that

$$s_1 + \cdots + s_k - s'_1 - \cdots - s'_k = x.$$

Since  $x$  was arbitrary we have  $kS - kS = \mathbb{F}_2^n$ . Since  $A \cong_k S$ , we have  $|kS| = |kA| \leq k^B|A| = k^B|S|$ . Applying Proposition 1.1 with sets  $S$  and  $(k-1)S$  gives

$$|kS - kS| \leq |2(k-1)S - 2(k-1)S| \leq k^{4B}|S|.$$

Hence we have the inequality  $2^n \leq k^{4B}|A|$ , which is what we wanted to prove.  $\square$

We call a Freiman isomorph of  $A$  which sits densely inside some subspace a *model* for  $A$ . It is useful to have a good model for a set  $A$ , since the tools of Fourier analysis are then available. The next lemma is an example of this. For more on models, see [11].

**Lemma 4.4** (Chang-Bogolyubov). *Suppose that  $A \subseteq \mathbb{F}_2^n$  has density  $\alpha$ , and let  $k$  be a positive integer. Then  $kA - kA$  contains a subspace  $H \leq \mathbb{F}_2^n$  with*

$$\text{codim}(H) \leq 32\alpha^{-1/(k-1)} \log(1/\alpha).$$

*Proof.* Set  $N = 2^n$ , and let  $\rho = \frac{1}{2}\alpha^{1/(2k-2)}$ . Let  $r_{2k}(x)$  be the number of representations of  $x$  as  $a_1 + \cdots + a_k - a'_1 - \cdots - a'_k$ . This being the convolution of  $k$  copies of  $A$  and  $k$  copies of  $-A$ , we may write it using the Fourier inversion formula as

$$r_{2k}(x) = N^{-1} \sum_{\xi} |\widehat{A}(\xi)|^{2k} (-1)^{\xi^T x}. \quad (4.1)$$

Observe that  $r_{2k}(x) > 0$  if and only if  $x \in kA - kA$ . Now split the sum (4.1) as  $\Sigma_1 + \Sigma_2$ , where

$$\Sigma_1 := \sum_{\xi: |\widehat{A}(\xi)| \geq \rho|A|} |\widehat{A}(\xi)|^{2k} (-1)^{\xi^T x}$$

and

$$\Sigma_2 := \sum_{\xi: |\widehat{A}(\xi)| < \rho|A|} |\widehat{A}(\xi)|^{2k} (-1)^{\xi^T x}.$$

By Lemma 4.2 there is a subspace  $H \leq \mathbb{F}_2^n$ ,  $\text{codim}(H) \leq 8\rho^{-2} \log(1/\alpha)$ , such that  $\xi^T x = 0$  whenever  $|\widehat{A}(\xi)| \geq \rho|A|$  and  $x \in H$ . For  $x \in H$ , then, we have

$$\Sigma_1 \geq |\widehat{A}(0)|^{2k} = \alpha^{2k} N^{2k}.$$

We also have the estimate

$$|\Sigma_2| \leq \rho^{2k-2} \alpha^{2k-2} N^{2k-2} \sum_{\xi} |\widehat{A}(\xi)|^2 = \rho^{2k-2} \alpha^{2k-1} N^{2k} < \Sigma_1.$$

Thus  $r_{2k}(x) > 0$  whenever  $x \in H$ , which proves the lemma.  $\square$

*Proof of Proposition 4.1.* Let  $k = \lceil B \log B \rceil$ . Since  $|4kA| \leq (4k)^B |A|$ , we may apply Lemma 4.3 to assert that  $A \cong_{4k} S$ , where  $S$  is a subset of  $\mathbb{F}_2^n$  and  $2^n \leq (4k)^{4B} |A|$ . Since  $|S| = |A|$ , the density of  $S$  in  $\mathbb{F}_2^n$  is at least  $\sigma := (4k)^{-4B}$ . Now Lemma 4.4 guarantees that  $kS - kS$  contains a subspace of size at least

$$2^{-32\sigma^{-1/(k-1)} \log(1/\sigma)} |A| = 2^{-128B(4k)^{4B/(k-1)} \log(4k)} |A| \geq 2^{-CB \log B} |A|,$$

for some absolute constant  $C$ . Since  $kS - kS \cong_2 kA - kA$ , this means that  $kA - kA$  also contains a subspace of this size, which we shall call  $H$ .

Now by assumption we have

$$|A + H| \leq |(k+1)A - kA| \leq (2k+1)^B |A| \leq 2^{C'B \log B} |H|,$$

and so by Lemma 1.2 we may find  $X$ ,  $|X| \leq 2^{C'B \log B}$ , such that  $A \subseteq X + H - H$ . Thus  $A$  is indeed contained in the union of  $2^{C'B \log B}$  cosets of some subspace of size at most  $|A|$ .  $\square$

## REFERENCES

- [1] A. Balog and E. Szemerédi, *A statistical theorem of set addition*, *Combinatorica* **14** (1994), no. 3, 263–268.
- [2] J. Bourgain, *On the dimension of Kakeya sets and related maximal inequalities*, *GAFA* **9** (1999), no. 2, 256–282.
- [3] M. C. Chang, *A polynomial bound in Freiman’s theorem*, *Duke Math. J.* **113** (2002), no. 3, 399–419.
- [4] ———, *On problems of Erdős and Rudin*, *J. Funct. Anal.* **207** (2004), no. 2, 444–460.
- [5] G. Freiman, *Foundations of a Structural Theory of Set Addition*, *Translations of Mathematical Monographs* **37**, Amer. Math. Soc., Providence, RI, USA, 1973.
- [6] W. T. Gowers, *A new proof of Szemerédi’s theorem for progressions of length four*, *GAFA* **8** (1998), no. 3, 529–551.
- [7] ———, *Rough structure and classification*, *GAFA 2000* (Tel Aviv, 1999), Special Volume, Part I, 79–117.
- [8] B. J. Green, *Finite field models in additive combinatorics*, submitted to *Surveys in Combinatorics* 2005.
- [9] ———, *Edinburgh lecture notes on Freiman’s theorem*, notes. Available at <http://www.dpms.cam.ac.uk/~bjg23/>
- [10] ———, *Restriction and Kakeya Phenomena*, notes from a course given in Part III of the Mathematical Tripos, Cambridge University 2002. Available at <http://www.dpms.cam.ac.uk/~bjg23/>
- [11] B. J. Green and I. Z. Ruzsa, *Sets with small sumset and rectification*, preprint.
- [12] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, *Graduate Texts in Mathematics*, 165. Springer-Verlag, New York, 1996.
- [13] H. Plünnecke, *Eigenschaften und Abschätzungen von Wirkingsfunktionen*, *BMwF-GMD-22 Gesellschaft für Mathematik und Datenverarbeitung*, Bonn 1969
- [14] I. Z. Ruzsa, *An analog of Freiman’s theorem in groups*, *Structure theory of set addition. Astérisque* **258** (1999), xv, 323–326.

- [15] ———, *Generalized arithmetical progressions and sumsets*, Acta Math. Hungar. **65** (1994), no. 4, 379–388.
- [16] ———, *An application of graph theory to additive number theory*, Scientia, Ser. A **3** (1989), 97–109
- [17] ———, *Sumsets*, submitted to proceedings of the European Congress of Mathematicians, Stockholm 2004.
- [18] T. C. Tao and V. Vu, *Additive Combinatorics*, book in preparation.

TRINITY COLLEGE, CAMBRIDGE, CB2 1TQ  
*E-mail address:* `bjg23@hermes.cam.ac.uk`