Combinatorics, Probability and Computing (2008) 17, 297–305. © 2007 Cambridge University Press
doi:10.1017/S0963548307008644 First published online 5 July 2007 Printed in the United Kingdom

A Note on Freĭman's Theorem in Vector Spaces

T. SANDERS

Department of Pure Mathematics and Mathematical Statistics,
Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WA, UK
(e-mail: tsanders@dpmms.ac.uk)

Received 14 December 2005; revised 10 April 2007

A famous result of Freĭman describes the sets A, of integers, for which $|A+A| \leqslant K|A|$. In this short note we address the analogous question for subsets of vector spaces over $\mathbb{F}_2$. Specifically we show that if A is a subset of a vector space over $\mathbb{F}_2$ with $|A+A| \leqslant K|A|$ then A is contained in a coset of size at most $2^{O(K^{3/2}\log K)}|A|$, which improves upon the previous best, due to Green and Ruzsa, of $2^{O(K^2)}|A|$. A simple example shows that the size may need to be at least $2^{\Omega(K)}|A|$.

1. Introduction

If A and B are subsets of an abelian group G then we define the *sumset*, $A+B$, to be the set of all elements formed by adding an element of A to an element of B, *i.e.*, $A+B = \{a+b : a \in A \text{ and } b \in B\}$. There is a famous result of Freĭman [4] which in some sense describes the sets $A \subset \mathbb{Z}$ for which $|A+A| \leqslant K|A|$. This note concerns what in modern parlance would be called the finite field analogue of Freĭman's result. Specifically it concerns the following theorem.

Theorem 1.1 (finite Field Freĭman). *Suppose that G is a vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ is a finite set with $|A+A| \leqslant K|A|$. Then A is contained in a coset of size at most $f(K)|A|$.*

While finite field models are an important tool for understanding problems in general abelian groups, this result has independent significance in coding theory and has been pursued by a number of authors. We do not attempt a comprehensive survey here, but mention a few papers which are important from our standpoint.

The paper [3] of Deshouillers, Hennecart and Plagne provides an overview of the problem and records a quantitative version of Theorem 1.1 due to Ruzsa; it is a relatively simple argument which shows that one may take $f(K) \leqslant K2^{\lfloor K^3 \rfloor - 1}$. The bulk of their paper concerns refined estimates for the case when K is small; by contrast our interest lies in the asymptotics.

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

In a recent paper of Green and Ruzsa [5], the authors improve Ruzsa's bound from [3] when they show that one may take $f(K) \leqslant K^2 2^{\lfloor 2K^2 - 2 \rfloor}$. In this note we refine this further by proving that one may take $f(K) \leqslant 2^{O(K^{3/2}\log K)}$. Formally, then, we shall prove the following theorem.

Theorem 1.2. *Suppose that G is a vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ is a finite set with $|A+A| \leqslant K|A|$. Then A is contained in a coset of size at most $2^{O(K^{3/2}\log K)}|A|$.*

For comparison we record the following well-known example. Let H be a finite subgroup of G and let $g_1 + H, \dots, g_{K-1} + H$ be $K-1$ linearly independent cosets of H in the quotient space G/H. Let A be the union of H and the representatives $g_1, \dots, g_{K-1}$. Then $|A| = |H| + K - 1 \sim |H|$ and

$$|A+A| = K(|H| + (K-1)/2) \sim K|H| \lesssim K|A|.$$

However, A contains a linearly independent set of size $\dim H + K - 1$, and so A is not contained in a coset of dimension less than $\dim H + K - 2$; hence, if H' is a coset containing A, then

$$|H'| \geqslant 2^{\dim H + K - 2} = 2^{K-2}|H| \gtrsim 2^{K-2}|A|.$$

This example perhaps suggests that one could take $f(K) \leqslant 2^{O(K)}$ in Theorem 1.1. In fact there are other more compelling reasons to believe this; however, it does not seem to reflect the underlying situation. This concern is addressed by the polynomial Freĭman–Ruzsa conjecture (attributed to Marton in [9]) which, if true, seems to have some very important applications. For a discussion of this see the book [11] of Tao and Vu.

2. Proof of Theorem 1.2

In [6], Green and Ruzsa extended Ruzsa's proof of Freĭman's theorem to arbitrary abelian groups. Our proof is a refinement of theirs.

Their method becomes significantly simpler in the vector space setting, and would immediately give us the following weak version of the main theorem.

Theorem 2.1. *Suppose that G is a vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ is a finite set with $|A+A| \leqslant K|A|$. Then A is contained in a coset of size at most $2^{O(K^2\log K)}|A|$.*

The proof involves three main steps. Our refinement occurs at the second of these; the other two are the same as in previous work.

- **Finding a good model.** First we use the fact that $|A+A| \leqslant K|A|$ to show that A can be embedded as a *dense* subset of $\mathbb{F}_2^n$ in a way which preserves much of its additive structure.
- **Bogolioùboff's argument.** Next we show that if A is a dense subset of a finite-dimensional vector space over $\mathbb{F}_2$ and $A+A$ is not much bigger than A, then $2A-2A$ contains a large subspace.
- **Pullback and covering.** Finally we use our embedding to pull back this subspace to a coset in the original setting. A covering argument then gives us the result.

In the remainder of the note we follow through this programme.

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

2.1. Finding a good model

The appropriate notion of structure preserving was introduced by Freĭman in [4]; we record the definition now. If G and G' are two abelian groups containing the sets A and A' respectively, then we say that $\phi : A \to A'$ is a *Freĭman s-homomorphism* if, whenever $a_1, \dots, a_s, b_1, \dots, b_s \in A$ satisfy

$$a_1 + \cdots + a_s = b_1 + \cdots + b_s,$$

we have

$$\phi(a_1) + \cdots + \phi(a_s) = \phi(b_1) + \cdots + \phi(b_s).$$

If ϕ has an inverse which is also an s-homomorphism, then we say that ϕ is a *Freĭman s-isomorphism*.

A simple but elegant argument of Green and Ruzsa establishes the existence of a small vector space into which we can embed our set via a Freĭman isomorphism. Specifically they prove the following proposition.

Proposition 2.2 ([6], Proposition 6.1). *Suppose that A is a subset of a vector space over $\mathbb{F}_2$. Suppose that $|A + A| \leqslant K|A|$. Then there is a vector space G' over $\mathbb{F}_2$ with $|G'| \leqslant K^{2s}|A|$, a set $A' \subset G'$, and a Freĭman s-isomorphism $\phi : A \to A'$.*

2.2. Bogolioùboff's argument

In this section we show that if A is a subset of a finite-dimensional vector space over $\mathbb{F}_2$ then $2A - 2A$ contains a large subspace. Originally (in [8]) Ruzsa employed an argument of Bogolioùboff with the Fourier transform. This was refined by Chang in [2], and the improvement of this note rests on a further refinement. We shall need some notation for the Fourier transform and we record this now.

Suppose that G is a finite-dimensional vector space over $\mathbb{F}_2$. We write $\widehat{G}$, called the dual group, for the set of functions

$$x \mapsto (-1)^{r.x} \quad \text{for } r \in G.$$

Here, of course, $r.x := r_1x_1 + \cdots + r_nx_n$. These functions are sometimes called characters or Walsh functions, and form a basis for the space of functions on G. As we shall see formally in a moment, the Fourier transform just writes functions in this basis.

We write μ_G for the Haar probability measure, or normalized counting measure on G, that is, the measure assigning to a set X mass $|X|/|G|$. If $V \leqslant G$ we shall typically identify μ_V with $\chi_V.\mu_G$ rescaled to have unit mass.

Haar measure is used to define the Fourier transform on functions $f : G \to \mathbb{C}$ by

$$\widehat{f} : \widehat{G} \to \mathbb{C}; \gamma \mapsto \int f(x)\gamma(x)d\mu_G(x);$$

slightly less formally,

$$\widehat{f}(r) = \frac{1}{|G|}\sum_{x \in G} f(x)(-1)^{r.x},$$

where we are identifying r with the map $x \mapsto (-1)^{r.x}$.

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

The reason we have normalized in the way we have is so that the Fourier inversion theorem takes the form

$$f(x) = \sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\gamma(x) \quad \text{for all } f : G \to \mathbb{C};$$

and Plancherel's theorem takes the form

$$\langle f, g\rangle := \int f(x)g(x)d\mu_G(x) = \sum_{\gamma \in \widehat{G}} \widehat{f}(\gamma)\widehat{g}(\gamma) \quad \text{for all } f, g : G \to \mathbb{C}.$$

Parseval's theorem is the special case $f = g$ of Plancherel's theorem.

These results are actually all we shall need from the general theory of the Fourier transform; however, for those interested, a more detailed exposition can be found in Rudin [7].

In [2] Chang proved the following result. (Although in [2] it is stated for $\mathbb{Z}/N\mathbb{Z}$, the same proof applies to any compact abelian group and in particular to finite-dimensional vector spaces over $\mathbb{F}_2$.)

Proposition 2.3. *Suppose that G is a finite-dimensional vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ has density α and $\mu_G(A + A) \leqslant K\mu_G(A)$. Then $2A - 2A$ contains a subspace of codimension $O(K \log \alpha^{-1})$.* □

The next proposition is our refinement of the above.

Proposition 2.4. *Suppose that G is a finite-dimensional vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ has density α and $\mu_G(A + A) \leqslant K\mu_G(A)$. Then $2A - 2A$ contains a subspace of codimension $O(K^{1/2} \log \alpha^{-1})$.* □

To prove this we require the following *pure density* version of the proposition.

Proposition 2.5 ([10], Theorem 2.4). *Suppose that G is a finite-dimensional vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ has density α. Then $2A - 2A$ contains a subspace of codimension $O(\alpha^{-1/2})$.*

The proof in [10] is significantly simpler in the vector space setting. Since the ideas are important we include the proof here; the basic technique is iterative.

Lemma 2.6 (Iteration lemma). *Suppose that G is a finite-dimensional vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ has density α. Then at least one of the following is true.*

(i) *$2A - 2A$ contains all of G.*

(ii) *There is a subspace V of $\widehat{G}$ with dimension 1, an element $x \in G$ and a set $A' \subset V^{\perp}$ with the following properties:*

- $x + A' \subset A$,
- $\mu_{V^{\perp}}(A') \geqslant \alpha(1 + 2^{-1}\alpha^{1/2})$.

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

Proof. As usual with problems of this type, studying the sumset $2A - 2A$ is difficult, so we turn instead to $g := \chi_A * \chi_A * \chi_{-A} * \chi_{-A}$, which has support equal to $2A - 2A$. One can easily compute the Fourier transform of g in terms of that of χ_A:

$$\widehat{g}(\gamma) = |\widehat{\chi_A}(\gamma)|^4 \quad \text{for all } \gamma \in \widehat{G},$$

from which it follows that g is very smooth. Specifically,

$$\begin{aligned}\sum_{\gamma\in\widehat{G}} |\widehat{g}(\gamma)|^{\frac{1}{2}} &= \sum_{\gamma\in\widehat{G}} |\widehat{\chi_A}(\gamma)|^2 \\ &= \alpha \quad \text{by Parseval's theorem.} \end{aligned} \tag{2.1}$$

We may assume that $\mu_G(2A - 2A) < 1$ since otherwise we are in the first case of the lemma, so $S := (2A - 2A)^c$ has positive density, say σ. Plancherel's theorem gives

$$0 = \langle \chi_S, g\rangle = \sum_{\gamma\in\widehat{G}} \overline{\widehat{\chi_S}(\gamma)}\widehat{g}(\gamma),$$

which implies that

$$|\widehat{\chi_S}(0_{\widehat{G}})\widehat{g}(0_{\widehat{G}})| \leqslant \sum_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_S}(\gamma)\widehat{g}(\gamma)|.$$

Then $\widehat{g}(0_{\widehat{G}}) = \alpha^4$, $\widehat{\chi_S}(0_{\widehat{G}}) = \sigma$ and $|\widehat{\chi_S}(\gamma)| \leqslant \|\chi_S\|_1 = \sigma$, so the above yields

$$\sigma\alpha^4 \leqslant \sigma \sum_{\gamma\neq 0_{\widehat{G}}} |\widehat{g}(\gamma)|,$$

which, in turn, implies that

$$\alpha^4 \leqslant \sum_{\gamma\neq 0_{\widehat{G}}} |\widehat{g}(\gamma)| \quad \text{since } \sigma > 0.$$

Finding a non-trivial character at which $\widehat{g}$ is large is now simple, since $\widehat{g} \in \ell^{\frac{1}{2}}(\widehat{G})$, and

$$\alpha^4 \leqslant \max_{\gamma\neq 0_{\widehat{G}}} |\widehat{g}(\gamma)|^{\frac{1}{2}} \left(\sum_{\gamma\in\widehat{G}} |\widehat{g}(\gamma)|^{\frac{1}{2}} \right) \leqslant \max_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_A}(\gamma)|^2.\alpha$$

by (2.1). Rearranging this we have

$$\max_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_A}(\gamma)| \geqslant \alpha^{\frac{3}{2}}.$$

Let γ be a character for which this maximum is attained. We now proceed with a standard L^∞-density-increment argument. Let $V := \{0_{\widehat{G}}, \gamma\}$ and $f := \chi_A - \alpha$. Then

$$\int f * \mu_{V^\perp} d\mu_G = 0 \quad \text{and} \quad \|f * \mu_{V^\perp}\|_1 \geqslant \|\widehat{f}\widehat{\mu_{V^\perp}}\|_\infty = |\widehat{\chi_A}(\gamma)|.$$

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

Adding these we conclude that

$$\begin{aligned}|\widehat{\chi_A}(\gamma)| &\leqslant 2\int (f * \mu_{V^\perp})_+ d\mu_G \\ &= 2\int (\chi_A * \mu_{V^\perp} - \alpha)_+ d\mu_G \\ &\leqslant 2(\|\chi_A * \mu_{V^\perp}\|_\infty - \alpha).\end{aligned}$$

Thus there is some $x \in G$ with

$$\chi_A * \mu_{V^\perp}(x) = \|\chi_A * \mu_{V^\perp}\|_\infty \geqslant \alpha(1 + 2^{-1}\alpha^{1/2}).$$

The result follows on taking $A' = x + A$. □

Proof of Proposition 2.5. We define a nested sequence of subspaces $V_0 \leqslant V_1 \leqslant \cdots \leqslant \widehat{G}$, elements $x_k \in V_k^\perp$ and subsets A_k of $V_k^\perp$ with density α_k, such that $x_k + A_k \subset A_{k-1}$. We begin the iteration with $V_0 := \{0_{\widehat{G}}\}$, $A_0 := A$ and $x_0 = 0_G$.

Suppose that we are at stage k of the iteration. If $\mu_{V_k^\perp}(2A_k - 2A_k) < 1$ then we apply Lemma 2.6 to A_k considered as a subset of $V_k^\perp$. We get a vector space V_{k+1} with $\dim V_{k+1} = 1 + \dim V_k$, an element $x_{k+1} \in G$ and a set A_{k+1} such that

$$x_{k+1} + A_{k+1} \subset A_k \quad \text{and} \quad \alpha_{k+1} \geqslant \alpha_k(1 + 2^{-1}\alpha_k^{1/2}).$$

It follows from the density increment that if $m_k = 2\alpha_k^{-1/2}$ then $\alpha_{k+m_k} \geqslant 2\alpha_k$. Define the sequence $(N_l)_l$ recursively by $N_0 = 0$ and $N_{l+1} = m_{N_l} + N_l$. The density α_{N_l} is easily estimated:

$$\alpha_{N_l} \geqslant 2^l\alpha \quad \text{and} \quad N_l \leqslant \sum_{s=0}^{l} 2\alpha_{N_s}^{-1/2} \leqslant 2\alpha^{-1/2}\sum_{s=0}^{l} 2^{-s/2} = O(\alpha^{-1/2}).$$

Since density cannot be greater than 1 there is some stage k with $k = O(\alpha^{-1/2})$ when the iteration cannot proceed, *i.e.*, for which $2A_k - 2A_k$ contains all of $V_k^\perp$. By construction of the A_ks there is a translate of A_k which is contained in $A_0 = A$ and hence $2A_k - 2A_k$ is contained in $2A - 2A$. It follows that $2A - 2A$ contains a subspace of G of codimension $k = O(\alpha^{-1/2})$. □

The key ingredient in the proof of Proposition 2.4 is the following iteration lemma, which has a number of similarities with Lemma 2.6.

Lemma 2.7. *Suppose that G is a finite-dimensional vector space over $\mathbb{F}_2$. Suppose that $A, B \subset G$ have $\mu_G(A + B) \leqslant K\mu_G(B)$. Write α for the density of A. Then at least one of the following is true.*

(i) *B contains a subspace of codimension $O(K^{1/2})$.*

(ii) *There is a subspace V of $\widehat{G}$ with dimension 1, elements $x, y \in G$ and sets $A', B' \subset V^\perp$ with the following properties:*

- *$x + A' \subset A$ and $y + B' \subset B$,*
- *$\mu_{V^\perp}(A') \geqslant \alpha(1 + 2^{-3/2}K^{-1/2})$,*
- *$\mu_{V^\perp}(A' + B') \leqslant K\mu_{V^\perp}(B')$.*

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

Proof. If $\mu_G(B) \geqslant (2K)^{-1}$ then we apply Proposition 2.5 to get that B contains a subspace of codimension $O(K^{1/2})$ and we are in the first case of the lemma. Hence we assume that $\mu_G(B) \leqslant (2K)^{-1}$.

Write β for the density of B. We have

$$\begin{aligned}(\alpha\beta)^2 &= \left(\int \chi_A * \chi_B d\mu_G\right)^2 \\ &\leqslant \mu_G(A+B)\int (\chi_A * \chi_B)^2 d\mu_G \quad \text{by Cauchy–Schwarz} \\ &\leqslant K\beta \int (\chi_A * \chi_B)^2 d\mu_G \quad \text{by hypothesis} \\ &= K\beta \sum_{\gamma\in\widehat{G}} |\widehat{\chi_A}(\gamma)|^2 |\widehat{\chi_B}(\gamma)|^2 \quad \text{by Parseval's theorem.} \end{aligned} \tag{2.2}$$

The main term in the sum on the right is the contribution from the trivial character, in particular

$$|\widehat{\chi_A}(0_{\widehat{G}})|^2 |\widehat{\chi_B}(0_{\widehat{G}})|^2 = \alpha^2\beta^2,$$

while

$$\begin{aligned}\sum_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_A}(\gamma)|^2 |\widehat{\chi_B}(\gamma)|^2 &\leqslant \max_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_A}(\gamma)|^2 \sum_{\gamma\in\widehat{G}} |\widehat{\chi_B}(\gamma)|^2 \\ &= \beta \max_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_A}(\gamma)|^2 \quad \text{by Parseval's theorem for } \chi_B.\end{aligned}$$

Putting these last two observations in (2.2) gives

$$\alpha^2\beta^2 \leqslant K\beta^3\alpha^2 + K\beta^2 \max_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_A}(\gamma)|^2.$$

Since $K\beta \leqslant 2^{-1}$ we can rearrange this to conclude that

$$\max_{\gamma\neq 0_{\widehat{G}}} |\widehat{\chi_A}(\gamma)| \geqslant (2K)^{-1/2}\alpha.$$

Let γ be a character for which this maximum is attained. We now proceed with a standard L^∞-density-increment argument. Let $V := \{0_{\widehat{G}}, \gamma\}$ and $f := \chi_A - \alpha$. Then

$$\int f * \mu_{V^\perp} d\mu_G = 0 \quad \text{and} \quad \|f * \mu_{V^\perp}\|_1 \geqslant \|\widehat{f}\widehat{\mu_{V^\perp}}\|_\infty = |\widehat{\chi_A}(\gamma)|.$$

Adding these we conclude that

$$\begin{aligned}|\widehat{\chi_A}(\gamma)| &\leqslant 2\int (f * \mu_{V^\perp})_+ d\mu_G \\ &= 2\int (\chi_A * \mu_{V^\perp} - \alpha)_+ d\mu_G \\ &\leqslant 2(\|\chi_A * \mu_{V^\perp}\|_\infty - \alpha).\end{aligned}$$

Thus there is some $x \in G$ with

$$\chi_A * \mu_{V^\perp}(x) \geqslant \alpha(1 + 2^{-3/2}K^{-1/2}).$$

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

Let $x' + V^\perp := G \setminus (x + V^\perp)$ be the *other* coset of $V^\perp$ in G. Write $A_1 = A \cap (x + V^\perp)$, $B_1 = B \cap (x + V^\perp)$ and $B_2 = B \cap (x' + V^\perp)$. Now $A_1 \subset A$ so

$$(A_1 + B_1) \cup (A_1 + B_2) \subset A + B_1 \cup B_2,$$

and $A_1 + B_1 \subset V^\perp$ while $A_1 + B_2 \subset x + x' + V^\perp$ so these two sets are disjoint and we conclude that

$$\begin{aligned}\mu_G(A_1 + B_1) + \mu_G(A_1 + B_2) &= \mu_G((A_1 + B_1) \cup (A_1 + B_2)) \\ &\leqslant \mu_G(A + B_1 \cup B_2) \\ &\leqslant K\mu_G(B_1 \cup B_2) \quad \text{by hypothesis} \\ &\leqslant K(\mu_G(B_1) + \mu_G(B_2)).\end{aligned}$$

Hence, by averaging, there is some i such that

$$\mu_G(A_1 + B_i) \leqslant K\mu_G(B_i).$$

We take $A' = x + A_1$ and, if $i = 1$, $B' = x + B_1$ and $y = x$, while if $i = 2$, $B' = x' + B_2$ and $y = x'$. The result follows. □

Proof of Proposition 2.4. We define a nested sequence of finite-dimensional subspaces $V_0 \leqslant V_1 \leqslant \cdots \leqslant \widehat{G}$, elements $x_k, y_k \in V_k^\perp$, and subsets A_k and B_k of $V_k^\perp$ such that $A_k + x_k \subset A_{k-1}$ and $B_k + y_k \subset B_{k-1}$ and $\mu_{V_k^\perp}(A_k + B_k) \leqslant K\mu_{V_k^\perp}(B_k)$. We write α_k for the density of A_k in $V_k^\perp$. Begin the iteration with $V_0 := \{0_{\widehat{G}}\}$, $B_0 = A_0 := A$ and $x_0 = y_0 = 0_G$.

Suppose that we are at stage k of the iteration. We apply Lemma 2.7 to A_k and B_k inside $V_k^\perp$ (which we can do since $\mu_{V_k^\perp}(A_k + B_k) \leqslant K\mu_{V_k^\perp}(B_k)$). It follows that either $2B_k - 2B_k$ contains a subspace of codimension $O(K^{1/2})$ in $V_k^\perp$ or we get a subspace $V_{k+1} \leqslant \widehat{V_k}$ with $\dim V_{k+1} = 1 + \dim V_k$, elements $x_{k+1}, y_{k+1} \in V_k^\perp$ and sets A_{k+1} and B_{k+1} with the following properties:

- $x_{k+1} + A_{k+1} \subset A_k$ and $y_{k+1} + B_{k+1} \subset B_k$,
- $\mu_{V^\perp}(A_{k+1}) \geqslant \alpha_k(1 + 2^{-3/2}K^{-1/2})$,
- $\mu_{V^\perp}(A_{k+1} + B_{k+1}) \leqslant K\mu_{V^\perp}(B_{k+1})$.

It follows from the density increment that if $m = 2^{3/2}K^{1/2}$ then $\alpha_{k+m} \geqslant 2\alpha_k$, and hence the iteration must terminate (because density can be at most 1) at some stage k with $k = O(K^{1/2}\log\alpha^{-1})$. The iteration terminates if $2B_k - 2B_k$ contains a subspace of codimension $O(K^{1/2})$ in $V_k^\perp$, from which it follows that $2A - 2A \supset 2B_k - 2B_k$ contains a subspace of codimension $k + O(K^{1/2}) = O(K^{1/2}\log\alpha^{-1})$. □

2.3. Pullback and covering

We now complete the proof of the main theorem using a covering argument.

We are given $A \subset G$ finite with $|A + A| \leqslant K|A|$. By Proposition 2.2 there is a finite vector space G' with $|G'| \leqslant K^{16}|A|$ and a subset A' with A' Freĭman 8-isomorphic to A. It follows that

$$\mu_{G'}(A') \geqslant K^{-16} \quad \text{and} \quad \mu_{G'}(A' + A') \leqslant K\mu_{G'}(A').$$

We apply Proposition 2.4 to conclude that $2A' - 2A'$ contains a subspace whose codimension is $O(K^{1/2}\log K)$. However, A is 8-isomorphic to A' so $2A - 2A$ is 2-isomorphic to $2A' - 2A'$ and it is easy to check that the 2-isomorphic pullback of a subspace is a coset so $2A - 2A$ contains a

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press

coset of size

$$2^{-O(K^{1/2}\log K)}|G'| \geqslant 2^{-O(K^{1/2}\log K)}|A|.$$

The following covering result of Chang [2] converts this large coset contained in $2A - 2A$ into a small coset containing A. It is true in more generality than we state; we only require the version below.

Proposition 2.8. *Suppose that G is a vector space over $\mathbb{F}_2$. Suppose that $A \subset G$ is a finite set with $|A + A| \leqslant K|A|$. Suppose that $2A - 2A$ contains a coset of size $\eta|A|$. Then A is contained in a coset of size at most $2^{O(K\log K\eta^{-1})}|A|$.* □

Theorem 1.2 follows immediately from this proposition and the argument preceding it.

3. Concluding remarks

It is worth making a couple of concluding remarks. First, all the implicit constants in the work are effective; however, they are not particularly neat or significant so it does not seem to be important to calculate them. Secondly, and more importantly, it seems likely that one could modify Proposition 2.4 to fall within the more general framework of approximate groups pioneered by Bourgain in [1]. It does not seem that this would lead to any improvement in Freĭman's theorem for $\mathbb{Z}$, essentially because of the need to narrow the Bohr sets at each stage of the iteration.

Acknowledgements

I should like to thank Tim Gowers and Ben Green for encouragement and supervision and an anonymous referee for helpful expository suggestions.

References

[1] Bourgain, J. (1999) On triples in arithmetic progression. *Geom. Funct. Anal.* **9** 968–984.
[2] Chang, M.-C. (2002) A polynomial bound in Freĭman's theorem. *Duke Math. J.* **113** 399–419.
[3] Deshouillers, J.-M., Hennecart, F. and Plagne, A. (2004) On small sumsets in $(\mathbb{Z}/2\mathbb{Z})^n$. *Combinatorica* **24** 53–68.
[4] Freĭman, G. A. (1973) *Foundations of a Structural Theory of Set Addition*, Vol. 37 of *Translations of Mathematical Monographs*, AMS, Providence, RI. Translated from the Russian.
[5] Green, B. J. and Ruzsa, I. Z. (2006) Sets with small sumset and rectification. *Bull. London Math. Soc.* **38** 43–52.
[6] Green, B. J. and Ruzsa, I. Z. (2007) Freĭman's theorem in an arbitrary abelian group. *J. London Math. Soc.*, **75** 163–75.
[7] Rudin, W. (1962) *Fourier Analysis on Groups*, Vol. 12 of *Interscience Tracts in Pure and Applied Mathematics*, Wiley–Interscience.
[8] Ruzsa, I. Z. (1994) Generalized arithmetical progressions and sumsets. *Acta Math. Hungar.* **65** 379–388.
[9] Ruzsa, I. Z. (1999) An analog of Freĭman's theorem in groups. In *Structure Theory of Set-Addition. Astérisque* **258** 323–326.
[10] Sanders, T. Additive structures in sumsets. Preprint. `math.NT/0605520`. *Math. Proc. Cambridge Philos. Soc.*, to appear.
[11] Tao, T. C. and Vu, V. H. (2006) *Additive Combinatorics*, Vol. 105 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press.

https://doi.org/10.1017/S0963548307008644 Published online by Cambridge University Press