*J. Aust. Math. Soc.* **86** (2009), 61–74
doi:10.1017/S1446788708000359

# A NOTE ON THE FREIMAN AND BALOG–SZEMERÉDI–GOWERS THEOREMS IN FINITE FIELDS

**BEN GREEN ✉ and TERENCE TAO**

(Received 2 November 2006; accepted 12 November 2007)

Communicated by I. E. Shparlinski

## Abstract

We prove quantitative versions of the Balog–Szemerédi–Gowers and Freiman theorems in the model case of a finite field geometry $\mathbb{F}_2^n$, improving the previously known bounds in such theorems. For instance, if $A \subseteq \mathbb{F}_2^n$ is such that $|A + A| \leqslant K|A|$ (thus $A$ has small additive doubling), we show that there exists an affine subspace $H$ of $\mathbb{F}_2^n$ of cardinality $|H| \gg K^{-O(\sqrt{K})}|A|$ such that $|A \cap H| \geqslant (2K)^{-1}|H|$. Under the assumption that $A$ contains at least $|A|^3/K$ quadruples with $a_1 + a_2 + a_3 + a_4 = 0$, we obtain a similar result, albeit with the slightly weaker condition $|H| \gg K^{-O(K)}|A|$.

2000 *Mathematics subject classification*: primary 11B99.

*Keywords and phrases*: Freiman's theorem, finite field models, Balog–Szemerédi–Gowers theorem.

## 1. Introduction

In this paper we will be working with the group $\mathbb{F}_2^n$, the vector space of dimension $n$ over the two-element field $\mathbb{F}_2$. This serves as a convenient model setting in which to do additive combinatorics.

If $A, B \subseteq \mathbb{F}_2^n$ are two sets, then we define their sumset $A + B$ to be the set of all pairwise sums $a + b$ with $a \in A$, $b \in B$. A fundamental result concerning sumsets is the following theorem of Ruzsa [8].

THEOREM 1.1 (Ruzsa's analogue of Freiman's theorem). *Let $K \geqslant 1$ be an integer, and suppose that $A \subseteq \mathbb{F}_2^n$ is a set with $|A + A| \leqslant K|A|$. Then $A$ is contained in a subspace $H \leqslant \mathbb{F}_2^n$ with $|H| \leqslant F(K)|A|$, for some $F(K)$ depending only on $K$.*

The first author is a Clay Research Fellow, and is pleased to acknowledge the support of the Clay Mathematics Institute. The second author is supported by a grant from the MacArthur Foundation.

© 2009 Australian Mathematical Society 1446-7887/2009 $16.00

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

Ruzsa proved this result with $F(K) = K^2 2^{K^4}$. This was then improved by Sanders [9], who obtained[1] $F(K) = 2^{O(K^{3/2} \log K)}$. In a recent preprint [7] the present authors obtain the bound $F(K) = 2^{2K+o(K)}$. This is tight apart from the $o(K)$ term, as can be seen by considering the rather trivial example in which $A$ consists of independent vectors $\{e_1, \dots, e_n\}$ with $n \sim 2K$.

It was already pointed out in [8] that Theorem 1.1 does not quite have the form one would like. Attempting to put *all* of $A$ inside a subspace $H$ is inefficient, as the preceding trivial example illustrates. If one is prepared to place just a portion of $A$ inside a subspace, then conjecturally it is possible to do much better. The following conjecture is attributed in [8] to Marton.

CONJECTURE 1.2 (Polynomial Freiman–Ruzsa conjecture). *Suppose that $K \geqslant 1$ and that $A \subseteq \mathbb{F}_2^n$ has $|A + A| \leqslant K|A|$. Then there is a subspace $H$ of $\mathbb{F}_2^n$ such that $|H| \ll K^{O(1)}|A|$ and $|A \cap H| \gg K^{-O(1)}|A|$.*

It follows from standard covering results in additive combinatorics (see for example [10, Ch. 2]) that $A$ is in fact covered by $K^{O(1)}$ translates of $H$. We will not discuss Conjecture 1.2 any further here: the survey [4] has more information.

It was implicitly observed by Gowers [3, Ch. 7] and then by the authors [6, Ch. 6] that a weak version of Conjecture 1.2 essentially follows from the ideas of Ruzsa [8] on Freiman's theorem in $\mathbb{Z}$. This result was written down (with a somewhat more complicated proof than necessary) in [5].

THEOREM 1.3 (Intersection version of Freiman's theorem in $\mathbb{F}_2^n$). *Suppose that $K \geqslant 1$ and that $A \subseteq \mathbb{F}_2^n$ has $|A + A| \leqslant K|A|$. Then there is a subspace $H$ of $\mathbb{F}_2^n$ with $|H| \ll K^{O(1)}|A|$ such that $|A \cap H| \gg \exp(-K^{O(1)})|A|$.*

This result, of course, is the same as Conjecture 1.2 except that $|A \cap H|/|A|$ may now be exponentially small in $K$. Our first main aim in this paper is to obtain a rather precise version of this result.

THEOREM 1.4 (First main theorem). *Let $K \geqslant 1$, and let $A, B \subseteq \mathbb{F}_2^n$ be such that $|A + B| \leqslant K|A|^{1/2}|B|^{1/2}$. Then there exists a linear subspace $H \subseteq \mathbb{F}_2^n$ with $|H| \gg K^{-O(\sqrt{K})}|A|$ and $x, y \in \mathbb{F}_2^n$ such that*

$$|A \cap (x + H)|^{1/2}|B \cap (y + H)|^{1/2} \geqslant \frac{1}{2K}|H|.$$

REMARK. We note that the small doubling condition implies that $K^{-2}|A| \leqslant |B| \leqslant K^2|A|$, and so we also have $|H| \gg K^{-O(\sqrt{K})}|B|$.

The idea of working with two sets $A, B$ instead of one turns out (for inductive reasons) to be essential to the argument; this idea was suggested to us by Tom Sanders. It has the following easy corollary.

[1] As usual we use $X = O(Y)$ or $X \ll Y$ to denote an estimate of the form $X \leqslant CY$ for some absolute constant $C$.

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

COROLLARY 1.5. *Let $A \subset \mathbb{F}_2^n$ be such that $|A+A| \leqslant K|A|$ for some $K \geqslant 1$. Then there exist a subspace $H \subseteq \mathbb{F}_2^n$ and $x \in \mathbb{F}_2^n$ such that $|H| \gg K^{-O(\sqrt{K})}|A|$ and $|A \cap (x+H)| \geqslant |H|/2K$.*

Results of Freiman type are particularly powerful when applied in conjunction with statements of Balog–Szemerédi type. These results state that if a set $A$ has some weak 'statistical' additive structure (usually $A$ is assumed to have many *additive quadruples*, that is, quadruples $(a_1, a_2, a_3, a_4) \in A^4$ with $a_1 + a_2 = a_3 + a_4$) then there is a large subset $A' \subseteq A$ for which $|A' + A'|$ is small. Such an application was first made in [1]. A major advance was made by Gowers [2], who proved a result of Balog–Szemerédi type with good quantitative bounds.

THEOREM 1.6 (Balog–Szemerédi–Gowers theorem). *Let $G$ be any abelian group, and suppose that $A \subseteq G$ is a finite set with at least $|A|^3/K$ additive quadruples. Then there is $A' \subseteq A$ with $|A'| \gg K^{-O(1)}|A|$ such that $|A' + A'| \ll K^{O(1)}|A'|$.*

This theorem is now proven in many places in the literature, see for instance [10, Theorem 2.29]. In combination with Theorem 1.3, the Balog–Szemerédi–Gowers theorem implies the following result.

THEOREM 1.7 (Balog–Szemerédi–Gowers–Freiman theorem in $\mathbb{F}_2^n$). *Suppose that $A \subseteq \mathbb{F}_2^n$ is a set with at least $|A|^3/K$ additive quadruples. Then there is a subspace $H$ of $\mathbb{F}_2^n$ with $|H| \gg \exp(-K^{O(1)})|A|$ and an $x \in \mathbb{F}_2^n$ such that $|A \cap (x+H)| \gg \exp(-K^{O(1)})|H|$.*

Our second main aim in this paper is to prove a more precise version of this latter result. We shall first need some notation.

DEFINITION 1.8 (Normalized energy). Given any nonempty sets $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$, define the *normalized energy*

$$\omega(A_1, A_2, A_3, A_4) := \frac{|\{(a_1, a_2, a_3, a_4) \in A_1 \times A_2 \times A_3 \times A_4 : a_1 + a_2 + a_3 + a_4 = 0\}|}{(|A_1||A_2||A_3||A_4|)^{3/4}}. \tag{1.1}$$

Thus, for instance, the statement that $A$ has at least $|A|^3/K$ additive quadruples is equivalent to the assertion that

$$\omega(A, A, A, A) \geqslant 1/K$$

(note that in the characteristic two group $\mathbb{F}_2^n$, there is no distinction between addition and subtraction). Noting that the number of quadruples with $a_1 + a_2 + a_3 + a_4 = 0$ is bounded by $\prod_{i \neq j} |A_i|$ for any $j$, we see by taking products over $j = 1, \ldots, 4$ that $0 \leqslant \omega(A_1, A_2, A_3, A_4) \leqslant 1$. A simple application of Cauchy–Schwarz also gives the inequality

$$\omega(A, B, A, B) \geqslant \frac{|A|^{1/2}|B|^{1/2}}{|A+B|}. \tag{1.2}$$

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

THEOREM 1.9 (Second main theorem). *Let $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$ be nonempty sets such that*

$$\omega(A_1, A_2, A_3, A_4) \geqslant \frac{1}{K}$$

*for some $K \geqslant 1$. Then there exists a linear subspace $H \subseteq \mathbb{F}_2^n$ with $|H| \gg K^{-O(K)}|A_i|$ for $i = 1, 2, 3, 4$ and $x_1, x_2, x_3, x_4 \in \mathbb{F}_2^n$ such that*

$$\prod_{i=1}^{4} |A_i \cap (x_i + H)|^{1/4} \geqslant \frac{1}{2K}|H|.$$

The proof of this result is closely related to that of Theorem 1.4. More importantly it is *direct* in the sense that the Balog–Szemerédi–Gowers theorem is not required. It therefore demonstrates that the Balog–Szemerédi–Gowers and Freiman theorems, which are traditionally proven using very different methods, can instead be treated in a unified manner. Note, however, that we do not recover the polynomial-type bounds in Theorem 1.6 by our methods. Once again there is a simple corollary when just one set is involved.

COROLLARY 1.10. *Let $A \subseteq \mathbb{F}_2^n$ have at least $|A|^3/K$ additive quadruples for some $K \geqslant 1$. Then there exists an affine subspace $H \subseteq \mathbb{F}_2^n$ with $|H| \gg K^{-O(K)}|A|$ and $|A \cap H| \geqslant |H|/2K$.*

Our arguments used to prove Theorems 1.4 and 1.9 are completely self-contained, and can be briefly summarized as follows. First, in Section 2, we use Fourier-analytic methods to establish a special case of Theorem 1.9 (or Theorem 1.4) when the four sets $A_1, A_2, A_3, A_4$ are ‘coherently flat’, in the sense that the Fourier coefficients are either simultaneously large or simultaneously small—see in particular Proposition 2.4. Then, in Section 3, we run an energy increment argument to reduce to this coherently flat case in Theorem 1.4. In Section 4 we perform a similar argument to prove Theorem 1.9.

## 2. The coherently flat case

Our first task is to prove a variant of Theorems 1.4 and 1.9 in the case where we have four sets $A_1, A_2, A_3, A_4$ that are ‘coherently flat’, which basically corresponds to the regime in which Fourier analysis tools are effective.

DEFINITION 2.1 (Fourier transform). If $f : \mathbb{F}_2^n \to \mathbb{R}$, we define the Fourier transform $\hat{f} : \mathbb{F}_2^n \to \mathbb{R}$ by the formula

$$\hat{f}(\xi) := \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n} f(x)\,(-1)^{\xi \cdot x},$$

where $(x_1, \ldots, x_n) \cdot (\xi_1, \ldots, \xi_n) := x_1\xi_1 + \cdots + x_n\xi_n$.

Now we use a definition from [10].

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

DEFINITION 2.2 (Spectrum). If $A \subseteq \mathbb{F}_2^n$ is nonempty and $0 < \alpha \leqslant 1$, define the *$\alpha$-spectrum* $\mathrm{Spec}_\alpha(A)$ to be the set of all frequencies $\xi \in \mathbb{F}_2^n$ such that

$$|\hat{1}_A(\xi)| \geqslant \alpha|A|/2^n.$$

The spectrum $\mathrm{Spec}_\alpha(A)$ can be viewed as collecting the directions in which $A$ is significantly biased; indeed, to say that $\xi \in \mathrm{Spec}_\alpha(A)$ is equivalent to the assertion that the proportion of $A$ in the subspace $\{x \in \mathbb{F}_2^n \mid \xi \cdot x = 0\}$ is either greater than $(1+\alpha)/2$ or less than $(1-\alpha)/2$.

Observe that, if $A$ is an affine subspace, then $\hat{1}_A(\xi)$ is equal to either $|A|/2^n$ or zero; in other words, given any $\xi$, either $\xi \in \mathrm{Spec}_1(A)$ or $\xi \notin \mathrm{Spec}_\delta(A)$ for all $\delta > 0$. Slightly more generally, we see that, if $A_1, A_2, A_3, A_4$ are cosets of the same subspace, then, for any $\xi$, either

$$\xi \in \mathrm{Spec}_1(A_1) \cap \cdots \cap \mathrm{Spec}_1(A_4) \quad \text{or} \quad \xi \notin \mathrm{Spec}_\delta(A_1) \cup \cdots \cup \mathrm{Spec}_\delta(A_4)$$

for all $\delta > 0$. This motivates the following definition of a quadruple of sets that 'resemble' four cosets of the same subspace in some Fourier sense.

DEFINITION 2.3 (Coherently flat quadruples). Suppose that $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$ are nonempty and that $\delta \in (0, 1/2)$ is a small parameter. We say that the quadruple $(A_1, A_2, A_3, A_4)$ is *coherently $\delta$-flat* if, for each $\xi \in \mathbb{F}_2^n$, one of the following is true:

(i) ($\xi$ orthogonal to all $A_i$) $\xi \in \mathrm{Spec}_{9/10}(A_i)$ for all $i = 1, 2, 3, 4$; or

(ii) ($\xi$ nonorthogonal to all $A_i$) $\xi \notin \mathrm{Spec}_\delta(A_i)$ for all $i = 1, 2, 3, 4$.

We observe that we may translate one or more of the $A_i$ by an arbitrary $x_i \in \mathbb{F}_2^n$ without affecting the coherent flatness property.

The main result of this section is as follows.

PROPOSITION 2.4 (Freiman-type theorem, coherently flat case). *Let $K \geqslant 1$. Suppose $(A_1, A_2, A_3, A_4)$ is a coherently $(1/\sqrt{2K})$-flat quadruple whose energy satisfies the lower bound $\omega(A_1, A_2, A_3, A_4) \geqslant 1/K$. Then there is a linear subspace $H \subseteq \mathbb{F}_2^n$ with*

$$|H| \geqslant \frac{4}{5}\prod_{i=1}^{4}|A_i|^{1/4}, \tag{2.1}$$

*together with $x_1, x_2, x_3, x_4 \in \mathbb{F}_2^n$ such that*

$$\prod_{i=1}^{4}|A_i \cap (x_i + H)|^{1/4} \geqslant \frac{1}{2K}|H|. \tag{2.2}$$

PROOF. Set

$$\Lambda := \mathrm{Spec}_{9/10}(A_1) \cap \cdots \cap \mathrm{Spec}_{9/10}(A_4).$$

We claim that $\Lambda$ is a linear subspace of $\mathbb{F}_2^n$. Indeed, if this were not the case then we could find $\xi, \xi' \in \Lambda$ such that $\xi + \xi' \notin \Lambda$. Without loss of generality we may assume

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

that $\xi + \xi' \notin \mathrm{Spec}_{9/10}(A_1)$. Then by the coherently $(1/\sqrt{2K})$-flat hypothesis we see that $\xi + \xi' \notin \mathrm{Spec}_{1/\sqrt{2K}}(A_1)$. On the other hand, we have $\xi, \xi' \in \mathrm{Spec}_{9/10}(A_1)$, which by the triangle inequality (cf. [10, Lemma 4.37]) implies that $\xi + \xi' \in \mathrm{Spec}_{8/10}(A_1)$. This is a contradiction, and so $\Lambda$ is indeed a linear subspace.

Using the Fourier transform (see for instance [10, Lemma 4.9]), we observe the identity

$$\begin{aligned}\sum_{\xi \in \mathbb{F}_2^n} \prod_{i=1}^{4} \widehat{1}_{A_i}(\xi) &= \frac{\prod_{i=1}^4 |A_i|^{3/4}}{2^{3n}} \omega(A_1, A_2, A_3, A_4) \\ &\geqslant \frac{\prod_{i=1}^4 |A_i|^{3/4}}{2^{3n}K}.\end{aligned}$$

On the other hand, the coherently $(1/\sqrt{2K})$-flat hypothesis, Hölder's inequality and Plancherel imply that

$$\begin{aligned}\Bigg| \sum_{\xi \in \mathbb{F}_2^n \backslash \Lambda} \prod_{i=1}^{4} \widehat{1}_{A_i}(\xi) \Bigg| &\leqslant \sum_{\xi \in \mathbb{F}_2^n \backslash \Lambda} \prod_{i=1}^{4} \left( \frac{|A_i|}{2^n \sqrt{2K}} \right)^{1/2} |\widehat{1}_{A_i}(\xi)|^{1/2} \\ &\leqslant \prod_{i=1}^{4} \left( \frac{|A_i|}{2^n \sqrt{2K}} \right)^{1/2} \left( \sum_{\xi \in \mathbb{F}_2^n} |\widehat{1}_{A_i}(\xi)|^2 \right)^{1/4} \\ &= \prod_{i=1}^{4} \left( \frac{|A_i|}{2^n \sqrt{2K}} \right)^{1/2} \left( \frac{|A_i|}{2^n} \right)^{1/4} \\ &= \frac{1}{2} \frac{\prod_{i=1}^4 |A_i|^{3/4}}{2^{3n}K}.\end{aligned}$$

Subtracting the two estimates, we conclude that

$$\sum_{\xi \in \Lambda} \prod_{i=1}^{4} \widehat{1}_{A_i}(\xi) \geqslant \frac{1}{2} \frac{\prod_{i=1}^4 |A_i|^{3/4}}{2^{3n}K}. \tag{2.3}$$

Write $H$ for the orthogonal complement of $\Lambda$, that is to say

$$H := \Lambda^{\perp} := \{x \in \mathbb{F}_2^n \mid x \cdot \xi = 0 \text{ for all } \xi \in \Lambda\}.$$

The left-hand side of (2.3) can be rewritten as

$$\frac{1}{2^{3n}|H|} |\{(a_1, a_2, a_3, a_4) \in A_1 \times A_2 \times A_3 \times A_4 : a_1 + a_2 + a_3 + a_4 \in H\}|.$$

This is bounded above by

$$\frac{1}{2^{3n}|H|} |A_2||A_3||A_4| \sup_{x_1 \in \mathbb{F}_2^n} |A_1 \cap (x_1 + H)|.$$

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

It follows from (2.3) that there exists $x_1 \in \mathbb{F}_2^n$ such that

$$|A_1 \cap (x_1 + H)||A_2||A_3||A_4| \geqslant \frac{|H|}{2K}(|A_1| \ldots |A_4|)^{3/4}.$$

We may similarly find $x_2, x_3, x_4$ such that similar inequalities hold with the $A_i$ permuted. Taking geometric means of these four estimates and rearranging we obtain (2.2).

It remains to prove (2.1). Observe from Plancherel's theorem and the definition of $\Lambda$ that, for any $i = 1, 2, 3, 4$,

$$\frac{|A_i|}{2^n} = \sum_{\xi \in \mathbb{F}_2^n} |\hat{1}_{A_i}(\xi)|^2 \geqslant \sum_{\xi \in \Lambda} \left( \frac{9}{10} \frac{|A_i|}{2^n} \right)^2.$$

It follows that

$$|\Lambda| \leqslant \frac{5 \times 2^n}{4|A_i|},$$

and so upon taking geometric means we conclude that

$$|\Lambda| \leqslant \frac{5 \times 2^n}{4 \prod_{i=1}^4 |A_i|^{1/4}}.$$

Since $|H| = 2^n/|\Lambda|$, the claim (2.1) follows. □

## 3. Proof of Theorem 1.4

We now prove Theorem 1.4. We begin by proving an elementary lemma. Let $F : [0, 1] \times [0, 1] \to \mathbb{R}^+$ be the explicit function

$$F(x, y) := \sqrt{x}(\sqrt{y} + \sqrt{1 - y}).$$

Thus for instance $F(1/2, 1/2) = F(1, 1) = F(1, 0) = 1$.

LEMMA 3.1 (Near-minima of $F$). *Suppose that $\alpha, \beta, \epsilon$ are reals with $0 \leqslant \alpha, \beta \leqslant 1$ and $0 < \varepsilon \leqslant 1/100$, and that*

$$F(\alpha, \beta),\ F(1 - \alpha, \beta),\ F(\beta, \alpha),\ F(\beta, 1 - \alpha) \leqslant 1 + \varepsilon. \tag{3.1}$$

*Then either both $\alpha$ and $\beta$ are within $4\varepsilon$ of $1/2$, or else they are both within $2\varepsilon$ of 0 or 1.*

PROOF. The hypotheses are invariant under interchanging $\alpha$ and $\beta$, or by swapping $\alpha$ to $1 - \alpha$ or $\beta$ to $1 - \beta$. Thus without loss of generality we may assume that $1/2 \leqslant \alpha \leqslant \beta$. We have

$$\alpha + \sqrt{\alpha(1 - \alpha)} = F(\alpha, \alpha) \leqslant F(\beta, \alpha) \leqslant 1 + \varepsilon;$$

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

using the inequality $\sqrt{\alpha(1-\alpha)} \geqslant 2\alpha(1-\alpha)$ and rearranging we obtain

$$(2\alpha - 1)\,(1-\alpha) \leqslant \varepsilon.$$

It follows immediately that $\alpha$ is within $2\varepsilon$ of either $1/2$ or 1. In the latter case we are done, so suppose that $\alpha$ is within $2\varepsilon$ of $1/2$. We have

$$F(\beta, \alpha)^2 \leqslant (1+\varepsilon)^2 \leqslant 1 + 3\varepsilon,$$

which expands to

$$\beta\Big(1 + 2\sqrt{\tfrac{1}{4} - (\tfrac{1}{2} - \alpha)^2}\,\Big) \leqslant 1 + 3\varepsilon$$

and whence

$$\beta(1 + \sqrt{1 - 16\varepsilon^2}\,) \leqslant 1 + 3\varepsilon.$$

This implies that $\beta$ is within $4\varepsilon$ of $1/2$, and the claim follows. □

As a consequence of this lemma, we obtain the following key inductive step required for Theorem 1.4. It is convenient to introduce the notation

$$\mathrm{Dbl}(A, B) := |A+B|/|A|^{1/2}|B|^{1/2}.$$

Since $|A+B| \geqslant \max(|A|, |B|)$ we observe that

$$\mathrm{Dbl}(A, B)^{-2}|A| \leqslant |B| \leqslant \mathrm{Dbl}(A, B)^2|A|. \tag{3.2}$$

Lemma 3.2 (Nonflatness implies doubling decrement). *Suppose that $A, B \subseteq \mathbb{F}_2^n$ are nonempty sets with $\mathrm{Dbl}(A, B) \leqslant K$ for some $K \geqslant 1$, and suppose that $(A, B, A, B)$ is not coherently $(1/\sqrt{2K})$-flat. Then there are $A' \subseteq A$, $B' \subseteq B$ with $|A'|/|A|, |B'|/|B| \gg K^{-10}$ and*

$$\mathrm{Dbl}(A', B') \leqslant K - \tfrac{1}{100}\sqrt{K}. \tag{3.3}$$

Proof. By hypothesis, we can find $\xi \in \mathbb{F}_2^n$ such that

$$\xi \notin \mathrm{Spec}_{9/10}(A) \cap \mathrm{Spec}_{9/10}(B) \tag{3.4}$$

and

$$\xi \in \mathrm{Spec}_{1/\sqrt{2K}}(A) \cup \mathrm{Spec}_{1/\sqrt{2K}}(B). \tag{3.5}$$

Observe that $\xi$ must be nonzero.

For $j \in \mathbb{F}_2$ we set

$$A_j := \{x \in A \mid x \cdot \xi = j\} \quad \text{and} \quad B_j := \{x \in B \mid x \cdot \xi = j\},$$

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

and write $\alpha := |A_0|/|A|$ and $\beta := |B_0|/|B|$. Then

$$|\hat{1}_A(\xi)| = |2\alpha - 1|\frac{|A|}{2^n} \quad \text{and} \quad |\hat{1}_B(\xi)| = |2\beta - 1|\frac{|B|}{2^n}$$

and so (3.4) is equivalent to the assertion

$$|2\alpha - 1| < \tfrac{9}{10} \quad \text{or} \quad |2\beta - 1| < \tfrac{9}{10}$$

while (3.5) is equivalent to the assertion

$$|2\alpha - 1| \geqslant \frac{1}{\sqrt{2K}} \quad \text{or} \quad |2\beta - 1| \geqslant \frac{1}{\sqrt{2K}}.$$

Applying Lemma 3.1 in the contrapositive we conclude that one of the four quantities $F(\alpha, \beta)$, $F(1-\alpha, \beta)$, $F(\beta, \alpha)$, $F(1-\beta, \alpha)$ is greater than $1 + 1/(100\sqrt{K})$. By swapping $A$ and $B$, or by shifting either $A$ or $B$ by $\xi$, we may assume without loss of generality that

$$F(\alpha, \beta) > 1 + \frac{1}{100\sqrt{K}}.$$

In particular we see that $\beta \neq 0, 1$ and $\alpha \neq 0$, so that $A_0, B_0, B_1$ are nonempty; a variant of this argument also gives $|A_0| \gg K^{-10}|A|$ and $|B_j| \gg K^{-10}|B|$ for $j \in \mathbb{F}_2$. We can rewrite the above inequality as

$$\sum_{j \in \mathbb{F}_2} \frac{K}{1 + 1/(100\sqrt{K})}|A_0|^{1/2}|B_j|^{1/2} > K|A|^{1/2}|B|^{1/2}.$$

On the other hand,

$$K|A|^{1/2}|B|^{1/2} \geqslant |A + B| \geqslant \sum_{j \in \mathbb{F}_2} |A_0 + B_j|,$$

and so there exists $j \in \mathbb{F}_2$ such that

$$\mathrm{Dbl}(A_0, B_j) \leqslant \frac{K}{1 + 1/(100\sqrt{K})} \leqslant K - \frac{1}{100}\sqrt{K}.$$

The claim follows. □

We can iterate the above lemma at most $O(\sqrt{K})$ times, noting that the doubling constant cannot drop below 1, to obtain the following result.

COROLLARY 3.3 (Large coherently flat subsets). *Suppose that* $A, B \subseteq \mathbb{F}_2^n$ *are nonempty sets with* $\mathrm{Dbl}(A, B) \leqslant K$ *for some* $K \geqslant 1$. *Then there exists* $A' \subseteq A$, *and* $B' \subseteq B$ *with* $|A'|/|A|, |B'|/|B| \gg K^{-O(\sqrt{K})}$, $\mathrm{Dbl}(A', B') \leqslant K$, *and such that* $(A', B', A', B')$ *is coherently* $(1/\sqrt{2K})$*-flat.*

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

Proof of Theorem 1.4. We apply Corollary 3.3 to extract $A'$, $B'$ with the stated properties. Now we observe the identities

$$\omega(A', B', A', B') = \frac{1}{(|A'||B'|)^{3/2}} \sum_{x \in A'+B'} |\{(a, b) \in A' \times B' : a + b\}|^2$$

and

$$\sum_{x \in A'+B'} |\{(a, b) \in A' \times B' : a + b\}| = |A'||B'|.$$

Applying the Cauchy–Schwarz inequality we conclude that

$$\omega(A', B', A', B') \geqslant \frac{|A'|^{1/2}|B'|^{1/2}}{|A' + B'|} = \frac{1}{\mathrm{Dbl}(A', B')} \geqslant \frac{1}{K}.$$

Applying Proposition 2.4, we find $H, x_1, x_2, x_3, x_4$ such that

$$|H| \geqslant \tfrac{4}{5}|A'|^{1/2}|B'|^{1/2} \geqslant K^{-O(\sqrt{K})}|A|^{1/2}|B|^{1/2}$$

and

$$|A \cap (x_1 + H)|^{1/4}|B \cap (x_2 + H)|^{1/4}|A \cap (x_3 + H)|^{1/4}|B \cap (x_4 + H)|^{1/4} \geqslant \frac{1}{2K}|H|.$$

Without loss of generality we may assume that $|A \cap (x_1 + H)| \geqslant |A \cap (x_3 + H)|$ and $|B \cap (x_2 + H)| \geqslant |B \cap (x_4 + H)|$, thus

$$|A \cap (x_1 + H)|^{1/2}|B \cap (x_2 + H)|^{1/2} \geqslant \frac{1}{2K}|H|.$$

The claim follows. □

## 4. Proof of Theorem 1.9

We can adapt the arguments of the previous section to prove Theorem 1.9. We begin with the analogue of Lemma 3.1. We now require the explicit function $G : [0, 1]^4 \to \mathbb{R}^+$ defined by

$$G(\alpha_1, \alpha_2, \alpha_3, \alpha_4) := \sum_{\substack{j_1, j_2, j_3, j_4 \in \mathbb{F}_2 \\ j_1+j_2+j_3+j_4=0}} \prod_{i=1}^{4} \alpha_{i,j_i}^{3/4},$$

where we write $\alpha_{i,0} := \alpha_i$ and $\alpha_{i,1} := 1 - \alpha_i$.

Applying Young's inequality in the form

$$|f_1 * f_2 * f_3 * f_4(0)| \leqslant \prod_{i=1}^{4} \biggl( \sum_{j \in \mathbb{F}_2} |f_i(j)|^{4/3} \biggr)^{3/4}$$

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

with $f_i(j) := \alpha_{i,j}^{3/4}$, we see that $G$ is always bounded by 1. Equality occurs in this inequality if and only if each of the $f_i$ are concentrated on a single point in $\mathbb{F}_2$, or else are all constant in $\mathbb{F}_2$. We shall need a robust version of this observation in the following result.

LEMMA 4.1 (Near-maxima of $G$). *Suppose that $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \epsilon$ are reals and that $0 \leqslant \alpha_1, \ldots, \alpha_4 \leqslant 1$ and $0 < \varepsilon \leqslant 1/1000$. Suppose that*

$$G(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \geqslant 1 - \varepsilon.$$

*Then either the four quantities $\alpha_i$ are all within $3\sqrt{\varepsilon}$ of $1/2$, or else the four quantities $\min(\alpha_i, 1 - \alpha_i)$ are all at most $10\varepsilon$.*

PROOF. Observe that

$$G(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \frac{1}{2}\prod_{i=1}^{4}(\alpha_i^{3/4} + (1-\alpha_i)^{3/4}) + \frac{1}{2}\prod_{i=1}^{4}(\alpha_i^{3/4} - (1-\alpha_i)^{3/4}).$$

Applying the arithmetic–geometric mean inequality

$$x_1x_2x_3x_4 \leqslant \frac{x_1^4 + x_2^4 + x_3^4 + x_4^4}{4},$$

we obtain

$$8 - \sum_{i=1}^{4}(\alpha_i^{3/4} + (1-\alpha_i)^{3/4})^4 - \sum_{i=1}^{4}(\alpha_i^{3/4} - (1-\alpha_i)^{3/4})^4 \leqslant 8\varepsilon.$$

After some rearrangement, the left-hand side may be seen to equal

$$\sum_{i=1}^{4} \frac{3\alpha_i(1-\alpha_i)\,(1-2\alpha_i)^2}{1 + 2\alpha_i^{1/2}(1-\alpha_i)^{1/2}},$$

which is at least

$$\sum_{i=1}^{4} \frac{3}{2}\alpha_i(1-\alpha_i)\,(1-2\alpha_i)^2.$$

By positivity we thus have

$$|\alpha_i||1-\alpha_i||\tfrac{1}{2} - \alpha_i|^2 \leqslant 4\varepsilon/3,$$

for $i = 1, 2, 3, 4$. A short back-of-an-envelope computation confirms that each of the $\alpha_i$ is either within $3\sqrt{\varepsilon}$ of $1/2$, or else within $10\varepsilon$ of 0 or 1.

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

This is not quite as strong as the statement of the lemma, because different $\alpha_i$ may end up in different sides of the dichotomy. Suppose, for contradiction, that this occurs. Namely, suppose without loss of generality that $\alpha_1$ is within $3\sqrt{\varepsilon}$ of $1/2$. Then

$$\frac{1}{2}\prod_{i=1}^{4}|\alpha_i^{3/4}-(1-\alpha_i)^{3/4}| \leqslant 0.085$$

and so

$$\frac{1}{2}\prod_{i=1}^{4}(\alpha_i^{3/4}+(1-\alpha_i)^{3/4}) \geqslant \frac{9}{10}.$$

Since $x^{3/4}+(1-x)^{3/4} \leqslant 2^{1/4}$ for $0 \leqslant x \leqslant 1$, we obtain

$$\alpha_i^{3/4}+(1-\alpha_i)^{3/4} \geqslant \frac{9}{5\times 2^{3/4}} \geqslant 1.07$$

for $i=2, 3, 4$. It follows that none of $\alpha_2, \alpha_3, \alpha_4$ is within $10\epsilon$ of $0$ or $1$, and hence all of these must be within $3\sqrt{\varepsilon}$ of $1/2$ as well. □

Now we obtain the analogue of Lemma 3.2.

LEMMA 4.2 (Nonflatness implies energy increment). *Let $K \geqslant 1$. Suppose that $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$ are nonempty sets with $\omega(A_1, A_2, A_3, A_4) \geqslant 1/K$, and suppose that $(A_1, A_2, A_3, A_4)$ is not coherently $(1/\sqrt{2K})$-flat. Then for each $i=1, 2, 3, 4$ there are sets $A_i' \subseteq A_i$ with $|A_i'|/|A_i| \gg K^{-10}$ such that*

$$\omega(A_1', A_2', A_3', A_4') \geqslant \frac{1}{K-10^{-4}}. \tag{4.1}$$

PROOF. By hypothesis, we can find $\xi$ such that

$$\xi \notin \mathrm{Spec}_{9/10}(A_1)\cap\cdots\cap\mathrm{Spec}_{9/10}(A_4)$$

and

$$\xi \in \mathrm{Spec}_{1/\sqrt{2K}}(A_1)\cup\cdots\cup\mathrm{Spec}_{1/\sqrt{2K}}(A_4).$$

Again $\xi$ must be nonzero. We then set $A_{i,j} := \{x \in A_i \mid \xi\cdot x = j\}$ for $i=1, 2, 3, 4$ and $j \in \mathbb{F}_2$, and set $\alpha_i := |A_{i,0}|/|A_i|$. Then

$$\min_{i=1,2,3,4} |2\alpha_i - 1| < 9/10 \tag{4.2}$$

and

$$\max_{i=1,2,3,4} |2\alpha_i - 1| \geqslant 1/\sqrt{2K}. \tag{4.3}$$

Applying Lemma 4.1 in the contrapositive we conclude that

$$G(\alpha_1, \alpha_2, \alpha_3, \alpha_4) < 1 - \frac{1}{1000K},$$

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

and consequently

$$\sum_{\substack{j_1,j_2,j_3,j_4\in\mathbb{F}_2\\ j_1+j_2+j_3+j_4=0}} \left(\prod_{i=1}^{4}|A_{i,j_i}|^{3/4}+\frac{1}{10^4K}\prod_{i=1}^{4}|A_i|^{3/4}\right) < \left(1-\frac{1}{10^4K}\right)\prod_{i=1}^{4}|A_i|^{3/4}.$$

Now observe the identity

$$\omega(A_1, A_2, A_3, A_4)\prod_{i=1}^{4}|A_i|^{3/4} = \sum_{\substack{j_1,j_2,j_3,j_4\in\mathbb{F}_2\\ j_1+j_2+j_3+j_4=0}} \omega(A_{1,j_1}, A_{2,j_2}, A_{3,j_3}, A_{4,j_4})\prod_{i=1}^{4}|A_{i,j_i}|^{3/4}$$

(with the convention that $\omega = 0$ when one or more of the four sets is empty). Since $\omega(A_1, A_2, A_3, A_4) \geqslant 1/K$, we conclude from the pigeonhole principle that there exist $j_1, j_2, j_3, j_4 \in \mathbb{F}_2$ with $j_1 + j_2 + j_3 + j_4 = 0$ such that

$$\omega(A_{1,j_1}, A_{2,j_2}, A_{3,j_3}, A_{4,j_4})\prod_{i=1}^{4}|A_{i,j_i}|^{3/4} \geqslant \frac{1}{K-10^{-4}}\left(\prod_{i=1}^{4}|A_{i,j_i}|^{3/4}+\frac{1}{10^4K}\prod_{i=1}^{4}|A_i|^{3/4}\right).$$

Since $\omega$ is bounded above by 1, this already implies that $|A_{i,j_i}| \gg K^{-10}|A_i|$ for $i = 1, 2, 3, 4$. We also see that

$$\omega(A_{1,j_1}, A_{2,j_2}, A_{3,j_3}, A_{4,j_4}) \geqslant \frac{1}{K-10^{-4}},$$

and the claim follows. □

We may iterate this lemma at most $O(K)$ times to obtain the following result.

COROLLARY 4.3 (Large coherently flat subsets). *Suppose that $A_1, A_2, A_3, A_4 \subseteq \mathbb{F}_2^n$ are nonempty sets with $\omega(A_1, A_2, A_3, A_4) \geqslant 1/K$ for some $K \geqslant 1$. Then there exist $A_i' \subseteq A_i$ with $|A_i'|/|A_i| \geqslant K^{-O(K)}$, $\omega(A_1', A_2', A_3', A_4') \geqslant 1/K$, and such that $(A_1', A_2', A_3', A_4')$ is coherently $(1/\sqrt{2K})$-flat.*

Theorem 1.9 then follows from this corollary and Proposition 2.4 by repeating the arguments of the previous section.

## References

[1] A. Balog and E. Szemerédi, ‘A statistical theorem of set addition’, *Combinatorica* **14** (1994), 263–268.

[2] W. T. Gowers, ‘A new proof of Szemerédi’s theorem for arithmetic progressions of length four’, *Geom. Funct. Anal.* **8** (1998), 529–551.

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press

[3] ———, 'A new proof of Szemerédi's theorem', *Geom. Funct. Anal.* **11**(3) (2001), 465–588.

[4] B. J. Green, 'The polynomial Freiman–Ruzsa conjecture', unpublished notes. Available at http://www.dpmms.cam.ac.uk/∼bjg23.

[5] B. J. Green and T. Sanders, 'Boolean functions with small spectral norm', *Geom. Funct. Anal.* **18**(1) (2008), 144–162.

[6] B. J. Green and T. C. Tao, 'An inverse theorem for the Gowers $U^3$-norm, with applications', *Proc. Edinb. Math. Soc.* **51**(1) (2008), 73–153.

[7] ———, 'Freiman's theorem in finite fields via extremal set theory', Preprint.

[8] I. Z. Ruzsa, 'An analog of Freiman's theorem in groups. Structure theory of set addition', *Astérisque* **258** (1999), 323–326.

[9] T. Sanders, 'A note on Freiman's theorem in vector spaces', *Combin. Probab. Comput.* **17**(2) (2008), 297–305.

[10] T. C. Tao and V. H. Vu, *Additive Combinatorics* (Cambridge University Press, Cambridge, 2006).

BEN GREEN, Centre for Mathematical Sciences, Wilberforce Road,
Cambridge CB3 0WA, UK
e-mail: b.j.green@dpmms.cam.ac.uk

TERENCE TAO, Department of Mathematics, UCLA,
Los Angeles CA 90095-1555, USA
e-mail: tao@math.ucla.edu

https://doi.org/10.1017/S1446788708000359 Published online by Cambridge University Press