An equivalence between inverse sumset theorems and inverse conjectures for the $U^3$ norm

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

AND TERENCE TAO‡
UCLA Department of Mathematics, Los Angeles, CA 90095-1555, U.S.A.
e-mail: tao@math.ucla.edu

(Received 17 June 2009)

Abstract
We establish a correspondence between inverse sumset theorems (which can be viewed as classifications of approximate (abelian) groups) and inverse theorems for the Gowers norms (which can be viewed as classifications of approximate polynomials). In particular, we show that the inverse sumset theorems of Frei\"man type are equivalent to the known inverse results for the Gowers $U^3$ norms, and moreover that the conjectured polynomial strengthening of the former is also equivalent to the polynomial strengthening of the latter. We establish this equivalence in two model settings, namely that of the finite field vector spaces $\mathbb{F}_p^n$, and of the cyclic groups $\mathbb{Z}/N\mathbb{Z}$.

In both cases the argument involves clarifying the structure of certain types of approximate homomorphism.

1. Introduction

Approximate groups. The notion of an approximate group has come to be seen as a central one in additive combinatorics. Let $K \geq 1$ be a parameter (the “roughness” parameter), and
suppose that \( A \) is a finite subset of some ambient abelian group \( G = (G, +) \) (such as the integers \( \mathbb{Z} \)). We say that \( A \) is a \( K \)-approximate group if \( A \) is symmetric (that is to say \(-x \in A \) whenever \( x \in A \)) and if the sumset \( A + A := \{a + a' : a, a' \in A \} \) is covered by \( K \) translates of \( A \). Thus, for instance, the arithmetic progression \( \{-N, \ldots, N\} \) in the integers \( \mathbb{Z} \) for any \( N \geq 1 \) is a 3-approximate group, while the 1-approximate group are nothing more than the finite subgroups of \( G \).

The basic theory of approximate abelian groups was developed by Ruzsa in several papers \([20, 21, 22]\); see also \([24]\) for some extensions to non-abelian groups.

Perhaps the most basic question to ask about an approximate group is that of the extent to which it resembles an actual group. A language for formalising this was introduced by the second author in \([25]\), and in the abelian case it reads as follows.

**Definition 1.1 (Control).** Let \( A \) and \( B \) be two sets in some ambient abelian group, and \( K \geq 1 \). We say that \( B \) \( K \)-controls \( A \) if \( |B| \leq K |A| \) and if there is some set \( X \) in the ambient group with \( |X| \leq K \) and such that \( A \subseteq B + X \).

Two of the landmark results of additive combinatorics may be stated in this language. The first of these may be found in \([22]\) and the second in \([4]\), a paper which builds upon \([6]\) and \([20]\).

**Theorem 1.2** (Inverse sumset theorem for \( F_2^\infty \)). Suppose that \( A \subseteq F_2^\infty \) is a \( K \)-approximate group for some \( K \geq 2 \). Then \( A \) is \( e^Kc \)-controlled by a (genuine) finite subgroup of \( F_2^\infty \).

**Theorem 1.3** (Inverse sumset theorem for \( \mathbb{Z} \)). Suppose that \( A \subseteq \mathbb{Z} \) is a \( K \)-approximate group for some \( K \geq 2 \). Then \( A \) is \( e^Ko(1) \)-controlled by a symmetric generalized arithmetic progression \( P = \{l_1x_1 + \cdots + l_dx_d : |l_i| \leq L_i \text{ for all } 1 \leq i \leq d\} \) with dimension \( d \leq K^C \).

**Remark 1.4.** In this paper the letter \( C \) will always denote a constant, but different instances of the notation may indicate different constants. The restriction \( K \geq 2 \) is purely a notational convenience, so that we may write \( K^C \) instead of \( CK^C \).

These theorems, the background to them and their proofs are now discussed in many places. See, for example, the book \([26]\). Neither result is usually formulated in precisely this fashion, but simple arguments involving the covering lemmas in \([26, \text{ chapter 2}]\) may be used to deduce the above forms from the standard ones. The proofs of the above two theorems extend easily to the case of bounded torsion \( G \) and torsion-free \( G \) respectively. It is also possible to establish a result valid for all abelian groups at once, and containing the above two results as special cases: see \([11]\) for details.

There seems to be a general feeling that the bounds in these results are not optimal, and the so-called Polynomial Freiman–Ruzsa conjecture (PFR) has been proposed as a suggestion for what might be true.

**Conjecture 1.5** (PFR over \( F_2^\infty \)). Suppose that \( A \subseteq F_2^\infty \) is a \( K \)-approximate group. Then \( A \) is \( K^C \)-controlled by a finite subgroup.

**Conjecture 1.6** (Weak PFR over \( \mathbb{Z} \)). Suppose that \( A \subseteq \mathbb{Z} \) is a \( K \)-approximate group. Then \( A \) is \( e^{Ko(1)} \)-controlled by a symmetric generalized arithmetic progression \( P = \{l_1x_1 + \cdots + l_dx_d : |l_i| \leq L_i \} \) with dimension \( d \leq K^{o(1)} \), where \( o(1) \) denotes a quantity bounded in magnitude by \( c(K) \) for some function \( c \) of \( K \) that goes to zero as \( K \to \infty \).
Conjecture 1.5 has been stated in several places and, in the unpublished work of Ruzsa [10], was discussed, establishing a number of equivalent forms of it. According to Ruzsa [20], the first person to make a conjecture equivalent to the PFR over $\mathbb{F}_2^\infty$ was Katalin Márton. Conjecture 1.6, concerning approximate subgroups of $\mathbb{Z}$, does not to our knowledge appear explicitly in the literature, although something close to it was suggested by Gowers [9]. One might very optimistically conjecture that a $K$-approximate subgroup of $\mathbb{Z}$ is $K^c$-controlled by the affine image of the set of lattice points inside a convex body of dimension $O(\log K)$. Such a conjecture might deserve to be called the PFR over $\mathbb{Z}$ (rather than the weak PFR), since it is nontrivial even if $K$ is a suitably small power of $|A|$. A number of issues are rather unclear concerning such a formulation, one of them being whether it suffices to consider boxes rather than arbitrary convex bodies. This question appears to involve somewhat subtle issues from convex geometry and we will not consider it, or indeed any aspect of the stronger version of the PFR over $\mathbb{Z}$, any further in this paper.

**Approximate polynomials.** We turn now to what appears to be a completely unrelated topic. Let $G = (\mathbb{G}, +)$ be a finite abelian group, and recall the definition of the Gowers norms. If $f: G \to \mathbb{C}$ is a function we define:

$$
\|f\|_{U^3(G)} := (\mathbb{E}_{x,h \in G} f(x) f(x+h) f(x+2h))^{1/2} \\
\|f\|_{U^4(G)} := (\mathbb{E}_{x,h_1,h_2 \in G} f(x) f(x+h_1) f(x+h_2) f(x+h_1+h_2))^{1/4} \\
\|f\|_{U^5(G)} := (\mathbb{E}_{x,h_1,h_2,h_3 \in G} f(x) f(x+h_1) f(x+h_2) f(x+h_3) f(x+h_1+h_2+h_3))^{1/8}
$$

and so forth, where we use the averaging notation $\mathbb{E}_{x \in A} f(x) := (1/|A|) \sum_{x \in A} f(x)$. In this paper we shall be working primarily with the $U^3(G)$-norm. It is clear that if $\|f\|_\infty \leq 1$ and $\|f\|_{U^3(G)} = 1$ then we necessarily have $f(x) = e(\phi(x))$, where $\phi: G \to \mathbb{R}/\mathbb{Z}$ is a quadratic polynomial in the sense that $\Delta_{h_1} \Delta_{h_2} \Delta_{h_3} \phi(x) = 0$ for all $h_1, h_2, h_3, x \in G$, where $\Delta_h \phi(x) := \phi(x+h) - \phi(x)$. To justify the terminology, observe that when $G = \mathbb{Z}/N\mathbb{Z}$ with $N$ odd it is an easy matter to check that any quadratic polynomial has the form $\phi(x) = 1/Nax^2 + 1/Nbx + c$ for $a, b \in \mathbb{Z}/N\mathbb{Z}$ and $c \in \mathbb{R}/\mathbb{Z}$, where $1/N : \mathbb{Z}/N\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ is the usual embedding.

The inverse problem for the Gowers $U^3$-norm asks what can be said about functions $f: G \to \mathbb{C}$ for which $\|f\|_\infty \leq 1$ and $\|f\|_{U^3(G)} > 1/K$. In view of the above discussion, it is reasonable to call such functions $f$ $K$-approximate quadratics.

The analogue of control in this setting is correlation. We say that a function $f: G \to \mathbb{C}$ $\delta$-correlates with another function $F: G \to \mathbb{C}$ if the inner product $\langle f, F \rangle := \mathbb{E}_{x \in G} f(x) \overline{F(x)}$ is at least $\delta$.

In the finite field setting, the following inverse theorem was shown in [23].

**Theorem 1.7** (Inverse theorem for $U^3(\mathbb{F}_2^n)$). Suppose that $f: \mathbb{F}_2^n \to \mathbb{C}$ is a $K$-approximate quadratic for some $K \geq 2$. Then $f$ $\exp(-Kc)$-correlates with a phase $(-1)^\psi$ for some quadratic polynomial $\psi: \mathbb{F}_2^n \to \mathbb{F}_2$.

**Remark.** The phase $\psi(x)$ may be written explicitly, relative to a basis, as $\psi(x) := x \cdot Mx + b \cdot x + c$, where $M: \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a linear transformation, $b \in \mathbb{F}_2^n, c \in \mathbb{F}_2$, and $b \cdot x$ is the usual dot product in $\mathbb{F}_2$.

In $\mathbb{Z}/N\mathbb{Z}$ there is an analogous result, which we recall in Theorem 1.9 below. To state it we recall some of the terminology from [13] concerning nilsequences.
Definition 1.8 (Nilsequences). A 2-step nilmanifold is a homogeneous space \(G/\Gamma\), where \(G\) is a nilpotent Lie groups of step at most 2, and \(\Gamma\) is a discrete cocompact subgroup. A fundamental 2-step nilmanifold is one of the following three examples of a 2-step nilmanifold:

(i) (Unit circle) \(G = \mathbb{R}\) and \(\Gamma = \mathbb{Z}\);
(ii) (Skew torus) \(G = \left(\begin{array}{cc}1 & \mathbb{Z} \\ \mathbb{Z} & 1 \end{array}\right)\) and \(\Gamma = \left(\begin{array}{cc}1 & \mathbb{Z} \\ \mathbb{Z} & 1 \end{array}\right)\);
(iii) (Heisenberg nilmanifold) \(G = \left(\begin{array}{cc}1 & \mathbb{R} \\ \mathbb{R} & 0 \end{array}\right)\) and \(\Gamma = \left(\begin{array}{cc}1 & \mathbb{Z} \\ \mathbb{Z} & 1 \end{array}\right)\).

We place smooth metrics on each of these nilmanifolds; the exact choice of metric is not important. An elementary 2-step nilmanifold is a Cartesian product of finitely many fundamental 2-step nilmanifolds, with the product metric. Again, the exact convention for defining the product metric is not important. An elementary 2-step nilsequence is a sequence of the form \(n \mapsto F(g^n_{x_0})\), where \(G/\Gamma\) is an elementary 2-step nilmanifold, \(F: G/\Gamma \to \mathbb{C}\) is a Lipschitz function, \(g \in G\), and \(x_0 \in \Gamma\).

Remarks. If one only had the unit circle and not the skew torus and Heisenberg nilmanifold, the notion of an elementary 2-step nilsequence would collapse to that of a quasiperiodic sequence. It is not hard to see that the unit circle and skew torus can be embedded into the Heisenberg nilmanifold, and so one may work entirely with products of Heisenberg nilmanifolds if one wished. For further discussion of nilsequences see [1, 2, 13, 16, 17].

Theorem 1.9 (Inverse theorem for \(U^3(\mathbb{Z}/N\mathbb{Z})\)). Suppose that \(f: \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}\) is a \(K\)-approximate quadratic for some \(K \geq 2\). Then \(f \exp(-K^C)\)-correlates with an elementary 2-step nilsequence \(F(g^n_{x_0})\), where \(F: G/\Gamma \to \mathbb{C}\) is Lipschitz with Lipschitz constant at most \(\exp(K^C)\), \(g \in G\), \(x_0 \in G/\Gamma\) and \(G/\Gamma\) is an elementary 2-step nilsystem of dimension at most \(K^C\).

Remarks. The proofs of Theorems 1.7 and 1.9 depend very heavily on earlier work of Gowers [7, 8]. In Theorem 1.9 one can replace the notion of an elementary 2-step nilsequence \(n \mapsto F(g^n_{x_0})\) by the more concrete notion of a bracket phase polynomial

\[
\sum_{j=1}^{d} \alpha_j \left\{ \beta_j n \right\} + \sum_{k=1}^{d'} \delta_k \left\{ \eta_k n \right\}
\]

where \(\alpha_j, \beta_j, \gamma_j, \delta_k, \eta_k \in \mathbb{R}\), \(\{x\}\) is the fractional part of \(x\) (defined to lie in \((-1/2, 1/2])\), and \(d, d'\) are integers of size at most \(K^C\). See [2, 13] for further discussion.

Once again, it is not generally thought that the bounds in these two results are best possible. The following two conjectures might be referred to as the Polynomial inverse conjectures for the \(U^3\) Gowers norms, or PGI(3) for short.

Conjecture 1.10 (PGI(3) over \(\mathbb{F}_2^n\)). Suppose that \(f: \mathbb{F}_2^n \to \mathbb{C}\) is a \(K\)-approximate quadratic. Then \(f \exp(-K^C)\)-correlates with a quadratic phase \((-1)^{\psi}(\cdot)\).

Conjecture 1.11 (Weak PGI(3) over \(\mathbb{Z}/N\mathbb{Z}\)). Suppose that \(f: \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}\) is a \(K\)-approximate quadratic. Then \(f \exp(-K^{o(1)})\)-correlates with an elementary 2-step nilsequence \(F(g^n_{x_0})\), where \(F: G/\Gamma \to \mathbb{C}\) is Lipschitz of order at most \(\exp(K^{o(1)})\), \(g \in G\), \(x_0 \in G/\Gamma\) and \(G/\Gamma\) is an elementary 2-step nilsystem of of dimension at most \(K^{o(1)}\).

Remarks. The second of these conjectures deserves some comment. Usually, when inverse conjectures for the Gowers norms are discussed (for example in [15]) there is no restriction to elementary nilsequences. We have made this restriction here to simplify the discussion,
and in particular to avoid the need to involve the quantitative theory of 2-step nilmanifolds in general as was done in the first two sections of [16]. However it transpires that Conjecture 1·11 is implied by the same conjecture without the restriction to elementary nilsequences, simply because every 2-step nilsequence may be closely approximated by a weighted sum of elementary 2-step nilsequences. We omit the details of this deduction, which can be obtained from the calculations in [12, appendix B].

We do not dare, at this stage, to even formulate a strong PGI(3) conjecture over \( \mathbb{Z}/N\mathbb{Z} \). To do so would appear to involve rather subtle issues connected with the exact definition of complexity of a nilsequence.

We are now in a position to state our main results.

**Theorem 1·12 (Equivalence of PFR and PGI(3), finite field version).** Conjecture 1·5 and Conjecture 1·10 are equivalent.

*Remark.* A similar result would hold over \( \mathbb{F}_p \), for any fixed prime \( p \), though the exponents obtained would depend on \( p \).

**Theorem 1·13 (Equivalence of PFR and PGI(3), \( \mathbb{Z} \)-version).** Conjecture 1·6 and Conjecture 1·11 are equivalent.

The fact that Conjecture 1·5 implies Conjecture 1·10 follows by a modification of Samorodnitsky’s argument [23], and similarly the fact that Conjecture 1·6 implies Conjecture 1·11 follows from modification of [13]. Both arguments are strongly dependent on the work of Gowers mentioned earlier. The details of these deductions are a little technical and are discussed in Appendix A. However, the main novelty of our paper lies in the opposite implications PGI(3) \( \Rightarrow \) PFR, the discussion of which forms the main body of this paper.

*Remark.* The methods used to prove Theorems 1·12, 1·13 also establish an equivalence between Theorem 1·2 and Theorem 1·7, and between Theorem 1·3 and Theorem 1·9, though such an equivalence is redundant given that all four theorems have already been proven in the literature.

Let us conclude by remarking that Shachar Lovett informed us that he independently observed Theorem 1·12.

### 2. The finite field case

We turn now to the proof that Conjecture 1·5 implies Conjecture 1·10, that is to say the PGI(3) implies the PFR over the finite field \( \mathbb{F}_2 \). The argument proceeds via the following intermediate result concerning the structure of approximate homomorphisms on the infinite vector space \( \mathbb{F}_2^\infty : = \bigcup_n \mathbb{F}_2^n \).

**Lemma 2·1 (Approximate homomorphisms).** Assume Conjecture 1·10. Suppose that \( S \subseteq \mathbb{F}_2^n \) is a set of cardinality \( \sigma 2^n \) for some \( 0 < \sigma < 1/2 \), and that \( \phi : S \to \mathbb{F}_2^\infty \) is a Freiman homomorphism on \( S \), i.e. \( \phi(x_1) + \phi(x_2) = \phi(x_3) + \phi(x_4) \) whenever \( x_1, x_2, x_3, x_4 \in S \) are such that \( x_1 + x_2 = x_3 + x_4 \). Then there is an affine linear map \( \psi : \mathbb{F}_2^n \to \mathbb{F}_2^\infty \) such that \( \phi(x) = \psi(x) \) for at least \( \sigma C 2^n \) values of \( x \in S \).

*Remark.* By combining this lemma with known additive-combinatorial results one could obtain the conclusion of Lemma 2·1 under a priori weaker assumptions, for example that \( \mathbb{P}(\phi(x_1) + \phi(x_2) = \phi(x_3) + \phi(x_4) | x_1 + x_2 = x_3 + x_4) \) is large. Indeed a map of this type
restricts to a Frei\v{m}an homomorphism on a large set \( S \) by arguments of Gowers and Ruzsa (see [8, section 7]).

Let us first show how Conjecture 1-6 follows from Lemma 2-1. Suppose that \( A \subseteq \mathbb{F}_2^n \) is a \( K \)-approximate group, and let \( n \) be minimal such that there exists a linear map \( \pi : \mathbb{F}_2^n \to \mathbb{F}_2^n \) which is a Frei\v{m}an isomorphism\(^1\) from \( A \) to \( \pi(A) \); this quantity \( n \), which one can view as a sort of “rank” or “dimension” for \( A \), is finite since \( A \) is finite. If there is some\(^2\) \( x \in \mathbb{F}_2^n \setminus 4\pi(A) \) then we could compose \( \pi \) with the projection map \( \psi : \mathbb{F}_2^n \to \mathbb{F}_2^n/\langle x \rangle \) to obtain a linear map \( \pi : \mathbb{F}_2^n \to \mathbb{F}_2^{n-1} \) which is a Frei\v{m}an isomorphism when restricted to \( A \), contrary to the assumed minimality of \( n \). It follows that \( 4\pi(A) = \mathbb{F}_2^n \). But \( \pi(A) \) is Frei\v{m}an isomorphic to \( A \), which is a \( K \)-approximate group. It follows that the doubling constant \( 2|\pi(A)|/|\pi(A)| \) is at most \( K \), and hence by Ruzsa’s sumset estimates (cf. [26, corollary 2.23]) that \( 2^n = |4\pi(A)| \leq K^n|A| \).

What we have done here is find a “dense model” \( \pi(A) \subseteq \mathbb{F}_2^n \) of the set \( A \); the simple argument we used to do so is the finite field analogue of an argument of Ruzsa [20] that we shall recall later in the paper. Write \( S = \pi(A) \) and \( \phi \) for the inverse of \( \pi \), restricted to \( S \). Then \( \phi \) is a Frei\v{m}an homomorphism on \( S \) and the set \( A \) is precisely the image \( \phi(S) \). Applying Lemma 2-1, we see that at least \( K^n|A| \) of the elements of \( A \) are contained in a coset of an \( n \)-dimensional subspace \( H \subseteq \mathbb{F}_2^n \). Finally, it follows immediately from standard covering lemmas (cf. [26, section 2-4]) that \( A \) is \( K^n \)-controlled by \( H \).

It remains, then, to establish Lemma 2-1. The key observation linking Frei\v{m}an homomorphisms to approximate quadratics is the following lemma.

**Lemma 2-2.** Suppose that \( S \subseteq \mathbb{F}_2^n \) is a set of size \( \sigma 2^n \) for some \( 0 < \sigma < 1/2 \) and that \( \phi : S \to \mathbb{F}_2^n \) is a Frei\v{m}an homomorphism. The image of \( \phi \) certainly lies in some finite-dimensional subspace \( \mathbb{F}_2^N \). If \( f : \mathbb{F}_2^N + N \to [-1, 1] \) is the function \( f(x, y) := 1_S(x)(-1)^{\phi(x)-y} \), then \( \| f \|_{U^3(\mathbb{F}_2^N)} \geq \sigma \).

**Proof.** Consider a parallelopiped \( (x + \omega \cdot h, y + \omega \cdot k)_{\omega \in \{0, 1\}^3} \) in the support of \( f \), where \( h = (h_1, h_2, h_3), k = (k_1, k_2, k_3), x, h_1, h_2, h_3 \in \mathbb{F}_2^3 \) and \( y, k_1, k_2, k_3 \in \mathbb{F}_2^3 \). Then \( x + \omega \cdot h \in S \) for all \( \omega \in \{0, 1\}^3 \). Since \( \phi \) is a Frei\v{m}an homomorphism on \( S \), we see that \( \phi(x + \omega \cdot h) \) depends linearly on \( \omega \), and so \( \phi(x + \omega \cdot h) \cdot (y + \omega \cdot k) \) depends quadratically on \( \omega \). Since \( \{0, 1\}^3 \) is three-dimensional, we conclude that

\[
\sum_{\omega \in \{0, 1\}^3} (-1)^{\omega \cdot \phi(x + \omega \cdot h) \cdot (y + \omega \cdot k)} = 0
\]

where \( |\omega| \) is the number of 1s in the coefficients of \( \omega \) (actually, as we are working in \( \mathbb{F}_2 \) here, the \( (-1)^{\omega \cdot \phi} \) factor could in fact be ignored). From this and the definition of \( f \) and the \( U^3(\mathbb{F}_2^N) \) norm we conclude that

\[
\| f \|_{U^3(\mathbb{F}_2^N)} = \| 1_S \|_{U^3(\mathbb{F}_2^N)}.
\]

The behaviour in the \( y \) index is now trivial, and therefore

\[
\| 1_S \|_{U^3(\mathbb{F}_2^N)} = \| 1_S \|_{U^3(\mathbb{F}_2^3)}.
\]

\(^1\) A Frei\v{m}an homomorphism is a Frei\v{m}an homomorphism which is invertible and whose inverse is also a Frei\v{m}an homomorphism.

\(^2\) We use \( kA = A + \cdots + A \) to denote the \( k \)-fold iterated sumset of \( A \), thus \( 4\pi(A) = \pi(A) + \pi(A) + \pi(A) + \pi(A) \). Note in \( \mathbb{F}_2 \) that there is no distinction between sums and differences, thus for instance \( 4\pi(A) = 2\pi(A) - 2\pi(A) \).
Meanwhile, \( \|1_S\|_{L^1(F_2)} \geq \sigma \) by hypothesis. The claim now follows from the monotonicity of the Gowers norms (see, for example, [26, equation 11.7]).

Now suppose \( S, \sigma \) are as in the statement of Lemma 2.1, and let \( N \) and \( f \) be as in the above lemma. Assuming Conjecture 1.10 for this choice of \( f \), there exists a quadratic polynomial \( \Psi : \mathbb{F}_2^{n+N} \rightarrow \mathbb{F}_2 \) such that

\[
|E_{x \in \mathbb{F}_2^n} E_{y \in \mathbb{F}_2^n} 1_S(x)(-1)^{\phi(x) \cdot y} (1)^{\psi(x,y)}| \geq \sigma^C.
\]

Thus, for at least \( \geq \sigma^C 2^n \) values of \( x \in S \), one has

\[
|E_{y \in \mathbb{F}_2^n} (1)^{\phi(x) \cdot y} (1)^{\psi(x,y)}| \geq \sigma^C.
\] (2.1)

Let us fix \( x \) so that (2.1) holds. We may split \( \Psi(x, y) \) as

\[
\Psi(x, y) = \Psi(0, y) + \Psi(x, 0) - \Psi(0, 0) + B(x, y)
\] (2.2)

where \( B \) is the “mixed derivative” of \( \Psi \), defined as

\[
B(x, y) := \Psi(x, y) - \Psi(x, 0) - \Psi(0, y) + \Psi(0, 0).
\]

From (2.1) it thus follows that

\[
|E_{y \in \mathbb{F}_2^n} (1)^{\phi(x) \cdot y} (1)^{B(x, y)} (1)^{\psi(0, y)}| \geq \sigma^C.
\]

As \( \Psi \) is quadratic, \( B \) is bilinear in \( x \) and \( y \), and hence \( B(x, y) = \psi(x) \cdot y \) for some linear map \( \psi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \). We conclude that

\[
|E_{y \in \mathbb{F}_2^n} (1)^{\phi(x) - \psi(x) \cdot y} (1)^{\psi(0, y)}| \geq \sigma^C,
\]

which means that the function \( y \mapsto (1)^{\psi(0, y)} \) has a Fourier coefficient of size at least \( \sigma^C \) at \( \phi(x) - \psi(x) \). Hence by Plancherel’s theorem the number of such large Fourier coefficients is at most \( \sigma^{-2C} \). We conclude that \( \phi(x) - \psi(x) \) takes at most \( \sigma^{-2C} \) values on at least \( \sigma^C 2^n \) values of \( x \in S \), and the claim follows from the pigeonhole principle.

3. The integer case

We turn now to the proof that Conjecture 1.11 implies Conjecture 1.5. This argument goes along similar lines to that in the previous section, but is somewhat more involved since one must deal with nilsequences rather than quadratic forms. We present the argument in such a way as to emphasise the close parallels with the preceding section.

Once again matters rest on a reduction to an inverse theorem for approximate homomorphisms. We write \([N]\) for the set \([1, \ldots, N]\).

**Lemma 3.1 (Approximate homomorphisms).** Assume Conjecture 1.11. Suppose that \( N \) is a positive integer, that \( S \subseteq [N] \) is a set of cardinality \( \sigma N \), and that \( \phi : S \rightarrow \mathbb{Z} \) is a Freiman homomorphism on \( S \). Then there is a generalised arithmetic progression \( P \subseteq [N] \) of dimension \( \sigma^{-o(1)} \) and size at least \( \exp(-\sigma^{-o(1)}) N \) together with a Freiman homomorphism \( \psi : P \rightarrow \mathbb{Z} \) such that \( \phi(x) = \psi(x) \) for at least \( \exp(-\sigma^{-o(1)}) N \) values of \( x \in S \).

The proof that this lemma implies Conjecture 1.5 is not particularly onerous and goes along much the same lines as the argument in the previous section. Supposing that \( A \subseteq \mathbb{Z} \) is a \( K \)-approximate subgroup, Ruzsa’s “model lemma” [19, theorem 2] implies that there is a \( N \leq K^C |A| \) together with a subset \( A' \subseteq A \) of cardinality at least \( |A|/2 \) and a Freiman isomorphism \( \pi : A' \rightarrow S \) to a subset \( S \subseteq [N] \). Write \( \phi := \pi^{-1} \), and observe that \( \phi : S \rightarrow \mathbb{Z} \)
has image $\phi(S) = A'$. Noting that $|S| \geq K^{-C}N$, it follows from Lemma 3.1 and the fact that Freiman isomorphisms take generalised progressions to generalised progressions (see [26, proposition 5.24]) that at least $\exp(-K^{o(1)})|A|$ of $A$ is contained in a generalised progression in $\mathbb{Z}$ of dimension $K^{o(1)}$ and cardinality at most $N \leq K^{C}|A|$. Once again, standard covering arguments complete the deduction of Conjecture 1.5.

It remains to prove Lemma 3.1. The starting point is the following analogue of Lemma 2.2, showing how to convert Freiman homomorphisms to approximate quadratics.

**Lemma 3.2.** Let $N, M \geq 1$ be integers, let $S \subset [N]$ be such that $|S| \geq \sigma N$, and let $\phi : S \to \mathbb{Z}/MN\mathbb{Z}$ be a Freiman homomorphism. Define a function $f : \mathbb{Z}/4N\mathbb{Z} \to \mathbb{C}$ by

$$f(x + 4Ny) := \begin{cases} 1_\delta(x)e_M(\phi(x)y) & \text{if } x \in [N], y \in \mathbb{Z}/MN\mathbb{Z}; \\ 0 & \text{otherwise,} \end{cases}$$

where $e_M(x) := e^{2\pi i x/M}$, and $4Ny \in \mathbb{Z}/4N\mathbb{Z}$ is defined in the obvious manner for $y \in \mathbb{Z}/MN\mathbb{Z}$. Then $\|f\|_{u^1(\mathbb{Z}/4N\mathbb{Z})} \geq \sigma/4$.

**Proof.** Every parallelepiped in the support of $f$ is of the form $(x + \omega \cdot h, 4N(y + \omega \cdot k))_{\omega \in \{0,1\}^3}$, where $y \in \mathbb{Z}/MN\mathbb{Z}$, $k = (k_1, k_2, k_3) \in (\mathbb{Z}/MN\mathbb{Z})^3$, and $x + \omega \cdot h \in S$. By arguing exactly as in Lemma 2.2 we have that

$$\sum_{\omega \in \{0,1\}^3} (-1)^{\omega \cdot \phi(x + \omega \cdot h)}(y + \omega \cdot k) = 0$$

and so

$$\|f\|_{u^1(\mathbb{Z}/4N\mathbb{Z})} = \|1_\delta\|_{u^1(\mathbb{Z}/4N\mathbb{Z})}$$

where $\hat{S} := \{x + 4Ny : x \in S; y \in \mathbb{Z}/MN\mathbb{Z}\}$ is the support of $f$. But we have

$$\|1_\delta\|_{u^1(\mathbb{Z}/4N\mathbb{Z})} \geq \sigma/4$$

and the claim follows as before from the monotonicity of the Gowers norms.

We return now to the proof of Lemma 3.1. That lemma deals with Freiman homomorphisms $\phi : S \to \mathbb{Z}$. However such a map is a Freiman homomorphism if and only if the composition $\pi_M \circ \phi$ is a Freiman homomorphism for all sufficiently large $M$, and so we may suppose instead that $\phi$ maps $S$ to $\mathbb{Z}/MN\mathbb{Z}$ for some $M$.

Let $f$ be as in Lemma 3.2. Assuming Conjecture 1.11, it follows that there is some elementary 2-step nilmanifold $G/\Gamma$ of dimension at most $\sigma^{-o(1)}$, a function $F : G/\Gamma \to \mathbb{C}$ of Lipschitz constant at most $\exp(\sigma^{-o(1)})$, $g \in G$, and $x_0 \in G/\Gamma$ such that

$$|E_{x \in [N]}E_{y \in [M]}1_\delta(x)e_M(\phi(x)y)F(g^{x+4Ny}x_0)| \geq \exp(-\sigma^{-o(1)}).$$

Writing $x_0 = g_0\Gamma$ for some $g_0 \in G$ of distance at most $\exp(\sigma^{-o(1)})$ from the origin, and rewriting $g^{x+4Ny}x_0 = g_0\tilde{g}^{x+4Ny}\Gamma$ where $\tilde{g} := g_0^{-1}gg_0$, we see (after shifting $F$ by $g_0$ and replacing $g$ by $\tilde{g}$ if necessary) that we may normalise $x_0$ to be at the origin $\Gamma$. By embedding the skew torus in the Heisenberg group if necessary we may take $G$ to be a product of Heisenberg groups and hence, in particular, connected and simply-connected.

The vertical torus $[G, G]/(\Gamma \cap [G, G])$ of the elementary 2-step nilmanifold can be identified with a torus $(\mathbb{R}/\mathbb{Z})^{d_2}$ for some $d_2 \leq \sigma^{-o(1)}$. By standard harmonic analysis arguments (see, for example, [12, lemma A.9]) the Lipschitz function may be decomposed into a linear
Equivalence of PFR and PGI(3)

combination of at most $\exp(\sigma^{-o(1)})$ Fourier characters along the vertical direction with coefficients of magnitude at most $\exp(\sigma^{-o(1)})$, plus an error of $\exp(-\sigma^{-o(1)})$ in $L^\infty$. Applying the pigeonhole principle it follows that one may assume that $F$ is a vertical character, which means that there exists a character $\chi : [G, G]/(\Gamma \cap [G, G]) \to S^1$ such that

$$F(g_2 x) = \chi(g_2) F(x)$$

(3.1)

for all $x \in G/\Gamma$ and $g_2 \in [G, G]$ (where we lift $\chi$ to $[G, G]$ in the obvious fashion).

The Lipschitz function $|F|$ is now invariant under the action of the vertical torus and descends to a function on the horizontal torus $G/\Gamma[G, G]$, which can be identified with a torus $({\mathbb R}/\mathbb Z)^{d_1}$ for some $d_1 \leq \sigma^{-o(1)}$. By applying a Lipschitz partition of unity we may assume that $|F|$ (and hence $F$) is supported in a small ball in this torus, of radius less than $\exp(-\sigma^{-o(1)})$ say.

By the pigeonhole principle, we can now find $\geq \exp(-\sigma^{-o(1)}) N$ values of $x \in S$ such that

$$|\mathbb E_{y \in [M]} e_M(\phi(x) y) F(g^{x+4Ny} \Gamma)| \geq \exp(-\sigma^{-o(1)})$$

By pigeonholing in $x$ (reducing the number of available $x$ by a factor of $\exp(-\sigma^{-o(1)})$), we may assume that for all these $x$ the point $g^x\Gamma$ lies in a small ball $B$ in $G/\Gamma$, of radius less than $\exp(\sigma^{-o(1)})$.

We turn now to the task of simplifying $F(g^{x+4Ny}\Gamma)$; this may be thought of, roughly, as a quest to find a suitable analogue for the decomposition (2.2). To begin with let us expand $g^x$ as $\{g^x\}|g^x|$, where $\{g^x\} \in \Gamma$ and $\{g^x\}$ lies in a fundamental domain of $G/\Gamma$ that contains $B$ in its interior. As usual, write $[g, h] := ghg^{-1}h^{-1}$ for the commutator of two elements $g$ and $h$ in some ambient group. Now in any 2-step nilpotent group $G$ we have $[x^n, y] = [x, y]^n$ for all $x, y \in G$ and all $n \in \mathbb Z$; this follows from the commutator identity $[xy, z] = [y, z]x[x, z]$, which is valid in all groups. It follows that

$$g^{x+4Ny} = g^{4Ny}\{g^x\} = [g^{4N}, \{g^x\}]^y\{g^x\}g^{4Ny}\Gamma.$$ 

Since $F$ is a vertical character, we thus see that

$$F(g^{x+4Ny}\Gamma) = \chi([g^{4N}, \{g^x\}]^y\{g^x\}g^{4Ny}\Gamma)$$

and so

$$|\mathbb E_{y \in [M]} e_M\left(\frac{1}{M} \phi(x) - \psi(x)\right) F(g^{x+4Ny}\Gamma)| \geq \exp(-\sigma^{-o(1)})$$

for at least $\exp(-\sigma^{-o(1)}) N$ values of $x \in S$, where $\psi(x) \in \mathbb R/\mathbb Z$ is the phase such that

$$\chi([g^{4N}, \{g^x\}]) = e(\psi(x)).$$

By construction, $\{g^x\}$ is supported in a small ball centred at some $g_0 \in G$, of radius less than $\exp(-\sigma^{-o(1)})$. Provided that this ball is chosen small enough, the Lipschitz nature of $F$ guarantees that

$$|\mathbb E_{y \in [M]} e_M\left(\frac{1}{M} \phi(x) - \psi(x)\right) F(g_0g^{4Ny}\Gamma)| \geq \exp(-\sigma^{-o(1)}).$$

Recall that $|F|$ has small support, on account of the partition of unity that was brought into play earlier in the argument. We now let $F_0 : G/\Gamma \to \mathbb C$ be another function of Lipschitz

---

3 Several papers of the authors – for example the appendix of [12] – contain example computations of $\{g^x\}$ and $\{g^x\}$ on the Heisenberg group for fundamental domains like $\{-\frac{1}{2}, \frac{1}{2}\}$ or $[0, 1]^3$. 
constant at most $\exp(\sigma^{-o(1)})$ and with vertical character $\chi$ which has magnitude 1 on the support of $F(g_0)$; there are no topological obstructions to building such an $F_0$ if the support of $|F|$ is small enough (think, for example, of the function $\psi(0, y, z) e(z)$ on the Heisenberg nilmanifold $G/\Gamma$, where $\psi$ is supported on a small ball and equals 1 on a very small ball about the origin in the fundamental domain $(-1/2, 1/2)$).

With this function $F_0$ constructed we may write

$$F(g_0 g^{4N\gamma}) = \tilde{F}(g^{4N\gamma}) F_0(g^{4N\gamma})$$

where $\tilde{F} : G/\Gamma \to \mathbb{C}$ is the function

$$\tilde{F}(x) := F(g_0 x) \overline{F_0(x)}.$$

Observe that the function $\tilde{F}(x)$ is invariant under the action of the vertical torus, and thus descends to a function on $(\mathbb{R}/\mathbb{Z})^d$, which by abuse of notation we also call $\tilde{F}$. Thus

$$F(g_0 g^{4N\gamma}) = \tilde{F}(\pi(g^{4N\gamma})) F_0(g^{4N\gamma}),$$

where $\pi : G/\Gamma \to (\mathbb{R}/\mathbb{Z})^d$ is the projection onto the horizontal torus.

The function $\tilde{F}$ is Lipschitz with constant at most $\exp(\sigma^{-o(1)})$, and so (by [12, lemma A.9]) can be decomposed into a combination of at most $\exp(\sigma^{-o(1)})$ characters with coefficients at most $\exp(\sigma^{-o(1)})$, plus an error of size $\exp(-\sigma^{-o(1)})$. Meanwhile, $\pi(g^{4N\gamma}) \in (\mathbb{R}/\mathbb{Z})^d$ evolves linearly in $y$. By the pigeonhole principle, refining the set of available $x$ some more, we may thus assume that

$$|E_{y \in [M]} e\left(\left[\frac{1}{M} \phi(x) - \psi(x)\right] y\right) e(\xi_0 y) F_0(g^{4N\gamma})| \geq \exp(-\sigma^{-o(1)}).$$ (3.2)

for some $\xi_0 \in \mathbb{R}/\mathbb{Z}$ independent of $x$, and for at least $\exp(-\sigma^{-o(1)}) N$ values of $x$. Thus, the function $y \mapsto F_0(g^{4N\gamma})$ has a large Fourier coefficient at $1/M \phi(x) - \psi(x) + \xi_0$.

In the finite field argument we applied Plancherel’s theorem at this point. Here the appropriate tool is the large sieve, a kind of approximate version of Plancherel which states that a function $f : [M] \to \mathbb{C}$ cannot have large Fourier coefficients at many separated points. The following (standard) statement of it may be found in [5, chapter 27]: if the points $\theta_1, \ldots, \theta_K \in \mathbb{R}/\mathbb{Z}$ are $\delta$-separated then

$$\sum_{j=1}^K \left| \sum_{y \in [M]} f(y) e(y \theta_j) \right|^2 \leq (M + \delta^{-1}) \sum_{y \in [M]} |f(y)|^2.$$ 

Applying this to (3.2) and the remark following it, we see that the large Fourier coefficients $1/M \phi(x) - \psi(x) + \xi_0$ of the function $y \mapsto F_0(g^{4N\gamma})$ can be covered by at most $\exp(\sigma^{-o(1)})$ arcs of length $1/M$ on the unit circle $\mathbb{R}/\mathbb{Z}$. Pigeonholing, and refining the set of $x$ by yet another factor of $\exp(-\sigma^{-o(1)})$, we may assume that $1/M \phi(x) - \psi(x) + \xi_0$ lies inside a fixed arc of length $1/100M$. This implies, refining the set of $x$ one more time, that we may find a $\xi_1 \in \mathbb{R}/\mathbb{Z}$ such that for at least $\exp(-\sigma^{-o(1)}) N$ values of $x \in S$, $1/M \phi(x) - \psi(x) + \xi_1 \in [-1/100M, 1/100M]$.

By direct computations on the Heisenberg group along the lines of those in [12] we see that $\pi([g^s]) = (\alpha_1 x, \ldots, \alpha_d x)$ for some $\alpha_1, \ldots, \alpha_d \in \mathbb{R}/\mathbb{Z}$, and then that

$$\chi([g^{4N}, [g^s]]) = e\left(\sum_{j=1}^d \beta_j (\alpha_j x - \gamma_j)\right)$$
for some $\beta_j, \gamma_j \in \mathbb{R}/\mathbb{Z}$ independent of $x$. Here the fractional part $\{t\}$ of $t \in \mathbb{R}$ is chosen to lie in $(-\frac{1}{2}, \frac{1}{2})$, and the need for the shift $\gamma_j$ arises from the fact that $(g^\gamma)$ is chosen to lie in a fundamental domain of $G/\Gamma$ containing $B$ in its interior.

This means, of course, that
\[
\psi(x) = \sum_{j=1}^{d_1} \beta_j (\alpha_j x - \gamma_j).
\]

The set of all $x \in [N]$ such that $\pi(g^x \Gamma)$ lies within $\exp(-\sigma^{-o(1)})$ of the origin is a Bohr set of rank at most $\sigma^{-o(1)}$ and radius at least $\exp(-\sigma^{-o(1)})$, and hence by [20, theorem 3-1] (reproduced as Theorem B·2 in the appendix) it contains a proper symmetric generalised arithmetic progression $P$ of dimension at most $\sigma^{-o(1)}$ and cardinality at least $\exp(-\sigma^{-o(1)})N$.

By discarding generators of $P$ if necessary we may assume that all sidelengths of $P$ are at least $C_0$ for some constant $C_0$ to be specified later. By standard covering lemmas such as [26, lemma 2-14] we may cover $[N]$ by at most $\exp(\sigma^{-o(1)}N)$ translates of $P$, so by the pigeonhole principle we may assume that all the $x$ under discussion, that is to say those $x$ for which $\alpha_j x \approx \gamma_j$, are contained in a single translate $x_0 + P$ of $P$. Note that each map $x \mapsto \{\alpha_j x - \gamma_j\}$ is a Freiman homomorphism on $x_0 + P$ and hence so is the entire phase $\psi$.

If we let $Q$ be the set of all $x \in x_0 + P$ such that $\psi(x) - \xi_1$ lies within $1/100M$ of a multiple $1/M\phi(x)$ of $1/M$, where $\phi(x) \in \mathbb{Z}/M\mathbb{Z}$, then we conclude upon rounding to the nearest multiple of $1/M$ that $\tilde{\phi}$ is a Freiman homomorphism on $Q$. Also, from construction we see that $\phi(x) = \tilde{\phi}(x)$ for at least $\exp(-\sigma^{-o(1)})N$ values of $x \in S \cap Q$.

To conclude the argument one needs to show that $Q$ contains a generalised arithmetic progression of dimension at most $\sigma^{-o(1)}$ and cardinality at least $\exp(-\sigma^{-o(1)})N$ (since one can then cover $Q$ by at most $\exp(\sigma^{-o(1)})$ translates of such a progression). This will follow straightforwardly from the following lemma which, though it looks to be of a standard type, does not appear to be in the literature. A proof may be found in Appendix B.

**Lemma B·1.** Let $\epsilon \in (0, 1/2)$ be a real number. Suppose that $P$ is a $d$-dimensional proper progression with sidelengths $N_1, \ldots, N_d > C/\epsilon$ and that $\eta : P \to \mathbb{R}/\mathbb{Z}$ is a Freiman homomorphism which vanishes at some point of $P$. Then the set $\{x \in P : \|\eta(x)\|_{\mathbb{R}/\mathbb{Z}} \leq \epsilon\}$ contains a progression of dimension at most $d+1$ and size at least $(Cd)^{-d} \epsilon^{d+1} |P|$.

We shall apply the lemma with $\epsilon = 1/100$, this being valid if the constant $C_0$ was chosen to be large enough earlier on. Recall that there are many $x \in S \cap (x_0 + P)$ such that $1/M\phi(x) - \psi(x) + \xi_1 \in [-1/100M, 1/100M]$. Pick one such $x^*$, and take $\xi_2$ to be such that $1/M\phi(x^*) - \psi(x^*) + \xi_2 = 0$ and $\|\xi_1 - \xi_2\|_{\mathbb{R}/\mathbb{Z}} \leq 1/100M$. Now we simply apply Lemma B·1 to the progression $x_0 + P$, taking $\eta = M(\psi - \xi_2)$ and $\epsilon = 1/100$. The progression $Q$ contains the set $\{x \in x_0 + P : \|\eta(x)\|_{\mathbb{R}/\mathbb{Z}} \leq 1/100\}$, and of course $\eta$ vanishes at $x^*$. It follows from Lemma B·1 that $Q$ does indeed contain a generalised arithmetic progression of dimension at most $\sigma^{-o(1)}$ and cardinality at least $\exp(-\sigma^{-o(1)})N$, and this concludes the proof of Theorem 1·13.

### 4. Higher order correspondences

It appears that the correspondence between inverse sumset theorems and inverse conjectures for the Gowers norms have some partial higher order analogues, although the situation here is much less well understood. To illustrate this phenomenon, consider the following result, recently proven in [3, 27]. Here and for the rest of the section
we write \( \mathbb{F} := \mathbb{F}_5 \) for definiteness, although the same arguments would work for \( \mathbb{F}_p \) for any fixed prime \( p \geq 5 \). There are definite issues in extremely low characteristic: see for example [14, 18].

**Theorem 4.1 (GI(4) over \( \mathbb{F}^n \)).** For every \( K \geq 2 \) there exists an \( \varepsilon > 0 \) such that if \( f : \mathbb{F}^n \to \mathbb{C} \) is a \( K \)-approximate cubic in the sense that \( \| f \|_\infty \leq 1 \) and \( \| f \|_{U^4(\mathbb{F}^n)} \geq 1/K \), then \( f \) \( \varepsilon \)-correlates with a (genuine) cubic phase \( e_\varphi(\psi) \), where \( e_\varphi(x) := e^{2\pi i x/|\mathbb{F}|} \) and \( \psi : \mathbb{F}^n \to \mathbb{F} \) is cubic in the sense that \( \Delta_{h_1} \ldots \Delta_{h_4} \psi(x) = 0 \) for all \( x, h_1, \ldots, h_4 \in \mathbb{F}^n \).

We shall use this theorem to establish the following variant of Lemma 2.1.

**Proposition 4.2 (Approximate quadratic homomorphisms).** Suppose that \( \sigma \in (0, 1/2) \), that \( S \subseteq \mathbb{F}^n \) is a set of cardinality \( |\mathbb{F}|^n \), and that \( \phi : S \to \mathbb{F}^\infty \) is a Freiman quadratic on \( S \) in the sense that \( \sum_{\omega \in [0,1]^3} (-1)^{\omega} \phi(x + h \cdot \omega) = 0 \) whenever \( x \in \mathbb{F}^n \) and \( h = (h_1, h_2, h_3) \) with \( h_1, h_2, h_3 \in \mathbb{F}^n \) are such that \( x + \omega \cdot h \in S \). Then there is a quadratic map \( \psi : \mathbb{F}^n \to \mathbb{F}^\infty \) such that \( \phi(x) = \psi(x) \) for at least \( \varepsilon |\mathbb{F}|^n \) values of \( x \in S \), where \( \varepsilon = \varepsilon(\sigma) > 0 \) depends only on \( \sigma \).

The initial stages of the proof are very similar to those of Theorem 1.12 and we just sketch them. As before, we let \( N \) be large enough that \( \phi \) takes values in \( \mathbb{F}^N \), and considers the function \( f : \mathbb{F}^{n+N} \to \mathbb{C} \) defined by \( f(x, y) := 1_S(x) e_\varphi(\phi(x) \cdot y) \). A routine modification of Lemma 2.2 reveals that

\[
\| f \|_{U^4(\mathbb{F}^{n+N})} \geq \delta
\]

and by Theorem 4.1 we can find a cubic \( \Psi : \mathbb{F}^{n+N} \to \mathbb{F} \) such that

\[
|\mathbb{E}_{x \in \mathbb{F}^n} \mathbb{E}_{y \in \mathbb{F}^n} 1_S(x) e_\varphi(\phi(x) \cdot y - \Psi(x, y))| \geq \delta 1,
\]

where here we use \( X \geq \delta Y \) to denote the estimate \( X \geq C_\delta^{-1} Y \) for some \( C_\delta \) depending only on \( \delta \). Thus for \( \delta |\mathbb{F}|^n \) values of \( x \in S \), one has

\[
|\mathbb{E}_{y \in \mathbb{F}^n} e_\varphi(\phi(x) \cdot y - \Psi(x, y))| \geq \delta 1.
\]

The next step is to perform a decomposition of \( \Psi \) analogous to (2.2), but unfortunately the analogous decomposition is not so favourable. Namely, one has

\[
\Psi(x, y) = \Psi(0, y) + Q_x(y) + \psi(x) \cdot y + P(x)
\]

where \( Q_x : \mathbb{F}^N \to \mathbb{F} \) is a quadratic polynomial that varies affine-linearly in \( x \), \( \psi : \mathbb{F}^n \to \mathbb{F}^N \) is a quadratic polynomial, and \( P : \mathbb{F}^n \to \mathbb{F} \) is a cubic polynomial. We thus have

\[
|\mathbb{E}_{y \in \mathbb{F}^n} e_\varphi((\phi(x) - \psi(x)) \cdot y - Q_x(y) - \Psi(0, y))| \geq \delta 1
\]

(4.1) for \( \delta |\mathbb{F}|^n \) values of \( x \in S \).

The factor of \( e_\varphi(-Q_x(y)) \) in the functions \( f_x(y) := e_\varphi((\phi(x) - \psi(x)) \cdot y - Q_x(y)) \) prevents one from immediately using Plancherel’s theorem as in Section 2. However, from standard Gauss sum estimates (see e.g. [14, lemma 1.6]) we do have

\[
|(f_x, f_{x'})| \ll |\mathbb{F}|^{-\text{rk}(Q_x - Q_{x'})/2}
\]

(4.2) for any \( x, x' \). Here the rank of a quadratic form \( Q \) can be defined as the rank of the symmetric matrix describing the homogeneous part of \( Q \). By standard linear algebra there is a vector subspace \( V_Q \subseteq \mathbb{F}^n \) with \( \dim(V_Q) = \text{rk}(Q) \) such that \( Q(y) \) is a quadratic function of the inner products \( \langle v, y \rangle \), \( v \in V_Q \).
From (4.2) and a standard duality argument related to the large sieve (see, for example, [5, chapter 27, theorem 1]) one can show that there cannot exist \( k \) different \( x_1, \ldots, x_k \in S \) obeying (4.1) with \( \text{rk}(Q_{x_i} - Q_{x_j}) \geq k \), if \( k \) is large enough depending on \( \delta \). By the greedy algorithm, we may thus find \( x_1, \ldots, x_k \) with \( k \leq \delta \) such that \( \min_{1 \leq i \leq k} \text{rk}(Q_{x_i} - Q_{x_j}) \leq \delta \) for all \( x \) obeying (4.1). By pigeonholing in the \( x \) parameter, we conclude that there exists a quadratic form \( Q_{x_i} \) such that \( \text{rk}(Q_{x_i} - Q_{x_j}) \leq \delta \) for \( \delta |F|^n \) values of \( x \in S \). By translating we may normalise and take \( x_1 = 0 \).

Write \( Q_x' \) be the homogeneous quadratic component of \( Q_x - Q_0 \), so that \( Q_x' \) depends linearly on \( x \) and \( \text{rk}(Q_x') \leq \delta \) for \( \delta |F|^n \) values of \( x \in S \). Key to our argument is the following proposition concerning this situation, which may be of independent interest. It states that a linear function to the set of low-rank quadratics must, in a sense, be quite trivial.

**Proposition 4.3** (Triviality of linearly varying low-rank quadratic forms). *Let \( r \in \mathbb{N}_0 \) and suppose that \( \varepsilon \in (0, 1) \) is a real number. Suppose that \( x \mapsto Q_x \) is a linear map from \( F^n \) to the space of homogeneous quadratics over \( F^N \). For each such form \( Q_x \), associate the vector space \( V_x := V_{Q_x} \). Suppose that there is a set \( A \) of at least \( \alpha |F|^n \) values of \( x \) for which \( \text{rk}(Q_x') \leq r \). Then there is some vector space \( V \leq F^n, \dim(V) \leq r \), such that \( V_x \leq V \) for at least \( \alpha'(\alpha, r)|F|^n \) values of \( x \in A \), where \( \alpha : (0, 1] \times \mathbb{N}_0 \rightarrow \mathbb{R} \) takes positive values.*

**Proof.** We claim that under the stated hypotheses there is some vector \( v \) which lies in at least \( \alpha_0(\alpha, r)|F|^n \) of the spaces \( V_x \), where \( \alpha_0 \) is a function taking positive values. The proposition then follows quickly by induction on \( r \), upon passing to a coset of the codimension one subspace \( v^\perp \leq F^n \) which contains at least \( \alpha |v^\perp| \) elements of \( A \).

Now by a standard application of Cauchy–Schwarz (see, e.g, [26, corollary 2.10]) there are at least \( \alpha^4|F|^{3n} \) additive quadruples in \( A \), that is to say quadruples \( (x_1, x_2, x_3, x_4) \in A^4 \) with \( x_1 + x_2 = x_3 + x_4 \). We say that such a quadruple is good if \( V_{x_i} \cap (V_{x_j} + V_{x_k}) = \{0\} \) for all 24 choices of distinct \( i, j, k \in \{1, 2, 3, 4\} \).

**Case 1.** At least half of the additive quadruples in \( A \) are good. Fix a good quadruple \( (x_1, x_2, x_3, x_4) \in A^4 \). Let \( y, h, k \in F^n \) be arbitrary, and select \( h' \in (h + V_{x_1}^\perp) \cap (V_{x_2}^\perp \cap V_{x_3}^\perp) \) and \( k' \in (k + V_{x_1}^\perp) \cap V_{x_4}^\perp \). Straightforward linear algebra (and the goodness of the quadruple \( (x_1, x_2, x_3, x_4) \)) confirms that this is possible.

From the linearity of the map \( x \mapsto Q_x \) we have

\[
Q_{x_1}(y) + Q_{x_2}(y) - Q_{x_3}(y) - Q_{x_4}(y) = 0
\]

and

\[
Q_{x_1}(y + h') + Q_{x_2}(y + h') - Q_{x_3}(y + h') - Q_{x_4}(y + h') = 0.
\]

Since \( h' \in V_{x_2}^\perp \cap V_{x_3}^\perp \) the second of these implies that

\[
Q_{x_1}(y + h') + Q_{x_2}(y) - Q_{x_3}(y) - Q_{x_4}(y + h') = 0.
\]

Subtracting the first equation yields

\[
Q_{x_1}(y) - Q_{x_1}(y + h') - Q_{x_4}(y) + Q_{x_4}(y + h') = 0.
\]

Substituting \( y + k' \) for \( y \), recalling that \( k' \in V_{x_4}^\perp \), and subtracting, this implies that

\[
Q_{x_1}(y) - Q_{x_1}(y + h') - Q_{x_1}(y + k') + Q_{x_1}(y + h' + k') = 0.
\]
But $h - h'$ and $k - k'$ both lie in $V_{x_1}^\perp$, and so this implies that

$$Q_{x_1}(y) - Q_{x_1}(y + h) - Q_{x_1}(y + k) + Q_{x_1}(y + h + k) = 0.$$ 

Since $Q_{x_1}$ is a homogeneous quadratic and $h, k$ (and $y$) were arbitrary, this last equation implies that $Q_{x_1}$ is in fact zero.

Since no $x$ can be the $x_1$ term of more than $|\mathbb{F}|^{2n}$ additive quadruples, it follows that $Q_x = 0$ for at least $1/100\alpha^4|\mathbb{F}|^n$ values of $x$. On the other hand, the set of $x$ where $Q_x = 0$ is a subspace of $\mathbb{F}^n$, and the claim is thus verified in this case.

**Case 2.** At least half of the additive quadruples in $A$ are bad. Then (for example) there are at least $1/100\alpha^4|\mathbb{F}|^{3n}$ quadruples $(x_1, x_2, x_3, x_4) \in A^4$ with $V_{x_i} \cap (V_{x_2} + V_{x_3}) \neq \{0\}$. Since the first three terms $x_1, x_2$ and $x_3$ of an additive quadruple determine the fourth, it follows easily that there is some choice of $x_2, x_3$ such that $V_{x_i} \cap (V_{x_2} + V_{x_3}) \neq \{0\}$ for at least $1/100\alpha^2|\mathbb{F}|^n$ values of $x_1$. Since $V_{x_2} + V_{x_3}$ is a vector space of dimension at most $2r$, the claim follows in this case with $\alpha_0(\alpha, r) = (1/100)\alpha^2|\mathbb{F}|^{-2r}$.

We have verified the claim (with $\alpha_0(\alpha, r) = (1/100)\alpha^4|\mathbb{F}|^{-2r}$, say) in all cases and hence the proposition is proved.

**Remark.** An inspection of the argument reveals that the function $\alpha'(\alpha, r)$ in this proposition can be taken to have the form $(\alpha/C)^C$.

Let us return now to (4.1), which stated that

$$|\mathbb{E}_{y \in \mathbb{F}^N} e_{\mathbb{F}}(\phi(x) - \Psi(x)) \cdot y - Q_x(y) - \Psi(0, y))| \gg \delta^1$$

for $\gg \delta|\mathbb{F}|^n$ values of $x \in S$. In the subsequent discussion we passed to a further subset of $\gg \delta|\mathbb{F}|^n$ values of $x$ for which $\text{rk}(Q_x - Q_0) \ll \delta^1$. Writing $Q_x'$ for the homogeneous quadratic part of $Q_x - Q_0$, we may use Proposition 4.3 to assert that there is some subspace $V \leq \mathbb{F}^N$, $\dim V \leq \delta^1$, such that $Q_x'(y)$ is a quadratic function of the inner products $\langle v, y \rangle$, $v \in V$. The coefficients of this quadratic function vary linearly in $x$, but this is unimportant.

By foliating into cosets of $V^\perp$, we may find a $1$-bounded function $F$ supported on some coset $t + V^\perp$ and a quadratic polynomial $\tilde{\Psi} : \mathbb{F}^n \to \mathbb{F}^N$ such that

$$\mathbb{E}_{y \in \mathbb{F}^N} F(y) e_{\mathbb{F}}((\phi(x) - \tilde{\Psi}(x)) \cdot y) \gg \delta^1$$

for $\gg \delta|\mathbb{F}|^n$ values of $x \in S$. Note that the quadratic $\tilde{\Psi}$ has been adjusted to take account for the possibility that $Q_x$ contains linear terms in $y$ (which also depend affine-linearly on $x$).

To conclude the argument we simply apply the Plancherel argument from Section 2. This tells us that there are $\ll \delta^1$ values of $r$ for which

$$\mathbb{E}_{y \in \mathbb{F}^N} F(y) e_{\mathbb{F}}(r \cdot y) \gg \delta^1.$$ 

It follows from the pigeonhole principle that there is some $r$ such that $\phi(x) - \tilde{\Psi}(x) = r$ for $\gg \delta|\mathbb{F}|^n$ values of $x \in S$, which implies Proposition 4.2.

**Remark.** Because of the use of the rank reduction argument in the proof of Proposition 4.3, the proof above does not seem to imply any implication between a conjectural polynomial version of Theorem 4.1, and a polynomial version of Proposition 4.2. Also, we do not know if the implication can be reversed; the proof of Theorem 4.1 in [3, 27], is somewhat different from the arguments in [7, 8, 13, 23], relying instead on ergodic theory and cohomological tools.

**Appendix A. Deduction of PGI(3) from PFR**

In this appendix we sketch how the polynomial Frei–Ruzsa conjectures (Conjectures 1-5, 1-6) imply their respective polynomial inverse conjectures for the Gowers norms
Equivalence of PFR and PGI(3)

(Conjectures 1.10, 1.11). Roughly speaking, the idea is to run the arguments in [23] or [13] verbatim, but substituting the polynomial Freiman–Ruzsa conjectures in one key step of the argument where the usual inverse sumset theorems (basically, Theorem 1.2 or 1.3 respectively) are currently used instead. It should be noted that the bulk of this implication is due to Gowers [7, 8].

Our sketch will be somewhat brief and in particular we will assume familiarity with either [23] or [13] as appropriate. In the finite field case (i.e. the deduction of Conjecture 1.10 from Conjecture 1.5) the modification is particularly straightforward; one simply repeats the argument in [23], but replacing [23, theorem 6.9] (which is essentially Theorem 1.2) by Conjecture 1.5 instead. To spell out the steps in a little more detail, suppose that $K \geq 2$, and let $f : \mathbb{F}_2^n \to \mathbb{C}$ be a $K$-approximate quadratic: that is to say $\|f\|_{U^1(\mathbb{F}_2^n)} \geq 1/K$. By repeating the arguments up to and including [23, lemma 6.7], one can find a function $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that the set

$$\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : \phi(x + y) = \phi(x) + \phi(y); |\hat{f}_x(x)|, |\hat{f}_y(y)|, |\hat{f}_{x+y}(x + y)| \geq K^{-C}\}$$

has density $\geq K^{-C}$ in $\mathbb{F}_2^n \times \mathbb{F}_2^n$, where $f_z(y) := f(x+y)\overline{f}(x)$ and $\hat{f}(x) = \mathbb{E}_{y \in \mathbb{F}_2^n} f(y)(-1)^{x \cdot y}$ is the usual Fourier transform. Now let

$$A := \{x \in \mathbb{F}_2^n : |\hat{f}_x(x)| \geq K^{-C}\}.$$

Arguing as in [23, section 6], but using Conjecture 1.5 instead of [23, theorem 6.9], one finds a linear transformation $D : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $z \in \mathbb{F}_2^n$ such that $\phi(x) = Dx + z$ for a proportion at least $cK^{-C}$ of all $x \in A$, and thus

$$\mathbb{E}_{x \in \mathbb{F}_2^n} |\hat{f}_x(Dx + z)|^2 \geq K^{-C}.$$

By modulating $f$ by a suitable linear phase we may normalise so that $z = 0$. Continuing the argument in [23, section 6] one concludes that the subspace $U := \{x \in \mathbb{F}_2^n : Dx = D'x\}$ of $\mathbb{F}_2^n$ has density $\geq K^{-C}$, and so by further continuation of the argument one can find a symmetric transformation $B : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with zero diagonal coefficients such that

$$\mathbb{E}_{x \in \mathbb{F}_2^n} |\hat{f}_x(Bx)|^2 \geq K^{-C}.$$

From the structure of $B$ one can $B = M + M'$ for some transformation $M : \mathbb{F}_2^n \to \mathbb{F}_2^n$. A little Fourier analysis then shows that the function $(-1)^{x \cdot M} f(x)$ has a $U^2(\mathbb{F}_2^n)$ norm of at least $K^{-C}$, and so has an inner product of at least $K^{-C}$ with a linear character, and Conjecture 1.10 follows.

We turn now to the integer case, i.e. the deduction of Conjecture 1.11 from Conjecture 1.6. This requires a little more modification, because the arguments in [13] proceeded not via inverse sumset theorems, but instead via the (closely related) device of Bogulybov-type theorems.\(^4\) We think, in particular of [13, lemma 6.3]). However, as noted in [7], one could substitute inverse sumset theorems for Bogolyubov-type theorems at this stage.

We turn to the details. Let $K \geq 2$ and suppose that $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ is a $K$-approximate quadratic where, for simplicity, $N$ is odd (this in fact implies the general case, an exercise we leave to the reader). Applying [13, proposition 5.4], there is a set $H' \subset \mathbb{Z}/N\mathbb{Z}$ of size $|H'| \geq K^{-C}N$ and a function $\xi : H' \to \mathbb{Z}/N\mathbb{Z}$ whose graph

$$\Gamma' := \{(h, \xi(h)) : h \in H'\}$$

\(^4\) It is possible that polynomial variants of these Bogolyubov-type theorems also hold, but so far as we know conjectures of this type are strictly stronger than Conjectures 1.5 and 1.6.
is such that $|9\Gamma' - 8\Gamma'| \leq K^CN$, and such that
\[ |\hat{f}_h(\xi)| \geq K^{-C} \]
for all $h \in H''$, where $f_h(x) := f(x + h)\widehat{f}(x)$ as before, and $\hat{f}(\xi) := \mathbb{E}_{\xi \in \mathbb{Z}/N\mathbb{Z}} f(x)e_N(x\xi)$ is the usual Fourier transform.

Applying [13, proposition 9-1], one obtains a regular Bohr set $B_1 := B(S, \rho)$ with $|S| \leq K^C$, $1/16 \leq \rho \leq 1/8$ and $x_0, \xi \in \mathbb{Z}/N\mathbb{Z}$, as well as a locally linear function $M : B(S, 1/4) \to \mathbb{Z}/N\mathbb{Z}$ such that
\[ \mathbb{E}_{h \in B_1} \mathbb{1}_{H''}(x_0 + h)\mathbb{1}_{\xi h + 2Mh + \xi_0} \geq K^{-C}. \] (A.1)

This was eventually used in [13] to deduce Theorem 1-9. An inspection of that deduction reveals that the argument would also work just as well if the Bohr set $B(S, \rho)$ were replaced with a symmetric progression of dimension at most $K^C$ and cardinality at least $\exp(-K^C)N$. Furthermore, if one could instead replace $B(S, \rho)$ with a progression of dimension at most $K^{o(1)}$ and cardinality at least $\exp(K^{-o(1)})N$ then one could conclude Conjecture 1-11 instead of Theorem 1-9. Thus, our only task is to alter the argument of [13, proposition 9-1], using the additional input of Conjecture 1-5, to obtain such a progression in place of $B(S, \rho)$.

By Conjecture 1-6 $\Gamma'$ has large intersection with a translate of a symmetric generalised arithmetic progression $P$ of dimension at most $K^{o(1)}$ and cardinality at most $e^{K^{o(1)}}N$. By [26, theorem 3-40], $P$ contains a proper symmetric generalised arithmetic progression $P' \ni \{l_1x_1 + \cdots + l_dx_d : |l_i| \leq L_i\}$ in $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ of dimension $d \leq K^{o(1)}$ and volume at least $e^{K^{o(1)}}N$. The progression $P' - P'$ need not be a graph. However, since $P' - P' + \Gamma' \subset 2P - P$ has size at most $e^{K^{o(1)}}N$, and $\Gamma'$ is a graph, we see that the intersection of $P'$ with the vertical axis $\{0\} \times \mathbb{Z}/N\mathbb{Z}$ has cardinality at most $e^{K^{o(1)}}$, thus $P'$ is in some sense “almost a graph” up to factors of $e^{K^{o(1)}}$. Applying [13, lemma 8-3] one can then find a Bohr set $B(S, 1/4)$ in $\mathbb{Z}/N\mathbb{Z}$ with $|S| \leq K^{o(1)}$ such that $P - P \cap (\{0\} \times B(S, 1/4)) = \{0\}$. In particular, the set $P'' := P' \cap (\mathbb{Z}/N\mathbb{Z} \times B(S, 1/8))$ is a graph.

One can write $P'' := \phi(B)$, where $B$ is the box $\{l_1, \ldots, l_d \in \mathbb{Z} : |l_i| \leq L_i\}$ in $\mathbb{Z}^d$ and $\phi : \mathbb{Z}^d \to (\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z})$ is the homomorphism $\phi(l_1, \ldots, l_d) := l_1x_1 + \cdots + l_dx_d$. Observe that $P'' = \phi(B \cap B(S', 1/8))$ for some Bohr set $B(S', 1/8)$ in $\mathbb{Z}^d$. Applying Lemma B-1 $|S'|$ times we see that $B \cap B(S', 1/8)$ contains a symmetric generalised arithmetic progression $Q$ of dimension at most $K^{o(1)}$ and volume at least $e^{-K^{o(1)}}N$. By shrinking $Q$ slightly we may in fact assume that $Q - Q \subset B \cap B(S', 1/8)$. Then $\phi(Q - Q)$ is a graph, or equivalently that $\phi(Q)$ is Freiman isomorphic to its projection $\pi(\phi(Q))$ to the first factor $\mathbb{Z}/N\mathbb{Z}$ of $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Since $P'$ was proper, we see that $\pi(\phi(Q))$ is also proper. We then conclude that
\[ \phi(Q) = \{(x, Mx + \xi) : x \in \pi(\phi(Q))\} \]
where $\xi \in \mathbb{Z}/N\mathbb{Z}$, and $M : \pi(\phi(Q)) \to \mathbb{Z}/N\mathbb{Z}$ is locally linear.

As $Q$ is a progression, we can find $Q' - Q'$ inside $Q$ where $Q' \subset Q$ is another progression with dimension at most $K^{o(1)}$ and cardinality at least $e^{-K^{o(1)}}N$. The set $\phi(Q')$ has relative density at least $e^{-K^{o(1)}}N$ inside $P$, which has a doubling constant of at most $e^{K^{o(1)}}$, so by standard covering lemma arguments (see e.g. [26, lemma 2-14]) one can cover $P$ by at most $e^{K^{o(1)}}$ translates of $\phi(Q') - \phi(Q') \subset \phi(Q)$. In particular, by the pigeonhole principle, some translate of $\phi(Q)$ intersects $\Gamma'$ in at least $e^{-K^{o(1)}}N$ points. If one then repeats
the arguments used to prove [13, proposition 9.1] one obtains what was claimed, namely an analogue of (A.1) with $B(S, \rho)$ replaced by a progression of dimension $K^{o(1)}$ and size at least \( \exp(-K^{o(1)})N \).

**Appendix B. Bohr sets in generalised progressions**

The aim of this appendix is to prove Lemma B.1, the statement of which was as follows.

**Lemma B.1.** Let \( \epsilon \in (0, 1/2) \) be a real number. Suppose that \( P \) is a \( d \)-dimensional proper progression with sidelengths \( N_1, \ldots, N_d > C/\epsilon \) and that \( \eta: P \rightarrow \mathbb{R}/\mathbb{Z} \) is a Freiman homomorphism which vanishes at some point of \( P \). Then the set \( \{x \in P : \|\eta(x)\|_{\mathbb{R}/\mathbb{Z}} \leq \epsilon\} \) contains a progression of dimension at most \( d \) and size at least \( (Cd)^{d} \epsilon^{d+1}|P| \).

**Proof.** The progression \( P \) is an affine image of some box \( [N_1] \times \cdots \times [N_d] \), and the lift of \( \eta \) to this box is an affine map of the form \( x \rightarrow \alpha_1 x_1 + \cdots + \alpha_d x_d + \beta \). Henceforth we abuse notation by identifying \( P \) with the box \( [N_1] \times \cdots \times [N_d] \). We are told that there is a point \( x^* \) such that \( \eta(x^*) = 0 \). By reparametrisation if necessary, we may assume that \( x^* \) is in the same quadrant of \( P \) as the origin, thus \( x^* \in [N_1/2] \times \cdots \times [N_d/2] \). It turns out to be inconvenient later on if \( x^* \) is too close to the boundary of \( P \), so we begin with a preliminary argument to find a point \( x^{**} \) which is deeper in the interior of \( P \) than \( x^* \), and at which \( \eta \) is still small. To do this consider some \( m := \lceil 2/\epsilon \rceil + 1 \) points \( x_1, \ldots, x_m \in P \) such that the \( j \)th coordinate of \( x_i \) is roughly \( iN_i/3m \). By the pigeonhole principle there must be some pair of indices \( s < t \) such that \( \|\eta(x_i - x_j)\|_{\mathbb{R}/\mathbb{Z}} \leq \epsilon/2 \), and then the point \( x^{**} := x^* + x_i - x_j \) will have the property that all of its coordinates lie between \( \epsilon N_j/10 \) and \((1 - \epsilon/10)N_j\) (note that we implicitly used here the fact that \( N_j > C/\epsilon \)).

Let us nowcentre so that \( x^{**} \) is at the origin. Since \( x^{**} \) was chosen to be somewhat central to \( P \), the progression \( P \) certainly contains the symmetric progression \( P' := \prod_{j=1}^{d} [-N'_j, N'_j] \) in this new coordinate system, where \( N'_j := \epsilon N_j/10 \). Henceforth we work entirely in this new coordinate system and with this new progression \( P' \). The Freiman homomorphism \( \eta: P' \rightarrow \mathbb{R}/\mathbb{Z} \) now takes the form \( \eta(x) = \alpha_1 x_1 + \cdots + \alpha_d x_d + \beta \) where \( \|\beta\|_{\mathbb{R}/\mathbb{Z}} \leq \epsilon/2 \), and we may of course assume that \( 0 \leq \alpha_j < 1 \) for each \( j \).

At this point, one could conclude the argument (with worse bounds than claimed) using [26, lemma 4.20, lemma 4.22], because the set where \( \eta \) is small is essentially a Bohr set in \( P' \). To get the sharper bounds claimed in the theorem, we use a well-known lemma of Ruzsa [20, theorem 3.1], in which the structure of Bohr sets was elucidated using the geometry of numbers.

**Lemma B.2.** Suppose that \( M \geq 1 \) is an integer, that \( r_1, \ldots, r_d \) are residues (mod \( M \)) such that \( \gcd(r_1, \ldots, r_k, M) = 1 \), and that \( \epsilon_1, \ldots, \epsilon_d \in (0, 1/2) \) are real numbers. Then the Bohr set

\[
B(r_1, \ldots, r_d; \epsilon_1, \ldots, \epsilon_d) := \{x \in \mathbb{Z}/M\mathbb{Z} : \|r_1 x/M\|_{\mathbb{R}/\mathbb{Z}} \leq \epsilon_1, \ldots, \|r_d x/M\|_{\mathbb{R}/\mathbb{Z}} \leq \epsilon_d\}
\]

contains a \( d \)-dimensional progression (that is, the image of a box under an affine map from \( \mathbb{Z}^d \) to \( \mathbb{Z}/M\mathbb{Z} \)) of cardinality at least \( d^{-d} \epsilon_1 \cdots \epsilon_d M \).

Let \( M_1 \geq \cdots \geq M_d \) be a very large odd coprime integers and set \( M := M_1 \cdots M_d \). Set \( r_j := M_{j+1} \cdots M_d \) for \( j = 1, \ldots, d-1 \) and \( r_d := 1 \). For each \( j = 1, \ldots, d \) choose an integer \( s_j, 0 \leq s_j < M_j \), such that \( |s_j/M_j - \alpha_j| \leq 1/M_j \). Set \( r_{j+1} := r_j s_1 + \cdots + r_d s_d \). Finally, set \( \epsilon_j := N'_j/2M_j \) for \( j = 1, \ldots, d \) and \( \epsilon_{d+1} := \epsilon/4 \). Our contention is that the Bohr
set $B' = B(r_1, \ldots, r_d; \varepsilon_1, \ldots, \varepsilon_{d+1})$ is contained in a set which is Freĭman isomorphic to $\{x \in P : \|\eta(x)\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon\}$, at which point Lemma B.1 follows easily from Lemma B.2. To begin with we show that the Bohr set $B = B(r_1, \ldots, r_d; \varepsilon_1, \ldots, \varepsilon_d)$ is contained in a Freĭman-isomorphic copy of $P$. Suppose that $x \in \mathbb{Z}/M\mathbb{Z}$ lies in $B = B(r_1, \ldots, r_d; \varepsilon_1, \ldots, \varepsilon_d)$. If $x \in \mathbb{Z}/M\mathbb{Z}$, we may write

$$x = x_1 + x_2M_1 + \cdots + x_dM_1 \cdots M_{d-1}$$

for unique integers $x_1, \ldots, x_d$ with $|x_j| < M_j/2$. Observe that

$$\frac{r_1x}{M} \equiv \frac{x_1}{M_1} \pmod{1}, \quad \frac{r_2x}{M} \equiv \frac{x_1}{M_1M_2} + \frac{x_2}{M_2} \pmod{1},$$

and so on. If $x \in B$ then these may be applied in succession to obtain $\|r_1x/M - x_1/M_1\|_{\mathbb{R}/\mathbb{Z}} = 0$,

$$\left\| \frac{r_2x}{M} - \frac{x_2}{M_2} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{\varepsilon_1}{M_2}, \quad \left\| \frac{r_3x}{M} - \frac{x_3}{M_3} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{\varepsilon_1}{M_2M_3} + \frac{\varepsilon_2}{M_3},$$

and so on. If the $M_j$ are chosen appropriately (with $M_1$ much bigger than $M_2$ and so on) this implies that $\|x_j/M_j\| \leq 2\varepsilon_j$ for $j = 1, \ldots, d$, which implies that $|x_j| \leq N'_j$ for all $j$.

Now we have

$$\left\| \frac{s_1x_1}{M_1} + \cdots + \frac{s_dx_d}{M_d} - \eta(x) \right\|_{\mathbb{R}/\mathbb{Z}} \leq \left\| \frac{s_1}{M_1} - \alpha_1 \right\|_{\mathbb{R}/\mathbb{Z}} |x_1| + \cdots + \left\| \frac{s_d}{M_d} - \alpha_d \right\|_{\mathbb{R}/\mathbb{Z}} |x_d| \leq \frac{N'_1}{M_1} + \cdots + \frac{N'_d}{M_d} \leq \frac{\varepsilon}{8},$$

provided that the $M_j$ are chosen large enough in terms of $N'_1, \ldots, N'_d$ and $\varepsilon$.

Furthermore the inequalities (B.1) imply that $\|s_1r_1x/M - s_1x_1/M_1\| = 0$,

$$\left\| \frac{s_2r_2x}{M} - \frac{s_2x_2}{M_2} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{s_2\varepsilon_1}{M_2} \leq \varepsilon_1,$$

$$\left\| \frac{s_3r_3x}{M} - \frac{s_3x_3}{M_3} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{s_3\varepsilon_1}{M_2M_3} + \frac{s_3\varepsilon_2}{M_3} \leq \frac{\varepsilon_1}{M_2} + \varepsilon_2,$$

and so on. Adding, we clearly obtain

$$\left\| \frac{r_{d+1}x}{M} - \frac{s_1x_1}{M_1} - \cdots - \frac{s_dx_d}{M_d} \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{\varepsilon}{8}$$

provided that the $M_i$ are selected to be large enough.

Combining this with (B.2), we obtain

$$\left\| \frac{r_{d+1}x}{M} - \alpha_1x_1 - \cdots - \alpha_dx_d \right\|_{\mathbb{R}/\mathbb{Z}} \leq \frac{\varepsilon}{4},$$

and hence if $x \in B$ we certainly have $\|\alpha_1x_1 + \cdots + \alpha_dx_d\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon/2$ and hence $\|\eta(x)\|_{\mathbb{R}/\mathbb{Z}} \leq \varepsilon$.

Acknowledgements. This work was completed while the authors were attending the programme on Ergodic Theory and Harmonic Analysis at MSRI and they would like to thank the Institute for providing excellent working conditions.

REFERENCES

[1] V. Bergelson, B. Host and B. Kra. Multiple recurrence and nilsequences (with an appendix by I. Z. Ruzsa). Invent. Math. 160, 2 (2005), 261–303.
Equivalence of PFR and PGI(3)