Combinatorics, Probability and Computing (2009) 18, 861–870. © Cambridge University Press 2009
doi:10.1017/S0963548309009870 First published online 30 March 2009

Structure Along Arithmetic Patterns in Sequences of Vectors

P. CANDELA

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge,
Wilberforce Road, Cambridge CB3 0WB, UK
(e-mail: pc308@cam.ac.uk)

Received 20 March 2008; revised 4 January 2009

We discuss a new direction in which the use of some methods from arithmetic combinatorics can be extended. We consider functions taking values in Euclidean space and supported on subsets of $\{1, 2, \ldots, N\}$. In this context we present a proof of a natural generalization of Szemerédi's theorem. We also prove a similar generalization of a theorem of Sárkőzy using a vector-valued Fourier transform, adapting an argument of Green and obtaining effective bounds.

1. Introduction

Many central results in arithmetic combinatorics rely on techniques to analyse a complex-valued function on a finite abelian group using tools such as the discrete Fourier transform and results from combinatorics. A question regarding the arithmetic structure of a subset A of $[N] = \{1, 2, \ldots, N\}$ is often addressed by applying these techniques to the function $A(x)$ defined on $[N]$ by $A(x) = 1$ if $x \in A$, and $A(x) = 0$ otherwise.

Here, instead of $A(x)$, we consider a vector-valued function $V : [N] \to \mathbb{S}^{N-1} \cup \{\mathbf{0}\}$, where $\mathbb{S}^{N-1}$ denotes the unit sphere in Euclidean space $\mathbb{R}^N$. We shall consider questions which combine the vector structure and the arithmetic structure.

Let us suppose for the moment that V is non-zero on all of $[N]$. One simple pattern that we can seek is the existence of two vectors $V(x)$, $V(y)$, with their standard inner product $\langle V(x), V(y)\rangle$ in some prescribed subset of $[-1, 1]$. Note that for no fixed $\gamma \in [-1, 1)$ can we expect to always find x and y such that $\langle V(x), V(y)\rangle \leqslant \gamma$, as shown by the counterexample consisting of a constant function V. Nor can we expect $\langle V(x), V(y)\rangle \geqslant \gamma$ for a prescribed *positive* γ, for V could be an orthonormal basis of $\mathbb{R}^N$. However, given $0 < \gamma \leqslant 1$, if N is large then we can expect to find distinct x, y with $\langle V(x), V(y)\rangle \geqslant -\gamma$. Indeed, since

$$0 \leqslant \left\langle \sum_x V(x), \sum_y V(y) \right\rangle = N + \sum_{x \neq y} \langle V(x), V(y)\rangle,$$

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

we see that

$$\exists\, x \neq y, \quad \langle V(x), V(y)\rangle \geqslant -\frac{1}{N-1}, \tag{1.1}$$

so it suffices to have $N \geqslant 1+\gamma^{-1}$.

Let us now consider a function V which is not supported on all of $[N]$. We shall denote such a function by V_A, where A is a proper subset of $[N]$, and for each $x \in A$, $V_A(x) \in \mathbb{S}^{N-1}$, and $V_A(x) = \mathbf{0}$ otherwise. By the above argument, if $|A| \geqslant 1+\gamma^{-1}$, then we can find distinct x, y in A such that $\langle V_A(x), V_A(y)\rangle \geqslant -\gamma$. We may then ask whether this property can hold in conjunction with some prescribed arithmetic relationship between x and y. A simple question of this kind, involving both the vector structure and the arithmetic structure, was put by Gowers.

Question 1.1. *Given $\alpha, \gamma > 0$, if N is sufficiently large, A is any subset of $[N]$ of density α, and $V_A : [N] \to \mathbb{S}^{N-1} \cup \{\mathbf{0}\}$ is supported on A, must there exist distinct x, y in A differing by a square and such that $\langle V_A(x), V_A(y)\rangle \geqslant -\gamma$?*

A positive answer yields a 'vector-valued' version of a theorem of Sárkőzy. The theorem in question states that if $A \subset [N]$ has size αN and $N > N_1(\alpha)$ is sufficiently large, then there exist distinct elements x, x' in A such that $x - x'$ is a square. Furstenberg proved an infinitary version of this theorem using ergodic theory. Sárkőzy's proof in [5] gave the first effective bound on $N_1(\alpha)$. In [3], using Fourier analysis on $\mathbb{Z}_N$, Green gave a relatively simple proof of the following version of the theorem.

Theorem 1.2. *There is a constant C such that, if A is a subset of $[N]$ of density at least $C(\log\log N)^{-1/11}$, then A contains two distinct elements differing by a square.*

Note that if V_A took values in $\mathbb{S}^M$ with M bounded as $N \to \infty$, then a positive answer to Question 1.1 would follow easily from Theorem 1.2. Indeed, we could then partition $\mathbb{S}^M$ into K regions, with K dependent only on M and γ, in such a way that two vectors in the same region have inner product at least $-\gamma$, and then we could pass to a subset A' of A of size at least $|A|/K$ with all corresponding vectors in the same region. Applying Theorem 1.2 to A', we would obtain the required result. (For instance, we could cover the sphere with $K \geqslant 2^{cM}$ spherical caps of appropriate radius, for some positive $c = c(\gamma)$; this would result in a lower bound for N triply exponential in M.) From now on we shall focus on the full-dimensional case of Question 1.1, *i.e.*, when V_A can take any value in $\mathbb{S}^{N-1}$.

In Section 3 we will answer Question 1.1 positively using a vector-valued Fourier transform and adapting the iterative argument used by Green in [3]. This will give a bound for N which is doubly exponential in α and γ.

To introduce the next result let us elaborate on the simple property (1.1). Given α, γ and a function V_A as in Question 1, we define a graph G_γ with vertex set A and edges consisting of pairs of elements $x, y \in A$ such that $\langle V_A(x), V_A(y)\rangle \geqslant -\gamma$. Then we can deduce that G_γ has large cliques. Indeed, by (1.1) we know that G_γ has no independent set of size greater than $1+\gamma^{-1}$, so it follows from Ramsey's theorem ([1], VI.1, Theorem 1) and the simple bound $\binom{n}{t} \leqslant n^t$ that G_γ contains a clique of size at least about $(\alpha N)^\gamma$. We can then ask whether, for any fixed α, γ, k, for

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

sufficiently large N there exists always a complete subgraph of order k in G_γ with, in addition, some prescribed arithmetic structure on the vertices of the subgraph. Considering arithmetic progressions as the epitome of additive structure, the following question arises naturally.

Question 1.3. *Given $\alpha, \gamma > 0$ and a positive integer k, if N is sufficiently large, A is a subset of $[N]$ of density α, and $V_A : [N] \to \mathbb{S}^{N-1} \cup \{\mathbf{0}\}$ is supported on A, must there exist an arithmetic progression P of length k in A such that for any $x, y \in P$ we have $\langle V_A(x), V_A(y)\rangle \geqslant -\gamma$?*

In the next section we present an argument which answers this question positively, thus giving a 'vector-valued' analogue of the finitary version of Szemerédi's theorem, although the dependence of the bound for N on α, γ is much worse than that which we shall obtain for Question 1.1 in Theorem 3.1 below.

2. A vector-valued version of Szemerédi's theorem

We recall the finitary version of Szemerédi's theorem.

Theorem 2.1. *Let k be a positive integer and let $\alpha > 0$. There exists a positive integer $N = N(k, \alpha)$ such that every subset of $[N]$ of size at least αN contains an arithmetic progression of length k.*

We shall use the following well-known corollary, which is easily obtained by adapting an argument of Varnavides from [7].

Corollary 2.2. *Let k be a positive integer and let $\alpha > 0$. Then there exists a positive integer $N_0 = N_0(k, \alpha)$ and a constant $c = c(k, \alpha) > 0$ such that if $N > N_0$ and A is a subset of $[N]$ of size at least αN, then there are at least cN^2 distinct arithmetic progressions of length k in A.*

Our aim is to prove the following result.

Theorem 2.3. *Let k be a positive integer and let $\alpha, \gamma > 0$. Then there exists $N_0 = N_0(k, \alpha, \gamma)$ such that for any $N > N_0$, any subset $A \subset [N]$ of density at least α, and any function $V_A : [N] \to \mathbb{S}^{N-1} \cup \{\mathbf{0}\}$ supported on A, there is an arithmetic progression P of length k in A with $\langle V_A(x), V_A(y)\rangle \geqslant -\gamma$ for any $x, y \in P$.*

Ultimately we are interested in whether this theorem can be proved with bounds for N_0 which fall in line with the usual bounds from additive combinatorics, such as the bounds for Theorem 2.1 proved by Gowers in [2]. A first step is to find a proof of Theorem 2.3 which uses, in a relatively simple manner, known results like Theorem 2.1, albeit perhaps producing bad bounds for N_0. Finding such a proof was the object of discussions of the author with Demetres Christofides and Simon Griffiths. Christofides eventually showed us the argument below, which we present here with his kind permission.

Recall that the *Ramsey–Turan number* $RT(n; k, m)$ is the maximum number of edges a graph of order n can have subject to not containing K_k (the complete graph of order k) and having

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

independence number less than m. The argument we shall present uses Corollary 2.2 and the following very simple bound:[1]

$$RT(n;3;\delta n) < \delta n^2. \tag{2.1}$$

The following result is easily seen to imply Theorem 2.3, given property (1.1).

Theorem 2.4. *Let k, r be positive integers, and let $\alpha > 0$. There exists $N_0 = N_0(\alpha, k, r)$ such that if $N > N_0$, A is a subset of $[N]$ of density at least α, and G is a graph on A with no independent set of size r, then there is a k-term arithmetic progression in A which is also a K_k in G.*

Note that this theorem follows from an argument from [4] which uses the Graham–Rothschild theorem (see the proof of Theorem 2.2 in that paper). The following argument provides an alternative proof.

Proof (Christofides). Let us first deal with the case $k = 3$. We need to find a triangle in the graph G with the vertices in arithmetic progression. Suppose first that $r = 3$, so that the complement $\overline{G}$ is triangle-free. Suppose there is no triangle in G with vertices forming a progression in A. Note that any edge in G or in the complement $\overline{G}$ belongs to at most three progressions of length three in A. Since by Corollary 2.2 there are at least $v_\alpha N^2$ such progressions in A, it follows that, for G to have no triangle with vertices forming a progression, $\overline{G}$ must contain at least $v'_\alpha(\alpha N)^2$ edges, where $v'_\alpha > 0$ depends only on α. Using (2.1) we deduce that $\overline{G}$ has independence number at least $v'_\alpha \alpha N$, so we can find a complete subgraph of G of order at least $v'_\alpha \alpha N$. Applying the case $k = 3$ of Theorem 2.1 (*i.e.*, Roth's theorem) to the corresponding subset of $[N]$, we find a three-term progression in A with all three edges in G, a contradiction.

The following iterative argument deals with the case $r > 3$. By assumption we have that $\overline{G}$ contains no K_r, and we suppose for a contradiction that G contains no triangle with vertices forming a progression. Again, by Corollary 2.2 and the fact that an edge belongs to at most three progressions of length three, we have that $\overline{G}$ must have at least $v_1 N^2$ edges, where v_1 depends only on α. Choosing vertex v_1 of maximum degree in $\overline{G}$, we have $|\overline{\Gamma}(v_1)| \geqslant v_1 N$, where $\overline{\Gamma}(v_1)$ denotes the neighbourhood of v_1 in $\overline{G}$. We then let $G^{(1)}$ be the induced subgraph $G[\overline{\Gamma}(v_1)]$. $G^{(1)}$ is a graph on at least $v_1 N$ vertices which contains no triangle with vertices forming a progression, and such that the complement $\overline{G^{(1)}} = \overline{G}[\overline{\Gamma}(v_1)]$ is K_{r-1}-free. Since $\overline{\Gamma}(v_1)$ has density at least v_1 in $[N]$, it contains $v_2 N^2$ three-term progressions, where $v_2 > 0$ depends only on v_1. Again, since an edge belongs to at most three progressions, and as $G^{(1)}$ does not contain a triangle with vertices forming a progression, it must be that $\overline{G^{(1)}}$ contains at least $v'_2 N^2$ edges, where v'_2 depends only on v_2. Choosing a vertex v_2 of maximum degree in $\overline{G^{(1)}}$, we pass to a graph $G^{(2)} := G^{(1)}[\overline{\Gamma}(v_2)]$ on at least $v'_2 N$ vertices which still does not contain a triangle with vertices in progression, and such that $\overline{G^{(2)}}$ is now K_{r-2}-free. Iterating this argument further, we eventually go down to a graph $G^{(r-3)}$ on at least $v'_{r-3} N$ vertices, containing no triangle with vertices forming a progression in A, and with $\overline{G^{(r-3)}}$ being K_3-free, so we are back in the situation of the previous paragraph and

[1] See [6] for a detailed description of Ramsey–Turan theory; the bound (2.1) is stated in Remark 63 in that paper.

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

we can conclude that $G^{(r-3)}$ does in fact contain a triangle with vertices forming a progression, a contradiction. This completes the proof for $k = 3$.

For any $k > 3$ we can argue similarly, using the fact that an edge belongs to at most $O_k(1)$ progressions of length k in A. □

One can see that the bound for N_0 obtained through this argument grows quite dramatically as r grows, and this gives a bound for N_0 in Theorem 2.3 with the same growth as γ decreases towards zero. It seems interesting to seek a better bound by looking for an argument that uses more of the vector structure and combines it more closely with the arithmetic structure of A. In the next section we illustrate what such an argument could look like by answering Question 1.1 using the Fourier transform of V_A.

3. A vector-valued version of a theorem of Sárkőzy, with a double exponential bound via Fourier analysis

We shall use the Hilbert space structure on $\mathbb{C}^N$, with the standard inner product $(u, v) \mapsto \langle u, v\rangle$ and the norm $\|u\| = \langle u, u\rangle^{1/2}$.

Given a function V_A, we can define its vector-valued Fourier transform

$$\begin{aligned} \hat{V}_A : \mathbb{Z}_N &\to \mathbb{C}^N \\ r &\mapsto \hat{V}_A(r) = \mathbb{E}_{x\in\mathbb{Z}_N} V_A(x)\omega^{-rx}, \end{aligned}$$

where $\omega = \exp(2\pi i/N)$ and, for a set B and a (scalar- or vector-valued) function F on B, $\mathbb{E}_{x\in B}F(x)$ denotes averaging over B, *i.e.*,

$$\mathbb{E}_{x\in B}F(x) = \frac{1}{|B|}\sum_{x\in B} F(x).$$

We shall call the quantity $\|\mathbb{E}_{x\in\mathbb{Z}_N} V_A(x)\|^2$ the *vector* density of V_A, to distinguish it from the *set* density of V_A, *i.e.*, $\mathbb{E}_{x\in\mathbb{Z}_N} A(x)$.

Given a scalar-valued function $f : \mathbb{Z}_N \to \mathbb{C}$, we define the convolution $V_A * f := \mathbb{Z}_N \to \mathbb{C}^N$, $x \mapsto \mathbb{E}_y V_A(y) f(x - y)$. The vector-valued Fourier transform has the following useful properties, which are clear analogues of the well-known basic properties of the scalar-valued Fourier transform:

$$\begin{aligned} &V_A(x) = \textstyle\sum_r \hat{V}_A(r)\omega^{rx} && \text{(Fourier inversion)}, \\ &\textstyle\sum_r \|\hat{V}_A(r)\|^2 = \mathbb{E}_x \|V_A(x)\|^2 && \text{(Parseval's identity)}, \\ &\widehat{V_A * f} = \hat{V}_A \hat{f}, \ \text{for any } f : \mathbb{Z}_N \to \mathbb{C} && \text{(convolution identity)}. \end{aligned}$$

We shall prove the following result.

Theorem 3.1. *There exists an absolute constant $C > 0$ with the following property. For any $\alpha, \gamma > 0$, if $N > \exp\exp(C(\gamma\alpha)^{-C})$, then, for any subset $A \subset [N]$ of density α, and any $V_A : [N] \to \mathbb{S}^{N-1} \cup \{\mathbf{0}\}$ supported on A, there exist x, y in A differing by a non-zero square and such that $\langle V_A(x), V_A(y)\rangle \geqslant -\gamma$.*

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

We prove this theorem using an iterative argument based on the idea of density increment (*cf.* [3]). Starting from the negation of Theorem 3.1, at each step of the argument we shall increase either the *set density* (which is initially α) or the *vector density* (initially δ), eventually obtaining a contradiction.

Recall the notation $\|A\|_u$ for the Fourier bias (or linear bias) of the set A,

$$\|A\|_u := \sup_{r\neq 0} |\mathbb{E}_{x\in\mathbb{Z}_N} A(x)\omega^{-rx}|.$$

For $c > 0$, A is said to be c-uniform if $\|A\|_u \leqslant c$. Let us describe the iterative argument in more detail.

Suppose first that A is $\alpha^{12}/2^{36}$-uniform. Then, provided N is sufficiently large, combining Lemmas 3.2, 3.4, and 3.6 below, we deduce the existence of a progression P, of length at least $N^{1/128}/20$ and square common difference, with the vector density increment

$$\|\mathbb{E}_P V_A\|^2 \geqslant \delta + \frac{\gamma^{12}\alpha^{24}}{2^{60}}.$$

From this point onwards we can keep increasing the vector density, using Lemmas 3.3, 3.4, and 3.6 repeatedly as follows. We pass to the progression P obtained above, use Lemma 3.3 with $\eta = \gamma^{12}\alpha^{24}/2^{60}$, and then use Lemmas 3.4 and 3.6 to obtain a new progression P' inside P, of length at least $|P|^{1/128}/20$ and square common difference, with the vector density increment

$$\|\mathbb{E}_{P'} V_A\|^2 \geqslant \|\mathbb{E}_P V_A\|^2 + \frac{(\gamma^{12}\alpha^{24}/2^{62})^{12}}{2^{22}} \geqslant \|\mathbb{E}_P V_A\|^2 + (\gamma\alpha^2/64)^{144}.$$

Iterating this argument, we keep increasing the vector density until it becomes greater than one, a contradiction.

The remaining possibility is that our initial set A is *not* $\alpha^{12}/2^{36}$-uniform. But then Lemma 3.5 allows us to increase the *set* density on some long progression P with square common difference. Iterating the set density increment, we either obtain a contradiction by increasing this density beyond one, or we eventually pass to a set A which is $\alpha^{12}/2^{36}$-uniform, in which case we are back in the previous case and we will eventually obtain a contradiction as well.

We shall now prove the main results used in the iterative argument. Let H denote both the set $[1, N/2]$ and its indicator function, and let S do the same for the set of non-zero squares in $[N]$ less than $N/2$. HV_A will denote the function $x \mapsto H(x)V_A(x)$.

Lemma 3.2. *Suppose that $A \subset [N]$ has density α, that $\|A\|_u \leqslant c$ with $0 < c \leqslant \alpha^{12}/2^{36}$, and that for any distinct $x, y \in A$ differing by a square we have $\langle V_A(x), V_A(y)\rangle < -\gamma$. Then*

$$\sum_{r\neq 0} \|\widehat{HV_A}(r)\| \|\hat{V}_A(r)\| |\hat{S}(r)| \geqslant \frac{\gamma\alpha^2}{8} N^{-1/2}.$$

Proof. By Fourier inversion we have

$$\mathbb{E}_{x,y} \langle HV_A(x), V_A(x+y)\rangle S(y) - \langle \widehat{HV_A}(0), \hat{V}_A(0)\rangle \hat{S}(0) = \sum_{r\neq 0} \langle \widehat{HV_A}(r), \hat{V}_A(r)\rangle \hat{S}(r). \quad (3.1)$$

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

By the triangle inequality and the Cauchy–Schwarz inequality in $\mathbb{C}^N$, the right-hand side is at most $\sum_{r\neq 0}\|\widehat{HV_A}(r)\|\,\|\hat{V}_A(r)\|\,|\hat{S}(r)|$, so it suffices to establish the appropriate lower bound for the left-hand side.

Letting H^c denote the complement of H in $[N]$, we have

$$0 \leqslant \langle \mathbb{E}_x HV_A(x), \mathbb{E}_y V_A(y)\rangle + \langle \mathbb{E}_x H^c V_A(x), \mathbb{E}_y V_A(y)\rangle,$$

and so we can assume without loss of generality, by swapping H and H^c if necessary (and accordingly replacing the operation of adding a square from S by that of subtracting it), that

$$\langle \widehat{HV_A}(0),\ \hat{V}_A(0)\rangle\, \hat{S}(0) \geqslant 0. \tag{3.2}$$

We also find, using the assumptions and Fourier inversion, that

$$\begin{aligned}\mathbb{E}_{x,y}\langle HV_A(x),\ V_A(x+y)\rangle\, S(y) &\leqslant -\gamma \mathbb{E}_{x,y} H(x)A(x)A(x+y)S(y)\\ &= -\gamma \sum_r \widehat{HA}(r)\hat{A}(-r)\hat{S}(r).\end{aligned} \tag{3.3}$$

Given (3.1), (3.2), and (3.3), it now suffices to show that

$$\sum_r \widehat{HA}(r)\hat{A}(-r)\hat{S}(r) \geqslant \frac{\alpha^2}{8} N^{-1/2}. \tag{3.4}$$

We have

$$\sum_r \widehat{HA}(r)\hat{A}(-r)\hat{S}(r) \geqslant \widehat{HA}(0)\hat{A}(0)\hat{S}(0) - \sum_{r\neq 0} |\widehat{HA}(r)|\,|\hat{A}(r)|\,|\hat{S}(r)|. \tag{3.5}$$

It is a standard fact that A, being c-uniform, cannot have too large intersection with H. More precisely, using the bound $|\hat{H}(r)| \leqslant 1/2|r|$ for $r \neq 0$, we have that

$$\left|\mathbb{E}_{x\in Z_N} H(x)A(x) - \frac{\alpha}{2}\right| \leqslant \sum_{r\neq 0} |\hat{A}(r)||\hat{H}(r)| \leqslant \|A\|_u^{1/2}\|\hat{A}\|_{\ell^2}^{1/2}\|\hat{H}\|_{\ell^{4/3}} \leqslant 8c^{1/2}.$$

It follows that

$$\begin{aligned}\widehat{HA}(0)\ \ \hat{A}(0)\ \ \hat{S}(0) &\geqslant (\alpha/2 - 8c^{1/2})\ \alpha\ \frac{1}{2N^{1/2}}\\ &\geqslant (\alpha^2/4 - 4\alpha c^{1/2})N^{-1/2}.\end{aligned} \tag{3.6}$$

Using Hölder's inequality and the estimate $\sum_r |\hat{S}(r)|^{12} \leqslant 2^{19}N^{-6}$ from [3], we see that

$$\begin{aligned}\sum_{r\neq 0} |\widehat{HA}(r)|\,|\hat{A}(r)|\,|\hat{S}(r)| &\leqslant \|A\|_u^{1/6} \sum_r |\widehat{HA}(r)|\,|\hat{A}(r)|^{5/6}\,|\hat{S}(r)|\\ &\leqslant \|A\|_u^{1/6}\ \|\widehat{HA}\|_{\ell^2}\ \|\hat{A}\|_{\ell^2}^{5/6}\ \|\hat{S}\|_{\ell^{12}}\\ &\leqslant \|A\|_u^{1/6}\ 2^{19/12}\ N^{-1/2}\\ &\leqslant 4c^{1/6}N^{-1/2}.\end{aligned} \tag{3.7}$$

Inequality (3.4) now follows from (3.5), (3.6), (3.7), and the assumption that $c \leqslant \alpha^{12}/2^{36}$. □

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

Lemma 3.3. *Let $\eta \geqslant 0$. If the vector density is at least η and for any distinct $x, y \in A$ differing by a square we have $\langle V_A(x), V_A(y)\rangle \leqslant 0$, then*

$$\sum_{r\neq 0} \|\widehat{HV_A}(r)\| \, \|\hat{V}_A(r)\| |\hat{S}(r)| \geqslant \frac{\eta}{4} N^{-1/2}.$$

Proof. This is similar to the proof of the previous lemma. We start with the inequality

$$\begin{aligned} |\mathbb{E}_{x,y} H(x) \langle V_A(x),\, V_A(x+y)\rangle S(y) - \langle \widehat{HV_A}(0),\, \hat{V}_A(0)\rangle \hat{S}(0)| \\ \leqslant \sum_{r\neq 0} \|\widehat{HV_A}(r)\| \, \|\hat{V}_A(r)\| \, |\hat{S}(r)|. \end{aligned} \tag{3.8}$$

We may assume without loss of generality that $\langle \widehat{HV_A}(0), \hat{V}_A(0)\rangle \geqslant \frac{\eta}{2}$, and since $\hat{S}(0) \geqslant 1/2N^{1/2}$, we have

$$\langle \widehat{HV_A}(0),\, \hat{V}_A(0)\rangle \hat{S}(0) \geqslant \frac{\eta}{4} N^{-1/2}. \tag{3.9}$$

By assumption $\mathbb{E}_{x,y} H(x) \langle V_A(x),\, V_A(x+y)\rangle S(y) \leqslant 0$, and so the left-hand side of (3.8) is indeed at least $\frac{\eta}{4} N^{-1/2}$. □

We now need to deduce from the conclusion of Lemmas 3.2 and 3.3 that V_A has some large non-trivial Fourier coefficient.

Lemma 3.4. *Suppose that for some $\epsilon > 0$ we have*

$$\sum_{r\neq 0} \|\widehat{HV_A}(r)\| \, \|\hat{V}_A(r)\| |\hat{S}(r)| \geqslant \epsilon N^{-1/2}.$$

Then there is a non-zero r' in $\mathbb{Z}_N$ such that

$$\|\hat{V}_A(r')\|^2 \geqslant \frac{\epsilon^{12}}{2^{19}}.$$

Proof. The left-hand side of the assumed inequality is at most

$$\sup_{r\neq 0} \|\hat{V}_A(r)\|^{1/6} \sum_r \|\widehat{HV_A}(r)\| \, \|\hat{V}_A(r)\|^{5/6} |\hat{S}(r)|.$$

Applying Hölder's inequality as in Lemma 3.2, we then see that

$$\sup_{r\neq 0} \|\hat{V}_A(r)\|^{\frac{1}{6}} \left(\sum_r \|\widehat{HV_A}(r)\|^2\right)^{\frac{1}{2}} \left(\sum_r \|\hat{V}_A(r)\|^2\right)^{\frac{5}{12}} \left(\sum_r |\hat{S}(r)|^{12}\right)^{\frac{1}{12}} \geqslant \epsilon N^{-1/2}.$$

We use the estimate $\sum_r |\hat{S}(r)|^{12} \leqslant 2^{19} N^{-6}$ again, and by Parseval's identity we also have the bounds $\sum_r \|\hat{V}_A(r)\|^2 \leqslant 1$ and $\sum_r \|\widehat{HV_A}(r)\|^2 \leqslant 1$. Using these in the inequality above we obtain

$$\sup_{r\neq 0} \|\hat{V}_A(r)\|^2 \geqslant \frac{\epsilon^{12}}{2^{19}}. \tag{3.10}$$

□

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

Now we proceed to deduce density increments from the previous results. For the iterative argument described above we need a vector density increment when $\sup_{r\neq 0}\|\hat{V}_A(r)\|^2$ is large, and a set density increment when $\sup_{r\neq 0}|\hat{A}(r)|$ is large.

Lemma 3.5 (Set density increment). *Let A be a subset of $[N]$ of density at least α. If $\|A\|_u \geqslant v$ and $N > (32/\alpha)^{39}$, then there is an arithmetic progression P in $[N]$, with* square common difference *and of length at least $N^{1/128}/20$, such that*

$$\mathbb{E}_P\, A\cap P \geqslant \mathbb{E}_{[N]}A + \frac{v^2\alpha}{8}.$$

The proof can be found in [3] and is very similar to the proof of the following result.

Lemma 3.6 (Vector density increment). *Let V_A have vector density $\|\mathbb{E}V_A\|^2 \geqslant \delta$. Suppose that there exists $r'\neq 0$ such that $\|\hat{V}_A(r')\|^2 \geqslant v$, and that $N > (8/v)^3$. Then there is an arithmetic progression P in $[N]$, with* square common difference *and of length at least $N^{1/128}/20$, such that*

$$\|\mathbb{E}_{x\in P}V_A(x)P(x)\|^2 \geqslant \delta + \frac{v}{8}.$$

Proof. We use Lemma 5.5 from [2], which tells us that if $N \geqslant 2^{2^{129}}$ then there is a non-zero $p \leqslant N^{1/4}$ such that $|p^2r'| \leqslant N^{127/128}$. Letting $B = \{p^2, 2p^2, \dots, Lp^2\}$ with $L = \frac{1}{20}N^{1/128}$, we have

$$|\hat{B}(r')| \geqslant \frac{L}{N}\Big(1 - \sup_{x=1,\dots,L}|1-\omega^{r'p^2x}|\Big) \geqslant \frac{L}{N}\left(1 - \frac{2\pi|p^2r'|L}{N}\right) \geqslant \frac{L}{2N}.$$

We then have, by the convolution identity and Plancherel's theorem,

$$\left(\delta+\frac{v}{4}\right)(\mathbb{E}_{[N]}B)^2 = \left(\delta+\frac{v}{4}\right)\frac{L^2}{N^2} \leqslant \sum_r \|\hat{V}_A(r)\|^2|\hat{B}(r)|^2 = \mathbb{E}_y\|(V_A * B)(y)\|^2.$$

Now let G denote the set of y such that $y-B$ is a genuine progression in $\{1,2,\dots,N\}$ (*i.e.*, a progression which remains one when $\mathbb{Z}_N$ is embedded in $\mathbb{Z}$). We can then split the last average as follows:

$$\mathbb{E}_y\|(V_A * B)(y)\|^2 = \mathbb{E}_y G(y)\,\|(V_A * B)(y)\|^2 + \mathbb{E}_y G^c(y)\,\|(V_A * B)(y)\|^2. \tag{3.11}$$

Since $p \leqslant N^{1/4}$ and $|B| \leqslant N^{1/128}$, the diameter of B is at most $N^{1/2+1/128} \leqslant N^{2/3}$, and therefore $|G^c| \leqslant N^{2/3}$. Thus we see that

$$\mathbb{E}_y G^c(y)\|(V_A * B)(y)\|^2 \leqslant N^{-1/3}(\mathbb{E}B)^2.$$

Using this in (3.11) we finally obtain

$$\left(\delta+\frac{v}{4}-N^{-1/3}\right)(\mathbb{E}B)^2 \leqslant \sup_{y\in G}\|(V_A * B)(y)\|^2.$$

Therefore, if $N^{-1/3} \leqslant v/8$, then there exists $y\in G$ such that the arithmetic progression $P = y - B$ verifies our claim. □

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press

We have proved all the results required for the iterative argument described at the beginning of this section. To obtain the bound for N stated in Theorem 3.1, let us now consider the argument in the worst-case scenario, *i.e.*, with the greatest possible finite number of steps before we obtain a contradiction. One step consists in a density increment. Writing T for the total number of steps, we have $T = T_s + T_v$, where T_s denotes the number of set density increments (iterations of Lemma 3.5), and T_v denotes the number of vector density increments (Lemma 3.2 or 3.3, followed by Lemmas 3.4 and 3.6). From the results above, it follows that $T \leqslant C'(\gamma\alpha)^{-C'}$ for some absolute constant C'. By Lemmas 3.5 and 3.6, at step j we pass to a subprogression P_j of size N_j verifying $N_j \geqslant N_{j-1}^{1/128}/20$ (where $N_0 = N$ is the length of the initial interval). By induction we have $N_j \geqslant N^{128^{-j}}/20^{1+128^{-1}+128^{-2}+\cdots+128^{-(j-1)}} \geqslant N^{128^{-j}}/400$ for each j. We obtain a contradiction if the last progression to which we pass (on which one of the two densities is greater than one) is non-empty, and for this to hold it suffices to have

$$N^{128^{-C'(\gamma\alpha)^{-C'}}} \geqslant 400.$$

References

[1] Bollobás, B. (1998) *Modern Graph Theory*, Vol. 184 of *Graduate Texts in Mathematics*, Springer.
[2] Gowers, W. T. (2001) A new proof of Szemerédi's theorem. *Geom. Funct. Anal.* **11** 465–588.
[3] Green, B. J. (2002) On arithmetic structures in dense sets of integers. *Duke Math. J.* **114** 215–238.
[4] Gunderson, D. S., Leader, I., Prömel, H. J. and Rödl, V. (2001) Independent arithmetic progressions in clique-free graphs on the natural numbers. *J. Combin. Theory Ser. A* **93** 1–17.
[5] Sárkőzy, A. (1978) On difference sets of sequences of integers I. *Acta. Math. Sci. Hungar.* **31** 125–149.
[6] Simonovits, M. and Sós, V. (2001) Ramsey–Turan theory. *Discrete Math.* **229** 293–340.
[7] Varnavides, P. (1959) On certain sets of positive density. *J. London Math. Soc.* **34** 358–360.

https://doi.org/10.1017/S0963548309009870 Published online by Cambridge University Press