Combinatorics, Probability and Computing (2003) 12, 643–651. © 2003 Cambridge University Press
DOI: 10.1017/S0963548303005753 Printed in the United Kingdom

A Sárközy Theorem for Finite Fields

RANDALL McCUTCHEON

Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA
(e-mail: rmcctchn@memphis.edu)

Received 1 May 2002; revised 16 April 2003

A classical result of Sárközy states that, for any $k \in \mathbb{N}$ and any positive density subset E of $\mathbb{N}$, there exist elements x and y of E and $n \neq 0$ such that $x - y = n^k$. A version of this result for finite fields is derived from a recent theorem of P. Larick, a short proof of which is also given.

1. Introduction

A conjecture of L. Lovász in the 1970s stated that if A is a set of natural numbers having the property that $A - A = \{a - b : a, b \in A\}$ contains no squares, *i.e.*, no member of the set $S = \{n^2 : n \in \mathbb{N}\}$, then $\overline{d}(A) = \limsup_{N\to\infty} \frac{|A \cap \{1,\ldots,N\}|}{N} = 0$. This conjecture was affirmatively established by A. Sárközy in [7]. Sárközy then in [8] indicated that his method also works with S replaced by $S' = \{n^k : n \in \mathbb{N}\}$, where $k \in \mathbb{N}$ is arbitrary. In particular the following is true.

Theorem A. *Let $\epsilon > 0$ and suppose $k \in \mathbb{N}$. There exists a $q \in \mathbb{N}$ such that, for every $N \geqslant q$ and every set $A \subset \{1,\ldots,N\}$ satisfying $|A| > \epsilon N$, $(A - A) \cap \{n^k : n \in \mathbb{N}\} \neq \emptyset$.*

Theorem A was given an independent proof via ergodic-theoretic methods by H. Furstenberg. Indeed, in [5] it is established that one may in fact obtain the conclusion $(A - A) \cap \{p(n) : n \in \mathbb{N}\} \neq \emptyset$, where $p(x) \in \mathbb{Q}[x]$ with $p(\mathbb{Z}) \subset \mathbb{Z}$ and $p(0) = 0$.

Our first purpose is to give the following version of Sárközy's theorem for finite fields. (Here and throughout the paper, F^* will denote the set of nonzero elements of a field F.)

Theorem B. *Let $\epsilon > 0$ and $k \in \mathbb{N}$. There exists an $M \in \mathbb{N}$ having the property that, if F is any finite field with $|F| \geqslant M$ and $A \subset F$ with $|A| > \epsilon|F|$, then $(A - A) \cap \{g^k : g \in F^*\} \neq \emptyset$.*

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

Recall that a sequence $(\Phi_n)_{n\in\mathbb{N}}$ of finite subsets of a countably infinite additive abelian group G is a Følner sequence if, for every $g \in G$, $\frac{|(g+\Phi_n)\cap\Phi_n|}{|\Phi_n|} \to 1$ as $n \to \infty$. By a unitary (respectively, measure-preserving) action of a vector space W on a Hilbert (respectively, probability) space X we mean a homomorphism $u \to T_u$ of $(W,+)$ into the group of unitary operators (respectively, invertible measure-preserving transformations) on X (so that $T_{u+v} = T_u T_v$).

Our proof of Theorem B depends heavily on the following recent theorem of P. Larick [6]. Indeed, our second purpose is to disseminate a concise proof of this result (the original proof, in addition to being not widely available, is prohibitively long).

Theorem C. *Let F be a countable field, let $(\Phi_n)_{n\in\mathbb{N}}$ be a Følner sequence for F, and let $r_i(x) \in F[x]$ with $r_i(0) = 0$, $1 \leqslant i \leqslant l$. If $(U_g)_{g\in F^l}$ is a unitary action on a Hilbert space $\mathscr{H}$ then, for all $f \in \mathscr{H}$,*

$$\lim_{n\to\infty} \frac{1}{|\Phi_n|} \sum_{g\in\Phi_n} U_{(r_1(g),\ldots,r_l(g))} f = Pf,$$

where P is the orthogonal projection onto $\{h \in \mathscr{H} : U_{(r_1(g),\ldots,r_l(g))}h = h \text{ for all } g \in F\}$.

In the final section we indicate that, using the full strength of Theorem C, one may establish somewhat more than is guaranteed by Theorem B.

The proofs we shall present here are intended as an accessible and instructive blend of the algebraic, functional-analytic, ergodic-theoretic and combinatorial methodologies germane to ergodic Ramsey theory. For a more comprehensive treatment of polynomial density combinatorics in vector spaces, the reader is referred to the forthcoming article [4].

2. Derivation of Theorem B

The following recurrence theorem for measure-preserving vector space actions is an easy corollary of Theorem C.

Corollary 2.1. *Let W be a finite-dimensional vector space over a countable field F, let $(\Phi_n)_{n\in\mathbb{N}}$ be a Følner sequence for F, and suppose $(T_w)_{w\in W}$ is a measure-preserving action of W on a probability space $(X,\mathscr{A},\mu)$. If $r : F \to W$ is a polynomial with $r(0) = 0$ and $A \in \mathscr{A}$, then $\lim_{n\to\infty} \frac{1}{|\Phi_n|} \sum_{g\in\Phi_n} \mu(A \cap (T_{r(g)})A) \geqslant \mu(A)^2$.* □

If G is a commutative group and $E \subset G$, then we write $d^*(E)$ for the supremum, taken over all Følner sequences $(\Phi_n)_{n\in\mathbb{N}}$, of $\limsup_n \frac{|E\cap\Phi_n|}{|\Phi_n|}$.

Corollary 2.2. *Let $\epsilon > 0$, let W be a finite-dimensional vector space over a countable field F, and suppose $(\Phi_n)_{n\in\mathbb{N}}$ is an increasing Følner sequence for W consisting of additive subgroups. If $r : F \to W$ is a polynomial with $r(0) = 0$, then there exists an $N \in \mathbb{N}$ such that, if $E \subset \Phi_N$ with $|E| > \epsilon|\Phi_N|$, then $(E - E) \cap \{r(g) : g \in F^*\} \neq \emptyset$.*

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

Proof. A routinely established consequence of Corollary 2.1 and Furstenberg's correspondence principle (see for example [1]) is that if $E \subset W$ with $d^*(E) > 0$, then there exist many (in particular, nonzero) $g \in F$ with $r(g) \in (E - E)$. We will assume the negation of what we want to prove and derive a contradiction to this fact.

Suppose then for every $N \in \mathbb{N}$ we have $E_N \subset \Phi_N$ with $|E_N| > \epsilon|\Phi_N|$ and $(E_N - E_N) \cap \{r(g) : g \in F^*\} = \emptyset$. We claim that, upon possibly shifting the E_Ns, we may assume in addition that $|E_N \cap \Phi_j| \geqslant \epsilon|\Phi_j|$ for $1 \leqslant j < N$.

Let us establish the claim. First note that E_N must intersect some coset (in Φ_N) of Φ_{N-1} in a set of size at least $\epsilon|\Phi_{N-1}|$. Shifting E_N by subtracting a representative of this coset and replacing E_N by its shift yields the inequality $|E_N \cap \Phi_{N-1}| \geqslant \epsilon|\Phi_{N-1}|$ without affecting the inequality $|E_N \cap \Phi_N| \geqslant \epsilon|\Phi_N|$. Next, our shifted E_N must intersect some coset (in Φ_{N-1}) of Φ_{N-2} in a set of size at least $\epsilon|\Phi_{N-2}|$. Shifting E_N again by subtracting a representative of this coset and replacing E_N by its shift does not affect the prior two inequalities (we shifted by a member of Φ_{N-1}) while yielding the new inequality $|E_N \cap \Phi_{N-2}| \geqslant \epsilon|\Phi_{N-2}|$. Iterating this process, we establish the truth of the claim.

Now, choose $D_1 \subset \Phi_1$ such that $R_1 = \{N : E_N \cap \Phi_1 = D_1\}$ is an infinite set. According to the claim above, $|D_1| \geqslant \epsilon|\Phi_1|$. Having chosen $D_1, \ldots, D_t$ and $R_1, \ldots, R_t$ such that $D_i \subset \Phi_i$, $|D_i| \geqslant \epsilon|\Phi_i|$, and $R_i = \{N \in R_{i-1} : E_N \cap \Phi_i = D_i\}$ is an infinite set, $2 \leqslant i \leqslant t$, choose $D_{t+1} \subset \Phi_{t+1}$ with $|D_{t+1}| \geqslant \epsilon|\Phi_{t+1}|$ and $R_{t+1} = \{N \in R_t : E_N \cap \Phi_{t+1} = D_{t+1}\}$ infinite. Note that $D_1 \subset D_2 \subset \cdots$ and $R_1 \supset R_2 \supset \cdots$. Let $D = \bigcup_{i=1}^{\infty} D_i$. With respect to the Følner sequence (Φ_n), we have $\overline{d}(D) \geqslant \epsilon$. However, by construction $(D - D) \cap \{g^k : g \in F^*\} = \emptyset$, contradicting the observation made in the first paragraph. □

We now consider the ring of polynomials $\mathbb{Z}_p[x]$, where p is prime. For $N \in \mathbb{N}$, let $K_N = \{f \in \mathbb{Z}_p[x] : \deg f < N\}$. Then (K_N) is an increasing Følner sequence consisting of additive subgroups that exhausts $\mathbb{Z}_p[x]$, and we have a corresponding notion of density with respect to this Følner sequence: $\overline{d}(E) = \limsup_{N\to\infty} \frac{|E \cap K_N|}{|K_n|}$ for $E \subset \mathbb{Z}_p[x]$. Our first step toward a proof of Theorem B is now the following lemma.

Lemma 2.3. *Let $k \in \mathbb{N}$ and suppose p is prime. If $E \subset \mathbb{Z}_p[x]$, $\overline{d}(E) > 0$, then $(E - E) \cap \{g^k : 0 \neq g \in \mathbb{Z}_p[x]\} \neq \emptyset$.*

Proof. Let $\mathbf{Q}$ be the field of rational functions $\frac{f}{g}$, $f, g \in \mathbb{Z}_p[x]$, and let $\{\Phi_N\}$ be an increasing Følner sequence for $\mathbf{Q}$ consisting of additive subgroups. Choose N as per Corollary 2.2 (taking $F = W = \mathbf{Q}$) with $r(g) = g^k$ and $\epsilon = \frac{\overline{d}(E)}{2}$. Pick $f \in \mathbb{Z}_p[x]$ with $f\Phi_N \subset \mathbb{Z}_p[x]$ and let $G = f^k\Phi_N$. Then G is a subgroup of $\mathbb{Z}_p[x]$ having the property that if D is contained in any coset of G with $|D| \geqslant \epsilon|G|$ then $(D - D) \cap \{g^k : 0 \neq g \in \mathbb{Z}_p[x]\} \neq \emptyset$.

Now choose M so that $G \subset K_M$ and $|E \cap K_M| \geqslant \epsilon|K_M|$. Then $|E \cap (d + G)| \geqslant \epsilon|G|$ for some $d \in K_M$, whereby we have $(E - E) \cap \{g^k : 0 \neq g \in \mathbb{Z}_p[x]\} \neq \emptyset$ by the observation made in the previous paragraph. □

Part (a) of the next lemma follows immediately from the proof of the previous one.

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

Lemma 2.4. *Let $k \in \mathbb{N}$ and $\epsilon > 0$. Suppose p is prime.*

(a) *There exists an $R \in \mathbb{N}$ such that if $m \geqslant R$ and $E \subset K_m$ with $|E| > \epsilon |K_m|$ then $(E - E) \cap \{g^k : 0 \neq g \in K_R\} \neq \emptyset$.*
(b) *There exists an $R \in \mathbb{N}$ such that if F is a finite field having p^m elements, $m \geqslant R$, then if $D \subset F$ with $|D| > \epsilon |F|$ we have $(D - D) \cap \{g^k : g \in F^*\} \neq \emptyset$.*

Proof. We need only prove part (b). Let R be as in part (a) and suppose D and F are as stated. We may assume that $\mathbb{Z}_p$ is a subfield of F. Let w be a generator for $(F^*, \cdot)$ (so that, in particular, the minimal polynomial of w over $\mathbb{Z}_p$ is of degree m). Then the map $\tau : K_m \to F$ given by $\tau(f(x)) = f(w)$ is a bijection and the set $E = \tau^{-1}(D)$ satisfies the conditions of part (a), so that there exists a nonzero $g = g(x) \in K_R$ with $g^k = g(x)^k \in E - E$. In other words, E contains a configuration $\{e(x), e(x) + g(x)^k\}$, from which it follows that D contains $\{e(w), e(w) + g(w)^k\}$. Finally $g(w)$ cannot be zero, as $\deg g(x) < m$. □

Proof of Theorem B. Let $\epsilon > 0$ and $k \in \mathbb{N}$ and choose q as in Theorem A. Now, if F is any field of characteristic $p \geqslant q$, then F contains a subfield G isomorphic to $\mathbb{Z}_p$, so if $A \subset F$ with $|A| \geqslant \epsilon |F|$ then A intersects some additive coset of G with relative density at least ϵ, and Theorem A gives in turn the desired conclusion to Theorem B.

For any prime $p < q$, let R be as in Lemma 2.4 and put $L(p) = p^R$. Then, if F is a field of characteristic p with $|F| > L(p)$, Lemma 2.4(b) applies to F, which again gives the desired conclusion. Let M be the maximum of q and the largest of the $L(p)$, $p < q$. □

3. Proof of Theorem C

We need the following two facts. The first lemma follows Bergelson (see [2, Theorem 1.4], [3, Proposition 5.7], [4], *etc.*) and is motivated by van der Corput's difference theorem on equidistribution.

Lemma VDC. *Let $(G, +)$ be an abelian group and let $(\Phi_n)_{n \in \mathbb{N}}$ be a Følner sequence for G. Let $(x_g)_{g \in G}$ be a bounded sequence in a Hilbert space, and suppose for all but finitely many $h \in G$,*

$$\limsup_{n \to \infty} \frac{1}{|\Phi_n|} \sum_{g \in \Phi_n} \langle x_g, x_{g+h} \rangle = 0.$$

Then $\lim_{n \to \infty} \| \frac{1}{|\Phi_n|} \sum_{g \in \Phi_n} x_g \| = 0$. □

The next tool we introduce is the classical mean ergodic theorem.

Theorem MET. *Let G be a countable abelian group and let $(X, \mathscr{A}, \mu, \{T_g\}_{g \in G})$ be a measure-preserving system with $\mu(X) = 1$. If $(\Phi_n)_{n \in \mathbb{N}}$ is any Følner sequence for G, then*

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

for all $f \in L^2(X, \mathscr{A}, \mu)$ *the limit*

$$\lim_{n\to\infty} \frac{1}{|\Phi_n|} \sum_{g\in\Phi_n} T_g f = Pf$$

exists in the norm topology. Moreover, P *is the orthogonal projection onto the space of* $\{T_g\}_{g\in G}$*-invariant functions.* □

Let F be a countably infinite field of characteristic p and let $w \in \mathbb{N}$. If $r : F \to F^w$ is polynomial in each coordinate with $r(0) = \mathbf{0}$ and $h \in F$, put $D_h r(x) = r(x+h) - r(x) - r(h)$. Clearly $D_h(r+s)(x) = D_h r(x) + D_h s(x)$. Define $\deg_p r(x)$ to be the minimal positive integer n such that the n-fold iteration $(D_{h_n}(D_{h_{n-1}}(\cdots D_{h_1} r))\cdots) = 0$ for all choices h_i. It is an easy consequence of the binomial theorem that (taking $w = 1$) $\deg_p x^n = 1$ if an only if n is a power of p. More generally, one may show with a bit of effort that $\deg_p x^n$ is equal to $\sum_{i=0}^{\infty} a_i(n)$, where $n = \sum_{i=0}^{\infty} a_i(n) p^i$ is the base-p expansion of n. However, we do not need this fact, so we do not prove it here.

Theorem 3.1. *Let* $t_1 < \cdots < t_l \in \mathbb{N}$ *with* $p \not| t_i$, $1 \leqslant i \leqslant l$. *If* $(U_g)_{g\in F^l}$ *is a unitary action on a Hilbert space* $\mathscr{H}$ *and* $(\Phi_n)_{n\in\mathbb{N}}$ *is a Følner sequence for* F *then, for all* $f \in \mathscr{H}$,

$$\lim_{n\to\infty} \frac{1}{|\Phi_n|} \sum_{g\in\Phi_n} U_{(g^{t_1},\ldots,g^{t_l})} f = Pf, \tag{3.1}$$

where P *is the orthogonal projection onto* $\mathscr{H}_{\mathrm{inv}} = \{h \in \mathscr{H} : U_g h = h \text{ for all } g \in F^l\}$.

Proof. We use induction on $d = \max_{1\leqslant i\leqslant l} \deg_p x^{t_i}$. For $d = 1$ this is just Theorem MET. Assume the conclusion holds for $d-1$. As an immediate consequence of the induction hypothesis, we have the following fact.

Fact 3.2. *Let* $s_1, \ldots, s_z \in \mathbb{N}$ *be distinct with* $p \not| s_i$, *and* $\deg_p x^{s_i} \leqslant d-1$, $1 \leqslant i \leqslant z$. *Then* $\{(g^{s_1}, \ldots, g^{s_z}) : g \in F\}$ *additively generates* F^z.

The proof of Fact 3.2 from the induction hypothesis is immediate. If the set in question was contained in a proper subgroup $G \subset F^z$, then it would be an easy matter to construct a unitary F^z-action with G-invariant functions f that were not F^z-invariant. For such an f we would have $\lim_{n\to\infty} \frac{1}{|\Phi_n|} \sum_{g\in\Phi_n} U_{(g^{s_1},\ldots,g^{s_z})} f = f$, contradicting (3.1).

Let $y = 1$ and $w = l$ if $t_1 > 1$, and let $y = 2$ and $w = l-1$ otherwise. Put $q(x) = (x^{t_y}, \ldots, x^{t_l})$. (So $q(x)$ maps into F^w.) Recall next that we write $D_k q(x)$ for $q(x+k) - q(x) - q(k)$.

Proposition 3.3. *There exists a natural number* R *and a polynomial* $\Pi(x_1, \ldots, x_R)$, *such that if* $k_1, \ldots, k_R \in F$ *with* $\Pi(k_1, \ldots, k_R) \neq 0$ *then* $\{D_{k_i} q(g) : g \in F, 1 \leqslant i \leqslant R\}$ *spans* F^w.

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

Proof. First we separate the linear exponents from the nonlinear exponents in $D_k q(x)$, writing $D_k q(x) = n_k(x) + b_k(x)$, with only nonlinear exponents occurring in $n_k(x)$ and

$$b_k(x) = \sum_{i=1}^{w} \mathbf{e}_i \sum_{j=1}^{R_i} c(i,j) k^{t_i - p^{l(i,j)}} x^{p^{l(i,j)}},$$

where each $c(i,j) \neq 0$ and $l(i,1) = 0$, $1 \leqslant i \leqslant w$. Here $\mathbf{e}_1 = (1,0,\ldots,0)$, $\mathbf{e}_2 = (0,1,0,\ldots,0)$, $\ldots$, $\mathbf{e}_w = (0,\ldots,0,1)$.

Let $z = (z_1,\ldots,z_w)$ be an arbitrary element of F^w. Let $R = \sum_{i=1}^{w} R_i$ and choose M so that $p^{l(i,j)} | M$ for all i, j. For $k_1,\ldots,k_R \in F$, we consider the system of equations (in variables $g_1,\ldots,g_R$)

$$\sum_{s=1}^{R} c(i,j) k_s^{(t_i - p^{l(i,j)})M} g_s^{p^{l(i,j)}} = f_{ij}^{p^{l(i,j)}},\ 1 \leqslant i \leqslant w,\ 1 \leqslant j \leqslant R_i, \tag{3.2}$$

where $f_{ij} = z_i$ if $j = 1$ and $f_{ij} = 0$ if $j > 1$. Observe that if equations (3.2) hold, then for any $h \in F$,

$$\begin{aligned} \sum_{s=1}^{R} b_{k_s^M}(g_s h) &= \sum_{i=1}^{w} \sum_{j=1}^{R_i} h^{p^{l(i,j)}} \mathbf{e}_i c(i,j) \sum_{s=1}^{R} k_s^{(t_i - p^{l(i,j)})M} g_s^{p^{l(i,j)}} \\ &= \sum_{i=1}^{w} \sum_{j=1}^{R_i} h^{p^{l(i,j)}} \mathbf{e}_i f_{ij}^{p^{l(i,j)}} = h \sum_{i=1}^{w} \mathbf{e}_i z_i = (hz_1, hz_2, \ldots, hz_w) \end{aligned} \tag{3.3}$$

(since $f_{ij} = 0$ if $j > 1$ and $l(i,1) = 0$).

Recall that $p^{l(i,j)} | M$ for all i, j. Equation (3.2) will be true if

$$\sum_{s=1}^{R} c(i,j) k_s^{(t_i - p^{l(i,j)})M / p^{l(i,j)}} g_s = f_{ij},\ 1 \leqslant i \leqslant w,\ 1 \leqslant j \leqslant R_i.$$

This linear system of R equations (recall that $R = \sum_{i=1}^{w} R_i$) in R variables $g_1,\ldots,g_R$ will have a solution if its coefficient matrix has nonzero determinant. Letting $m(i,j) = (t_i - p^{l(i,j)})M / p^{l(i,j)}$, this coefficient matrix is given by

$$A(k_1,\ldots,k_R) = \begin{bmatrix} c(1,1)k_1^{m(1,1)} & \cdots & c(1,1)k_R^{m(1,1)} \\ \vdots & & \vdots \\ c(1,R_1)k_1^{m(1,R_1)} & \cdots & c(1,R_1)k_R^{m(1,R_1)} \\ \vdots & & \vdots \\ c(w,1)k_1^{m(w,1)} & \cdots & c(w,1)k_R^{m(w,1)} \\ \vdots & & \vdots \\ c(w,R_w)k_1^{m(w,R_w)} & \cdots & c(w,R_w)k_R^{m(w,R_w)} \end{bmatrix}.$$

Note first that $\Pi(k_1,\ldots,k_R) = \det A(k_1,\ldots,k_R)$ is a polynomial in variables $k_1,\ldots,k_R$, which will clearly be nonzero if the exponents in different rows are distinct; that is, if $m(i,j) = m(x,y)$ implies $i = x$ and $j = y$. To see that this is so, observe that if we start with the equation $m(i,j) = m(x,y)$, divide both sides by M, add 1 to both sides and

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

cross-multiply, we get $t_i p^{l(x,y)} = t_x p^{l(i,j)}$. Since neither t_i nor t_x has p as a factor, this does it.

Now we need to deal with $n(x)$. Recall that $n(x)$ contained terms with exponents other than powers of p, so we can write $n(x) = \sum_{i=1}^{L} a_i(k) x^{s_i p^{n_i}}$, with $p \not| s_i$ and $s_i > 1$, $1 \leqslant i \leqslant L$. Let $l_2, \ldots, l_z$ be an enumeration of the distinct s_is and put $l_1 = 1$.

By Fact 3.2, $\{(h^{l_1}, h^{l_2}, \ldots, h^{l_z}) : h \in F\}$ spans F^z, so there exist $h_1, \ldots, h_t$ such that $\sum_{j=1}^{t} (h_j^{l_1}, h_j^{l_2}, \ldots, h_j^{l_z}) = (1, 0, \ldots, 0)$. This implies (recall $l_1 = 1$) that $\sum_{j=1}^{t} h_j = 1$ and $\sum_{j=1}^{t} h_j^{s_i} = 0$, $1 \leqslant i \leqslant L$, which in turn gives $\sum_{j=1}^{t} h_j^{s_i p^{n_l}} = \left(\sum_{j=1}^{t} h_j^{s_i}\right)^{p^{n_l}} = 0$, $1 \leqslant i \leqslant L$, so that

$$\sum_{j=1}^{t} n_k(x h_j) = \sum_{j=1}^{t} \sum_{i=1}^{r} a_i(k) x^{s_i p^{n_i}} h_j^{s_i p^{n_i}} = \sum_{i=1}^{r} a_i(k) x^{s_i p^{n_i}} \left(\sum_{j=1}^{t} h_j^{s_i p^{n_i}} \right) = 0. \tag{3.4}$$

So, by (3.3) and (3.4),

$$\begin{aligned} \sum_{s=1}^{R} \sum_{j=1}^{t} D_{k_s} q(g_s h_j) &= \sum_{s=1}^{R} \left(\sum_{j=1}^{t} n_{k_s}(g_s h_j) \right) + \sum_{j=1}^{t} \left(\sum_{s=1}^{R} b_{k_s}(g_s h_j) \right) \\ &= 0 + \sum_{j=1}^{t} (h_j z_1, \ldots, h_j z_w) = (z_1, \ldots, z_w) = z. \end{aligned}$$

Since z was arbitrary this completes the proof of Proposition 3.3. □

We now complete the proof of Theorem 3.1. Without loss of generality we may assume that $\mathscr{H}$ is separable. For a subspace $\mathscr{G} \subset \mathscr{H}$, let $\mathscr{P}(\mathscr{G})$ be the assertion '(3.1) holds for all $f \in \mathscr{G}$'. It is easy to see that if $(\mathscr{H}_i)_{i=1}^{\infty}$ is a sequence of subspaces of $\mathscr{H}$ with $\mathscr{H}_i \subset \mathscr{H}_{i+1}$ for all i, then $\mathscr{P}(\mathscr{H}_i)$ for all i implies $\mathscr{P}(\overline{\bigcup_{i=1}^{\infty} \mathscr{H}_i})$. Thus by Zorn's lemma and separability, there exists a closed subspace $\mathscr{H}_m$ maximal with respect to the $\mathscr{P}$ property.

Let Q be the orthogonal projection onto $\mathscr{H}_m$. As $\mathscr{H}_m$ must be U_g-invariant for all $g \in F^l$, Q commutes with all U_g. For all $0 \neq f \in \mathscr{H}_m^{\perp}$, (3.1) does not hold. Our plan is to show that if $\mathscr{H}_m^{\perp}$ is non-empty, there exists $0 \neq f \in \mathscr{H}_m^{\perp}$ such that (3.1) *does* hold. This will complete the proof.

Suppose $0 \neq f_0 \in \mathscr{H}_m^{\perp}$. Put $\lambda(x) = (x^{t_1}, \ldots, x^{t_l})$, and for $k \in F$, let P_k be the orthogonal projection onto $\{f \in \mathscr{H} : U_{\lambda_k(g)} f = f \text{ for all } g \in F\}$. One may show that P_k commutes with Q for all $k \in F$. Let $\Pi(x_1, \ldots, x_R)$ be as guaranteed by Proposition 3.3. Let $H_0 = \{k \in F : \Pi(k, x_2, \ldots, x_R) \neq 0\}$. If $P_k f_0 = 0$ for all $k \in H_0$, let $z = 0$, and stop. Otherwise, pick $k_1 \in H_0$ such that $f_1 = P_{k_1} f_0 \neq 0$.

Having chosen $k_1, k_2, \ldots, k_y \in F$ and $f_y = (\prod_{i=1}^{y} P_{k_i}) f_0$ (where $y < R$), let $H_y = \{k \in F : \Pi(k_1, k_2, \ldots, k_y, k, x_{y+2}, \ldots, x_R) \neq 0\}$. If $P_k f_y = 0$ for all $k \in H_y$, let $z = y$, and stop. Otherwise pick $k_{y+1} \in H_y$ such that $f_{y+1} = P_{k_{y+1}} f_y \neq 0$, and continue.

If this process fails to terminate with some $z < R$, then $0 \neq f_R = f$ is in the range of P_{k_i}, $1 \leqslant i \leqslant R$, and, $\Pi(k_1, \ldots, k_R) \neq 0$. If $t_1 > 1$ then $q(x) = \lambda(x)$ and, according to Proposition 3.3, $\{\lambda_{k_i}(g) : g \in F, 1 \leqslant i \leqslant R\}$ spans F^l. This implies $f \in \mathscr{H}_{\text{inv}}$, a contradiction. Hence $t_1 = 1$, and Proposition 3.3 tells us that $\{\lambda_{k_i}(g) : g \in F, 1 \leqslant i \leqslant R\}$ spans $\{0\} \times F^{l-1}$. Thus $U_{\lambda(g)} f = U_{(g,0,\ldots,0)} f$ for all $g \in F$ and (3.1) holds by MET.

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

Suppose on the other hand this process does terminate with some $z < R$. Let $f = f_z = (\prod_{i=1}^{z} P_{k_i}) f_0$. Since $f_0 \in \mathscr{H}_m^{\perp}$, and each P_{k_i} commutes with Q, then $f \in \mathscr{H}_m^{\perp}$, and of course $f \neq 0$. For all but possibly finitely many $k \in F$ (namely, all $k \in H_z$), $P_k f = 0$. We now utilize Lemma VDC. Put $x_g = U_{\lambda(g)} f$. Then, for all but finitely many k,

$$\limsup_{n\to\infty} \frac{1}{|\Phi_n|} \sum_{g\in\Phi_n} \langle x_g, x_{g+k} \rangle = \limsup_{n\to\infty} \frac{1}{|\Phi_n|} \sum_{g\in\Phi_n} \langle U_{-\lambda(k)} f, U_{\lambda_k(g)} f \rangle$$
$$= \langle P_k (U_{\lambda(k)} f), P_k f \rangle = 0.$$

The conclusion of Lemma VDC now gives (3.1), since $Pf = 0$. □

Proof of Theorem C. For ease of notation, we will write $U(v)$ instead of U_v in this short proof. Write $(r_1(g), \ldots, r_l(g)) = \sum_{i=1}^{w} \mathbf{e}_{t_i} c_i g^{x_i}$, where $c_i \in F$, $x_i \in \mathbb{N}$, and $1 \leqslant t_i \leqslant l$ for each i. (Here $(\mathbf{e}_i)_{i=1}^{l}$ is the standard basis for F^l.) Next write $x_i = y_i p^{z_i}$, $1 \leqslant i \leqslant w$, where $p \nmid y_i$, and let $\{s_1, \ldots, s_n\} = \{y_1, \ldots, y_w\}$, with $s_1 < s_2 < \cdots < s_n$. Now, for $1 \leqslant j \leqslant n$, put

$$V_g^{(j)} = U\left(\sum_{\substack{1\leqslant i\leqslant w \\ y_i = s_j}} \mathbf{e}_{t_i} c_i g^{p^{z_i}} \right).$$

Finally, let $V_{(g_1,\ldots,g_n)} = \prod_{j=1}^{n} V_{g_j}^{(j)}$. Then $(V_g)_{g\in F^n}$ is a unitary action, and we can easily check that

$$V_{(g^{s_1},\ldots,g^{s_n})} = V_{g^{s_1}}^{(1)} \cdots V_{g^{s_n}}^{(n)} = U\left(\sum_{i=1}^{w} \mathbf{e}_{t_i} c_i g^{y_i p^{z_i}} \right) = U((r_1(g), \ldots, r_l(g)).$$

The desired result now follows immediately from Theorem 3.1 (applied to the unitary action V) and Fact 3.2, from which it follows that the V-invariant subspace of $\mathscr{H}$ is precisely the subspace invariant under each $U((r_1(g), \ldots, r_l(g))$. □

4. Some extensions

The following, a special case of a more general result in [4], extends Theorem B from the Introduction.

Theorem 4.1. *Suppose F_0 is a finite field. Let $\epsilon > 0$, $k \in \mathbb{N}$ and $r_i(x) \in F_0[x]$ with $r_i(0) = 0$, $1 \leqslant i \leqslant k$. Write $r(g) = (r_1(g), \ldots, r_k(g))$. There exists $M \in \mathbb{N}$ having the property that if F is any finite field containing F_0 with $|F| \geqslant M$ and $A \subset F^k$ with $|A| > \epsilon |F|^k$, then $(A - A) \cap \{(r(g) : g \in F^*\} \neq \emptyset$.*

We will now give some idea of the principal modification necessary in order to obtain Theorem 4.1 from Theorem C. Let us consider the special case $k = 1$, $F_0 = \mathbb{Z}_p$, $r(x) = 3g^2 + 5g^7$. The first step is a version of Lemma 2.3.

Lemma 4.2. *If $E \subset \mathbb{Z}_p[x]$ with $\overline{d}(E) > 0$ then $(E - E) \cap \{3g^2 + 5g^7 : g \in \mathbb{Z}_p[x]\} \neq \emptyset$.*

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press

Proof. Put $\epsilon = \frac{\bar{d}(E)}{2}$. Let $\mathbf{Q}$ and $\{\Phi_N\}$ be as in Lemma 2.3. Then $\{\Phi_N \times \Phi_N\}$ is a Følner sequence for $\mathbf{Q}^2$, and we may choose by Corollary 2.2 some N having the property that, if $E \subset \Phi_N \times \Phi_N$ with $|E| > \epsilon|\Phi_N|^2$, then $(E-E) \cap \{(3g^2, 5g^7) : g \in \mathbf{Q}^*\} \neq \emptyset$. Choose $f \in \mathbb{Z}_p[x]$ such that $f\Phi_N \subset \mathbb{Z}_p[x]$ and let $G = f^2\Phi_N \times f^7\Phi_N$. Note that if $E \subset G$ with $|E| > \epsilon G$ then $(E-E) \cap \{(3g^2, 5g^7) : 0 \neq g \in \mathbb{Z}_p[x]\} \neq \emptyset$.

Now let $E' = \{(y,z) \in \mathbb{Z}_p[x] \times \mathbb{Z}_p[x] : y+z \in E\}$. For every n, pick $j_n > n$ such that for every $g \in K_n$, $|(g + K_{j_n}) \cap K_{j_n}| > (1-\epsilon)|K_{j_n}|$. Then, for large n,

$$\begin{aligned} |E' \cap (K_n \times K_{j_n})| &= \sum_{x \in K_n} |\{y : y \in K_{j_n} \text{ and } x + y \in E\}| \\ &= \sum_{x \in K_n} |K_{j_n} \cap (E - x)| \\ &= \sum_{x \in K_n} |(K_{j_n} + x) \cap E| \\ &\leqslant \sum_{x \in K_n} (|K_n \cap E| - |(K_{j_n} + x) \setminus K_{j_n}|) > \epsilon |K_n|\, |K_{j_n}|. \end{aligned}$$

Choosing n sufficiently large that $G \subset K_n \times K_{j_n}$, some coset of G intersects E' in a set of size at least $\epsilon|G|$, and hence E' contains a configuration $\{(a,b), (a+3g^2, b+5g^7)\}$, $0 \neq g \in \mathbb{Z}_p[x]$. Therefore $\{c, c+3g^2+5g^7\} \subset E$, where $c = a+b$. □

The remainder of the derivation follows roughly along the lines of Section 2. □

References

[1] Bergelson, V. (1987) Ergodic Ramsey Theory. In *Logic and Combinatorics* (Arcata, CA, 1985), Vol. 65 of *Contemp. Math.*, AMS, Providence, RI, pp. 63–87.

[2] Bergelson, V. (1987) Weakly mixing PET. *Ergodic Theory Dynam. Systems* **7** 337–349.

[3] Bergelson, V. (2000) The multifarious Poincaré recurrence theorem. *Descriptive Set Theory and Dynamical Systems* (Marseille–Luminy, 1996), Vol. 277 of *London Math. Soc. Lecture Note Series*, Cambridge University Press, Cambridge, pp. 31–57.

[4] Bergelson, V., Leibman, A. and McCutcheon, R. Polynomial Szemerédi theorem for countable modules over integral domains and finite fields. Manuscript.

[5] Furstenberg, H. (1981) *Recurrence in Ergodic Theory and Combinatorial Number Theory*, M. B. Porter Lectures, Princeton University Press, Princeton, NJ.

[6] Larick, P. (1998) Results in polynomial recurrence for actions of fields. PhD Dissertation, The Ohio State University.

[7] Sárközy, A. (1978) On difference sets of sequences of integers, I. *Acta Math. Acad. Sci. Hungar.* **31** 125–149.

[8] Sárközy, A. (1978) On difference sets of sequences of integers, III. *Acta Math. Acad. Sci. Hungar.* **31** 355–386.

https://doi.org/10.1017/S0963548303005753 Published online by Cambridge University Press