CHARACTER-FREE APPROACH TO PROGRESSION-FREE SETS

VSEVOLOD F. LEV

Abstract. We present an elementary combinatorial argument showing that the density of a progression-free set in a finite r-dimensional vector space is $O(1/r)$.

1. Introduction

A set A of elements of an abelian group is called *progression-free* if for any $a, b, c \in A$ with $a + c = 2b$ one has $a = c$. In [M95] Meshulam proved that for any progression-free subset A of a finite abelian group G of odd order and rank $r \geq 1$ there exist a subgroup $G_0 < G$ of rank at least $r - 1$ and a progression-free subset $A_0 \subseteq G_0$ such that the densities $\alpha := |A|/|G|$ and $\alpha_0 := |A_0|/|G_0|$ satisfy

$$\alpha_0 \geq \frac{\alpha - |G|^{-1}}{1 - \alpha}.$$

Using straightforward induction one easily derives that the density of a progression-free subset of a finite abelian group of odd order and rank r is $O(1/r)$.

The argument of [M95] relies on Fourier analysis, considered now the standard tool for obtaining estimates of this sort. In this note we introduce a completely elementary approach, allowing us to establish Meshulam's result in a purely combinatorial way for the particular case of the additive group of a finite vector space.

Theorem 1. *Let q be a power of an odd prime and $r \geq 1$ an integer. If $A \subseteq \mathbb{F}_q^r$ is a progression-free set of density $\alpha := q^{-r}|A|$, then there exists a co-dimension 1 affine subspace of $\mathbb{F}_q^r$ such that the density of A on this subspace is at least*

$$\frac{\alpha - q^{-r}}{1 - \alpha}.$$

We remark that if q, r, A, and α are as in Theorem 1, and if $g \in \mathbb{F}_q^r$ and $V < \mathbb{F}_q^r$ is a linear subspace of co-dimension 1 such that the affine subspace $g + V$ satisfies the conclusion of the theorem, then the density of A on $g + V$ is $\alpha_0 := |A \cap (g + V)|/|V|$. Hence, if we let $A_0 := (A - g) \cap V$, then A_0 is a progression-free subset of V of density $\alpha_0 \geq (\alpha - q^{-r})/(1 - \alpha)$.

We set up the necessary notation in the next section and prove Theorem 1 in Section 3.

We admit that our proof is, in a sense, parallel to that of Meshulam, and therefore may not count as totally new. We hope, however, that it can be susceptible to various extensions where using characters is impossible or wasteful.

2. Preliminaries

Recall that the averaging operator on a finite non-empty set S is defined by

$$\mathsf{E}_{s\in S} f(s) := \frac{1}{|S|}\sum_{s\in S} f(s),$$

where f is a real-valued function on S. Occasionally, we use abbreviations as $\mathsf{E}_S(f)$, or just $\mathsf{E}\, f$, whenever the range is implicit from the context. By 1_S we denote the indicator function of S.

For the rest of this section we assume that f is a real-valued function on a finite abelian group G. The L^2-norm of f is

$$\|f\|_2 := \big(\mathsf{E}(f^2)\big)^{1/2},$$

and the balanced part of f is

$$\tilde f := f - \mathsf{E}\, f,$$

where averaging extends onto the whole group G.

Given a linear homogeneous equation E in k variables with integer coefficients, by $\mathcal{S}_G(E)$ we denote the solution set of E is $G^k := G\times\cdots\times G$ (k factors), and we let

$$\Lambda_E[f] := \mathsf{E}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} f(g_1)\cdots f(g_k);$$

thus, for instance,

$$\Lambda_{x-y=0}[f] = \mathsf{E}_{(g,g)\in G\times G} f^2(g) = \|f\|_2^2. \tag{1}$$

A basic observation is that if all coefficients of E are co-prime with the order of the group G then, fixing any $k-1$ coordinates of a k-tuple in G^k, there is a unique way to choose the remaining coordinate so that the resulting k-tuple falls into $\mathcal{S}_G(E)$. Consequently, for any real-valued function f on G and proper non-empty subset $I\subset[k]$ we have

$$\mathsf{E}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} \prod_{i\in I}\tilde f(g_i) = 0.$$

As a result, if all coefficients of the equation E are co-prime with the order of the group G, then

$$\Lambda_E[\tilde f] = \Lambda_E[f] - (\mathsf{E}\, f)^k : \tag{2}$$

to see this just notice that

$$\Lambda_E[f] = \mathsf{E}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} f(g_1)\cdots f(g_k)$$
$$= \sum_{\delta_1,\dots,\delta_k=0}^{1} (\mathsf{E}\, f)^{\delta_1+\dots+\delta_k} \cdot \mathsf{E}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} \prod_{1\le i\le k\colon\, \delta_i=0} \tilde{f}(g_i),$$

and that, by the observation just made, the quantity

$$\mathsf{E}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} \prod_{1\le i\le k\colon\, \delta_i=0} \tilde{f}(g_i)$$

vanishes, unless $\delta_1 = \ldots = \delta_k$.

Let f be a real-valued function on a finite abelian group G. For a subgroup $H \le G$ we denote by $f|H$ the function on the quotient group G/H, defined by

$$f|H\colon g + H \mapsto \mathsf{E}_{g+H} f.$$

We note that $f|\{0\} = f$, while $f|G = \mathsf{E}\, f$ is a constant function (on the trivial group), and that $\mathsf{E}(f|H) = \mathsf{E}\, f$; furthermore, it is easily verified that $\tilde{f}|H = \widetilde{f|H}$.

3. Proof of Theorem 1

We are now ready to prove Theorem 1. In the heart of our argument is the identity, established in the following lemma.

Lemma 1. *Let q be a prime power, $r \ge 1$ an integer, and E a homogeneous linear equation with integer coefficients, co-prime with q. If f is a real-valued function on the vector space $\mathbb{F}_q^r$, then*

$$\Lambda_E[\tilde{f}] = \sum_{V<\mathbb{F}_q^r\colon\ \operatorname{codim} V=1} \Lambda_E[\tilde{f}|V].$$

Proof. Denote by k the number of variables in E. Writing (for typographical reasons) $G = \mathbb{F}_q^r$ and agreeing that summation over V extends onto linear subspaces $V < \mathbb{F}_q^r$

of co-dimension 1, we get

$$\begin{aligned}\sum_V \Lambda_E[\tilde f|V] &= \sum_V \mathsf{E}_{(\bar g_1,\dots,\bar g_k)\in\mathcal{S}_{G/V}(E)} (\tilde f|V)(\bar g_1)\dots(\tilde f|V)(\bar g_k)\\ &= \sum_V \mathsf{E}_{(\bar g_1,\dots,\bar g_k)\in\mathcal{S}_{G/V}(E)} \mathsf{E}_{g_1\in\bar g_1,\dots,g_k\in\bar g_k} \tilde f(g_1)\cdots\tilde f(g_k)\\ &= \sum_V \mathsf{E}_{\substack{g_1,\dots,g_k\in G\\ (g_1+V,\dots,g_k+V)\in\mathcal{S}_{G/V}(E)}} \tilde f(g_1)\cdots\tilde f(g_k)\\ &= \mathsf{E}_{g_1,\dots,g_k\in G} \tilde f(g_1)\cdots\tilde f(g_k) \sum_{V\colon (g_1+V,\dots,g_k+V)\in\mathcal{S}_{G/V}(E)} |G/V|.\end{aligned}$$

We now notice that the number of summands in the inner sum is equal to $(q^r-1)/(q-1)$ (the total number of co-dimension 1 subspaces) if $(g_1,\dots,g_k)\in\mathcal{S}_G(E)$, and is equal to $(q^{r-1}-1)/(q-1)$ (the number of co-dimension 1 subspaces, containing a fixed non-zero element of G) if $(g_1,\dots,g_k)\notin\mathcal{S}_G(E)$. Since $|G/V|=q$ for any subspace V of co-dimension 1, we have

$$\sum_{V\colon (g_1+V,\dots,g_k+V)\in\mathcal{S}_{G/V}(E)} |G/V| = \frac{q^r-q}{q-1} + q^r\cdot 1_{\mathcal{S}_G(E)}(g_1,\dots,g_k).$$

Hence

$$\sum_V \Lambda_E[\tilde f|V] = q^r \mathsf{E}_{g_1,\dots,g_k\in G} \tilde f(g_1)\cdots\tilde f(g_k)\cdot 1_{\mathcal{S}_G(E)}(g_1,\dots,g_k),$$

and it remains to observe that the right-hand side is the definition of $\Lambda_E[\tilde f]$ in disguise. □

Applying Lemma 1 to the equation $x-y=0$ and using (1), we obtain

Corollary 1. *Let q be a prime power and $r\ge 1$ an integer. If f is a real-valued function on the vector space $\mathbb{F}_q^r$, then*

$$\|\tilde f\|_2^2 = \sum_{V<\mathbb{F}_q^r\colon\ \operatorname{codim} V=1} \|\tilde f|V\|_2^2.$$

Corollary 1 can be considered as an analogue of the Parseval identity. Next, we need a tool for the the "cubes versus squares" comparison.

Claim 1. *Let M be a real number and f a non-constant real-valued function on the finite abelian group G. Suppose that E is a linear homogeneous equation in $k\ge 3$ variables with integer coefficients, co-prime with the order of G. If either k is odd* *and*

$$\Lambda_E[\tilde f] \le -M^{k-2}\|\tilde f\|_2^2,$$

or k is even and

$$\Lambda_E[\tilde f] \ge M^{k-2}\|\tilde f\|_2^2,$$

then $\max_G \tilde f \ge M$ *and, consequently,*

$$\max_G f \ge \mathsf{E}\, f + M.$$

Proof. Assuming $\max_G \tilde f < M$, we get

$$\mathop{\mathsf{E}}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} (\tilde f(g_1)-\tilde f(g_2))^2(M-\tilde f(g_3))\cdots(M-\tilde f(g_k)) > 0.$$

Multiplying out the brackets in the left-hand side and using linearity of the averaging operator, we get a sum of $3\cdot 2^{k-2}$ terms, of which, in view of the coprimality assumption, not vanishing are only

$$2(-1)^{k-1} \mathop{\mathsf{E}}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} \tilde f(g_1)\cdots\tilde f(g_k)$$

and

$$M^{k-2} \mathop{\mathsf{E}}_{(g_1,\dots,g_k)\in\mathcal{S}_G(E)} (\tilde f(g_i))^2; \quad i\in\{1,2\}.$$

Of these three terms the first is equal to $2(-1)^{k-1}\Lambda_E[\tilde f]$, while coprimality ensures that the other two are both equal to $M^{k-2}\|\tilde f\|_2^2$. We conclude that

$$(-1)^k\Lambda_E[\tilde f] < M^{k-2}\|\tilde f\|_2^2,$$

contradicting the assumptions. □

We notice that Claim 1 is, in a sense, sharp: say, if G, E, and k are as in the claim, and the coefficients of E add up to 0, then for any fixed element $g\in G$, writing $N := |G|$ we have

$$\Lambda_E[\widetilde{1}_{G\setminus\{g\}}] = (-1)^k N^{-(k-2)}\|\widetilde{1}_{G\setminus\{g\}}\|_2^2$$

(both sides being equal to $(-1)^k N^{-k}(N-1)$), whereas $\max_G \widetilde{1}_{G\setminus\{g\}} = N^{-1}$.

Suppose that q, r, E, and f are as in Lemma 1. Comparing

$$\sum_{V<\mathbb{F}_q^r:\ \operatorname{codim} V=1} \Lambda_E[\tilde f|V] = \Lambda_E[\tilde f]$$

(which is the conclusion of the lemma) and

$$\sum_{V<\mathbb{F}_q^r:\ \operatorname{codim} V=1} \|\tilde{f}|V\|_2^2 = \|\tilde{f}\|_2^2$$

(by Corollary 1), and observing that $\|\tilde{f}|V\|_2 = 0$ implies $\Lambda_E[\tilde{f}|V] = 0$, we conclude that if f is not a constant function, then there exists a co-dimension 1 subspace $V < \mathbb{F}_q^r$ with $\|\tilde{f}|V\|_2 \neq 0$ and

$$\Lambda_E[\tilde{f}|V] \le \frac{\Lambda_E[\tilde{f}]}{\|\tilde{f}\|_2^2} \cdot \|\tilde{f}|V\|_2^2.$$

If E is an equation in three variables, then by Claim 1 there exists $g \in \mathbb{F}_q^r$ such that

$$\mathsf{E}_{g+V} f = (f|V)(g) \ge \mathsf{E} f - \frac{\Lambda_E[\tilde{f}]}{\|\tilde{f}\|_2^2}.$$

We summarize as follows.

Proposition 1. *Let q be a prime power, $r \ge 1$ an integer, and E a homogeneous linear equation in three variables with the coefficients, co-prime with q. If f is a non-constant real function on the vector space $\mathbb{F}_q^r$, then there exists a co-dimension 1 affine subspace $g+V$ (where $g \in \mathbb{F}_q^r$ and $V < \mathbb{F}_q^r$ is a linear subspace) such that*

$$\mathsf{E}_{g+V} f \ge \mathsf{E} f - \frac{\Lambda_E[\tilde{f}]}{\|\tilde{f}\|_2^2}.$$

We are now in a position to complete the proof of Theorem 1, and this is where the property of being progression-free comes into play.

Suppose that G is a finite abelian group and $A \subseteq G$ is a subset of density $\alpha := \mathsf{E}\,1_A$. By (1) and (2), we have

$$\|\widetilde{1}_A\|_2^2 = \Lambda_{x-y=0}[\widetilde{1}_A] = \mathsf{E}\,1_A^2 - (\mathsf{E}\,1_A)^2 = \alpha(1-\alpha).$$

If $N := |G|$ is odd and A is progression-free, then $\Lambda_{x-2y+z=0}[1_A] = N^{-1}\alpha$ by the definition of the operator Λ_E; hence (2) gives

$$\Lambda_{x-2y+z=0}[\widetilde{1}_A] = -\alpha(\alpha^2 - N^{-1}).$$

Thus,

$$\mathsf{E}\,1_A - \frac{\Lambda_{x-2y+z}[\widetilde{1}_A]}{\|\widetilde{1}_A\|_2^2} = \alpha + \frac{\alpha^2 - N^{-1}}{1-\alpha} = \frac{\alpha - N^{-1}}{1-\alpha}$$

and Theorem 1 follows from this equality and Proposition 1.

References

[M95] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory, Ser. A* **71**(1) (1995), 168–172.

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel

E-mail address: seva@math.haifa.ac.il