THE ERDŐS–GINZBURG–ZIV THEOREM

STEVE FAN

Abstract. The Erdős–Ginzburg–Ziv theorem in additive number theory states that if $(G,+,0)$ is a finite abelian group of order $n \geq 1$ and if $\mathcal{A}$ is a sequence of elements in G of length $2n-1$, then $\mathcal{A}$ contains a subsequence $\mathcal{B}$ of length n such that $\sum_{b\in\mathcal{B}} b = 0$. In this short note we shall present a proof of this theorem using the polynomial method.

1. Introduction

Throughout this note, we shall always denote by $+$ the binary operation on a finite abelian group. Our goal is to prove the following result of Erdős, Ginzburg and Ziv [2].

Theorem 1.1. *Let G be a finite abelian group with $|G| = n$. Then any sequence $\mathcal{A}$ of elements in G of length $2n-1$ contains a subsequence $\mathcal{B}$ of length n such that $\sum_{b\in\mathcal{B}} b = 0$.*

Let us begin by proving the following lemma.

Lemma 1.2. *Let k and l be positive integers. Let G_1 and G_2 be finite abelian groups with $|G_1| = k$ and $|G_2| = l$. Suppose that Theorem 1.1 holds for G_1 and G_2. Then Theorem 1.1 also holds for $G = G_1 \oplus G_2$.*

Proof. Let $\mathcal{A}$ be a sequence of elements in G of length $2kl-1$. By assumption, there exist $(x_1^{(1)}, y_1^{(1)}), ..., (x_k^{(1)}, y_k^{(1)}) \in \mathcal{A}$ such that $\sum_{i=1}^k x_i^{(1)} = 0$. Let $\mathcal{A}_1$ be the subsequence obtained from $\mathcal{A}$ by discarding $(x_1^{(1)}, y_1^{(1)}), ..., (x_k^{(1)}, y_k^{(1)})$. If $l = 1$, then

$$\sum_{i=1}^k (x_i^{(1)}, y_i^{(1)}) = \left(\sum_{i=1}^k x_i^{(1)}, \sum_{i=1}^k y_i^{(1)}\right) = (0,0).$$

If $l > 1$, then the length of $\mathcal{A}_1$ is $(2l-1)k - 1 > 2k-1$. It follows that there exist $(x_1^{(2)}, y_1^{(2)}), ..., (x_k^{(2)}, y_k^{(2)}) \in \mathcal{A}_1$ such that $\sum_{i=1}^k x_i^{(2)} = 0$. In general, we obtain by iterating this procedure a rearranged subsequence $\{(x_i^{(j)}, y_i^{(j)})\}$ of $\mathcal{A}$ with $1 \leq i \leq k$ and $1 \leq j \leq 2l-1$, such that $\sum_{i=1}^k x_i^{(j)} = 0$ for all $1 \leq j \leq 2l-1$. Among the elements $\sum_{i=1}^k y_i^{(1)}, ..., \sum_{i=1}^k y_i^{(2l-1)} \in G_2$, we can find $1 \leq j_1 < ... < j_l \leq 2l-1$ such that

$$\sum_{r=1}^l \sum_{i=1}^k y_i^{(j_r)} = 0.$$

It follows that

$$\sum_{r=1}^l \sum_{i=1}^k (x_i^{(j_r)}, y_i^{(j_r)}) = \left(\sum_{r=1}^l \sum_{i=1}^k x_i^{(j_r)}, \sum_{r=1}^l \sum_{i=1}^k y_i^{(j_r)}\right) = (0,0).$$

This completes the proof. □

By a similar argument one can prove the following result.

Lemma 1.3. *Let k and l be positive integers. Suppose that Theorem 1.1 holds for $\mathbb{Z}/k\mathbb{Z}$ and $\mathbb{Z}/l\mathbb{Z}$. Then Theorem 1.1 also holds for $\mathbb{Z}/kl\mathbb{Z}$.*

Proof. Let $\mathcal{A}$ be a sequence of integers of length $2kl-1$. As in the proof of Lemma 1.2, we can find a rearranged subsequence $\{a_i^{(j)}\}$ of $\mathcal{A}$ with $1 \leq i \leq k$ and $1 \leq j \leq 2l-1$, such that $\sum_{i=1}^k a_i^{(j)} \equiv 0 \pmod{k}$ for all $1 \leq j \leq 2l-1$. Let $\sum_{i=1}^k a_i^{(j)} = b_j k$ for every $1 \leq j \leq 2l-1$, where $b_j \in \mathbb{Z}$. Among the integers $b_1, ..., b_{2l-1}$, there exist positive integers $1 \leq j_1 < ... < j_l \leq 2l-1$ such that $\sum_{r=1}^l b_{j_r} \equiv 0 \pmod{l}$. Thus we have

$$\sum_{r=1}^{l} \sum_{i=1}^{k} a_i^{(j_r)} = k \sum_{r=1}^{l} b_{j_r} \equiv 0 \pmod{kl}.$$

This finishes the proof of the lemma. □

Let G be a finite abelian group. By the fundamental theorem of finite abelian groups we see that

$$G \simeq \bigoplus_{i=1}^{r} \mathbb{Z}/d_i\mathbb{Z}$$

with positive integers $d_1 \mid d_2 \mid ... \mid d_r$. In view of Lemmas 1.2 and 1.3, we will be able to finish the proof of Theorem 1.1 if we can prove the following special case of it.

Proposition 1.4. *Let p be an arbitrary prime. Then any sequence $\mathcal{A}$ of elements in $\mathbb{Z}/p\mathbb{Z}$ of length $2p-1$ contains a subsequence $\mathcal{B}$ of length p such that $\sum_{b \in \mathcal{B}} b = 0$.*

It is not hard to see that Theorem 1.1 is best possible. Indeed, it suffices to consider the case $G = \mathbb{Z}/n\mathbb{Z}$ with $n > 1$. Then the sequence $\mathcal{A} = \{a_i\}_{i=1}^{2n-2}$ with $a_1 = ... = a_{n-1} = 0$ and $a_n = ... = a_{2n-2} = 1$ contains no subsequence $\mathcal{B}$ of length n such that $\sum_{b \in \mathcal{B}} b = 0$.

There are many proofs of Proposition 1.4. Here we shall follow [1] to present a proof using the polynomial method, or more specifically, the combinatorial Nullstellensatz developed by Alon, Nathanson and Ruzsa. The primary purpose of selecting this proof over the others is to showcase the power and beauty of the polynomial method which has many interesting applications in combinatorics, graph theory, additive number theory, transcendental number theory (e.g. auxiliary polynomials), algebraic geometry, incidence geometry and so forth.

2. The Combinatorial Nullstellensatz

In this section, we shall introduce the ingredients of the polynomial method that we need for the proof of Proposition 1.4. The key results are two theorems which Alon [1] calls Combinatorial Nullstellensatz due to their close connection to Hilbert's Nullstellensatz. To derive these two theorems, we need the following lemma [1, Lemma 2.1].

Lemma 2.1. *Let R be a domain with identity 1. Suppose that $P \in R[x_1, ..., x_n]$ is a polynomial with the property that for each $1 \leq i \leq n$, the degree of P as a polynomial in x_i is at most d_i, where each d_i is a non-negative integer. Let $S_1, ..., S_n \subseteq R$ be subsets of R with $|S_i| > d_i$ for all $1 \leq i \leq n$, and let $S := S_1 \times ... \times S_n$. If P vanishes on S, then P is identically zero.*

Proof. We induct on n. For $n = 1$, we see that P is a polynomial of one variable of degree at most d_1 that has at least $|S_1| > d_1$ zeros. Thus $P \equiv 0$. Suppose that the lemma is true for $n-1$, where $n \geq 2$ is a positive integer. Write

$$P(x_1, ..., x_n) = \sum_{k=0}^{d_n} P_k(x_1, ..., x_{n-1}) x_n^k,$$

where the degree of each $P_k(x_1, ..., x_{n-1}) \in R[x_1, ..., x_{n-1}]$ as a polynomial in x_i is at most d_i for all $1 \leq i \leq n-1$. For every fixed $(s_1, ..., s_{n-1}) \in S_1 \times ... \times S_{n-1}$, the polynomial $P(s_1, ..., s_{n-1}, x_n)$ vanishes on S_n. By the base case, we have $P(s_1, ..., s_{n-1}, x_n) \equiv 0$. It follows that $P_k(s_1, ..., s_{n-1}) = 0$ for all $0 \leq k \leq d_n$. Hence each P_k vanishes on $S_1 \times ... \times S_{n-1}$. By induction, we have $P_k(x_1, ..., x_{n-1}) \equiv 0$ for all $0 \leq k \leq d_n$. This implies that $P \equiv 0$. □

We are now ready to prove the first part of Alon's combinatorial Nullstellensatz [1, Theorem 1.1].

Theorem 2.2. *Let F be a field and let $S_1, ..., S_n \subseteq F$ be nonempty subsets of F. Put $S := S_1 \times ... \times S_n$ and let $f \in F[x_1, ..., x_n]$ be a polynomial which vanishes on S. Define*

$$g_i(x_1, ..., x_n) := \prod_{s \in S_i} (x_i - s) \in F[x_1, ..., x_n] \tag{1}$$

for each $1 \leq i \leq n$. Then there exist polynomials $h_1, ..., h_n \in F[x_1, ..., x_n]$ with $\deg h_i \leq \deg f - \deg g_i$ for all $1 \leq i \leq n$ such that $f = \sum_{i=1}^n h_i g_i$.

Proof. Let $|S_i| := d_i + 1$ for all $1 \leq i \leq n$, where $d_i \geq 0$. Let $I \subseteq F[x_1, ..., x_n]$ be the ideal generated by $g_1, ..., g_n$ and let $\bar{f}$ be the reduction of f modulo I. Note that

$$g_i(x_1, ..., x_n) = x_i^{d_i+1} + P_i(x_i)$$

for some polynomial $P_i \in F[x_i]$ with $\deg P_i \leq d_i$. It follows that for each $1 \leq i \leq n$, the degree of $\bar{f}$ as a polynomial in x_i is at most d_i. Moreover, there exist polynomials $h_1, ..., h_n \in F[x_1, ..., x_n]$ such that

$$f(x_1, ..., x_n) = \bar{f}(x_1, ..., x_n) + \sum_{i=1}^n h_i(x_1, ..., x_n) g_i(x_1, ..., x_n).$$

Since $\deg(h_i g_i) \leq \deg f$, we deduce that $\deg h_i \leq \deg f - \deg g_i$. Since $f, g_1, ..., g_n$ all vanish on S, we have that $\bar{f}$ also vanishes on S. From Theorem 2.2 it follows that $\bar{f} \equiv 0$. This shows that $f = \sum_{i=1}^n h_i g_i$. □

The following theorem, which constitutes the second part of the combinatorial Nullstellensatz [1, Theorem 1.2], is an immediate corollary of Theorem 2.2.

Theorem 2.3. *Let F be a field and let $S_1, ..., S_n \subseteq F$ be subsets of F with $|S_i| > d_i$ for all $1 \leq i \leq n$, where each d_i is a non-negative integer. Put $S := S_1 \times ... \times S_n$ and let $f \in F[x_1, ..., x_n]$ be a polynomial of degree $d := \sum_{i=1}^n d_i$ such that the coefficient of $\prod_{i=1}^n x_i^{d_i}$ in f is nonzero. Then f does not vanish at all points of S.*

Proof. Without loss of generality, we may assume that $|S_i| = d_i + 1$ for all $1 \leq i \leq n$. Assume to the contrary that f vanishes on S. By Theorem 2.2, there exist polynomials $h_1, ..., h_n \in F[x_1, ..., x_n]$ with $\deg h_i \leq d - d_i - 1$ for all $1 \leq i \leq n$ such that $f = \sum_{i=1}^n h_i g_i$, where g_i is defined as in (1). By assumption, the coefficient of $\prod_{i=1}^n x_i^{d_i}$ in f is nonzero.

Thus there exists $1 \leq j \leq n$ such that the coefficient of $\prod_{i=1}^n x_i^{d_i}$ in $h_j g_j$ is nonzero. But $h_j g_j = x_j^{d_j+1} h_j + h_j P_j$ and $\deg(h_j P_j) \leq \deg h_j + d_j \leq d-1$. Hence the term $\prod_{i=1}^n x_i^{d_i}$ appears in $x_j^{d_j+1} h_j$. This is clearly impossible. □

An interesting application of Theorem 2.3 is the following result known as the permanent lemma [1, Lemma 8.1].

Lemma 2.4. *Let F be a field and let $A = (a_{ij}) \in M_n(F)$ be an $n \times n$ matrix with*

$$\mathrm{per}(A) := \sum_{\sigma} \prod_{i=1}^n a_{i\sigma(i)} \neq 0,$$

where σ ranges over all permutations on $\{1, ..., n\}$. Let $S_1, ..., S_n \subseteq F$ be subsets of F with $|S_i| \geq 2$ for all $1 \leq i \leq n$. Then for any $b = (b_1, ..., b_n) \in F^n$, there exists $u = (u_1, ..., u_n) \in S_1 \times ... \times S_n$ such that if $v = uA = (v_1, ..., v_n)$, then $v_j \neq b_j$ for all $1 \leq j \leq n$.

Proof. Consider the polynomial

$$P(x_1, ..., x_n) := \prod_{j=1}^n \left(\sum_{i=1}^n a_{ij} x_i - b_j \right) \in F[x_1, ..., x_n].$$

Note that $\deg P = n$ and $\mathrm{per}(A) \neq 0$ is the coefficient of the term $\prod_{j=1}^n x_j$ in P. It follows by Theorem 2.3 that there exists $u = (u_1, ..., u_n) \in S_1 \times ... \times S_n$ such that $P(u_1, ..., u_n) \neq 0$. This implies that $v_j = \sum_{i=1}^n a_{ij} u_i \neq b_j$ for all $1 \leq j \leq n$. □

Note that the conclusion of Lemma 2.4 is still true if we replace the condition $\mathrm{per}(A) \neq 0$ with $\det A \neq 0$. Indeed, we may suppose that $|S_i| = 2$ for all $1 \leq i \leq n$. Let $b = (b_1, ..., b_n) \in F^n$ be an arbitrary vector and let $T := \{uA \colon u \in S\}$, where $S := S_1 \times ... \times S_n$. Since A is invertible, we have $|T| = 2^n$. On the other hand, it follows from the inclusion-exclusion principle that

$$|\{v = (v_1, ..., v_n) \in T \colon v_i = b_i \text{ for some } 1 \leq i \leq n\}| \leq \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} 2^{n-k} = 2^n - 1.$$

Thus there exists $v = (v_1, ..., v_n) \in T$ such that $v_i \neq b_i$ for all $1 \leq i \leq n$. Note also that in the case $F \subseteq \mathbb{R}$, the triangle inequality implies that any invertible matrix $A \in M_n(F)$ with non-negative entries must have nonzero permanent.

3. Proof of Proposition 1.4

Now it is an easy matter to derive Proposition 1.4 from Lemma 2.4. Let p be any prime and take $G = \mathbb{Z}/p\mathbb{Z}$. Let $\pi \colon \mathbb{Z} \to G$ be the natural projection. Let $\mathcal{A} = \{a_i\}_{i=1}^{2p-1}$ be any sequence of elements in F of length $2p-1$. For every $1 \leq i \leq 2p-1$, let $a_i^* \in \mathbb{Z}$ be the least non-negative integer such that $\pi(a_i^*) = a_i$. Without loss of generality, we may suppose that $0 \leq a_1^* \leq ... \leq a_{2p-1}^* < p$. If there exists $1 \leq i \leq p-1$ for which $a_i^* = a_{i+p-1}^*$, then $a_i = a_{i+1} = ... = a_{i+p-1}$ and thus we have

$$\sum_{j=i}^{i+p-1} a_j = p a_i = 0$$

in G. Otherwise, let $A \in M_{p-1}(G)$ be the $(p-1) \times (p-1)$ matrix all of whose entries are 1. Then $\mathrm{per}(A) = (p-1)! \neq 0$. Let $S_i := \{a_i, a_{i+p-1}\}$ for all $1 \leq i \leq p-1$. Then $|S_i| = 2$ for all $1 \leq i \leq p-1$. By Lemma 2.4, for any $b = (b_1, ..., b_{p-1}) \in G^{p-1}$ with $b_1, ..., b_{p-1}$ being distinct elements in $G \setminus \{-a_{2p-1}\}$ there exists $u = (u_1, ..., u_{p-1}) \in S_1 \times ... \times S_{p-1}$ such that if $v = uA = (v_1, ..., v_{p-1})$, then

$$v_j = \sum_{i=1}^{p-1} u_i \neq b_j$$

for all $1 \leq j \leq p-1$. Hence we must have

$$\sum_{i=1}^{p-1} u_i = -a_{2p-1}.$$

This completes the proof of Proposition 1.4.

4. Concluding Remarks

The original proof of Proposition 1.4 is completely elementary. It relies on the following lemma [2] which can be proved by induction.

Lemma 4.1. *Let $p > 2$ be an odd prime and $\mathcal{A}$ a sequence of elements of $\mathbb{Z}/p\mathbb{Z}$ of length $2 \leq s < p$. Suppose further that not all elements of $\mathcal{A}$ are equal. Then the set*

$$\left\{ \sum_{a \in \mathcal{A}} \epsilon_a a \colon \text{each } \epsilon_a \in \{0,1\} \right\} \subseteq \mathbb{Z}/p\mathbb{Z}$$

has cardinality at least $s+1$.

We now describe how Proposition 1.4 follows from Lemma 4.1. The case $p = 2$ is trivial. Let $p > 2$ be an odd prime and let $\mathcal{A} = \{a_i\}_{i=1}^{2p-1}$ be any sequence of elements in $\mathbb{Z}/p\mathbb{Z}$ of length $2p-1$. As in Section 3, we may suppose that $0 \leq a_1^* \leq ... \leq a_{2p-1}^* < p$ and that $a_i \neq a_{i+p-1}$ for all $1 \leq i \leq p$. If $\sum_{i=1}^{p} a_i = 0$, then we are done. Suppose now that $\sum_{i=1}^{p} a_i \neq 0$. Let $b_i := a_{i+p} - a_{i+1} \neq 0$ for each $1 \leq i \leq p-1$. If $b_1 = ... = b_{p-1} = b$, then there exists a positive integer $1 \leq k \leq p-1$ such that

$$k = -b^{-1} \sum_{i=1}^{p} a_i$$

holds in $\mathbb{Z}/p\mathbb{Z}$. Taking $\epsilon_1 = ... = \epsilon_k = 1$ and $\epsilon_{k+1} = ... = \epsilon_p = 0$ we find that

$$\sum_{i=1}^{p} a_i + \sum_{i=1}^{p-1} \epsilon_i b_i = b \left(b^{-1} \sum_{i=1}^{p} a_i + k \right) = 0.$$

Otherwise, Lemma 4.1 applied to the sequence $\{b_i\}_{i=1}^{p-1}$ implies that there exist $\epsilon_1, ..., \epsilon_{p-1} \in \{0,1\}$ such that

$$\sum_{i=1}^{p-1} \epsilon_i b_i = -\sum_{i=1}^{p} a_i.$$

In either case, we conclude that there exist $\epsilon_1, ..., \epsilon_{p-1} \in \{0, 1\}$ such that

$$\sum_{i=1}^{p} a_i + \sum_{i=1}^{p-1} \epsilon_i b_i = 0.$$

After cancellation, the left-hand side is a sum of precisely p elements of $\mathcal{A}$ with distinct indices. This proves Proposition 1.4.

There is also a 2-dimensional counterpart of Theorem 1.1 due to Reiher [3] which states that any set S of $4n-3$ planar lattice points contains a subset S' of cardinality n such that the centroid of all points from S' is also a lattice point. This was conjectured in 1983 by Kemnitz and was proved in 2003 by Reiher using the following theorem of Chevalley and Warning (see [4]).

Theorem 4.2. *Let $\mathbb{F}_q$ be a finite field and let $P_1, ..., P_m \in \mathbb{F}_q[x_1, ..., x_n]$ be m polynomials such that $\sum_{i=1}^{m} \deg P_i < n$. If $P_1, ..., P_m$ share a common zero, then $P_1, ..., P_m$ have another common zero.*

As a matter of fact, the Chevalley-Warning theorem can be derived easily from Theorem 2.3 (see [1, Theorem 3.1]). More generally, let $f(n, d)$ denote the least positive integer f such that any set S of f lattice points in $\mathbb{R}^d$ contains a subset S' of cardinality n whose centroid is also a lattice point. Then $f(n, 1) = 2n - 1$ and $f(n, 2) = 4n - 3$. The problem of determining $f(n, d)$ for $d \geq 3$ is still open.

References

[1] N. Alon, *Combinatorial Nullstellensatz*, Comb. Prob. Comput. **8** (1999), 7–29.

[2] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel **10F** (1961), 41–43.

[3] Ch. Reiher, *On Kemnitz' conjecture concerning lattice-points in the plane*, Ramanujan J. **13** (2007), 333–337.

[4] W. M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Math., vol. 536, Springer-Verlag, Berlin-New York, 1976.

Department of Mathematics, Dartmouth College, Hanover, NH 03755, USA
Email address: steve.fan.gr@dartmouth.edu