Sumsets and Zero-sum Problems

Zhi-Wei Sun

Nanjing University
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

June 12, 2020

Abstract

In this talk we introduce sumsets and zero-sum problems. In particular, we focus on the Cauchy-Davenport theorem, Chevalley-Warning theorem and Erdős-Ginzburg-Ziv theorem.

Part I. Sumsets

A Basic Result

Theorem: Let A and B be subsets of a multiplicative group G. If $|A| + |B| > |G|$, then

$$AB := \{ab : \ a \in A \text{ and } b \in B\}$$

coincides with G.

Proof. Suppose that $AB \neq G$. Then $g \notin AB$ for some $g \in G$. For any $a \in A$ and $b \in B$ we have $g \neq ab$ and hence $gb^{-1} \neq a$. So $A \cap gB^{-1} = \emptyset$ and hence

$$|G| \geqslant |A \cap gB^{-1}| = |A| + |gB^{-1}| = |A| + |B|. \quad \square$$

If $A_1, \ldots, A_n$ are subsets of an additive group G, then we call

$$A_1 + \ldots + A_n := \{a_1 + \ldots + a_n : \ a_1 \in A_1, \ldots, a_n \in A_n\}$$

the *sumset* of $A_1, \ldots, A_n$. When $A_1 = \ldots = A_n = A$, we write nA for $A_1 + \ldots + A_n$.

If A and B are subsets of an additive group G, then

$$|A| + |B| > |G| \implies A + B = G.$$

Additive bases

Let $A \subseteq \mathbb{N} = \{0, 1, 2, \ldots\}$ and $h \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. If

$$hA = \{a_1 + \ldots + a_h : \ a_1, \ldots, a_h \in A\}$$

coincides with A, then we say that A is an *additive base* of order h. If hA contains all sufficiently large natural numbers, then A is called an *asymptotic additive base* of order h.

Lagrange's Four-square Theorem: Each $n \in \mathbb{N}$ is the sum of four squares. In other words, the set $\{0^2, 1^2, 2^2, \ldots\}$ is an additive base of order 4.

Shnirel'man's density and Mann's theorem

Goldbach's Conjecture: Let P be the set of all primes. Then $P + P \supseteq \{4, 6, 8, \ldots\}$.

Shnirel'man's Density for $A \subseteq \mathbb{N}$ (L. G. Shnirel'man, 1933):

$$d(A) := \inf_{n \geqslant 1} \frac{|\{a \in A : 1 \leqslant a \leqslant n\}|}{n}.$$

Though $d(P) = 0$, Shnirel'man showed in 1933 that $d(P + P) > 0$, and that there exists a constant $c > 0$ such that each integer greater than one can be expressed as a sum of at most c primes; this is the first important progress on Goldbach's conjecture.

Mann's Theorem (conjectured by Shnirel'man and proved by Mann in 1942): Let A and B be subsets of $\mathbb{N}$ containing 0. Then

$$d(A + B) \geqslant \min\{1, d(A) + d(B)\}.$$

Remark. Any $A \subseteq \mathbb{N}$ with $0 \in A$ and $d(A) > 0$ is an additive base of order h for some $h \in \mathbb{Z}^+$. In fact, take $h \in \mathbb{Z}^+$ with $h \geqslant 1/d(A)$, then $hA = \mathbb{N}$ since $d(hA) \geqslant \min\{1, hd(A)\} = 1$.

Sumsets over $\mathbb{Z}$

Observe that $\{1, \ldots, k\} + \{1, \ldots, l\} = \{2, \ldots, k + l\}$.

Theorem. Let A and B be finite nonempty subsets of $\mathbb{Z}$. Then $|A + B| \geqslant |A| + |B| - 1$.

Proof. Write $A = \{a_1, \ldots, a_k\}$ with $a_1 < \ldots < a_k$, and $B = \{b_1, \ldots, b_l\}$ with $b_1 < \ldots < b_l$. Without loss of generality, we suppose that $k \leqslant l$. Note that

$$a_i + b_i < a_i + b_{i+1} < a_{i+1} + b_{i+1} \quad (i = 1, \ldots, k-1)$$

and

$$a_k + b_k < a_k + b_{k+1} < \ldots < a_k + b_l.$$

So we have found $2(k-1) + l - (k-1) = k + l - 1$ distinct numbers in $A + B$. Thus $|A + B| \geqslant |A| + |B| - 1$. $\square$

It can be shown further that $|A + B| = |A| + |B| - 1$ if and only if A and B are arithmetic progressions with the same common difference.

A general theorem

Using the above result, by induction one gets the following general result.

Theorem. Let $A_1, \ldots, A_n$ $(n > 1)$ be finite nonempty subsets of $\mathbb{Z}$. Then

$$|A_1 + \ldots + A_n| \geqslant |A_1| + \ldots + |A_n| - n + 1,$$

and equality holds if and only if $A_1, \ldots, A_n$ are arithmetic progressions with the same difference.

Corollary. Let A be a finite subsets of $\mathbb{Z}$ and let $n \in \{2, 3, \ldots\}$. Then

$$|nA| \geqslant n|A| - n + 1,$$

and equality holds if and only if A is an AP (arithmetic progression).

Freiman's Theorem

Freiman's Theorem (Freiman, 1966). Let A be a finite nonempty subset of $\mathbb{Z}$ with $|A+A| \leqslant c|A|$. Then A is contained in an n-dimensional AP

$$Q = Q(a; q_1, \ldots, q_n; l_1, \ldots, l_n) = \{a + x_1 q_1 + \cdots + x_n q_n : \ 0 \leqslant x_i < l_i\}$$

with $|Q| \leqslant c'|A|$, where c' and n only depend on c.

Remark. For a proof of Freiman's theorem, one may visit `http://maths.nju.edu.cn/~zwsun/Szemeredi.pdf`. This deep theorem plays a crucial role in the Fields medalist W. T. Gowers' quantitative proof [Geom. Func. Analysis Appl., 2001] of the famous Szemerédi theorem. Ben Green and I. Z. Ruzsa [J. London Math. Soc. 2007] extended Freiman's theorem to any abelian group.

Szemerédi's Theorem

The following deep result conjectured by P. Erdős and P. Turán in 1936, implies the classical van der Waerden theorem.

Szemerédi's Theorem (Acta Arith. 1975). Let $0 < \delta \leqslant 1$ and $k \in \{3, 4, \ldots\}$. If $n \in \mathbb{Z}^+$ is sufficiently large, then $A \subseteq \{1, \ldots, n\}$ with $|A| \geqslant \delta n$ contains an AP of length k.

In 1956 K. Roth proved this result for $k = 3$ by the circle method in analytic number theory. In 1969 E. Szemerédi handled the case $k = 4$ by a combinatorial method. The case of general k was settled by Szemerédi in 1975 in a paper which was regarded as "*a masterpiece of combinatorial reasoning*" by R. L. Graham. In 1977 H. Furstenberg used ergodic theory to give a new proof of Szemerédi's theorem. In 2001 W. T. Gowers employed Fourier analysis and combinatorics (including Frieman's theorem on sumsets) to reprove the theorem with explicit bounds.

Szemerédi's theorem plays an important role in the proof of the following result.

Green-Tao Theorem There are arbitrarily long APs of primes.

Dyson's g-transformation

F. Dyson simplified Mann's proof by introducing the so-called *Dyson g-transformation* which plays an important role in induction proofs of some additive results.

Let A and B be nonempty subsets of an abelian group G. For $g \in G$ we let

$$A(g) = A \cup (g + B) \supseteq A \text{ and } B(g) = (A - g) \cap B \subseteq B,$$

and call the pair $(A(g), B(g))$ the **Dyson g-transformation** of the pair (A, B).

We have $A(g) + B(g) \subseteq A + B$ since for $x \in g + B$ and $y \in B(g)$ clearly $x + y = (y + g) + (x - g) \in A + B$.

If A and B are finite, then $|A(g)| + |B(g)| = |A| + |B|$ since

$$|A(g)\backslash A| = |(g+B)\backslash A| = |g+(B\backslash(A-g))| = |B\backslash(A-g)| = |B\backslash B(g)|.$$

Cauchy-Davenport Theorem

Let p be a prime. Then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{a} = a + p\mathbb{Z} : a \in \mathbb{Z}\}$ is a field with p elements. If $A = \{\bar{1}, \ldots, \bar{k}\}$ and $B = \{\bar{1}, \ldots, \bar{l}\}$ with $|A| = k \leqslant p$ and $|B| = l \leqslant p$, then $A + B = \{\bar{2}, \ldots, \overline{k+l}\}$ and hence

$$|A + B| = \min\{p,\ k + l - 1\} = \min\{p,\ |A| + |B| - 1\}.$$

Cauchy-Davenport Theorem. Let p be any prime. If A and B are nonempty subsets of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, then

$$|A + B| \geqslant \min\{p,\ |A| + |B| - 1\}.$$

Remark. This theorem was first proved by Cauchy in 1813, and then rediscovered by Davenport in 1935.

By induction, the Cauchy-Davenport theorem can be extended to sumsets of n subsets of $\mathbb{F}_p$.

Theorem. Let p be a prime and let $A_1, \ldots, A_n$ be nonempty subsets of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Then

$$|A_+ \ldots + A_n| \geqslant \min\{p, |A_1| + \ldots + |A_n| - n + 1\}.$$

Proof of the Cauchy-Davenport theorem

Choose $b_0 \in B$ and set $B' = B - b_0$. Then $0 \in B'$, $|B'| = |B|$ and $|A + B| = |A + B'|$. So, without loss of generality, we may simply assume $0 \in B$. If $|A| + |B| > p$, then $A + B = \mathbb{F}_p$ and hence $|A + B| = p = \min\{p, |A| + |B| - 1\}$.

Below we show $|A| + |B| \leqslant p \Rightarrow |A + B| \geqslant |A| + |B| - 1$. Suppose that this is not true and choose nonempty $A, B \subseteq \mathbb{F}_p$ with $|B|$ minimal such that $|A| + |B| \leqslant p$ and $|A + B| < |A| + |B| - 1$. Clearly $|A|, |B| > 1$. As $|A + B| < p$ and $0 \in B$, we have $A \neq \mathbb{F}_p$. Choose $b \in B \setminus \{0\}$. If $A + b \subseteq A$, then $A + 2b \subseteq A + b \subseteq A$, ..., $A + (p - 1)b \subseteq A$. For any $a \in A$, $\{a + kb : \ 0 \leqslant k \leqslant p - 1\} \subseteq A$ which contradicts $A \neq \mathbb{F}_p$. So $A + b \not\subseteq A$.

Choose $g \in A$ with $g + b \notin A$ and consider the Dyson g-transformation $(A(g), B(g))$ of the pair (A, B). Note that

$$|A(g) + B(g)| \leqslant |A + B| < |A| + |B| - 1 = |A(g)| + |B(g)| - 1 < p,$$

Also, $0 \in B(g) = B \cap (A - g)$ and $|B(g)| < |B|$. This contradicts the choice of B.

Pollard's Theorem

Theorem (Pollard, 1974). Let p be a prime and let A and B be nonempty subsets of $\mathbb{F}_p$. For $t = 1, \ldots, \min\{|A|, |B|\}$ define

$$N_t = |\{g \in \mathbb{F}_p : \ |\{(a,b) : \ a \in A, \ b \in B, \ a+b = g\}| \geqslant t\}|.$$

Then

$$\frac{N_1 + \ldots + N_t}{t} \geqslant \min\{p, |A| + |B| - t\}$$

for all $t = 1, \ldots, \min\{|A|, |B|\}$.

This theorem in the case $t = 1$ gives the Cauchy-Davenport theorem.

Kneser's Theorem

In 1953 Kneser extended the Cauchy-Davenport theorem to general abelian groups.

Kneser's Theorem. Let G be an additive abelian group. Let A and B be finite nonempty subsets of G, and let $H = H(A+B)$ be the stablizer $\{g \in G : g + A + B = A + B\}$. If $|A+B| \leqslant |A| + |B| - 1$, then

$$|A+B| = |A+H| + |B+H| - |H|.$$

Corollary. Let G be an additive abelian group. Let $p(G)$ be the least order of a nonzero element of G, or $p(G) = +\infty$ if G is torsion-free. Then, for any finite nonempty subsets A and B of G, we have

$$|A+B| \geqslant \min\{p(G), |A| + |B| - 1\}.$$

Proof. Suppose that $|A+B| < |A| + |B| - 1$. Then $H = H(A+B) \neq \{0\}$ by Kneser's theorem. Therefore $|H| \geqslant p(G)$ and hence

$$|A+B| = |A+H| + |B+H| - |H| \geqslant |A+H| \geqslant |H| \geqslant p(G).$$

Part II. Finite Fields and Chevalley-Warning Theorem

Finite Fields

For a field F with identity e, if e, $2e = e + e$, $3e = e + e + e$, ... are all nonzero then we say that the *characteristic* of F is zero, if $ne = 0$ for some $n \in \mathbb{Z}^+$ then the least positive integer p with $pe = 0$ is called *characteristic* of F. The characteristic $\mathrm{ch}(F)$ of a field F is either zero or a prime. (Note that $(me)(ne) = (mn)e$.)

For any prime p, $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{a} = a + p\mathbb{Z}\}$ is a field of characteristic p.
Let p be a prime and let $n \in \mathbb{Z}^+$. It is known that there is a monic irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree n. Then

$$\mathbb{Z}_p[x]/(f(x)) = \{P(x) \bmod f(x) : \ P(x) \in \mathbb{Z}_p[x]\}$$

is a field with p^n elements.

A field F with $|F| = q \in \mathbb{Z}^+$ exists if and only if $q = p^n$ for some prime p and positive integer n. If $q > 1$ is a prime power, then any two fields of order q are isomorphic, and we write $\mathbb{F}_q$ to denote the (unique) field F of order q. $F^* = F \setminus \{0\}$ is a cyclic group of order $q - 1$.

Chevalley-Warning Theorem

Chevalley-Warning Theorem. Let F be any finite field of characteristic p. Let $f_i(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ for all $i = 1, \ldots, m$. Let $V = Z(f_1, \ldots, f_m)$ be the set of solutions to the system of equations

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0, \\ f_2(x_1, \ldots, x_n) = 0, \\ \ldots\ldots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \tag{$*$}$$

over F^n. If $\sum_{i=1}^{m} \deg(f_i) < n$, then $p \mid |V|$, and in particular $(*)$ cannot have a unique solution over F^n.

Proof

Write $|F| = q = p^a$ with $a \in \mathbb{Z}^+$. Then $F^* = F \setminus \{0\}$ is a cyclic group of order $q-1$. Let g be a primitive element of F (i.e., a generator of the cyclic group F^*). For any $k \in \mathbb{N}$ we have

$$g^k \sum_{x \in F} x^k = \sum_{x \in F} (gx)^k = \sum_{y \in F} y^k$$

and hence $(g^k - 1) \sum_{x \in F} x^k = 0$. If $q - 1 \nmid k$, then $g^k \neq 1$ and hence $\sum_{x \in F} x^k = 0$. Note also that $\sum_{x \in F} x^0 = q1 = 0$. So

$$\sum_{x \in F} x^k = 0 \quad \text{for all } k = 0, \ldots, q-2.$$

Continue the proof

For $x_1, \ldots, x_n \in F$, clearly

$$\prod_{i=1}^{m} \left(1 - f_i(x_1, \ldots, x_n)^{q-1}\right) = \begin{cases} 1 & \text{if } (x_1, \ldots, x_n) \in V, \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$|V|1 = \sum_{x_1,\ldots,x_n \in F} \prod_{i=1}^{m} \left(1 - f_i(x_1, \ldots, x_n)^{q-1}\right).$$

As $\sum_{i=1}^{m} \deg(f_i) < n$, we may write

$$\prod_{i=1}^{m} \left(1 - f_i(x_1, \ldots, x_n)^{q-1}\right) = \sum_{j_1+\ldots+j_n<n(q-1)} a_{j_1,\ldots,j_n} x_1^{j_1} \ldots x_n^{j_n}$$

with $a_{j_1,\ldots,j_n} \in F$. So

$$|V|1 = \sum_{j_1+\ldots+j_n<n(q-1)} a_{j_1,\ldots,j_n} \prod_{i=1}^{n} \sum_{x_i \in F} x_i^{j_i} = 0.$$

(since some $j_i < q-1$) and hence $|V| \equiv 0 \pmod{p}$.

Part III. Zero-sum Problems

Zero-sum sequences on an abelian group

Let G be an additive abelian group. For a sequence $(a_k)_{1 \leqslant k \leqslant n}$ of elements of G if $a_1 + \ldots + a_n = 0$ then the sequence is said to be a *zero-sum sequence*.

Let G be an additive abelian group of order n. Let $a_1, \ldots, a_n \in G$. Then

$$s_0 = 0,\ s_1 = a_1,\ s_2 = a_1 + a_2,\ \ldots, s_n = a_1 + \ldots + a_n$$

cannot be pairwise distinct as they all belong to the group G. So, for some $0 \leqslant i < j \leqslant n$ we have $a_{i+1} + \ldots + a_j = s_j - s_i = 0$.

EGZ Theorem

Erdős-Ginzburg-Ziv Theorem [Bull. Research Council Israel, 1961]. Let $a_1, \ldots, a_{2n-1} \in \mathbb{Z}$. Then $\sum_{i \in I} a_i \equiv 0 \pmod{n}$ for some $I \subseteq \{1, \ldots, 2n-1\}$ with $|I| = n$.

In the group-theoretic language, this can be restated as follows.

Another Version of the EGZ Theorem. Let $(a_k)_{1 \leqslant k \leqslant 2n-1}$ be a sequence of elements of the cyclic group $G = \mathbb{Z}/n\mathbb{Z}$. Then it has a zero-sum subsequence of length n

Note that we cannot replace $2n-1$ in the EGZ Theorem by $2n-2$. For example, if $a_1 = \ldots, a_{n-1} = 1$ and $a_n = \ldots, a_{2n-2} = 0$ then $\sum_{i \in I} a_i \not\equiv 0 \pmod{n}$ for all n-subsets of $\{1, \ldots, 2n-2\}$.

Reduction of the EGZ theorem to the case with n prime

Suppose that the EGZ theorem holds whenever n is prime. Now we use induction to show the EGZ theorem for any positive integer n.

The case $n = 1$ is trivial since $a_1 \in \mathbb{Z}$ is congruent to 0 mod 1.

Now let $n \in \{2, 3, \ldots\}$ and assume that the EGZ theorem holds for all smaller values of n. If n is prime, it is okay. Now let $n = dq$ with $1 < d \leqslant q < n$.

As $2n - 1 = 2dq - 1 \geqslant 2q - 1$, for some $I_1 \subseteq \{1, \ldots, 2n-1\}$ with $|I_1| = q$ such that $\sum_{i \in I_1} a_i \equiv 0 \pmod{2q-1}$. Since $2n - 1 - |I_1| = (2d-1)q - 1 \geqslant 2q - 1$, we can select $I_2 \subseteq \{1, \ldots, 2n-1\} \setminus I_1$ with $|I_2| = q$ such that $\sum_{i \in I_2} a_i \equiv 0 \pmod{q}$. Continue this process until we find pairwise disjoint q-subsets $I_1, \ldots, I_{2d-1}$ of $\{1, \ldots, 2n-1\}$ such that

$$\sum_{i \in I_j} a_i \equiv 0 \pmod{q} \quad \text{for all } j = 1, \ldots, 2d-1.$$

Note that $2n - 1 - (2d-1)q = q - 1 < 2q - 1$.

Reduction of the EGZ theorem to the prime case

For each $j = 1, \ldots, 2d-1$ write

$$\sum_{i \in I_j} a_i = q b_j \quad \text{with } b_j \in \mathbb{Z}.$$

By the induction hypothesis, for some d-subset J of $\{1, \ldots, 2d-1\}$ we have $\sum_{j \in J} b_j \equiv 0 \pmod{d}$. Let $I = \bigcup_{j \in J} I_j$. Then $|I| = \sum_{j \in J} |I_j| = dq = n$ and

$$\sum_{i \in I} a_i = \sum_{j \in J} \sum_{i \in I_j} a_i = \sum_{j \in J} q b_j = q \sum_{j \in J} b_j \equiv 0 \pmod{n}.$$

This concludes the induction step.

So, to finish the proof of the EGZ theorem, we only need to handle the prime case.

A Lemma

Lemma. Let p be a prime. If none of $a_1, \ldots, a_k \in \mathbb{Z}$ $(k < p)$ is divisible by p, then $|S_k| \geqslant k+1$, where

$$S_k = \left\{ \sum_{i \in I} a_i \bmod p : \ I \subseteq \{1, \ldots, k\} \right\}.$$

First Proof (by EGZ). As $p \nmid a_1$, we have $|S_1| = 2 = 1+1$. Now let $1 < k < p$ and assume that $|S_{k-1}| \geqslant k$. Clearly $S_{k-1} \subseteq S_k$. If $S_{k-1} \neq S_k$, then $|S_k| \geqslant |S_{k-1}| + 1 \geqslant k+1$.

Now suppose that $S_{k-1} = S_k$. Then $a_k \bmod p \in S_k = S_{k-1}$, $2a_k \bmod p \in S_k = S_{k-1}$, ..., $pa_k \bmod p \in S_k$. Hence $|S_k| \geqslant p \geqslant k+1$.

Second Proof. Let $\bar{a} = a + p\mathbb{Z}$ for $a \in \mathbb{Z}$. Then $A_i = \{\bar{0}, \overline{a_i}\} \subseteq \mathbb{Z}/p\mathbb{Z}$ and $|A_i| = 2$ for all $i = 1, \ldots, k$. By the Cauchy-Davenport theorem,

$$|A_1 + \ldots + A_k| \geqslant \min\{p, |A_1| + \ldots + |A_k| - k + 1\} = \min\{p, k+1\} = k+1.$$

Proof of the EGZ theorem in the prime case

Proof of the EGZ Theorem in the prime case. Let p be a prime, and let $a_1, \ldots, a_{2p-1}\mathbb{Z}$. We want to show that $\sum_{i\in I} a_i \equiv 0 \pmod{p}$ for some p-subset of $\{1, \ldots, 2p-1\}$. Without loss of generality, we suppose that $a_1' \leqslant \ldots \leqslant a_{2p-1}'$, where a_i' denotes the least nonnegative residue of a_i mod p.

If $a_i' = a_{i+p-1}'$ for some $i = 1 \ldots, p$, then $a_i' = \ldots = a_{i+p-1}'$ and hence $\sum_{j=0}^{p-1} a_{i+j} \equiv pa_i \equiv 0 \pmod{p}$.

Now suppose that $a_i' \neq a_{i+p-1}'$ for all $i = 1, \ldots, p$. By the Lemma,

$$S = \left\{ \sum_{i\in I} (a_{i+p-1} - a_i) \bmod p : \ I \subseteq \{1, \ldots, p-1\} \right\}$$

has cardinality at least $(p-1)+1 = p$. Thus S contains $\sum_{i=1}^{p} a_{i+p-1} \bmod p$ and hence for some $I \subseteq \{1, \ldots, p-1\}$ we have

$$\sum_{i\in I} a_i + \sum_{j\in\{1,\ldots,p\}\setminus I} a_{j+p-1} \equiv 0 \pmod{p}.$$

Another proof

Another Proof via the Chevalley-Warning Theorem.
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field of characteristic p. Define

$$f_1(x_1, \ldots, x_{2p-1}) = \sum_{k=1}^{2p-1} x_k^{p-1}, \ f_2(x_1, \ldots, x_{2p-1}) = \sum_{k=1}^{2p-1} a_k x_k^{p-1}.$$

They are polynomials over $\mathbb{F}_p$ with $\deg(f_1) + \deg(f_2) < 2p - 1$.
Clearly $f_i(0, \ldots, 0) = 0$ for $i = 1, 2$.

In view of the Chevalley-Warning Theorem, for some
$x_1, \ldots, x_{2p-1} \in F$ not all zero we have

$$f_1(x_1, \ldots, x_{2p-1}) = 0 \text{ and } f_2(x_1, \ldots, x_{2p-1}) = 0.$$

Thus $I = \{1 \leqslant i \leqslant 2p - 1 : \ x_i \neq 0\} \neq \emptyset$, $|I|1 = 0$ and
$\sum_{i \in I} a_i = 0$. Since $p \mid |I|$ and $0 < |I| < 2p$, we must have $|I| = p$.

Davenport's constant

Let G be a finite abelian group. The *Davenport constant* $D(G)$ is the least $k \in \mathbb{Z}^+$ such that any sequence $(a_1, \ldots, a_k)$ of elements of G has a nonempty zero-sum subsequence (i.e., $\sum_{i \in I} a_i = 0$ for some $\emptyset \neq I \subseteq \{1, \ldots, k\}$). It is clear that $D(G) \leqslant |G|$.

In 1966 Davenport showed that if K is an algebraic number field with ideal class group G, then $D(G)$ is the maximal number of prime ideals (counting multiplicity) in the decomposition of an irreducible algebraic integer in K.

Clearly, $D(\mathbb{Z}_n) = n$ for any positive integer n.

For each finite abelian group G with $|G| > 1$, there is a unique sequence $d_1, \ldots, d_r$ of positive integers with $d_1 > 1$ and $d_i \mid d_{i+1}$ for all $i = 1, \ldots, r-1$ such that $G \cong \mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_r}$; we call r the *rank* of G, d_r the *exponent* of G, and define

$$d^*(G) := \sum_{i=1}^{r} (d_i - 1).$$

Olson's theorem

For $G = \mathbb{Z}_{p^{a_1}} \oplus \ldots + \oplus \mathbb{Z}_{p^{a_r}}$ (where p is a prime and $a_1, \ldots, a_r \in \mathbb{Z}^+$), For the sequence consisting of $p^{a_1} - 1$ copies of $(1, 0, \ldots, 0) \in G$, p^{a_2-1} copies of $(0, 1, 0, \ldots, 0)$, ..., p^{a_r-1} copies of $(0, \ldots, 0, 1)$, it has no nonempty zero-sum subsequence. So $D(G) > d^*(G)$.

Olson's Theorem [J. Number Theory 1(1969)]. Let G be an abelian p-group with $|G| > 1$, where p is a prime. Then $D(G) = 1 + d^*(G)$. Moreover, for any $c, c_1, \ldots, c_{d^*(G)+1} \in G$ we have

$$\sum_{\substack{I \subseteq \{1,\ldots,d^*(G)+1\} \\ \sum_{s\in I} c_s = c}} (-1)^{|I|} \equiv 0 \pmod{p}.$$

Conjecture (Olson, 1969). For any $n, r \in \mathbb{Z}^+$ we have

$$D(\mathbb{Z}_n^r) = 1 + r(n-1).$$

Olson's theorem implies the EGZ theorem

Let q be a power of a prime p, and let $c, c_1, \ldots, c_{2q-1} \in \mathbb{Z}_q$. Then $(0, c), (1, c_1), \ldots, (1, c_{2q-1}) \in \mathbb{Z}_q \oplus \mathbb{Z}_q$. By Olson's theorem in the case $G = \mathbb{Z}_q^2 = \mathbb{Z}_q \oplus \mathbb{Z}_q$, we have

$$\sum_{\substack{I \subseteq [1,2q-1] \\ q \mid\mid I|,\ \sum_{s \in I} c_s = c}} (-1)^{|I|} \equiv 0 \pmod{p}.$$

In other words,

$$\left| \left\{ I \subseteq [1, 2q-1] : |I| = q \text{ and } \sum_{s \in I} c_s = c \right\} \right| \equiv [\![c = 0]\!] \pmod{p},$$

where for a predicate P we let $[\![P]\!]$ be 1 or 0 according as P holds or not. Thus, Olson's theorem implies the EGZ theorem.

Representative work of Wei-Dong Gao

In China, Prof. Wei-Dong Gao and his students study zero-sum problems.

Gao's Theorem [conjectured by Y. Caro] (Gao, J. Number Theory 1996). Let G be a finite additive abelian group. Let $E(G)$ be the smallest positive integer k such that for any $a_1, \ldots, a_k \in G$ the sequence $(a_1, \ldots, a_k)$ has a zero-sum subsequence of length $|G|$. Then $E(G) = D(G) + |G| - 1$.

Note that $D(\mathbb{Z}_n) = n$ and $E(\mathbb{Z}_n) = 2n - 1 = D(\mathbb{Z}_n) + |\mathbb{Z}_n| - 1$.

References:

1. W. D. Gao, *A combinatorial problem on finite abelian groups*, J. Number Theory **58**(1996), 100–103.

2. M. Devos, *Gao's theorem for nonabelian groups*, Open Problem Garden, `http://garden.irmacs.sfu.ca/?q=op/gaos_theorem_for_nonabelian_groups`

Conjecture: Gao's theorem holds for any finite group G.

A Polynomial Formula

Lemma (Z. W. Sun [Electron. Res. Announc. Amer. Math. Soc., 2003]). Let R be a ring with identity, and let $f(x_1, \ldots, x_k)$ be a polynomial over R. If $J \subseteq [1, k] = \{1, \ldots, k\}$ and $|J| \geqslant \deg f$, then

$$\sum_{I \subseteq J} (-1)^{|J|-|I|} f([\![1 \in I]\!], \ldots, [\![k \in I]\!])$$

coincides with $[\prod_{j \in J} x_j] f(x_1, \ldots, x_k)$, the coefficient of $\prod_{j \in J} x_j$ in $f(x_1, \ldots, x_k)$.

Proof. Write

$$f(x_1, \ldots, x_k) = \sum_{j_1, \ldots, j_k \geqslant 0} c_{j_1, \ldots, j_k} \prod_{s=1}^{k} x_s^{j_s},$$

and observe that if $\emptyset \neq J \subseteq [1, k]$ then

$$0 = \prod_{j \in J} (1 - 1) = \sum_{I \subseteq J} (-1)^{|I|}.$$

Continue the proof

Therefore

$$\begin{aligned}
&\sum_{I\subseteq J}(-1)^{|I|}f([\![1\in I],\ldots,[k\in I]\!])\\
=&\sum_{I\subseteq J}(-1)^{|I|}\sum_{\substack{j_1,\ldots,j_k\geqslant 0\\ \{s\colon j_s\neq 0\}\subseteq I}}c_{j_1,\ldots,j_k}\\
=&\sum_{\substack{j_1,\ldots,j_k\geqslant 0\\ \{s\colon j_s\neq 0\}\subseteq J}}\ \sum_{\{s\colon j_s\neq 0\}\subseteq I\subseteq J}(-1)^{|I|}c_{j_1,\ldots,j_k}\\
=&\sum_{\substack{j_1,\ldots,j_k\geqslant 0\\ \{s\colon j_s\neq 0\}\subseteq J}}\ \sum_{I'\subseteq J\setminus\{s\colon j_s\neq 0\}}(-1)^{|I'|}(-1)^{|\{s\colon j_s\neq 0\}|}c_{j_1,\ldots,j_k}\\
=&\sum_{\substack{j_1,\ldots,j_k\geqslant 0\\ \{s\colon j_s\neq 0\}=J}}(-1)^{|J|}c_{j_1,\ldots,j_k}=(-1)^{|J|}\left[\prod_{j\in J}x_j\right]f(x_1,\ldots,x_k),
\end{aligned}$$

where in the last step we note that if $\{s\colon j_s\neq 0\}=J$ and $j_s>1$ for some s then $j_1+\ldots+j_k>|J|\geqslant\deg f$ and hence $c_{j_1,\ldots,j_k}=0$.

A Useful Technique

Let m be an integer and let p be a prime. Fermat's little theorem tells that we can characterize whether p divides m as follows:

$$[\![p \mid m]\!] \equiv 1 - m^{p-1} \pmod{p}.$$

To handle general abelian p-groups in a similar way, we need to characterize whether a given power of p divides a. Thus, the following lemma is of technical importance. It first appeared in Sun's preprint `arXiv:math/NT/0305369` dated May 24, 2003.

Lemma [Z. W. Sun, Israel J. Math., 2009] Let p be a prime, and let $a \in \mathbb{N}$ and $m \in \mathbb{Z}$. Then we have the following congruence

$$\binom{m-1}{p^a-1} \equiv [\![p^a \mid m]\!] \pmod{p}.$$

Sun's Proof of the Olson Theorem without Group Rings

Olson's Theorem [J. Number Theory 1969]. Let G be an abelian p-group isomorphic to $\mathbb{Z}_{p^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{a_r}}$ where $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Given $c, c_1, \ldots, c_k \in G$ with $k \geqslant 1 + \sum_{t=1}^{r}(p^{a_t} - 1)$, we have

$$\sum_{\substack{I \subseteq [1,k] \\ \sum_{s \in I} c_s = c}} (-1)^{|I|} \equiv 0 \pmod{p}.$$

In particular, when $c = 0$ it follows that there is a nonempty $I \subseteq [1, k]$ with $\sum_{s \in I} c_s = 0$.

Remark. Olson's theorem determined the Davenport constant for any abelian p-group. Olson used the group ring method in his proof of this classical theorem.

Now we prove Olson's theorem without any use of the group ring method. Identify c with a vector $\langle c^{(1)} \bmod p^{a_1}, \ldots, c^{(r)} \bmod p^{a_r} \rangle$, and write c_s in the form $\langle c_s^{(1)} \bmod p^{a_1}, \ldots, c_s^{(r)} \bmod p^{a_r} \rangle$.

Sun's Proof of the Olson Theorem without Group Rings

Define

$$f(x_1,\dots,x_k)=\prod_{t=1}^{r}\binom{\sum_{s=1}^{k}c_s^{(t)}x_s-c^{(t)}-1}{p^{a_t}-1}.$$

Clearly $\deg f\leqslant\sum_{t=1}^{r}(p^{a_t}-1)<k=|[1,k]|$. Applying the polynomial formula with $J=[1,k]$ we get

$$\sum_{I\subseteq[1,k]}(-1)^{k-|I|}f([\![1\in I]\!],\dots,[\![k\in I]\!])=[x_1\cdots x_k]f(x_1,\dots,x_k)=0,$$

$$\sum_{I\subseteq[1,k]}(-1)^{k-|I|}\prod_{t=1}^{r}\binom{\sum_{s\in I}c_s^{(t)}-c^{(t)}-1}{p^{a_t}-1}=0.$$

$$\sum_{\substack{I\subseteq[1,k]\\ p^{a_t}\mid\sum_{s\in I}c_s^{(t)}-c^{(t)}}}(-1)^{|I|}\equiv 0\pmod p,\ \text{i.e.,}\ \sum_{\substack{I\subseteq[1,k]\\ \sum_{s\in I}c_s=c}}(-1)^{|I|}\equiv 0\pmod p.$$

Kemnitz's Conjecture

For a finite abelian group G, define $s(G)$ to be the least positive integer k such that any sequence $(a_1, \ldots, a_k)$ of elements of G has a zero-sum subsequence of length $\exp(G)$, where the exponent $\exp(G)$ of G is the least $n \in \mathbb{Z}^+$ with $nx = 0$ for all $x \in G$.

By the EGZ theorem, $s(\mathbb{Z}_n) = 2n - 1$ for any positive integer n.

What is the smallest integer $l = s(\mathbb{Z}_n^2)$ such that every sequence of l elements in $\mathbb{Z}_n^2 = \mathbb{Z}_n \oplus \mathbb{Z}_n$ contains a zero-sum subsequence of length n?

In 1983 Kemnitz [Ars Combin.] conjectured that $s(\mathbb{Z}_n^2) = 4n - 3$, and the conjecture can be reduced to the case with n prime.

In 1993 Alon and Dubiner showed that $s(\mathbb{Z}_n^2) \leqslant 6n - 5$. In 2000 Rónyai [Combinatorica] was able to prove that $s(\mathbb{Z}_p^2) \leqslant 4p - 2$ for every prime p; in 2001 W. D. Gao [J. Combin. Theory Ser. A] used Olson's group ring approach to deduce that $s(\mathbb{Z}_q^2) \leqslant 4q - 2$ for any prime power q.

These results were obtained by various algebraic methods.

Alon-Dubier Lemma

The following lemma plays an indispensable role in the study of the Kemnitz conjecture.

Alon-Dubiner Lemma. Let q be a prime power, and let $c_1, \ldots, c_{3q}$ be elements of $\mathbb{Z}_q^2$ with $c_1 + \ldots + c_{3q} = 0$. Then there is an $I \subseteq [1, 3q]$ with $|I| = q$ such that $\sum_{i \in I} c_i = 0$.

Proof. As $3q - 1 \geqslant 1 + (q-1) + (q-1) + (q-1)$, by Olson's theorem there is a nonempty $I \subseteq \{1, \ldots, 3q-1\}$ such that $\sum_{s \in I} c_s = 0$ in $\mathbb{Z}_q^2$ and also $\sum_{s \in I} 1 = 0$ in $\mathbb{Z}_q$. So $q \mid |I|$ and hence $|I| \in \{q, 2q\}$. If $|I| = 2q$, then $\overline{I} = \{1, \ldots, 3q\} \setminus I$ has cardinality q and

$$\sum_{t \in \overline{I}} c_t = \sum_{i=1}^{3q} c_i - \sum_{s \in I} c_s = 0.$$

A Consequence of the Polynomial Formula

In March 2003 Sun deduced the following result from his polynomial formula.

Theorem [Z. W. Sun, Electron. Res. Announc. Amer. Math. Soc. 9(2003)]. Let p be a prime and let $h > 0$ be an integer. Let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \ldots, 4p^h - 2$.

(i) Set $\mathcal{I} = \{I \subseteq [1, 4p^h - 2]\colon \sum_{i\in I} a_i \equiv \sum_{i\in I} b_i \equiv 0 \pmod{p^h}\}$. Then

$$|\{I \in \mathcal{I}\colon |I| = p^h\}| \equiv |\{I \in \mathcal{I}\colon |I| = 3p^h\}| + 2 \pmod{p}.$$

(ii) Suppose that

$$\sum_{\substack{I,J\subseteq[1,4p^h-3]\\ |I|=|J|=p^h-1,\ I\cap J=\emptyset}} \left(\prod_{i\in I} a_i\right)\left(\prod_{j\in J} b_j\right) \not\equiv 2 \pmod{p}.$$

Then there exists an $I \subseteq [1, 4p^h - 3]$ with $|I| = p^h$ such that $\sum_{i\in I} a_i \equiv \sum_{i\in I} b_i \equiv 0 \pmod{p^h}$.

Reiher's work

In his paper "*On Kemnitz's conjecture concerning lattice points in the plane*" written in Nov. 2003, C. Reiher, completely proved the Kemnitz conjecture which had been open for 20 years! This work represents one of the most important achievements in the theory of zero-sums.

Reiher's paper has 4 pages. Pages 1–3 are devoted to 5 sophisticated corollaries to the Chevalley-Warning theorem which are needed later. Actually this can be significantly simplified by using part (i) of our theorem with $a_{4p-2} = b_{4p-2} = 0$.

A Consequence of the Theorem. Let p be a prime and let $h > 0$ be an integer. Let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \ldots, 4p^h - 3$. Set $\mathcal{I} = \{I \subseteq [1, 4p^h - 3]\colon \sum_{i\in I} a_i \equiv \sum_{i\in I} b_i \equiv 0 \pmod{p^h}\}$. Then

$$\begin{aligned} &|\{I \in \mathcal{I}\colon |I| = p^h\}| + |\{I \in \mathcal{I}\colon |I| = p^h - 1\}| \\ \equiv &|\{I \in \mathcal{I}\colon |I| = 3p^h\}| + |\{I \in \mathcal{I}\colon |I| = 3p^h - 1\}| + 2 \pmod{p}. \end{aligned}$$

Reiher's Lemma

On the last page of his paper, C. Reiher provided a key lemma which is obtained by a combinatorial method rather than an algebraic method.

Reiher's Lemma. Let p be a prime and let $a_i, b_i \in \mathbb{Z}$ for $i = 1, \ldots, 4p-3$. Set

$$\mathcal{I} = \left\{ I \subseteq [1, 4p-3] \colon \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p} \right\}.$$

Then, either $\{I \in \mathcal{I} \colon |I| = p\} \neq \emptyset$ or

$$|\{I \in \mathcal{I} \colon |I| = p-1\}| \equiv |\{I \in \mathcal{I} \colon |I| = 3p-1\}| \pmod{p}.$$

Notation. For $J \subseteq [1, 4p-3]$ and $n = 1, 2, \ldots$ let

$$(n, J) := \left| \left\{ I \subseteq J \colon |I| = n \ \& \ \sum_{i \in I} a_i \equiv \sum_{i \in I} b_i \equiv 0 \pmod{p} \right\} \right|.$$

An Observation

Observation. We have

$$|J| \in \{3p-1, 3p-2\} \Rightarrow (2p, J) \equiv (p, J) - 1 \pmod{p}.$$

In fact, by the polynomial formula we mentioned before,

$$\sum_{I \subseteq J} (-1)^{|J|-|I|}(1-|I|^{p-1})\left(1-\left(\sum_{i\in I} a_i\right)^{p-1}\right)\left(1-\left(\sum_{i\in I} b_i\right)^{p-1}\right)$$

coincides with the coefficient of $\prod_{j\in J} x_j$ in the polynomial

$$\left(1-\left(\sum_{j\in J} x_j\right)^{p-1}\right)\left(1-\left(\sum_{j\in J} a_j x_j\right)^{p-1}\right)\left(1-\left(\sum_{j\in J} b_j x_j\right)^{p-1}\right),$$

which is zero since $|J| > 3p-3$. Thus

$$\sum_{\substack{I\subseteq J,\ |I|\in\{0,p,2p\} \\ \sum_{i\in I} a_i \equiv \sum_{i\in I} b_i \equiv 0 \pmod{p}}} (-1)^{|I|} \equiv 0 \pmod{p},$$

that is, $(0, J) - (p, J) + (2p, J) \equiv 0 \pmod{p}$.

Sketch of the proof

Sketch of the Proof. Assume that $\{I \in \mathcal{I}\colon |I| = p\} = \emptyset$, i.e., $(p, J) = 0$ for any $J \subseteq [1, 4p-3]$. Let N denote the number of partitions $[1, 4p-3] = I_1 \cup I_2 \cup I_3$ satisfying

$$|I_1| = p-1, \quad |I_2| = p-2, \quad |I_3| = 2p$$

and furthermore

$$\sum_{i \in I_1} a_i \equiv \sum_{i \in I_1} b_i \equiv 0 \pmod{p}, \quad \sum_{i \in I_3} a_i \equiv \sum_{i \in I_3} b_i \equiv 0 \pmod{p}$$

(and hence $\sum_{i \in [1,4p-3] \setminus I_2} a_i \equiv \sum_{i \in [1,4p-3] \setminus I_2} b_i \equiv 0 \pmod{p}$).

We count N in two ways.

Continue the proof

Observe that

$$N = \sum_{I_1} (2p, [1, 4p-3] \setminus I_1) \equiv \sum_{I_1} (-1) = -(p-1, [1, 4p-3]) \pmod{p}.$$

On the other hand,

$$\begin{aligned} N &= \sum_{I_2} (2p, [1, 4p-3] \setminus I_2) \\ &\equiv \sum_{[1,4p-3] \setminus I_2} (-1) = -(3p-1, [1, 4p-3]) \pmod{p}. \end{aligned}$$

So we have the congruence
$(p-1, [1, 4p-3]) \equiv (3p-1, [1, 4p-3]) \pmod{p}$.

Remark. The prime power version of Reiher's Lemma also holds.

Conclusion

Combining Reiher's Lemma, the Alon-Dubiner lemma and the above-mentioned consequence of the Theorem, we immediately obtain the following result of Reiher [Ramanujan J. 2007].

Kemnitz-Reiher Theorem. The Kemnitz conjecture is true, that is, any sequence of elements in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ with length at least $4n-3$ contains a zero-sum sequence of length n.

What does Reiher's solution teach us? When we apply a powerful algebraic method in combinatorics, we should also realize its disadvantage and should not forget combinatorial methods. **A combination of algebraic methods and combinatorial methods might be more powerful!**

By the way, Sun [Israel J. Math. 2009] established connections of the EGZ theorem, Olson's theorem and the Alon-Dubiner lemma to covering systems of $\mathbb{Z}$ by residue classes. But it seems that the Kemnitz-Reiher theorem cannot be connected with covers of $\mathbb{Z}$.

Open Problem

How to determine $s(\mathbb{Z}_n^d)$ for any $d, n \in \mathbb{Z}^+$?

In particular,

how to prove the conjecture that $s(\mathbb{Z}_p^3) = 9p - 8$ for any prime $p > 3$?

Thank you!