An on-line talk (June 19, 2020)

Introduction to Combinatorial Number Theory (V)

– Combinatorial Nullstellensatz and its Applications

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://maths.nju.edu.cn/∼zwsun

June 19, 2020

Abstract

In this talk we introduce Alon's Combinatorial Nullstellensatz (i.e., the so-called polynomial method), and its applications to Snevily's conjectures and restricted sumsets.

Part I. Combinatorial Nullstellensatz and its Backgrounds

Cramer's conjecture

Let $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. Any cyclic group of order n is isomorphic to the additive group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ of residue classes modulo n. If n is odd, then

$$1 + 1,\ 2 + 2,\ \ldots,\ n + n$$

are pairwise incongruent modulo n and hence they form a complete system of residues modulo n.
Let $a_1, \ldots, a_n \in \mathbb{Z}$. If $a_1 + 1, \ldots, a_n + n$ form a complete system of residues modulo n, then

$$\sum_{i=1}^{n} (a_i + i) \equiv 1 + \cdots + n \pmod{n}$$

and hence $\sum_{i=1}^{n} a_i \equiv 0 \pmod{n}$.

Cramer's Conjecture. Let $a_1, \ldots, a_n \in \mathbb{Z}$ with $n \mid \sum_{i=1}^{n} a_i$. Then there is a permutation $\sigma \in S_n$ such that $a_{\sigma(1)} + 1, \ldots, a_{\sigma(n)} + n$ form a complete system of residues mod n.

M. Hall's Theorem

In 1952 M. Hall [Proc. Amer. Math. Soc.] obtained an extension of Cramer's conjecture.

M. Hall's Theorem. Let $G = \{b_1, \ldots, b_n\}$ be an additive abelian group of order n, and let $a_1, \ldots, a_n$ be elements of G with $a_1 + \ldots + a_n = 0$. Then there exists a permutation $\sigma \in S_n$ such that

$$\{a_{\sigma(1)} + b_1, \ldots, a_{\sigma(n)} + b_n\} = G.$$

Remark. Hall used induction argument and his method is very technique. Up to now there are no other proofs of this theorem.

Observation. If $a_1, \ldots, a_n \in \mathbb{Z}$ are incongruent modulo n with $a_1 + \cdots + a_n \equiv 0 \pmod{n}$, then n divides

$$0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}$$

and hence n is *odd*.

A conjecture of Snevily

Snevily's Conjecture for Abelian Groups [Amer. Math. Monthly, 1999]. Let G be an additive abelian group of *odd* order. Then for any two subsets $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ of G with $|A| = |B| = k$, there is a permutation $\sigma \in S_k$ such that $a_{\sigma(1)} + b_1, \ldots, a_{\sigma(k)} + b_k$ are (pairwise) distinct.

Remark. The result does not hold for any group G of *even* order. In fact, there is an element $g \in G$ of order 2, and $A = B = \{0, g\}$ gives a counterexample.

Difficulty. No direct construction. Induction also does not work!

Snevily's conjecture looks **simple, beautiful and difficult!**

Latin transversal

Let M be an $n \times n$ matrix. A *line* of M is a row or a column of M. M is called a *Latin square* over a set S of cardinality n if all its entries come from the set S and no line of which contains an element more than once. A *transversal* of the matrix M is a collection of n cells no two of which lie in the same line. A *Latin transversal* of M is a transversal whose cells contain no repeated element.

If $G = \{a_1, \ldots, a_n\}$ is an additive group of order n, then the matrix $M = (a_i + a_j)_{1 \leqslant i,j \leqslant n}$ formed by the Cayley addition table is a Latin square over G.

Another Form of Snevily's Conjecture. Let $G = \{a_1, \ldots, a_N\}$ be an additive abelian group with $|G| = N$ odd, and let M be the Latin square $(a_i + a_j)_{1 \leqslant i,j \leqslant N}$ formed by the Cayley addition table. Then any $n \times n$ submatrix of M contains a Latin transversal.

Another Conjecture of Snevily

Snevily's Conjecture on Addition modulo n [Amer. Math. Monthly, 1999]. Let $0 < k < n$ and $a_1, \ldots, a_k \in \mathbb{Z}$. Then there exists $\pi \in S_k$ such that $a_1 + \pi(1), \ldots, a_k + \pi(k)$ are distinct modulo n.

Remark. A. E. Kézdy and H. S. Snevily [Combin. Probab. Comput. 2002] proved the conjecture for $k \leqslant (n+1)/2$ and found an application to tree embeddings.

Jäger-Alon-Tarsi Conjecture

In 1982, motivated by his study of graph theory, F. Jäger posed the following conjecture in the case $|F| = 5$.

Jäger-Alon-Tarsi Conjecture. Let F be a finite field with at least 4 elements, and let A be an invertible $n \times n$ matrix with entries in F. There there exists a vector $\vec{x} \in F^n$ such that both $\vec{x}$ and $A\vec{x}$ have no zero component.

In 1989 N. Alon and M. Tarsi [Combinarorica, 9(1989)] confirmed the conjecture in the case when $|F|$ is **not a prime**. Moreover their method resulted in the initial form of the Combinatorial Nullstellensatz which was refined by Alon in 1999.

Sumsets with distinct summands

For subsets $A_1, \ldots, A_n$ of an additive group G, we define

$$A_1 \dot{+} \cdots \dot{+} A_n = \{a_1 + \cdots + a_n : \ a_i \in A_i, \text{ and } a_i \neq a_j \text{ if } i \neq j\}.$$

When $A_1 = \cdots = A_n = A$, we denote $A_1 \dot{+} \cdots \dot{+} A_n$ by $n^{\wedge}A$. Note that

$$nA = (n-1)A + A, \quad \text{but} \quad n^{\wedge}A \neq (n-1)^{\wedge}A \dot{+} A.$$

For $A = [0, k-1] = \{0, 1, \ldots, k-1\}$ and $0 < n \leqslant k$, clearly

$$\begin{aligned} |n^{\wedge}A| =& |[0 + 1 + \cdots + (n-1), (k-1) + (k-2) + \cdots + (k-n)]| \\ =& kn - n^2 + 1 = n(|A| - n) + 1. \end{aligned}$$

Let A be any finite subset $\mathbb{Z}$. By construction, one can show

$$|n^{\wedge}A| \geq n|A| - n^2 + 1.$$

M.B. Nathanson [Trans. AMS 347(1995)] proved that if $2 \leqslant n < |A| - 2$ and $|n^{\wedge}A| = n|A| - n^2 + 1$ then A must be an AP.

Erdős-Heilbronn Conjecture

Erdős-Heilbronn Conjecture (1964). Let p be a prime and let $A \subseteq \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Then

$$|2^{\wedge}A| \geqslant \min\{p,\ 2|A| - 3\}.$$

Difficulty. Unlike $\mathbb{Z}$, the field $\mathbb{Z}_p$ has no suitable ordering. Direct construction does not work! Also, Dyson's g-transformation does not work for sumsets with distinct summands.

Erdős-Heilbronn Conjecture

Erdős-Heilbronn Conjecture (1964). Let p be a prime and let $A \subseteq \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Then

$$|2^{\wedge}A| \geqslant \min\{p,\ 2|A| - 3\}.$$

Difficulty. Unlike $\mathbb{Z}$, the field $\mathbb{Z}_p$ has no suitable ordering. Direct construction does not work! Also, Dyson's g-transformation does not work for sumsets with distinct summands.

Dias da Silva-Hamidoune Theorem [Bull. London Math. Soc., 1994]. Let F be any field and let $p(F)$ be the additive order of the multiplicative identity of F. For any finite $A \subseteq F$, we have

$$|n^{\wedge}A| \geqslant \min\{p(F),\ n(|A| - n) + 1\}.$$

Method: Exterior algebras and the representation theory of symmetric groups!

In 1995-1996 N. Alon, M. B. Nathanson and I. Z. Ruzsa were able to prove this via the so-called *polynomial method* related to Combinatorial Nullstellensatz.

Usual form of Alon's Combinatorial Nullstellensatz

Usual Form of the Combinatorial Nullstellensatz (CN) [Alon, Combin. Probab. Comput. 8(1999)]. Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F and let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. Suppose that $0 \leqslant k_i < |A_i|$ for $i = 1, \ldots, n$, $k_1 + \cdots + k_n = \deg f$ and

$$[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \ldots, x_n) \text{ (the coefficient of } x_1^{k_1} \cdots x_n^{k_n} \text{ in } f)$$

does not vanish. Then there are $a_1 \in A_1, \ldots, a_n \in A_n$ such that $f(a_1, \ldots, a_n) \neq 0$.

Advantage: This advanced algebraic tool enables us to establish existence via computation. It has many applications.

Strong form of the Combinatorial Nullstellensatz

Strong Form of the Combinatorial Nullstellensatz [Alon, Combin. Probab. Comput. 8(1999)]. Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F and let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. Set $g_i(x) = \prod_{a \in A_i}(x - a)$ for $i = 1, \ldots, n$. Then

$$f(a_1, \ldots, a_n) = 0 \text{ for all } a_1 \in A_1, \ldots, a_n \in A_n$$

if and only if there are

$$h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$$

with $\deg h_i \leqslant \deg f - \deg g_i$ for $i = 1, \ldots, n$, such that

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

Remark: Let I be the ideal of $F[x_1, \ldots, x_n]$ generated by $g_1(x_1), \ldots, g_n(x_n)$. Then the strong form of CN tells us that $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ vanishes on $Z(I) = A_1 \times \cdots \times A_n$ if and only if $f \in I$, where

$$Z(I) = \{(x_1, \ldots, x_n) \in F^n : \ P(x_1, \ldots, x_n) = 0 \text{ for all } P \in I\}.$$

Strong Form implies the Usual Form

Suppose that f vanishes on $A_1 \times \cdots \times A_n$. Then, by the Strong Form, we can write

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i) h_i(x_1, \ldots, x_n)$$

with $h_i(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ and $\deg h_i \leqslant \deg f - \deg g_i$. Since $k_1 + \cdots + k_n = \deg f$ and $k_i < |A_i|$ for $i = 1, \ldots, n$, we have

$$[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \ldots, x_n) = \sum_{i=1}^{n} [x_1^{k_1} \cdots x_n^{k_n}] x_i^{|A_i|} h_i(x_1, \ldots, x_n) = 0,$$

which contradicts the condition that the coefficient is nonzero.

A Lemma

Lemma [Alon, Nathanson and Ruzsa, Amer. Math. Monthly 1995; J. Number Theory 1996] Let F be a field and $A_1, \ldots, A_n$ its subsets which are finite and nonempty. Let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ have degree less than $k_i = |A_i|$ in x_i for each $i = 1, \ldots, n$. If $f(a_1, \ldots, a_n) = 0$ for all $a_1 \in A_1, \ldots, a_n \in A_n$, then $f(x_1, \ldots, x_n)$ is identically zero.

Proof. The case $n = 1$ is easy since a nonzero polynomial $P(x) \in F[x]$ of degree less than a positive integer k can't have k distinct zeroes in F.

Let $n > 1$ and assume that the Lemma holds with n replaced by $n - 1$. Write $f(x_1, \ldots, x_n) = \sum_{i=0}^{k_n - 1} f_i(x_1, \ldots, x_{n-1}) x_n^i$. For any $a_1 \in A_1, \ldots, a_{n-1} \in A_{n-1}$, as $f(a_1, \ldots, a_{n-1}, x_n) = 0$ for all $x_n \in A_n$ we have $f_i(a_1, \ldots, a_{n-1}) = 0$ for all $i = 0, \ldots, k_n - 1$. By the induction hypothesis, all the $f_i(x_1, \ldots, x_{n-1})$ are the zero polynomial. So $f(x_1, \ldots, x_n)$ is also identically zero.

Proof of the Strong Form

If there are $h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ such that

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i) h_i(x_1, \ldots, x_n),$$

then for any $a_1 \in A_1, \ldots, a_n \in A_n$ we have

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{n} g_i(a_i) h_i(a_1, \ldots, a_n) = 0.$$

Now we consider the converse. Write

$$f(x_1, \ldots, x_n) = \sum_{j_1, \ldots, j_n \geqslant 0} f_{j_1, \ldots, j_n} x_1^{j_1} \ldots x_n^{j_n}$$

and

$$x^j = g_i(x) q_{ij}(x) + r_i^{(j)}(x),$$

where $q_{ij}(x), r_i^{(j)}(x) \in F[x]$ and $\deg r_i^{(j)}(x) < \deg g_i(x) = |A_i|$. Note that both $r_i^{(j)}(x)$ and $g_i(x) q_{ij}(x) = x^j - r_i^{(j)}(x)$ have degree not exceeding j.

Continue the Proof

Clearly

$$f(x_1,\ldots,x_n)=\sum_{\substack{j_1,\ldots,j_n\geqslant 0\\ j_1+\cdots+j_n\leqslant \deg f}} f_{j_1,\ldots,j_n}\prod_{i=1}^{n}\left(g_i(x_i)q_{ij_i}(x_i)+r_i^{(j_i)}(x_i)\right)$$

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

where

$$\bar{f}(x_1,\ldots,x_n)=\sum_{j_1,\ldots,j_n\geqslant 0} f_{j_1,\ldots,j_n}\prod_{i=1}^{n} r_i^{(j_i)}(x_i)$$

and each $h_i(x_1,\ldots,x_n)$ is a suitable polynomial over F with $\deg g_i+\deg h_i\leqslant \deg f$. If $a_1\in A_1,\ldots,a_n\in A_n$, then

$$\bar{f}(a_1,\ldots,a_n)=\sum_{j_1,\ldots,j_n\geqslant 0} f_{j_1,\ldots,j_n}\prod_{i=1}^{n} a_i^{j_i}=f(a_1,\ldots,a_n)=0.$$

As the degree of $\bar{f}(x_1,\ldots,x_n)$ with respect to x_i is smaller than $|A_i|$, by the Lemma the polynomial $\bar{f}(x_1,\ldots,x_n)$ is identically zero.

Part II. Applications of Combinatorial Nullstellensatz to Snevily's Conjectures

For $\sigma \in S_k$ let $\mathrm{sign}(\sigma)$ be the sign of σ which takes 1 or -1 according as the permutation σ is even or odd.
For a matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant k}$ over a field, its determinant and permanent are given by

$$\det A = \sum_{\sigma \in S_k} \mathrm{sign}(\sigma) \prod_{i=1}^{k} a_{i,\sigma(i)} \text{ and } \mathrm{per} A = \sum_{\sigma \in S_k} \prod_{i=1}^{k} a_{i,\sigma(i)}.$$

Observe that

$$\begin{aligned}
&[x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)^2 \\
=&[x_1^{k-1} \cdots x_k^{k-1}] (\det(x_j^{i-1})_{1 \leqslant i,j \leqslant k})^2 \\
=&[x_1^{k-1} \cdots x_k^{k-1}] \sum_{\sigma \in S_k} \mathrm{sign}(\sigma) \prod_{j=1}^{k} x_j^{\sigma(j)-1} \sum_{\tau \in S_k} \mathrm{sign}(\tau) \prod_{j=1}^{k} x_j^{\tau(j)-1} \\
=&\sum_{\sigma \in S_k} \mathrm{sign}(\sigma)\mathrm{sign}(\sigma') = \sum_{\sigma \in S_k} (-1)^{\binom{k}{2}} = k!(-1)^{\binom{k}{2}}
\end{aligned}$$

where $\sigma'(j) = k - \sigma(j) + 1$ for $j = 1, \ldots, k$. (For $1 \leqslant i < j \leqslant k$, we clearly have $\sigma(i) > \sigma(j) \iff \sigma'(i) < \sigma'(j)$.)

Attack Snevily's conjecture on addition modulo n

A. E. Kézdy and H. S. Snevily [Combin. Probab. Comput. 2002] Let k and n be positive integers with $k \leqslant (n+1)/2$. Then, for any $a_1, \ldots, a_k \in \mathbb{Z}$, there exists $\pi \in S_k$ such that $a_1 + \pi(1), \ldots, a_k + \pi(k)$ are distinct modulo n.

Proof. For $x_i, x_j \in A = \{1, \ldots, k\}$, we have $|x_i - x_j| \leqslant k - 1 \leqslant \frac{n-1}{2} < \frac{n}{2}$, and

$$x_i + a_i \not\equiv x_j + a_j \pmod{n} \Leftrightarrow x_j - x_i \not\equiv a_i - a_j \pmod{n} \Leftrightarrow x_j - x_i \neq r_{ij}$$

where r_{ij} denotes the residue of $a_i - a_j$ in the interval $(-n/2, n/2]$. Thus, we only need to show that there are distinct $x_1, \ldots, x_k \in A = \{1, \ldots, k\}$ such that $x_j - x_i \neq r_{ij}$ for all $1 \leqslant i < j \leqslant k$. By the Combinatorial Nullstellensatz for the real field $\mathbb{R}$, it suffices to note that

$$[x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)(x_j - x_i - r_{ij})$$

$$= [x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)^2 = k!(-1)^{\binom{k}{2}} \neq 0.$$

Alon's contribution for cyclic groups of prime orders

Alon's Result [Israel J. Math. 2000]. Let p be an odd prime and let $A = \{a_1, \ldots, a_k\}$ be a subset of $\mathbb{Z}_p$ with cardinality $k < p$. Given **(not necessarily distinct)** $b_1, \ldots, b_k \in \mathbb{Z}_p$ there is a permutation $\sigma \in S_k$ such that $a_{\sigma(1)} + b_1, \ldots, a_{\sigma(k)} + b_k$ are (pairwise) distinct.

Remark. This result is slightly stronger than Snevily's conjecture for cyclic groups of prime order.

Proof. Let $A_1 = \cdots = A_k = \{a_1, \ldots, a_k\}$. We need to show that there exist $x_1 \in A_1, \ldots, x_k \in A_k$ such that $\prod_{1 \leqslant i < j \leqslant k}(x_j - x_i)(x_j + b_j - (x_i + b_i)) \neq 0$. By the Combinatorial Nullstellensatz for the filed $\mathbb{Z}_p$, it suffices to note that

$$[x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)(x_j + b_j - (x_i + b_i))$$

$$= [x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)^2 = k!(-1)^{\binom{k}{2}} \neq 0 \text{ (in } \mathbb{Z}_p).$$

An extension of Alon's result by Hou and Sun

Theorem. (Qing-Hu Hou and Z.-W. Sun [Acta Arith. 102(2002)]) Let $k \geqslant n \geqslant 1$ be integers, and left F be a field whose characteristic is zero or greater than $\max\{n, (k-n)n\}$. Let $A_1, \ldots, A_n$ be subsets of F with cardinality k, and let $b_1, \ldots, b_n \in F$. Then the sumset

$$\{a_1 + \ldots + a_n : \ a_i \in A_i, \ a_i \neq a_j \text{ and } a_i + b_i \neq a_j + b_j \text{ if } i \neq j\}$$

have more than $(k-n)n$ elements.

Actually, Hou and Sun proved a much more general result including the above theorem as a special case.

Snevily's Conjecture for cyclic groups

For odd composite number n, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ is not a field. How to prove Snevily's conjecture for the cyclic group $\mathbb{Z}_n$?

Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math., 2001]: Snevily's conjecture holds for any cyclic group of odd order.

Their key observation is that **a cyclic group of odd order n can be viewed as a subgroup of the multiplicative group of the finite field $\mathbb{F}_{2^{\varphi(n)}}$.** (Note that n divides $2^{\varphi(n)} - 1$ by Euler's theorem.) Thus, it suffices to show that

$$c := [x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)(b_j x_j - b_i x_i) \neq 0.$$

Now c depends on $b_1, \ldots, b_k$ so that the condition $\prod_{1 \leqslant i < j \leqslant k}(b_j - b_i) \neq 0$ might be helpful.

Computing c

$$
\begin{aligned}
c =& [x_1^{k-1} \dots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)(b_j x_j - b_i x_i) \\
=& [x_1^{k-1} \dots x_k^{k-1}] |(b_i x_i)^{j-1}|_{1 \leqslant i,j \leqslant k} \times |x_i^{j-1}|_{1 \leqslant i,j \leqslant k} \\
=& [x_1^{k-1} \dots x_k^{k-1}] \sum_{\sigma \in S_k} \operatorname{sign}(\sigma) \prod_{i=1}^{k} (b_i x_i)^{\sigma(i)-1} \sum_{\tau \in S_k} \operatorname{sign}(\tau) \prod_{i=1}^{k} x_i^{\tau(i)-1} \\
=& \sum_{\sigma \in S_k} \operatorname{sign}(\sigma)\operatorname{sign}(\sigma') \prod_{i=1}^{k} b_i^{\sigma(i)-1} = \sum_{\sigma \in S_k} (-1)^{\binom{k}{2}} \prod_{i=1}^{k} b_i^{\sigma(i)-1},
\end{aligned}
$$

where $\sigma'(i) = k - \sigma(i) + 1$ for all $i = 1, \dots, k$. As $\operatorname{ch}(F) = 2$, we have $1 = -1$ in F. Therefore

$$
\begin{aligned}
c =& \sum_{\sigma \in S_k} \operatorname{sign}(\sigma) \prod_{i=1}^{k} b_i^{\sigma(i)-1} \\
=& |b_j^{i-1}|_{1 \leqslant i,j \leqslant k} = \prod_{1 \leqslant i < j \leqslant k} (b_j - b_i) \neq 0 \text{ (Vandermonde).}
\end{aligned}
$$

My related work

Theorem [Z. W. Sun, J. Combin. Theory Ser A 103(2003)]. Let G be an additive abelian group whose finite subgroups are all cyclic. Let $b_1, \ldots, b_n$ be pairwise distinct elements of G, and let $A_1, \ldots, A_n$ be finite subsets of G with cardinality $k \geqslant m(n-1)+1$ where m is a positive integer.
(i) There are at least $(k-1)n - m\binom{n}{2} + 1$ multisets $\{a_1, \ldots, a_n\}$ such that $a_i \in A_i$ for $i = 1, \ldots, n$ and all the $ma_i + b_i$ are pairwise distinct.
(ii) If $b_1, \ldots, b_n$ are of odd order, then the sets

$$\{\{a_1, \ldots, a_n\}\colon a_i \in A_i,\ a_i \neq a_j \text{ and } ma_i + b_i \neq ma_j + b_j \text{ if } i \neq j\}$$

and

$$\{\{a_1, \ldots, a_n\}\colon a_i \in A_i,\ ma_i \neq ma_j \text{ and } a_i + b_i \neq a_j + b_j \text{ if } i \neq j\}$$

have more than $(k-1)n - (m+1)\binom{n}{2} \geqslant (m-1)\binom{n}{2}$ elements.

My related work

In the proof I used Alon's Combinatorial Nullstellensatz and Dirichlet's unit theorem in Algebraic Number Theory. The theorem follows from my stronger results on sumsets with polynomial restrictions for which we need the following auxiliary result.

Lemma (Sun). Let R be a commutative ring with identity. Let $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ be a matrix over R, and let $k,m_1,\ldots,m_n\in\mathbb{N}$.
(i) If $m_1\leqslant\cdots\leqslant m_n\leqslant k$, then we have

$$[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\Big(\sum_{s=1}^k x_s\Big)^{kn-\sum_{i=1}^n m_i}=\frac{(kn-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n(k-m_i)!}\det(A).$$

(ii) If $m_1<\cdots<m_n\leqslant k$ then

$$[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\cdot\Big(\sum_{s=1}^n x_s\Big)^{kn-\binom{n}{2}-\sum_{i=1}^n m_i}$$
$$=(-1)^{\binom{n}{2}}\frac{(kn-\binom{n}{2}-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n\prod_{\substack{m_i<j\leqslant k\\ j\neq m_{i+1},\ldots,m_n}}(j-m_i)}\mathrm{per}(A).$$

3-Dimensional Analogy of Snevily's Conjecture

In Snevily's conjecture the condition that $|G|$ is odd cannot be omitted. For general abelian groups, what can we say?

Theorem [Z. W. Sun, Math. Res. Lett. 15(2008)]. Let G be any additive abelian group with

$$\mathrm{Tor}(G) = \{g \in G : \ g \text{ has a finite order}\}$$

cyclic, and let A, B and C be finite subsets of G with cardinality $n > 0$. Then there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A, a numbering $\{b_i\}_{i=1}^n$ of the elements of B and a numbering $\{c_i\}_{i=1}^n$ of the elements of C, such that $a_i + b_i + c_i$ $(1 \leqslant i \leqslant n)$ are (pairwise) distinct. Consequently, each subcube of the Latin cube formed by the Cayley addition table of $\mathbb{Z}/N\mathbb{Z}$ contains a Latin transversal.

Remark. We don't require that $|G|$ is odd. The theorem fails for the noncyclic Klein group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Conjecture [Z. W. Sun, Math. Res. Lett. 15(2008)]. Any $n \times n \times n$ Latin cube contains a Latin transversal.

The DKSS Conjecture

The DKSS Conjecture (Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math., 2001]). Let G be a finite abelian group with $|G| > 1$, and let $p(G)$ be the smallest prime divisor of $|G|$. Let $k < p(G)$ be a positive integer. Assume that $A = \{a_1, a_2, \ldots, a_k\}$ is a k-subset of G and $b_1, b_2, \ldots, b_k$ are (not necessarily distinct) elements of G. Then there is a permutation $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct.

Remark. When $G = \mathbb{Z}_p$, the DKSS conjecture reduces to Alon's result. DKSS proved their conjecture for $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p^n$ via the Combinatorial Nullstellensatz.

W. D. Gao and D. J. Wang [Israel J. Math. 2004]: The DKSS conjecture holds when $k < \sqrt{p(G)}$, or G is an abelian p-group and $k < \sqrt{2p}$.

Tool of Gao and Wang: The DKSS method combining with group rings.

A Result of Feng, Sun and Xiang

Theorem [T. Feng, Z. W. Sun & Q. Xiang, Israel J. Math., 182(2011)]. Let G be a finite abelian group with $|G| > 1$. Let $A = \{a_1, \ldots, a_k\}$ be a k-subset of G and let $b_1, \ldots, b_k \in G$, where $k < p = p(G)$. Then there is a permutation $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct, provided either of (i)-(iii).

(i) A or B is contained in a p-subgroup of G.

(ii) Any prime divisor of $|G|$ other than p is greater than $k!$.

(iii) There is an $a \in G$ such that $a_i = a^i$ for all $i = 1, \ldots, k$.

Remark. By this result, the DKSS conjecture holds for any abelian p-group!

Tools: Characters of abelian groups, exterior algebras.

Key lemmas

$$a_1, \ldots, a_k \text{ (in a field) are distinct } \iff \prod_{i=1}^{k}(a_j - a_i) \neq 0.$$

Let $a_1, \ldots, a_k$ be elements of a finite abelian group G. How to characterize that $a_1, \ldots, a_k$ are distinct ?
We need the character group

$$\hat{G} = \{\chi : G \to K \setminus \{0\} |\ \chi(ab) = \chi(a)\chi(b) \text{ for any } a, b \in G\} \cong G,$$

where K is a field having an element of multiplicative order $|G|$.

Lemma 1 (Feng-Sun-Xiang). $a_1, \ldots, a_k \in G$ are distinct if and only if there are $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j))_{1\leq i,j\leq k} \neq 0$. Also, there exist $\chi_1, \ldots, \chi_k \in \hat{G}$ with $\mathrm{per}(\chi_i(a_j))_{1\leq i,j\leq k} \neq 0$ provided that $a_1, \ldots, a_k$ are distinct.

Lemma 2 (Feng-Sun-Xiang). Let $a_1, \ldots, a_k, b_1, \ldots, b_k \in G$ and $\chi_1, \ldots, \chi_k \in \hat{G}$. If $\det(\chi_i(a_j))_{1\leqslant i,j\leqslant k})$ and $\mathrm{per}(\chi_i(b_j))_{1\leqslant i,j\leqslant k})$ are nonzero, then for some $\pi \in S_k$ the products $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct.

Open Problem

How to prove the DKSS conjecture for general finite abelian groups?

In particular,

how to prove the DKSS conjecture for the cyclic group $\mathbb{Z}/n\mathbb{Z}$?

Arsovski solved the Snevily conjecture

In 2010 B. Arsovski [Israel J. Math. 182(2011)] proved Snevily's conjecture fully! A key lemma is closely related to the condition in a result of Feng, Sun and Xiang.

Combinatorial Lemma of Arsovski. Let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ be k-subsets of an arbitrary abelian group G. Then, there exists a permutation $\pi \in S_k$ such that for any permutation $\sigma \in S_k \setminus \{\pi\}$, the multisets

$$\{a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}\} \text{ and } \{a_1 b_{\sigma(1)}, \ldots, a_k b_{\sigma(k)}\}$$

are different.

Comments from a book of D. J. Grynkiewicz:

"Snevily's conjecture was finally solved by Arsovski, aided by the preparatory work of Feng, Sun and Xiang who had already shown that Snevily's conjecture could be deduced from a weakened version of Theorem 18.2, which remained a conjecture at the time."

Part III. Applications of Combinatorial Nullstellensatz to Restricted Sumsets

A lemma for restricted sumsets

Lemma (Alon, Nathanson & Ruzsa [J. Number Theory 56(1996)]). Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F and let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \setminus \{0\}$. Suppose that $\deg f \leqslant k_1 + \ldots + k_n$ where $k_i = |A_i| - 1$, and

$$[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \ldots, x_n)(x_1 + \ldots + x_n)^{k_1 + \cdots + k_n - \deg f} \neq 0.$$

Then

$$|\{a_1 + \cdots + a_n : \ a_i \in A_i, \text{and } f(a_1, \ldots, a_n) \neq 0\}| \geqslant k_1 + \cdots + k_n - \deg f + 1.$$

Proof. Assume that $C = \{a_1 + \cdots + a_n : a_i \in A_i, \ f(a_1, \ldots, a_n) \neq 0\}$ has cardinality not exceeding $K = \sum_{i=1}^n k_i - \deg f$. Then the polynomial

$$P(x_1, \ldots, x_n) := f(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^{K - |C|} \prod_{c \in C} (x_1 + \cdots + x_n - c)$$

is of degree $\sum_{i=1}^n k_i$ with the coefficient of $x_1^{k_1} \cdots x_n^{k_n}$ nonzero. Applying the Combinatorial Nullstellensatz, we find that $P(a_1, \ldots, a_n) \neq 0$ for some $a_1 \in A_1, \ldots, a_n \in A_n$. This is impossible since $a_1 + \cdots + a_n \in C$ if $f(a_1, \ldots, a_n) \neq 0$.

Alon-Nathanson-Ruzsa Theorem

Alon-Nathanson-Ruzsa Theorem [Amer. Math. Monthly 102(1995); J. Number Theory 56(1996)]. For finite nonempty subsets $A_1, \ldots, A_n$ of a field F with $|A_1| < \cdots < |A_n|$, we have

$$|A_1 \dot{+} \cdots \dot{+} A_n| \geqslant \min\left\{p(F),\ \sum_{i=1}^{n}(|A_i| - i) + 1\right\}.$$

Remark. When $|A_1| = \cdots = |A_n| = k \geqslant n$, we can choose $A_i' \subseteq A_i$ with $|A_i'| = k - n + i$ and then apply the ANR theorem to get

$$\begin{aligned}&|A_1 \dot{+} \cdots \dot{+} A_n| \geqslant |A_1' \dot{+} \cdots \dot{+} A_n'|\\ \geqslant &\min\left\{p(F),\ \sum_{i=1}^{n}(|A_i|' - i) + 1\right\} = \min\{p(F),\ (k-n)n+1\}.\end{aligned}$$

Via the Combinatorial Nullstellensatz, the ANR theorem reduces to

$$\begin{aligned}&[x_1^{k_1}\cdots x_n^{k_n}]\prod_{1\leqslant i<j\leqslant n}(x_j - x_i)\times(x_1+\cdots+x_n)^{\sum_{i=1}^n k_i - \binom{n}{2}}\\ =&\frac{(k_1+\cdots+k_n-\binom{n}{2})!}{k_1!\cdots k_n!}\prod_{1\leqslant i<j\leqslant n}(k_j-k_i).\end{aligned}$$

Some other results

Q. H. Hou and Z. W. Sun [Acta Arith. 102(2002)] studied the restricted sumset

$$C=\{a_1+\cdots+a_n:\ a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } a_i-a_j\notin S_{ij} \text{ if } i<j\}$$

with $|A_1|=\ldots=|A_n|=k+1$ via

$$[x_1^k\cdots x_n^k]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{2m}\times(x_1+\cdots+x_n)^{(k-m(n-1))n}$$

$$=(-1)^{m\binom{n}{2}}\frac{((k-m(n-1))n)!}{m!^n}\prod_{j=1}^{n}\frac{(jm)!}{(k-(j-1)m)!}.$$

Z. W. Sun and Y. N. Yeh [J. Number Theory 114(2005)] determined

$$[x_1^{k-n+1}\cdots x_n^k]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{2m-1}\times(x_1+\cdots+x_n)^{(k-m(n-1))n}$$

Zhao's supplement to the Hou-Sun result

Lilu Zhao [Finite Fields Appl. 28(2014)]: Let k, m, n be positive integers with $k > m(n-1)$, and let $k_i \in \{k, k+1\}$ for all $i = 1, \ldots, n$. Then

$$[x_1^{k_1-1} \ldots x_n^{k_n-1}] \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^{2m} \times (x_1 + \ldots + x_n)^{\sum_{i=1}^n (k_i-1) - mn(n-1)}$$

$$= \frac{\sum_{i=1}^n (k_i - 1) - mn(n-1)}{m!^n \prod_{j=0}^{s-1} (k - jm)} \prod_{j=1}^{n} \frac{(jm)!}{(k-1-m(j-1))!}.$$

Zhao deduced this from Aomoto's identity and a result of Gessel-Lv-Xin-Zhou [JCTA 115(2008)].

Theorem (Hou-Sun; Zhao). Let S_{ij} $(1 \leqslant i \neq j \leqslant n)$ be finite subsets of a field F with $|S_{ij}| = m$. Let $A_1, \ldots, A_n$ be finite subsets of F with $|A_1| = \ldots = |A_n| = k \in \mathbb{Z}^+$. Suppose that $p(F) > mn$. Then, for

$$C = \{a_1 + \ldots + a_n : \ a_1 \in A_1, \ldots, a_n \in A_n, \ a_i - a_j \notin S_{ij} \text{ if } i \neq j\},$$

we have $|C| \geqslant \min\{p(F), (k-1)n - mn(n-1) + 1\}$.

A Result of Liu and Sun

J.-X. Liu and Z.-W. Sun [J. Number Theory 97(2002)]. Let $A_1, \ldots, A_n$ be finite subsets of a field F with $|A_{i+1}| - |A_i| \in \{0, 1\}$ for $i = 1, \ldots, n-1$, and $|A_n| = k > m(n-1)$. Suppose that $P(x) \in F[x]$, $\deg P = m$ and $p(F) > (k-1)n - (m+1)\binom{n}{2}$. Then

$$\begin{aligned}&|\{a_1 + \cdots + a_n : \ a_i \in A_i, \ P(a_i) \neq P(a_j) \text{ if } i \neq j\}| \\ \geqslant &(k-1)n - (m+1)\binom{n}{2} + 1.\end{aligned}$$

Lemma: For positive integers k, m, n with $k - 1 \geqslant m(n-1)$ we have

$$\begin{aligned}&[x_1^{k-n} \cdots x_n^{k-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j^m - x_i^m) \times (x_1 + \cdots + x_n)^{(k-1)n-(m+1)\binom{n}{2}} \\ =&(-m)^{\binom{n}{2}} \frac{((k-1)n - (m+1)\binom{n}{2}))!1!2! \cdots (n-1)!}{(k-1)!(k-1-m)! \cdots (k-1-(n-1)m)!}.\end{aligned}$$

Solving a conjecture of Erdős and Selfridge

Applying the Liu-Sun result with $P(x) = x^2$ and using Gessel-Viennot's evaluation (see [Adv. in Math. 1985]) of some binomial determinants, E. Balandraud obtained the following result on subset sums.

E. Balandraud [Israel J. Math. 188(2012)]. Let p be a prime and let $A \subseteq \mathbb{Z}_p$ with $0 \notin A + A$. Then

$$\left|\left\{\sum_{a\in B} a :\ \emptyset \neq B \subseteq A\right\}\right| \geqslant \min\left\{p,\ \frac{|A|(|A|+1)}{2}\right\}.$$

Corollary (conjectured by Erdős and Selfridge). Let p be a prime. Then

$$\max\left\{|A| :\ \sum_{a\in B} a \neq 0 \text{ for any } \emptyset \neq B \subseteq A\right\}$$
$$= \max\left\{k \in \mathbb{Z} :\ \frac{k(k+1)}{2} < p\right\} = \left\lfloor \frac{\sqrt{8p-7}-1}{2} \right\rfloor$$

A Result of Z. W. Sun [J. Combin. Theory Ser. A 103(2003)]: Let $A_1, \ldots, A_n$ be finite subsets of a field F with cardinality $k > m(n-1)$. Suppose $p(F) > \max\{n, (k-1)n - (m+1)\binom{n}{2}\}$. For any $d_{ij} \in F$ $(1 \leqslant i < j \leqslant n)$ and $P(x) \in F[x]$ with degree m, we have

$$|\{a_1 + \cdots + a_n : \ a_i \in A_i, \ P(a_i) \neq P(a_j) \text{ and } a_i - a_j \neq d_{ij} \text{ if } i \neq j\}|$$
$$\geqslant (k-1)n - (m+1)\binom{n}{2} + 1.$$

Lemma (Z.-W. Sun): For positive integers k, m, n with $k - 1 \geqslant m(n-1)$, we have

$$[x_1^{k-1} \cdots x_n^{k-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)(x_j^m - x_i^m) \times (x_1 + \cdots + x_n)^K$$
$$= (-m)^{\binom{n}{2}} \frac{K!1!2! \cdots n!}{(k-1)!(k-1-m)! \cdots (k-1-(n-1)m)!},$$

where $K = (k-1)n - (m+1)\binom{n}{2}$.

Erdős-Heilbronn conjecture for finite groups

The original Erdős-Heilbronn conjecture is only concerned with cyclic groups of prime order.

P. Balister & J. P. Wheeler [Acta Arith. 140(2009)]:
Let G be a finite group written additively with $|G| > 1$. Then

$$|2^{\wedge}A| \geqslant \min\{p(G), 2|A| - 3\} \qquad \text{for any } A \subseteq G,$$

where $p(G)$ is the least order of a nonzero element of G, i.e., $p(G)$ is the smallest prime divisor of $|G|$.

Remark. (a) One auxiliary result needed is the Feit-Thompson theorem: *Any group of odd order is solvable.*

(b) It is not clear how to extend the result to $n^{\wedge}A$ or $A \dot{+} B$.

Linear extension of the Erdős-Heilbronn conjecture

For a prime p, $\mathbb{Z}_p$ is an additively cyclic group. On the other hand, $\mathbb{Z}_p$ is a field which involves both addition and multiplication.

A Conjecture of Z. W. Sun [Finite Fields Appl. 14(2008)]. Let $a_1, \ldots, a_n$ be nonzero elements of a field F. If $p(F) \neq n+1$, then for any finite $A \subseteq F$ we have

$$\begin{aligned}&|\{a_1x_1 + \cdots + a_nx_n : \ x_1, \ldots, x_n \text{ are distinct elements of } A\}| \\ &\quad \geqslant \min\{p(F) - \delta,\ n(|A| - n) + 1\},\end{aligned}$$

where

$$\delta = [\![n = 2 \ \&\ a_1 + a_2 = 0]\!] = \begin{cases} 1 & \text{if } n = 2 \ \&\ a_1 + a_2 = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Difficulty: We cannot apply the Combinatorial Nullstellensatz directly, for, the related coefficient involving $a_1, \ldots, a_n$ might be zero.

Prizes: I'd like to offer 200 US dollars for a complete proof.

Sun and Zhao's results

Theorem (Z.-W. Sun and L.-L. Zhao [JCTA 119(2012)]). The conjecture (posed by Sun) holds if $p(F) \geqslant n(3n-5)/2$.

Remark. Zhao and Sun also noted that the conjecture holds for $n = 3$.

An Auxiliary Theorem (Z.-W. Sun and L.-L. Zhao [JCTA 119(2012)]).
Let n be a positive integer, and let F be a field with $p(F) \geqslant (n-1)^2$. Let $a_1, \ldots, a_n \in F^* = F \setminus \{0\}$, and suppose that $A_i \subseteq F$ and $|A_i| \geqslant 2n-2$ for $i = 1, \ldots, n$. Then, for the set

$$C = \{a_1x_1 + \cdots + a_nx_n : \ x_1 \in A_1, \ldots, x_n \in A_n, \text{ and } x_i \neq x_j \text{ if } i \neq j\}$$

we have

$$|C| \geqslant \min\{p(F) - [\![n = 2 \ \&\ a_1 + a_2 = 0]\!], |A_1| + \cdots + |A_n| - n^2 + 1\}.$$

Corollary. Let $p > 7$ be a prime and let $A \subseteq F = \mathbb{Z}/p\mathbb{Z}$ with $|A| \geqslant \sqrt{4p-7}$. Let $n = \lfloor |A|/2 \rfloor$ and $a_1, \ldots, a_n \in F^*$. Then every element of F can be written in the linear form $a_1x_1 + \cdots + a_nx_n$ with $x_1, \ldots, x_n \in A$ distinct.

Sumsets with polynomial restrictions

Theorem (Z.-W. Sun and L.-L. Zhao [JCTA 119(2012)]). Let $P(x_1,\ldots,x_n)$ be a polynomial over a field F. Suppose that $k_1,\ldots,k_n$ are nonnegative integers with $k_1+\cdots+k_n=\deg P$ and $[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\ldots,x_n)\neq 0$. Let $A_1,\ldots,A_n$ be finite subsets of F with $|A_i|>k_i$ for $i=1,\ldots,n$. Then, for the restricted sumset

$$C=\{x_1+\cdots+x_n:\ x_1\in A_1,\ldots,x_n\in A_n,\ \text{and } P(x_1,\ldots,x_n)\neq 0\},$$

we have

$$|C|\geqslant \min\{p(F)-\deg P,\ |A_1|+\cdots+|A_n|-n-2\deg P+1\}.$$

Remark. In the case $P(x_1,\ldots,x_n)=1$ this theorem gives the Cauchy-Davenport theorem. When F is of characteristic zero (i.e., $p(F)=+\infty$), this theorem extends a result of Sun [Acta Arith. 99(2001)] on sums of subsets of $\mathbb{Z}$ with various linear restrictions.

Proof

If $p(F) \leqslant \deg P$ or $\sum_{i=1}^{n} |A_i| < n + 2\deg P$, then the desired inequality holds trivially. Below we assume that $p(F) > \deg P$ and $\sum_{i=1}^{n} |A_i| \geqslant n + 2\deg P$. Write

$$P(x_1, \ldots, x_n) = \sum_{j_1+\ldots+j_n \leqslant \deg P} c_{j_1,\ldots,j_n} x_1^{j_1} \ldots x_n^{j_n},$$

and define

$$P^*(x_1, \ldots, x_n) = \sum_{j_1+\ldots+j_n = \deg P} c_{j_1,\ldots,j_n} (x_1)_{j_1} \ldots (x_n)_{j_n} \in F[x_1, \ldots, x_n]$$

where $(x)_j = \prod_{0 \leqslant i < j} (x - ie)$ with e the identity of F. Note that

$$\begin{aligned} &[x_1^{k_1} \ldots x_n^{k_n}] P^*(x_1, \ldots, x_n) \\ =&[x_1^{k_1} \ldots x_n^{k_n}] \sum_{j_1+\ldots+j_n = \deg P} c_{j_1,\ldots,j_n} x_1^{j_1} \ldots x_n^{j_n} = c_{k_1,\ldots,k_n} \neq 0. \end{aligned}$$

Proof

For $i = 1, \ldots, n$ let

$$B_i = \{me : \ m \in [|A_i| - k_i - 1, |A_i| - 1]\}.$$

As $k_i < \deg P < p(F)$, we have $|B_i| = k_i + 1 > k_i$. By the Combinatorial Nullstellensatz, there are $m_i \in [|A_i| - k_i - 1, |A_i| - 1]$ $(i = 1, \ldots, n)$ such that $P^*(m_1 e, \ldots, m_n e) \neq 0$.
Let $M = \sum_{i=1}^{n} m_i - \deg P$. Then

$$M \geqslant \sum_{i=1}^{n} |(A_i| - k_i - 1) - \deg P = \sum_{i=1}^{n} |A_i| - n - 2\deg P \geqslant 0$$

and

$$[x_1^{m_1} \ldots x_n^{m_n}] P(x_1, \ldots, x_n)(x_1 + \ldots + x_n)^M$$

$$= [x_1^{m_1} \ldots x_n^{m_n}] \sum_{j_1 + \ldots + j_n = \deg P} c_{j_1, \ldots, j_n} x_1^{j_1} \ldots x_n^{j_n} \sum_{i_1 + \ldots + i_n = M} \frac{M!}{i_1! \ldots i_n!} x_1^{i_1} \ldots x_n^{i_n}$$

$$= \sum_{\substack{0 \leqslant j_i \leqslant m_i \\ \sum_{i=1}^{n} j_i = \deg P}} \frac{M!}{(m_1 - j_1)! \ldots (m_n - j_n)!} c_{j_1, \ldots, j_n}.$$

Continue the proof

Hence

$$m_1! \dots, m_n! [x_1^{m_1} \dots x_n^{m_n}] P(x_1, \dots, x_n)(x_1 + \dots + x_n)^M$$
$$= M! \sum_{j_1 + \dots + j_n = \deg P} (m_1 e)_{j_1} \dots (m_n e)_{j_n} c_{j_1, \dots, j_n} = M! P^*(m_1 e, \dots, m_n e).$$

If $|C| \leqslant M < p(F)$, then

$$[x_1^{m_1} \dots x_n^{m_n}] P(x_1, \dots, x_n)(x_1 + \dots + x_n)^{M - |C|} \prod_{x \in C} (x_1 + \dots + x_n - c)$$
$$= [x_1^{m_1} \dots x_n^{m_n}] P(x_1, \dots, x_n)(x_1 + \dots + x_n)^M \neq 0,$$

and hence by the Combinatorial Nullstellensatz there are $x_1 \in A_1, \dots, x_n \in A_n$ such that

$$P(x_1, \dots, x_n)(x_1 + \dots + x_n)^{M - |C|} \prod_{c \in M} (x_1 + \dots + x_n - c) \neq 0,$$

which contradicts the definition of C.

Continue the proof

So, either $p(F) \leqslant M \leqslant \sum_{i=1}^{n}(|A_i| - 1) - \deg P$, or

$$|C| \geqslant M + 1 \geqslant |A_1| + \ldots + |A_n| - n - 2\deg P + 1.$$

Suppose $|C| < \min\{p(F) - \deg P, \sum_{i=1}^{n} |A_i| - n - 2\deg P + 1\}$. Then

$$p(F) \leqslant M \leqslant \sum_{i=1}^{n}(|A_i| - 1) - \deg P.$$

For $i = 1, \ldots, n$ take $A_i' \subseteq A_i$ with $|A_i| > k_i$ such that $\sum_{i=1}^{n}(|A_i'| - 1) - \deg P = p(F) - 1 < p(F)$. (Note that $\sum_{i=1}^{n} k_i - \deg P = 0 < p(F)$.) Then

$$\begin{aligned} |C| \geqslant & |\{x_1 + \ldots + x_n : \ x_i \in A_i' \ \& \ P(x_1, \ldots, x_n) \neq 0\}| \\ & \geqslant \sum_{i=1}^{n} |A_i'| - n - 2\deg P + 1 = p(F) - \deg P \\ & = \min\left\{p(F) - \deg P, \sum_{i=1}^{n} |A_i| - n - 2\deg P + 1\right\}, \end{aligned}$$

which leads a contradiction.

Value sets of polynomials over a field

Theorem (Z.-W. Sun [Finite Fields Appl. 14(2008)]). Let F be a field, and let

$$f(x_1,\ldots,x_n)=a_1x_1^k+\ldots+a_nx_n^k+g(x_1,\ldots,x_n)\in F(x_1,\ldots,x_n)$$

with $k\in\mathbb{Z}^+=\{1,2,3,\ldots\}$, $a_1,\ldots,a_n\in F^*=F\setminus\{0\}$ and $\deg g<k$. Then, for any finite nonempty subsets $A_1,\ldots,A_n$ of F, we have

$$\begin{aligned}&|\{f(x_1,\ldots,x_n):\ x_1\in A_1,\ldots,x_n\in A_n\}|\\ \geqslant&\min\left\{p(F),\sum_{i=1}^n\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}.\end{aligned}$$

Remark. This theorem includes several known results as special cases. When $F=\mathbb{Z}/p\mathbb{Z}$ (with p prime) and $f(x_1,\ldots,x_n)=x_1+\ldots+x_n$, this theorem yields the Cauchy-Davenport theorem.

Proof

Let m be the largest nonnegative integer not exceeding n such that $\sum_{0<i\leqslant m}\lfloor(|A_i|-1)/k\rfloor < p(F)$. For each $0 < i \leqslant m$ let A'_i be a subset of A_i with cardinality $k\lfloor(|A_i|-1)/k\rfloor+1$. In the case $m < n$, $p = p(F)$ is a prime and we let A'_{m+1} be a subset of A_{m+1} with

$$\begin{aligned}|A'_{m+1}| =& k\left(p-1-\sum_{0<i\leqslant m}\left\lfloor\frac{|A_i|-1}{k}\right\rfloor\right)+1\\ &< k\left\lfloor\frac{|A_{m+1}|-1}{k}\right\rfloor+1\leqslant|A_{m+1}|.\end{aligned}$$

If $m+1 < j \leqslant n$ then we let $A'_j \subseteq A_j$ be a singleton. Whether $m = n$ or not, we have $\sum_{i=1}^{n}(|A'_i|-1) = k(N-1)$, where

$$N=\min\left\{p(F),\sum_{i=1}^{n}\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}.$$

Continue the proof

Set

$$C = \{f(x_1, \ldots, x_n) : x_1 \in A_1', \ldots, x_n \in A_n'\}.$$

Suppose that $|C| \leqslant N - 1$. Then

$$[x_1^{|A_1'|-1} \cdots x_n^{|A_n'|-1}] f(x_1, \ldots, x_n)^{N-1-|C|} \prod_{c \in C} (f(x_1, \ldots, x_n) - c)$$

$$= [x_1^{|A_1'|-1} \cdots x_n^{|A_n'|-1}] (a_1 x_1^k + \cdots + a_n x_n^k)^{N-1}$$

$$= \frac{(N-1)!}{\prod_{i=1}^n ((|A_i'|-1)/k)!} a_1^{(|A_1'|-1)/k} \cdots a_n^{(|A_n'|-1)/k} \neq 0.$$

By the Combinatorial Nullstellensatz, for some $x_1 \in A_1', \ldots, x_n \in A_n'$ we have

$$f(x_1, \ldots, x_n)^{N-1-|C|} \prod_{c \in C} (f(x_1, \ldots, x_n) - c) \neq 0$$

which contradicts the fact $f(x_1, \ldots, x_n) \in C$.

In view of the above,

$$|\{f(x_1, \ldots, x_n) : x_1 \in A_1, \ldots, x_n \in A_n\}| \geqslant |C| \geqslant N.$$

Restricted Value Sets of Polynomials

Theorem [Z. W. Sun, Finite Fields Appl. 14(2008)]. Let F be a field, and let

$$f(x_1,\ldots,x_n)=a_1x_1^k+\cdots+a_nx_n^k+g(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$$

with $a_1,\ldots,a_n\in F^*=F\setminus\{0\}$ and $\deg g<k$. If $A_1,\ldots,A_n$ are finite subsets of F with $|A_i|\geqslant i$ for $i=1,\ldots,n$, and $n\leqslant k=\deg f$, then

$$\begin{aligned}&|\{f(x_1,\ldots,x_n):\ x_i\in A_i,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}|\\ \geqslant&\min\left\{p(F),\ \sum_{i=1}^n\left\lfloor\frac{|A_i|-i}{k}\right\rfloor+1\right\}.\end{aligned}$$

A General Conjecture

Conjecture (Z. W. Sun [Finite Fields Appl. 14(2008)]). Let F be a field, and let

$$f(x_1,\ldots,x_n)=a_1x_1^k+\cdots+a_nx_n^k+g(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$$

with $a_1,\ldots,a_n\in F^*=F\setminus\{0\}$ and $\deg g<k$. If A is a finite subset of F with $|A|\geqslant n>k$ and $p(F)\neq n+1$, then

$$\begin{aligned}&|\{f(x_1,\ldots,x_n):\ x_1,\ldots,x_n \text{ are distinct elements of } A\}|\\ \geqslant&\min\left\{p(F)-\delta,\ \frac{n(|A|-n)}{k}-k\left\{\frac{n}{k}\right\}\left\{\frac{|A|-n}{k}\right\}+1\right\},\end{aligned}$$

where $\delta=[\![n=2\ \&\ \&\ a_1+a_2=0]\!]$.

Remark. In the case $k=1$ this reduces to the conjecture of Sun on linear extension of the Erdős-Heilbronn conjecture.

Theorem (H. Pan and Z.-W. Sun [J. Combin. Theory Ser. A 116(2009)]). The above conjecture holds when $a_1=\cdots=a_n$.

Lev's Conjecture

Let A and B be finite nonempty subsets of an additive abelian group G. In contrast with the Cauchy-Davenport theorem, J.H.B. Kemperman (1960) and P. Scherk (1955) proved that

$$|A+B| \geqslant |A|+|B|-\min_{c\in A+B}\nu_{A,B}(c),$$

where

$$\nu_{A,B}(c)=|\{(a,b)\in A\times B\colon a+b=c\}|;$$

in particular, we have $|A+B|\geqslant |A|+|B|-1$ if some $c\in A+B$ can be uniquely written as $a+b$ with $a\in A$ and $b\in B$.

Motivated by the Kemperman-Scherk theorem and the Erdős-Heilbronn conjecture, V. F. Lev (2005) proposed the following interesting conjecture.

Lev's Conjecture. Let A and B be finite nonempty subsets of an abelian group G. Set $A\dot{+}B=\{a+b:\ a\in A,\ b\in B,\ a\neq b\}$. Then

$$|A\dot{+}B|\geqslant |A|+|B|-2-\min_{c\in A+B}\nu_{A,B}(c).$$

Progress due to H. Pan and Z. W. Sun

H. Pan and Z.-W. Sun [Israel J. Math. 154(2006)]:
Let A and B be finite nonempty subsets of a field F. Let $P(x, y) \in F[x, y]$ and

$$C = \{a + b\colon a \in A,\ b \in B,\ \text{and } P(a, b) \neq 0\}.$$

If C is nonempty, then

$$|C| \geqslant |A| + |B| - \deg P - \min_{c \in C} \nu_{A,B}(c).$$

H. Pan and Z.-W. Sun [Israel J. Math. 154(2006)]:
Let A and B be finite nonempty subsets of an abelian group G with cyclic torsion subgroup. For $i = 1, \ldots, l$ let m_i and n_i be nonnegative integers and let $d_i \in G$. Suppose that

$$C = \{a+b\colon a \in A,\ b \in B,\ \text{and } m_i a - n_i b \neq d_i \text{ for all } i = 1, \ldots, l\} \neq \emptyset.$$

Then $|C| \geqslant |A| + |B| - \sum_{i=1}^{l}(m_i + n_i) - \min_{c \in C} \nu_{A,B}(c)$.

Remark. The proofs involve the Strong Form of the Combinatorial Nullstellensatz.

Difference-restricted sumsets

H. Pan and Z.-W. Sun [Israel J. Math. 154(2006)]. Let G be an abelian group, and let A, B, S be finite nonempty subsets of G with

$$C = \{a + b\colon a \in A,\ b \in B,\ \text{and } a - b \notin S\} \neq \emptyset.$$

(i) If G is torsion-free or elementary abelian, then

$$|C| \geqslant |A| + |B| - |S| - \min_{c \in C} \nu_{A,B}(c).$$

(ii) If $\mathrm{Tor}(G)$ (the torsion subgroup of G) is cyclic, then

$$|C| \geqslant |A| + |B| - 2|S| - \min_{c \in C} \nu_{A,B}(c).$$

Remark. Clearly $\min_{c \in C} \nu_{A,B}(c) \geqslant \min_{c \in A+B} \nu_{A,B}(c)$ since $C \subseteq A + B$. So, when $\mathrm{Tor}(G)$ is cyclic and $S = \{0\}$, part (ii) gives a result slightly weaker than Lev's conjecture.

H. Pan and Z.-W. Sun [JCTA 100(2002)]. Let F be a finite field with $\mathrm{ch}(F) = p \neq 2$. Let A, B and S be finite nonempty subsets of F, and let q be the largest power of p with $q \leqslant |S|$. Then

$$|\{a+b\colon a \in A,\ b \in B,\ \text{and } a-b \notin S\}| \geq \min\{p,\ |A|+|B|-|S|-q-1\}.$$

Main References:

1. Noga Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8**(1999), 7–29.

2. Zhi-Wei Sun, *A survey of problems and results on restricted sumsets*, in: Number Theory (S. Kanemitsu & J.-Y. Liu, eds.), World Sci., Singapore, 2007, pp. 190–213.

3. Zhi-Wei Sun and Lilu Zhao, *Linear exntension of the Erdos-Heilbronn conjecture*, J. Combin. Theory Ser. A **119** (2012), 364–381.

Thank you!