A talk given at Graz Univ.

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

May 7, 2026

Abstract

In this talk we introduce Alon's Combinatorial Nullstellensatz (i.e., the so-called polynomial method), which is a powerful tool in algebraic combinatorics. We will also present its various applications in additive combinatorics.

While in the past many of the basic combinatorial results were obtained mainly by ingenuity and detailed reasoning, the modern theory has grown out of this early stage, and often relies on deep, well developed tools.

—Noga Alon (ICM, Beijing, 2002)

Additive combinatorics is currently a highly active area of research. One remarkable feature of the field is the use of tools from many diverse fields of mathematics.

—Terence Tao & V. H. Vu (2006)

Part I. Combinatorial Nullstellensatz and its Backgrounds

Hilbert's Nullstellensatz

Hilbert's Nullstellensatz. Let F be an algebraically closed field, and let I be an ideal of the polynomial ring $F[x_1, \ldots, x_n]$. Let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. If

$$Z(f) = \{(a_1, \ldots, a_n) \in F^n : \ f(a_1, \ldots, a_n) = 0\}$$

contains

$$Z(I) = \{(a_1, \ldots, a_n) \in F^n : \ P(a_1, \ldots, a_n) = 0 \text{ for all } P \in I\},$$

then f belongs to

$$\sqrt{I} = \{P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] : \ P^m \in I \text{ for some } m > 0\}.$$

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.

In 2001, J. Nagy and P. P. Pach [arXiv:2107.03956] used the group-ring method to prove that the Jäger-Alon-Tarsi Conjecture holds when $|F| > 61$ and $|F| \neq 79$.

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 $f \in I$.

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

Two conjectures 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.

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.

For a matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant k}$ over a field, its determinant and permanent are given by

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

Observe that

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

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

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

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

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

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

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.

Lemma 1

Lemma 1. Let $b_1, \ldots, b_n$ be elements of a field F. Then

$$[x_1^{n-1} \cdots x_n^{n-1}] \det[(b_i x_i)^{j-1}]_{1 \leqslant i,j \leqslant n} \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$$

$$= (-1)^{\binom{n}{2}} \mathrm{per}[(b_i^{j-1}]_{1 \leqslant i,j \leqslant n})$$

and

$$[x_1^{n-1} \cdots x_n^{n-1}] \mathrm{per}[(b_i x_i)^{j-1}]_{1 \leqslant i,j \leqslant n} \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$$

$$= (-1)^{\binom{n}{2}} \det[b_i^{j-1}]_{1 \leqslant i,j \leqslant n} = (-1)^{\binom{n}{2}} \prod_{1 \leqslant i < j \leqslant n} (b_j - b_i).$$

Proof of Lemma 1

Actually we already proved the first equality. Here we give a proof of the second equality.

$$
\begin{aligned}
&[x_1^{k-1}\dots x_k^{k-1}]\mathrm{per}[(b_i x_i)^{j-1}]_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\\
=&[x_1^{n-1}\dots x_n^{n-1}]\sum_{\sigma\in S_n}\prod_{i=1}^{n}(b_i x_i)^{\sigma(i)-1}\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{i=1}^{n}x_i^{\tau(i)-1}\\
=&\sum_{\sigma\in S_n}\mathrm{sign}(\sigma')\prod_{i=1}^{n}b_i^{\sigma(i)-1}=\sum_{\sigma\in S_n}(-1)^{\binom{n}{2}}\mathrm{sign}(\sigma)\prod_{i=1}^{n}b_i^{\sigma(i)-1}\\
=&(-1)^{\binom{n}{2}}\det[b_i^{j-1}]_{1\leqslant i,j\leqslant n}=(-1)^{\binom{n}{2}}\prod_{1\leqslant i<j\leqslant n}(b_j-b_i),
\end{aligned}
$$

where $\sigma'(i)=n-\sigma(i)+1$ for all $i=1,\dots,n$.

What abelian groups can be embedded in $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

Lemma 2 (Z.-W. Sun [JCTA 103(2003)]). A finitely generated abelian group G can be embedded in the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers if and only if

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

is cyclic.

Proof. Note that $\mathrm{Tor}(G)$ is a finite subgroup of G and any finite subgroup of the group $\mathbb{C}^*$ is cyclic. So the "only if" direction is easy.

Now we consider the "if" direction. By the structure theorem for finitely generated abelian groups, G is isomorphic to the direct sum $\mathrm{Tor}(G) \oplus \mathbb{Z}^r$ for some $r \in \mathbb{N}$. Let $h = |\mathrm{Tor}(G)|$ and choose an even integer $h' > 2$ so that $h \mid h'$ and $\varphi(h')/2 \geqslant r + 1$. By Dirichlet's unit theorem, the unit group $U_{h'}$ of the ring $\mathbb{Z}[e^{2\pi i/h'}]$ is isomorphic to $(\mathbb{Z}/h'\mathbb{Z}) \oplus \mathbb{Z}^{\varphi(h')/2-1}$. Thus we can identify the additive group G with a subgroup of the multiplicative group $U_{h'}$ which is a subgroup of $\mathbb{C}^*$.

Proof of the Theorem

It suffices to work in the subgroup H of G generated by the finite set $A \cup B \cup C$. In view of Lemma 2, we can identity H with a subgroup of the multiplicative group $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, and hence view A, B, C as n-subsets of $\mathbb{C}^*$.

Since

$$[x_1^{n-1} \cdots x_n^{n-1}]\mathrm{per}[(c_i x_i)^{j-1}]_{1 \leqslant i,j \leqslant n} \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$$
$$= (-1)^{\binom{n}{2}} \prod_{1 \leqslant i < j \leqslant n} (c_j - c_i) \neq 0,$$

by the Combinatorial Nullstellensatz there are distinct $b_1, \ldots, b_n \in B$ such that $\mathrm{per}[(b_i c_i)^{j-1}]_{1 \leqslant i,j \leqslant n}) \neq 0$.

Proof of the Theorem (continued)

As

$$[x_1^{n-1} \cdots x_n^{n-1}] \det[(b_i c_i x_i)^{j-1}]_{1 \leqslant i,j \leqslant n} \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$$
$$= (-1)^{\binom{n}{2}} \operatorname{per}[(b_i c_i)^{j-1}]_{1 \leqslant i,j \leqslant n}) \neq 0,$$

by the Combinatorial Nullstellensatz there are distinct $a_1, \ldots, a_n \in A$ such that

$$\det[(a_i b_i c_i)^{j-1}]_{1 \leqslant i,j \leqslant n} = \prod_{1 \leqslant i < j \leqslant n} (a_j b_j c_j - a_i b_i c_i) \neq 0.$$

Thus $a_1 b_1 c_1, \ldots, a_n b_n c_n$ are indeed pairwise distinct.

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

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.

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."

Two open conjectures

Conjecture (Z.-W. Sun, 2013-09-03). Let G be an additive abelian group G of odd order. For any $A \subseteq G$ with $|A| = n > 2$, there always exists a numbering $a_1, a_2, \ldots, a_n$ of all the n elements of A such that the n sums

$$a_1 + a_2,\ a_2 + a_3,\ \ldots,\ a_{n-1} + a_n,\ a_n + a_1$$

are pairwise distinct.

Remark. (i) In 2020, Mr. Yu-Xuan Ji at Nanjing Univ. verified this for $|G| < 30$.

(ii) If $G = \{a_1, \ldots, a_n\}$ is an additive abelian group with $|G| = n$ odd, then $a_1 + \ldots + a_n = 0$ since $a \neq -a$ for all $a \in G \setminus \{0\}$.

Conjecture (Z.-W. Sun [J. Algebraic Combin. 54(2021), 893-912]). If a group G contains no element of order among $2, \ldots, n+1$, then any $A \subseteq G$ with $|A| = n$ can be written as $\{a_1, \ldots, a_n\}$ with $a_1, a_2^2, \ldots, a_n^n$ pairwise distinct.

Remark. We have proved this when $n \leqslant 3$ or G is a torsion-free abelian group. The conjecture is open for $G = \mathbb{Z}/p\mathbb{Z}$ with p an odd prime.

A theorem on torsion-free abelian groups

For an element a of an additive group G, we let ka be the sum of k copies of a for all $k = 1, 2, 3, \ldots$.

Theorem (Z.-W. Sun [J. Algebraic Combin. 54(2021), 893-912]). Let $a_1, \ldots, a_n$ be distinct elements of a torsion-free abelian group G. Then there is a permutation $\pi \in S_n$ such that all those $ka_{\pi(k)}$ $(k = 1, \ldots, n)$ are pairwise distinct.

Two Steps of the Proof:

(1) The subgroup H of G generated by $a_1, \ldots, a_n$ is finitely generated and torsion-free, it can be embedded into the additive group $\mathbb{C}$ of complex numbers by using algebraic number theory.

(2) Use the fact

$$[x_1^{n-1} \ldots x_n^{n-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)(jx_j - ix_i) \in \mathbb{C}[x_1, \ldots, x_n]$$
$$= (-1)^{n(n-1)/2} \mathrm{per}[i^{j-1}]_{1 \leqslant i,j \leqslant n} \neq 0.$$

Part III. Applications of Combinatorial Nullstellensatz to restricted sumsets

Erdős-Heilbronn Conjecture

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

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

and denote this by $n^{\wedge}A$ if $A_1 = \cdots = A_n$.

Erdős-Heilbronn Conjecture (1964). Let p be a prime and let $A \subseteq \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. Then $|2^{\wedge}A| \geqslant \min\{p, \ 2|A| - 3\}$.

Dias da Silva-Hamidoune Theorem [Bull. London Math. Soc., 1994]. Let A be a finite nonempty subset of a field F. For any positive integer n, we have

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

where $p(F)$ is the additive order of the identity of F.

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 Combinatorial Nullstellensatz.

A lemma for restricted sumsets

Lemma 1 (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

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

Via the ANR lemma, the ANR theorem reduces to

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

$$= \frac{(k_1 + \cdots + k_n - \binom{n}{2})!}{k_1! \cdots k_n!} \prod_{1 \leqslant i < j \leqslant n} (k_j - k_i).$$

Remark. The proof makes use of the Vandermonde determinant

$$\det[x_j^{i-1}]_{1 \leqslant i,j \leqslant n} = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i).$$

Joint work with Q.-H. Hou

Q. H. Hou and Z. W. Sun [Acta Arith. 102(2002)]: Let $m, n \in \mathbb{Z}^+$ and let $k \in \mathbb{Z}$ with $k-1 \geqslant m(n-1)$. Then

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

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

Theorem (Hou and Sun [Acta Arith. 102(2002)]). Let $A_1,\ldots,A_n$ be k-subsets of a field F and let S_{ij} be a $2m$-subset of F for $1\leqslant i<j\leqslant n$. If $p(F)>\max\{mn,(k-1-m(n-1))n\}$, then for the restricted sumset

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

we have $|C|\geqslant(k-1-m(n-1))n+1$.

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 Sun

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

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.

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

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

Remark: We cannot apply the Combinatorial Nullstellensatz directly, for, the related coefficient involving $a_1, \ldots, a_n$ might be zero. Z.-W. Sun and L.-L. Zhao [JCTA 119(2012)] confirmed the conjecture in the case $n = 3$ or $p(F) \geqslant n(3n-5)/2$.

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.

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

Theorem [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

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

Theorem [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

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

is nonempty. Then

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

An open conjecture

Conjecture (Z.-W. Sun [J. Algebraic Combin. 54 (2021)]). Let A be a finite subset of a field F with $|A| \geqslant n + \delta_{n,3}$, where $n \in \mathbb{Z}^+$. Then, for the set

$$S(A) = \left\{ \sum_{k=1}^{n} ka_k : \ a_1, \ldots, a_n \text{ are distinct elements of } A \right\},$$

we have the inequality

$$|S(A)| \geqslant \min\left\{ p(F),\ (|A| - n)\frac{n(n+1)}{2} + \frac{n(n^2-1)}{6} + 1 \right\}.$$

Remark. It is not difficult to see that when $n \neq 3$ we have

$$\left\{ \sum_{k=1}^{n} k\tau(k) : \ \tau \in S_n \right\} = \left\{ \frac{n(n+1)(n+2)}{6}, \ldots, \frac{n(n+1)(2n+1)}{6} \right\}$$

and the cardinality of this set is $\frac{n(n^2-1)}{6} + 1$. If we replace the field F by a finite group G with $|G| > 1$, and replace $p(F)$ by the least prime divisor $p(G)$ of $|G|$, then the modified version of the conjecture might still hold.

From the viewpoint of graph theory

In graph theory, given a graph with n vertices $v_1, \ldots, v_n$ and given a set A_i of colors for each vertex v_i, a *proper list coloring* is a choice function that maps every vertex v_i to a color a_i in the list A_i, such that no two adjacent vertices receive the same color. Thus, sumsets with distinct summands are related to list colorings of complete graphs.

For a subset A of an additive group G, obviously

$$2^{\wedge}A = \{a_1 + a_2 : \ a_1, a_2 \in A \text{ and } a_1 \neq a_2\}$$

and

$$3^{\wedge}A = \{a_1 + a_2 + a_3 : \ a_1, a_2, a_3 \in A \text{ and } a_1 \neq a_2 \neq a_3 \neq a_1\}.$$

This reminds us linear and circular permutations. Thus, it is natural to consider restricted sumsets related to list colorings of paths and cycles instead of complete graphs.

Two new kinds of restricted sumsets

In 2022 the speaker [OEIS A357130] introduced two new kinds of sumsets. Namely, for finite subsets $A_1, \ldots, A_n$ of an additive group G, Sun defined

$$L(A_1, \ldots, A_n) = \{a_1 + \cdots + a_n : \ a_i \in A_i, \text{ and } a_1 \neq a_2 \neq a_3 \neq \cdots \neq a_n\}$$

and

$$C(A_1, \ldots, A_n) = \{a_1 + \cdots + a_n : \ a_i \in A_i, \ a_1 \neq a_2 \neq a_3 \neq \cdots \neq a_n \neq a_1\}.$$

Note that

$$L(A_1, A_2) = C(A_1, A_2) = A_1 \dot{+} A_2, \text{ and } C(A_1, A_2, A_3) = A_1 \dot{+} A_2 \dot{+} A_3.$$

When $A_1 = \cdots = A_n = A$, we simply write $n\tilde{}A$ to denote $L(A_1, \ldots, A_n)$, and $n^{\circ}A$ to denote $C(A_1, \ldots, A_n)$.

A general conjecture

Conjecture (Z.-W. Sun, 2022-09-13). Let G be an additive group with $|G| > 1$, and let $A_1, \ldots, A_n$ $(n > 1)$ be finite subsets of G with $|A_i| > 1$ for all $i = 1, \ldots, n$. Then

$$|L(A_1, \ldots, A_n)| \geqslant \min\{p(G), |A_1| + \cdots + |A_n| - 2n + 1 + \{n\}_2\}$$

and

$$|C(A_1, \ldots, A_n)| \geqslant \min\{p(G), |A_1| + \cdots + |A_n| - 2n + (-1)^n(1 + \{n\}_2)\},$$

where $\{n\}_2$ denotes the least nonnegative residue of n modulo 2.

This conjecture is motivated by the following observation: For any integer $n > 1$ and $A = \{0, \ldots, k-1\}$ with $k \in \mathbb{Z}^+$, we have

$$|n\tilde{}A| = n|A| - 2n + 1 + \{n\}_2$$

and

$$|n^\circ A| = n|A| - 2n + (-1)^n(1 + \{n\}_2).$$

Joint work with Han Wang

In a paper [arXiv:2210.12044] joint with the speaker's student Han Wang, we prove the following results.

Theorem 1. Let n be any positive *even* integer, and let $A_1, \ldots, A_n$ be subsets of a field F with $|A_1| = \cdots = |A_n| \geqslant 2$. Suppose that $p(F) > \sum_{i=1}^n |A_i| - 2n$. Then

$$|L(A_1, \ldots, A_n)| \geqslant |C(A_1, \ldots, A_n)| \geqslant \sum_{i=1}^n |A_i| - 2n + 1.$$

Theorem 2. Let n be any positive *odd* integer, and let $A_1, \ldots, A_n$ be subsets of a field F with $|A_1| = \cdots = |A_n| \geqslant 2$. Suppose that $p(F) > \sum_{i=1}^n |A_i| - 2n + 1$. Then $|L(A_1, \ldots, A_n)| \geqslant \sum_{i=1}^n |A_i| - 2n + 2$.

Key Identities: Let n be a positive integer. If n is even, then

$$[x_1^k \ldots x_n^k](x_1 - x_2) \cdots (x_{n-1} - x_n)(x_n - x_1)(x_1 + \cdots + x_n)^{(k-1)n} = \frac{((k-1)n)!}{k!^n} 2k^{n/2}.$$

If n is odd, then

$$[x_1^k \cdots x_n^k](x_1 - x_2) \cdots (x_{n-1} - x_n)(x_1 + \cdots + x_n)^{(k-1)n+1} = \frac{((k-1)n+1)!}{(k!)^n} \times k^{\frac{n-1}{2}}.$$

Main References

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

2. S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, *Transversals of additive Latin squares*, Israel J. Math. **126** (2001), 17–28.

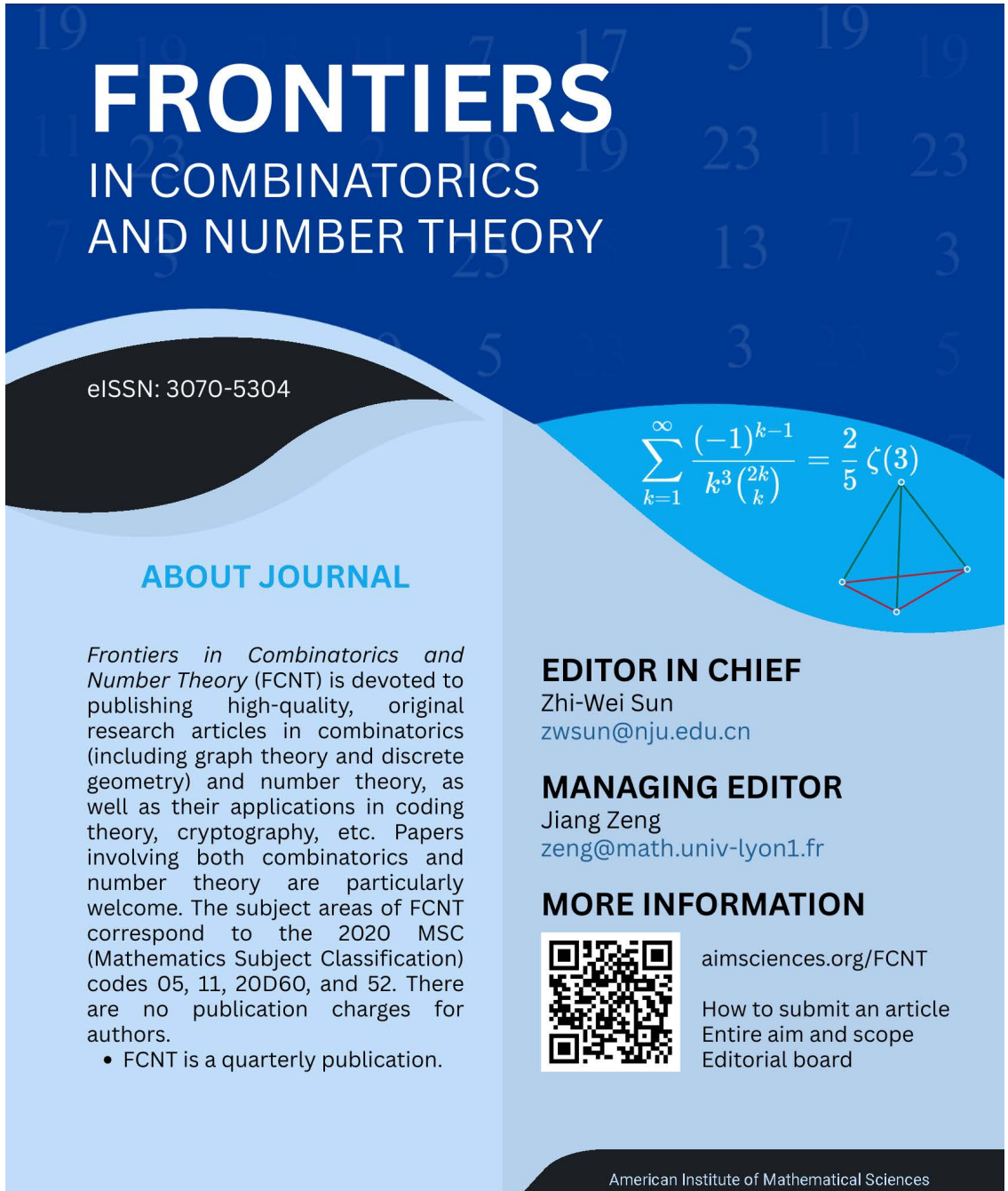
3. Zhi-Wei Sun, *A survey of problems and results on restricted sumsets*, in: Number Theory (S. Kanemitsu & J.-Y. Liu, eds.), World Sci., Singapore, 2007, pp. 190–213.

4. Zhi-Wei Sun, *An additive theorem and restricted sumsets*, Math. Res. Lett. **15** (2008), 1263–1276.

5. Han Wang and Zhi-Wei Sun, *On two new kinds of restricted sumsets*, arXiv:2210.12044, 2022.

Thank you!

Frontiers in Combinatorics and Number Theory



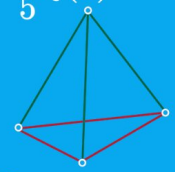
Frontiers in Combinatorics and Number Theory

FRONTIERS IN COMBINATORICS AND NUMBER THEORY

EDITORIAL BOARD

eISSN: 3070-5304

$$\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^3 \binom{2k}{k}} = \frac{2}{5}\zeta(3)$$



Editorial Board

EDITOR IN CHIEF

Zhi-Wei Sun
zwsun@nju.edu.cn

MANAGING EDITOR

Jiang Zeng
zeng@math.univ-lyon1.fr

MORE INFORMATION

aimsciences.org/FCNT

How to submit an article
Entire aim and scope
Editorial board