An on-line talk (July 31, 2020)

On Restricted Sumsets

Zhi-Wei Sun

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

July 31, 2020

Abstract

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

Part I. Combinatorial Nullstellensatz and the ANR Theorem

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 over $\mathbb{Z}$

For subsets $A_1, \ldots, A_n$ of an additive abelian group, their *sumset* is

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

We denote this by nA if $A_1 = \ldots = A_n = A$.

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 $|A + B| \geqslant |A| + |B| - 1$. $\square$

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

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

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 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

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

Via the Combinatorial Nullstellensatz, the ANR theorem reduces to

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

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

Another Lemma

As usual, we let $(x)_0 = 1$ and $(x)_n = x(x-1)\cdots(x-n+1)$ for $n = 1, 2, 3, \ldots$.

Lemma (Q.-H. Hou and Z.-W. Sun [Acta Arith. 102(2002)]; Z.-W. Sun and Y.-N. Yeh [J. Number Theory 114(2005)]). Let

$$P(x_1, \ldots, x_n) = \sum_{\substack{j_1, \ldots, j_n \geqslant 0 \\ j_1 + \cdots + j_n = m}} c_{j_1, \ldots, j_n} x_1^{j_1} \cdots x_n^{j_n} \in \mathbb{C}[x_1, \ldots, x_n]$$

and

$$P^*(x_1, \ldots, x_n) = \sum_{\substack{j_1, \ldots, j_n \geqslant 0 \\ j_1 + \cdots + j_n = m}} c_{j_1, \ldots, j_n} (x_1)_{j_1} \cdots (x_n)_{j_n}.$$

Suppose that $0 \leqslant \deg P \leqslant k_1 + \cdots + k_n$ where $k_1, \ldots, k_n$ are nonnegative integers. Then

$$[x_1^{k_1} \cdots x_n^{k_n}] P(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^{k_1 + \cdots + k_n - \deg P}$$

coincides with

$$\frac{(\sum_{i=1}^n k_i - \deg P)!}{k_1! \cdots k_n!} P^*(k_1, \ldots, k_n).$$

Proof of the Lemma

Proof. Let $K = k_1 + \cdots + k_n - \deg P$. Then

$$
\begin{aligned}
&[x_1^{k_1} \cdots x_n^{k_n}] P(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^K \\
=&[x_1^{k_1} \cdots x_n^{k_n}] \sum_{\substack{j_1, \ldots, j_n \geqslant 0 \\ j_1 + \cdots + j_n = m}} c_{j_1, \ldots, j_n} x_1^{j_1} \cdots x_n^{j_n} \sum_{\substack{i_1, \ldots, i_n \geqslant 0 \\ i_1 + \cdots + i_n = K}} K! \frac{x_1^{i_1} \cdots x_n^{i_n}}{i_1! \cdots i_n!} \\
=&K! \sum_{\substack{j_1, \ldots, j_n \geqslant 0 \\ j_1 + \cdots + j_n = m}} c_{j_1, \ldots, j_n} \frac{(k_1)_{j_1} \cdots (k_n)_{j_n}}{k_1! \cdots k_n!} \\
=&\frac{K!}{k_1! \cdots k_n!} P^*(k_1, \ldots, k_n).
\end{aligned}
$$

This concludes the proof.

Proof of the ANR result

According to this lemma, the ANR result

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

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

reduces to

$$P^*(k_1,\ldots,k_n)=\prod_{1\leqslant i<j\leqslant n}(k_j-k_i),$$

where

$$P(x_1,\ldots,x_n)=\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)=|x_i^{j-1}|_{1\leqslant i,j\leqslant n}=\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\prod_{i=1}^n x_i^{\sigma(i)-1}.$$

Note that

$$P^*(x_1,\ldots,x_n)=\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\prod_{i=1}^n(x_i)_{\sigma(i)-1}=|(x_i)_{j-1}|_{1\leqslant i,j\leqslant n}.$$

Polynomials of degree not exceeding n

$$V_n = \{P(x) \in \mathbb{C}[x] : \ \deg P \leqslant n\}$$

is a vector space over the complex field $\mathbb{C}$ of dimension $n+1$ with a base $x^0, x, \ldots, x^n$. If $P_j(x) \in \mathbb{C}[x]$ and $\deg P_j(x) = j$ for all $j = 0, \ldots, n$, then

$$\sum_{j=0}^{n} c_j P_j(x) = 0 \Rightarrow c_n = 0 \text{ and } \sum_{j=0}^{n-1} c_j P_j(x) = 0$$

$$\Rightarrow c_n = c_{n-1} = 0 \text{ and } \sum_{j=0}^{n-2} c_j P_j(x) = 0$$

$$\Rightarrow \ldots$$

$$\Rightarrow c_n = c_{n-1} = \ldots = c_0 = 0.$$

So $P_0(x), P_1(x), \ldots, P_n(x)$ are linear independent over $\mathbb{C}$ and hence they form a base of V_n.

Complete the proof via Stirling numbers

Both $1, x, \ldots, x^n$ and $(x)_0, (x)_1, \ldots, (x)_n$ are bases of V_n. Actually,

$$(x)_n = \sum_{k=0}^{n} (-1)^{n-k} s(n,k) x^k \text{ and } x^n = \sum_{k=0}^{n} S(n,k)(x)_k$$

for all $n = 0, 1, 2, \ldots$, where $s(n,k)$ $(0 \leqslant k \leqslant n)$ are Stirling numbers of the first kind, and $S(n,k)$ $(0 \leqslant k \leqslant n)$ are Stirling numbers of the second kind.

Combinatorial Interpretation of $s(n,k)$: The number of permutations $\sigma \in S_n$ which are products of exactly k disjoint permutation cycles.

Combinatorial Interpretation of $S(n,k)$: The number of ways to partition a set of cardinality n into k disjoint nonempty parts.

For $P(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i) = |x_i^{j-1}|_{1 \leqslant i,j \leqslant n}$, we have

$$P^*(x_1, \ldots, x_n) = |(x_i)_{j-1}|_{1 \leqslant i,j \leqslant n} = |x_i^{j-1}|_{1 \leqslant i,j \leqslant n} = \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i).$$

ANR Theorem implies the Dias da Silva-Hamidoune Theorem

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

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

Proof. The case $|A| < n$ is trivial. Below we assume $|A| \geqslant n$. Let $k = |A|$ and $A_n = A$. Choose subsets $A_{n-1}, \ldots, A_1$ with

$$|A_{n-1}| = k-1,\ |A_{n-2}| = k-2,\ \ldots,\ |A_1| = k-n+1.$$

Applying the ANR theorem, we get

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

Part II. Our Work after ANR

During my visit to Nankai Univ.

The Dias da Silva-Hamidoune Theorem states that for any finite subset A of a field F we have $|n^{\wedge}A| \geqslant \min\{p(F),\ n|A| - n^2 + 1\}$. During my visit to the Center of Combinatorics at Nakai Univ. (March-August 1999), I thought that for any k-subsets $A_1, \ldots, A_n$ of a field F we should have

$$|A_1 \dot{+} \ldots \dot{+} A_n| \geqslant \min\{p(F), kn - n^2 + 1\}.$$

Could I prove this via the polynomial method? For this purpose, I need to determine in the case $k \geqslant n$ the coefficient

$$c_n(k) = [x_1^{k-1} \ldots x_n^{k-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)^2 \times (x_1 + \ldots + x_n)^{kn-n^2}.$$

I was forced to use $\prod_{1 \leqslant i < j \leqslant n}(x_j - x_i)^2$ instead of $\prod_{1 \leqslant i < j \leqslant n}(x_j - x_i)$ because $2 \times \frac{n(n-1)}{2} + (kn - n^2) = (k-1)n$.

During my visit to Nankai Univ.

Observe that

$$\begin{aligned} c_n(n) =& [x_1^{n-1} \cdots x_n^{n-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)^2 \\ =& [x_1^{n-1} \cdots x_n^{n-1}] (|x_j^{i-1}|_{1 \leqslant i,j \leqslant n})^2 \\ =& [x_1^{n-1} \cdots x_n^{n-1}] \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{j=1}^{n} x_j^{\sigma(j)-1} \sum_{\tau \in S_n} \operatorname{sign}(\tau) \prod_{j=1}^{n} x_j^{\tau(j)-1} \\ =& \sum_{\sigma \in S_n} \operatorname{sign}(\sigma)\operatorname{sign}(\sigma') = \sum_{\sigma \in S_n} (-1)^{\binom{n}{2}} = (-1)^{n(n-1)/2} n! \end{aligned}$$

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

A conjecture on $c_n(k)$

To understand $c_n(k)$, on June 2-3, 1999 via computation I found that

$$\begin{aligned} c_2(k) =& [x_1^{k-1}x_2^{k-1}](x_2-x_1)^2(x_1+x_2)^{2k-4} = -2\frac{(2k-4)!}{(k-1)!(k-2)!}, \\ c_3(k) =& [x_1^{k-1}x_2^{k-1}x_3^{k-1}](x_2-x_1)^2(x_3-x_1)^2(x_3-x_2)^2(x_1+x_2+x_3)^{3k-9} \\ =& -12\frac{(3k-9)!}{(k-1)!(k-2)!(k-3)!}. \end{aligned}$$

On June 4, 1999 I conjectured that for $k \geqslant n \geqslant 0$ we have

$$c_n(k) = (-1)^{n(n-1)/2}(kn-n^2)!\frac{1!\ldots n!}{(k-1)!\ldots(k-n)!}.$$

At that time, I already noted that $c_n(n) = (-1)^{n(n-1)/2}n!$.

I told this conjecture to Qing-Hu Hou (a PhD student of William Y.-C. Chen) and we jointly studied this conjecture.

Dyson's Conjecture

Hou first showed that $c_n(n) = (-1)^{n(n-1)/2} n!$. Though I showed this by multiplication of two Vandermonde-type determinants, I did not tell this to Hou. Rather to my surprise, Hou got the value of $c_n(n)$ from a confirmed conjecture of F. Dyson.

F. J. Dyson's Conjecture (posed in 1962 and confirmed by J. Gunson and K. G. Wilson in 1962). Let $m_1, \ldots, m_n \in \mathbb{N}$. Then the constant term of the expansion of

$$\prod_{\substack{i,j=1 \\ i \neq j}}^{n} \left(1 - \frac{x_i}{x_j}\right)^{m_i}$$

is the multi-nomial coefficient $\binom{m_1,\ldots,m_n}{m_1,\ldots,m_n} = \frac{(m_1+\ldots+m_n)!}{m_1!\ldots m_n!}$.

Dyson's Conjecture in the case $m_1 = \ldots = m_n = m$ yields

Corollary. For $m \in \mathbb{N}$ and $n \in \mathbb{Z}^+$ we have

$$[x_1^{m(n-1)} \ldots x_n^{m(n-1)}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)^{2m} = (-1)^{mn(n-1)/2} \frac{(mn)!}{m!^n}.$$

Embarrassment

In August 1999, we finally proved my conjecture on $c_n(k)$ and applied it to show that for any k-subsets $A_1, \ldots, A_n$ of a field F we have

$$|A_1 \dot{+} \ldots \dot{+} A_n| \geqslant \min\{p(F), kn - n^2 + 1\}.$$

After the initial version of this paper was finished, I suddenly realized that this result also follows from the ANR Theorem. In fact, when $|A_i| = k \geqslant n$ we may choose $A_i' \subseteq A_i$ with $|A_i'| = k - n + i$. By the ANR Theorem,

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

This made me very embarrassed! Should we give up the paper?

Restricted Differences

Let $k \geqslant n \geqslant 0$ be integers. Recall that

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

$$= c_n(k) = (-1)^{n(n-1)/2}(kn-n^2)! \frac{1! \dots n!}{(k-1)! \dots (k-n)!}.$$

For $i, j \in \{1, \dots, n\}$ with $i \neq j$ let d_{ij} be an element of a field F. Then

$$[x_1^{k-1} \dots x_n^{k-1}](x_1 + \dots + x_n)^{kn-n^2} \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i + d_{ij})(x_j - x_i - d_{ji})$$

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

$$= (-1)^{n(n-1)/2}(kn-n^2)! \frac{1! \dots n!}{(k-1)! \dots (k-n)!}.$$

For k-subsets $A_1, \dots, A_n$ of F, we may get a lower bound for

$$|\{a_1 + \dots + a_n : \ a_1 \in A_1, \dots, a_n \in A_n, \ a_i - a_j \neq d_{ij} \text{ if } i \neq j\}|.$$

Restricted Differences

Let F be a field and let $A_1, \ldots, A_n$ be k-subsets of F. For $1 \leqslant i < j \leqslant n$ let S_{ij} be a subset of F with $|S_{ij}| = 2m$. We may study the restricted sumset

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

To get a lower bound for $|C|$ via the polynomial method, we need to determine

$$[x_1^{k-1} \ldots x_n^{k-1}] \prod_{1 \leqslant i < j \leqslant n} \prod_{s \in S_{ij}} (x_i - x_j - s) \times (x_1 + \ldots + x_n)^{(k-1-m(n-1))n}$$

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

This is $c_n(k)$ if $m = 1$. So we need to extend our formula for $c_n(k)$.

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

A linear operator

Hou and Sun defined a linear operator $\mathcal{L} : \mathbb{Q}[x_1, \ldots, x_n] \to \mathbb{Q}[x]$ by $\mathcal{L}(x_1^{j_1} \ldots x_n^{j_n}) = (x)_{j_1} \ldots (x)_{j_n}$. Thus, for

$$P(x_1, \ldots, x_n) = \sum_{j_1, \ldots, j_n} c_{j_1, \ldots, j_n} x_1^{j_1} \ldots x_n^{j_n} \in \mathbb{Q}[x_1, \ldots, x_n],$$

we have

$$\mathcal{L}(P(x_1, \ldots, x_n)) = \sum_{j_1, \ldots, j_n} c_{j_1, \ldots, j_n} (x)_{j_1} \ldots (x)_{j_n} = P^*(x, \ldots, x).$$

Let $f_m(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)^{2m}$. By a previous lemma,

$$\begin{aligned}
&[x_1^{k-1} \ldots x_n^{k-1}] f_m(x_1, \ldots, x_n)(x_1 + \ldots + x_n)^{(k-1-m(n-1))n} \\
=&\frac{((k-1-m(n-1))n)!}{(k-1)!^n} f_m^*(k-1, \ldots, k-1) \\
=&\frac{((k-1-m(n-1))n)!}{(k-1)!^n} \mathcal{L}(f_m)(k-1).
\end{aligned}$$

Joint work with Q.-H. Hou

In view of the above, we reduce the desired result to

$$\mathcal{L}(f_m)(x) = (-1)^{\frac{mn(n-1)}{2}} \frac{m!(2m)!\dots(nm)!}{(m!)^n}(x)_0(x)_m\dots(x)_{(n-1)m}.$$

To prove this, we take three steps.

Step I. Prove that $\prod_{j=0}^{n-1}(x)_{jm} \mid \mathcal{L}(f_m)(x)$.

Step II. Show that $\deg \mathcal{L}(f_m) \leqslant m\binom{n}{2}$. (Need several lemmas.)

Step III. Determine the constant c with

$$\mathcal{L}(f_m)(x) = c(x)_0(x)_m\dots(x)_{(n-1)m}.$$

via the identity

$$[x_1^{m(n-1)}\dots x_n^{m(n-1)}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{2m} = (-1)^{mn(n-1)/2}\frac{(mn)!}{m!^n}.$$

Joint work with J.-X. Liu

In July 2000, I thought that we may study the restricted sumset

$$C = \{a_1 + \ldots + a_n : \ a_1 \in A_1, \ldots, a_n \in A_n, \ P(a_i) \neq P(a_j) \text{ if } i \neq j\},$$

where A_i is a subset of field F and $P(x)$ is a polynomial of degree m over F. For this purpose, in view of the polynomial method, we should compute

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

ANR computed this when $m = 1$ and $k_1 < \ldots < k_n$. In 2000 I asked my graduate student Jian-Xin Liu to express the value of c as a product in the case $k_1 < \ldots < k_n$.

Let $P_m(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (x_j^m - x_i^m)$. We need to express

$$P_m^*(x_1, \ldots, x_n) = |x_j^{(i-1)m}|_{1 \leqslant i,j \leqslant n}^* = |(x_j)_{(i-1)m}|_{1 \leqslant i,j \leqslant n}$$

in a product form.

Joint work with J.-X. Liu

Liu told me that in the case $n = 2$,

$$P_m^*(x_1, x_2) = \begin{vmatrix} 1 & 1 \\ (x_1)_m & (x_2)_m \end{vmatrix} = (x_2)_m - (x_1)_m$$

cannot be written as a product form. Then I observed that

$$\begin{vmatrix} 1 & 1 \\ (x)_m & (x+1)_m \end{vmatrix} = (x+1)_m - (x)_m = mx(x-1)\dots(x-m+2).$$

This led me to conjecture that

$$|(x+j)_{im}|_{0\leqslant i,j\leqslant n-1} = 1!\dots(n-1)!m^{n(n-1)/2}\prod_{j=0}^{n-1}(x+j)_{(n-1-j)(m-1)},$$

equivalently,

$$\left|\binom{x+j}{im}\right|_{0\leqslant i,j\leqslant n-1} = m^{n(n-1)/2}\prod_{r=0}^{n-1}\frac{\binom{x+n-1-r}{(m-1)r}}{\binom{mr}{r}}.$$

Then, I asked J.-X. Liu to prove this by induction on n.

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

Joint work with Y.-N. Yeh

Z. W. Sun and Y. N. Yeh [J. Number Theory 114(2005)]: If $k, m, n \in \mathbb{Z}^+$ and $k-1 \geqslant m(n-1)$, then

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

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

Theorem (Sun and Yeh [J. Number Theory 114(2005)]). Let $m, n \in \mathbb{Z}^+$ and let S_{ij} be a $(2m-1)$-subset of F for $1 \leqslant i < j \leqslant n$. Let $k \in \mathbb{Z}$ with $k-1 \geqslant m(n-1)$, and let $A_i \subseteq F$ and $|A_i| = k-n+i$ for all $i = 1, \ldots, n$. If $p(F)$ is greater than $\max\{mn, (k-1-m(n-1))n\}$, 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 $|C| \geqslant (k-1-m(n-1))n+1$.

Joint work with H. Pan

Given two finite subsets A and B of a field F and a general $P(x,y) \in F[x,y]$, what can we say about the cardinality of the restricted sumset $\{a+b\colon a \in A,\ b \in B,\ \text{and } P(a,b) \neq 0\}$?

Lemma (H. Pan and Z. W. Sun [JCTA 100(2002)]). Let $P(x)$ be a polynomial over a field F. Let $\bar{F}$ be the algebraic closure of the field F and $m_P(\alpha)$ be the multiplicity of $\alpha \in \bar{F}$ as a root of $P(x)=0$ over $\bar{F}$. Suppose that there exist non-negative integers $k<l$ such that $[x^i]P(x)=0$ for all i with $k<i<l$. Then either $x^l \mid P(x)$, or $\deg P(x) \leqslant k$, or $N_q(P) \geqslant l-k$ for some integer $q \in \mathcal{P}(p)$, where $p=p(F)$, $\mathcal{P}(p)$ is $\{1\}$ or $\{p^n :\ n \in \mathbb{N}\}$ according as $p(F)=\infty$ or not,

$$N_q(P) = q|\{\alpha \in \bar{F}\setminus\{0\}\colon m_P(\alpha) \geqslant q\}| - \sum_{\alpha\in\bar{F}\setminus\{0\}} \{m_P(\alpha)\}_q$$

and $\{m\}_q$ is the least nonnegative residue of $m \in \mathbb{Z}$ modulo q.

Remark. $N_1(P)$ is the number of distinct roots in $\bar{F}\setminus\{0\}$ of the equation $P(x)=0$ over $\bar{F}$.

Joint work with H. Pan

H. Pan and Z. W. Sun [JCTA 100(2002)]: Let A and B be two finite nonempty subsets of a field F. Furthermore, let $P(x,y)$ be a polynomial over F of degree $d=\deg P(x,y)$ such that for some $i<|A|$ and $j<|B|$ we have $[x^iy^{d-i}]P(x,y)\neq 0$ and $[x^{d-j}y^j]P(x,y)\neq 0$. Define $P_0(x,y)$ to be the homogeneous polynomial of degree d such that $P(x,y)=P_0(x,y)+R(x,y)$ for some $R(x,y)\in F[x,y]$ with $\deg R(x,y)<d$, and put $P^*(x)=P_0(x,1)$. For any α in the algebraic closure $\bar{F}$ of F, let $m_{P^*}(\alpha)$ denote the multiplicity of α as a zero of $P^*(x)$. Then

$$\begin{aligned}&|\{a+b\colon a\in A,\ b\in B,\ \text{and } P(a,b)\neq 0\}|\\ &\geqslant \min\{p-m_{P^*}(-1),\ |A|+|B|-1-d-N(P^*)\},\end{aligned}$$

where $p=p(F)$ and

$$N(P^*)=\max_{q\in\mathcal{P}(p)} q|\{\alpha\in\bar{F}\setminus\{0,-1\}:\ m_{P^*}(\alpha)\geqslant q\}|.$$

A corollary

Corollary (H. Pan and Z.-W. Sun [JCTA 100(2002)]). Let F be a field with $p = p(F) \neq 2$, and let A, B and S be finite non-empty subsets of F. Then

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

where q is the largest element of $\mathcal{P}(p)$ not exceeding $|S|$.

Sumsets with general 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.

We prove the theorem by using the polynomial method **twice**!

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 $p(F) \geqslant n(3n-5)/2$.

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

Theorem (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 $\mathbb{C}^*$.

Main References:

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

2. Qing-Hu Hou and Z.-W. Sun, *Restricted sums in a field*, Acta Arith. **102** (2002), 239–249.

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

Thank you!