A talk given at Zhejiang University (March 25, 2011)

On Weighted Extension of the Erdős-Heilbronn Conjecture

Zhi-Wei Sun

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

March 25, 2011

Part A.
The Erdős-Heilbronn Conjecture

Sumsets and Restricted Sumsets

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

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

and

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

When $A_1 = \cdots = A_n = A$,

$$nA = A_1 + \cdots + A_n \quad \text{and} \quad n^{\wedge}A = A_1 \dot{+} \cdots \dot{+} A_n.$$

Note that

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

Sumsets over $\mathbb{Z}$

For $A = [0, k-1] = \{0, 1, \ldots, k-1\}$ and $B = [0, l-1]$ we have

$$|A + B| = |[0, k + l - 2]| = k + l - 1 = |A| + |B| - 1$$

and

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

For general finite subsets A and B of $\mathbb{Z}$, by construction one can show

$$|A + B| \geq |A| + |B| - 1 \quad \text{and} \quad |n^{\wedge}A| \geq n|A| - n^2 + 1.$$

Cauchy-Davenport Theorem

Cauchy-Davenport Theorem $(1813, 1935)$. Let p be a prime and let $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{a} = a + p\mathbb{Z} : \ a \in \mathbb{Z}\}$. For $A, B \subseteq \mathbb{Z}_p$ we have

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

Remark. By induction, if $A_1, \cdots, A_n \subseteq \mathbb{Z}_p$ then

$$|A_1 + \cdots + A_n| \geqslant \min\{p, \ |A_1| + \cdots + |A_n| - 1\}.$$

Erdős-Heilbronn Conjecture

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

Erdős-Heilbronn Conjecture

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

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!

Alon-Nathanson-Ruzsa Theorem

Alon-Nathanson-Ruzsa Theorem (1996). For finite nonempty subsets $A_1, \ldots, A_n$ of a field F with $|A_1| < \cdots < |A_n|$, we have

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

Method: The polynomial method via Combinatorial Nullstellensatz.

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

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

Alon's Combinatorial Nullstellensatz

Combinatorial Nullstellensatz [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

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

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.
Corollary. 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 $0 \leqslant k_i < |A_i|$ for $i = 1, \ldots, n$, 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

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

Via Combinatorial Nullstellensatz, the ANR theorem reduces to

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

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

Q. H. Hou and Z. W. Sun (2002) studied the restricted sumset

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

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 (2005) determined

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

A Result of Liu and Sun

J. X. Liu and Z. W. Sun (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

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

A Recent Result of Balandraud

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 recently obtained the following result on subset sums.

Balandraud [2009, arXiv:0907.3492]. 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 (Erdős-Selfridge conjecture). 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, 2003].

Let $A_1, \ldots, A_n$ be finite subsets of a field F with cardinality $k > m(n-1)$. Suppose that $p(F) > \max\{n, (k-1)n - (m+1)\binom{n}{2}\}$. 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: 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 $A \dot{+} B$.

Part B.
On Weighted extension of the Erdős-Heilbronn Conjecture

Weighted 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. 2008]. Let $a_1, \ldots, a_n$ be nonzero elements of a field F with $p(F) \neq n+1$. Then, for any finite $A \subseteq F$ we have

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

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

Z. W. Sun and D. M. Zhu: The conjecture holds if

$$\mathrm{per}((a_j^{i-1})_{1\leqslant i,j\leqslant n}) = \sum_{\sigma\in S_n}\prod_{i=1}^{n} a_{\sigma(i)}^{i-1} \neq 0.$$

Linear extension of the Erdős-Heilbronn conjecture

THEOREM (Z. W. Sun and L. L. Zhao, J. Combin. Theory Ser. A 119(2012), 364-381). The conjecture (posed by Sun) holds if $p(F) \geqslant n(3n-5)/2$.

Remark. Sun and Zhao also noted that the conjecture holds for $n = 3$.
The theorem follows from the next two results of Sun and Zhao.

Theorem 1 (Z. W. Sun & L. L. Zhao). Let $n > 0$ be an 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

$$A_i \subseteq F, \quad \text{and} \quad |A_i| \geqslant 2n-2 \text{ for } i = 1, \ldots, n.$$

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

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

Linear extension of the Erdős-Heilbronn conjecture

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.

Theorem 2. (Z. W. Sun & L. L. Zhao) 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

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

Deducing the Theorem from Theorems 1 and 2

Proof of the Theorem. Note that

$$\{a_1x_1 + \cdots + a_nx_n : \ x_1, \ldots, x_n \in A, \text{ and } x_i \neq x_j \text{ if } i \neq j\}$$
$$= \left\{ y_1 + \cdots + y_n : \ y_i \in A_i = a_iA, \text{ and } \prod_{1 \leqslant i < j \leqslant n} (a_j^{-1}y_j - a_i^{-1}y_i) \neq 0 \right\}.$$

If $p(F) - \binom{n}{2} \geqslant n|A| - n^2 + 1$, then it suffices to apply Theorem 2.

Now assume that $p(F) - \binom{n}{2} \leqslant n|A| - n^2$. Then

$$n|A| \geqslant p(F) - \binom{n}{2} + n^2 \geqslant \frac{3n^2 - 5n}{2} - \frac{n^2 - n}{2} + n^2 = 2n^2 - 2n$$

and hence $|A| \geqslant 2n - 2$. Note also that if $n > 1$ then $p(F) \geqslant n(3n-5)/2 \geqslant (n-1)^2$. Thus, by applying Theorem 1 we obtain the desired result.

Proof of Theorem 2

To avoid triviality, just assume that

$$p(F) > \deg P \quad \text{and} \quad \sum_{i=1}^{n} |A_i| \geqslant n + 2\deg P.$$

Write

$$P(x_1, \ldots, x_n) = \sum_{\substack{j_1,\ldots,j_n \geqslant 0 \\ j_1+\cdots+j_n \leqslant \deg P}} c_{j_1,\ldots,j_n} x_1^{j_1} \cdots x_n^{j_n} \quad \text{with } c_{j_1,\ldots,j_n} \in F,$$

and define

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

Proof of Theorem 2

Observe that

$$
\begin{aligned}
&[x_1^{k_1}\cdots x_n^{k_n}]P^*(x_1,\ldots,x_n)\\
=&\sum_{\substack{j_1,\ldots,j_n\geqslant 0\\ j_1+\cdots+j_n=\deg P}} c_{j_1,\ldots,j_n}[x_1^{k_1}\cdots x_n^{k_n}](x_1)_{j_1}\cdots(x_n)_{j_n}\\
=&\sum_{\substack{j_i\geqslant k_i \text{ for } i=1,\ldots,n\\ \sum_{i=1}^n j_i=\sum_{i=1}^n k_i}} c_{j_1,\ldots,j_n}[x_1^{k_1}\cdots x_n^{k_n}](x_1)_{j_1}\cdots(x_n)_{j_n}\\
=&c_{k_1,\ldots,k_n}=[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\ldots,x_n)\neq 0.
\end{aligned}
$$

Proof of Theorem 2

Let e denote the multiplicative identity of the field F. For each $i = 1, \ldots, n$, clearly the set

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

has cardinality $k_i + 1$ since $k_i \leqslant \deg P < p(F)$. Thus, by the Combinatorial Nullstellensatz, there are

$$m_1 \in [|A_1| - k_1 - 1, |A_1| - 1], \ \ldots, \ m_n \in [|A_n| - k_n - 1, |A_n| - 1]$$

such that

$$P^*(m_1 e, \ldots, m_n e) \neq 0.$$

Define

$$M = m_1 + \cdots + m_n - \deg P.$$

Clearly

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

Proof of Theorem 2

Observe that

$$[x_1^{m_1}\cdots x_n^{m_n}]P(x_1,\ldots,x_n)(x_1+\cdots+x_n)^M$$
$$=\sum_{\substack{j_1\in[0,m_1],\ldots,j_n\in[0,m_n]\\ j_1+\cdots+j_n=\deg P}}\frac{M!}{(m_1-j_1)!\cdots(m_n-j_n)!}c_{j_1,\ldots,j_n}$$

and thus

$$m_1!\cdots m_n![x_1^{m_1}\cdots x_n^{m_n}]P(x_1,\ldots,x_n)(x_1+\cdots+x_n)^M$$
$$=M!\sum_{\substack{j_1,\ldots,j_n\geqslant 0\\ j_1+\cdots+j_n=\deg P}}(m_1e)_{j_1}\cdots(m_ne)_{j_n}c_{j_1,\ldots,j_n}=M!P^*(m_1e,\ldots,m_ne).$$

Proof of Theorem 2

In the case $|C| \leqslant M < p(F)$, we have

$$[x_1^{m_1} \cdots x_n^{m_n}] P(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^{M-|C|} \prod_{c \in C} (x_1 + \cdots + x_n - c)$$

$$= [x_1^{m_1} \cdots x_n^{m_n}] P(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^{M} \neq 0,$$

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

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

which is impossible by the definition of C. Therefore, either

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

or

$$|C| \geqslant M + 1 \geqslant \sum_{i=1}^{n} |A_i| - n - 2 \deg P + 1.$$

By the above, if $p(F) > \sum_{i=1}^{n}(|A_i| - 1) - \deg P$ then we have

$$|C| \geqslant \sum_{i=1}^{n} |A_i| - n - 2\deg P + 1$$

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

In the case $p(F) \leqslant \sum_{i=1}^{n}(|A_i| - 1) - \deg P$, as $\sum_{i=1}^{n} k_i = \deg P$ there are $A_1' \subseteq A_1, \ldots, A_n' \subseteq A_n$ such that

$$|A_1'| > k_1, \ldots, |A_n'| > k_n, \text{ and } \sum_{i=1}^{n}(|A_i'|-1)-\deg P = p(F)-1 < p(F),$$

therefore

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

$$\geqslant \min\left\{p(F) - \deg P,\ \sum_{i=1}^{n} |A_i'| - n - 2\deg P + 1\right\}$$

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

Lemma 1

To prove Theorem 1 we need several technique lemmas.

Lemma 1. Let $a_1, \ldots, a_n$ be nonzero elements in a field F with $p(F) \neq 2$. Then, for some $\sigma \in S_n$ we have

$$a_{\sigma(2i-1)} + a_{\sigma(2i)} \neq 0 \quad \text{for all } 0 < i \leqslant \left\lfloor \frac{n}{2} \right\rfloor - \delta(a_1, \ldots, a_n),$$

where $\delta(a_1, \ldots, a_n) \in \{0, 1\}$ takes the value 1 if and only if there exists $a \in F^*$ such that $\{a_1, \ldots, a_n\} = \{a, -a\}$ and

$$|\{1 \leqslant i \leqslant n : \ a_i = a\}| \equiv |\{1 \leqslant i \leqslant n : \ a_i = -a\}| \equiv 1 \pmod 2.$$

Lemma 2

Lemma 2. Let $k_1, \ldots, k_n \in \mathbb{N}$ and $a_1, \ldots, a_n \in F^* = F \setminus \{0\}$, where F is a field with $p(F) \neq 2$. Set

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} (k_j - x_j)_{\sigma(j)-1} \, a_j^{\sigma(j)-1}$$

and let $\delta(a_1, \ldots, a_n)$ be as in Lemma 1. Then there are $m_1, \ldots, m_n \in \mathbb{N}$ not exceeding $\max\{2n-3, 0\}$ such that

$$m_1 + \cdots + m_n = \binom{n}{2} \quad \text{and} \quad f(m_1, \ldots, m_n) \neq 0,$$

if $\delta(a_1, \ldots, a_n) = 0$ or there are $1 \leqslant s < t \leqslant n$ with

$$a_s + a_t = 0, \;\; k_s + k_t \not\equiv 1 \pmod{p(F)}.$$

Lemma 3

Lemma 3 Let F be a field with $p(F) \neq 2$, and let $a_1, \ldots, a_n \in F^*$ $(n \geqslant 4)$ with $\delta(a_1, \ldots, a_n) = 1$. Suppose that

$$p(F) \geqslant \sum_{j=1}^{n} k_j - n^2 + n + 1$$

where $k_1, \ldots, k_n$ are integers not smaller than $2n - 3$. Then there are $1 \leqslant s < t \leqslant n$ such that

$$a_s + a_t = 0 \quad \text{and} \quad k_s + k_t \not\equiv 1 \pmod{p(F)},$$

unless $n = 4$ and there is a permutation $\sigma \in S_4$ such that

$$a_{\sigma(1)} = a_{\sigma(2)} = a_{\sigma(3)}, \quad k_{\sigma(1)} = k_{\sigma(2)} = k_{\sigma(3)} = 5$$

and $k_{\sigma(4)} = p(F) - 4$.

Lemma 4

Lemma 4. Let F be a field of prime characteristic with $p(F) = p > 7$ and let

$$a_1 = a_2 = a_3 = a \in F^* \quad \text{and} \quad a_4 = -a.$$

Let

$$k_1 = k_2 = k_3 = 5 \quad \text{and} \quad k_4 = p - 4.$$

Then there are $m_1, m_2, m_3, m_4 \in [0, 3]$ such that

$$m_1 + m_2 + m_3 + m_4 = \binom{4}{2} = 6$$

and

$$\sum_{\sigma \in S_4} \operatorname{sgn}(\sigma) \prod_{j=1}^{4} (k_j - m_j)_{\sigma(j)-1} \, a_j^{\sigma(j)-1} \neq 0.$$

Proof of Theorem 1

Set $A_i' = a_i A_i = \{a_i x_i : \ x_i \in A_i\}$ and $a_i' = a_i^{-1}$. Then

$$C = \{y_1 + \cdots + y_n : \ y_1 \in A_1', \ldots, y_n \in A_n', \text{ and } a_i' y_i \neq a_j' y_j \text{ if } i \neq j\}.$$

Below we let $n > 2$. Clearly $p(F) \geqslant (n-1)^2 > 2$. Define

$$N = \sum_{j=1}^{n} |A_j| - n^2.$$

We want to show that $|C| \geqslant \min\{p(F), N+1\}$.

Let's first assume that $p(F) > N$. Combining Lemmas 1-4, there are $m_1, \ldots, m_n \in [0, 2n-3]$ such that $m_1 + \cdots + m_n = \binom{n}{2}$ and

$$S = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} (|A_j'| - 1 - m_j)_{\sigma(j)-1} (a_j')^{\sigma(j)-1} \neq 0.$$

It suffices to deduce a contradiction under the assumption $|C| \leqslant N$.

Proof of Theorem 1

Let $P(x_1, \ldots, x_n)$ be the polynomial

$$\prod_{1 \leqslant i < j \leqslant n} (a'_j x_j - a'_i x_i) \times \prod_{j=1}^{n} x_j^{m_j} \times \prod_{x \in C} (x_1 + \cdots + x_n - c) \times (x_1 + \cdots + x_n)^{N - |C|}$$

Then $\deg P \leqslant \sum_{j=1}^{n} (|A'_j| - 1)$ and

$$\begin{aligned}
&[x_1^{|A'_1|-1} \cdots x_n^{|A'_n|-1}] P(x_1, \ldots, x_n) \\
&= \left[\prod_{j=1}^{n} x_j^{|A'_j|-1-m_j} \right] \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} (a'_j x_j)^{\sigma(j)-1} \times (x_1 + \cdots + x_n)^N \\
&= \sum_{\substack{\sigma \in S_n \\ \sigma(j) \leqslant |A'_j| - m_j \text{ for } j \in [1,n]}} \operatorname{sgn}(\sigma) \frac{N!}{\prod_{j=1}^{n} (|A'_j| - m_j - \sigma(j))!} \prod_{j=1}^{n} (a'_j)^{\sigma(j)-1}
\end{aligned}$$

and hence

$$\prod_{j=1}^{n}(|A_j'|-1-m_j)![x_1^{|A_1'|-1}\cdots x_n^{|A_n'|-1}]P(x_1,\ldots,x_n)=N!S\neq 0.$$

Thus, by the Combinatorial Nullstellensatz there are $y_1\in A_1',\ldots,y_n\in A_n'$ such that $P(y_1,\ldots,y_n)\neq 0$ which contradicts the definition of C.

Now we handle the case $p(F)\leqslant N$. Since

$$n(2n-2)-n^2\leqslant p(F)-1<\sum_{j=1}^{n}|A_j|-n^2,$$

we can choose $B_j\subseteq A_j$ with $|B_j|\geqslant 2n-2$ so that

$$M=\sum_{j=1}^{n}|B_j|-n^2=p(F)-1.$$

As $p(F)>M$, by the above we have

$$\begin{aligned}|C|\geqslant&|\{a_1x_1+\cdots+a_nx_n:\ x_1\in B_1,\ldots,x_n\in B_n,\text{ and } x_i\neq x_j \text{ if } i\neq j\}|\\ \geqslant&M+1=\min\{p(F),N\}.\end{aligned}$$

Thank you!