Problems and Results in Additive Combinatorics

Zhi-Wei Sun

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

August 2, 2010

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)

Section 1.
The Erdős-Heilbronn Conjecture and its Extensions

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 $A \dot{+} B$.

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

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

where

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

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

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

Linear extension of the Erdős-Heilbronn conjecture

Theorem (L. L. Zhao & Z. W. Sun, arxiv:0810.0467v2, 2009). The conjecture (posed by Sun) holds if $p(F) \geqslant n(3n-5)/2$.

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

Theorem. (L. L. Zhao & Z. W. Sun, arxiv:0810.0467v2, 2009) Let n be a positive integer, and let F be a field with $p(F) \geqslant (n-1)^2$. Let $a_1, \ldots, a_n \in F^* = F \setminus \{0\}$, and suppose that $A_i \subseteq F$ and $|A_i| \geqslant 2n-2$ for $i = 1, \ldots, n$. Then, for the set

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

we have

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

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. (L. L. Zhao & Z. W. Sun, arxiv:0810.0467v2, 2009) 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

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

On Value Sets of Polynomials

Let F be a field, and let

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

with $a_1,\ldots,a_n\in F^*=F\setminus\{0\}$ and $\deg g<k$.

Theorem [Z. W. Sun, Finite Fields Appl. 2008]. (i) For any nonempty subsets $A_1,\ldots,A_n$ we have

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

(ii) If $A_1,\ldots,A_n$ are finite subsets of F with $|A_i|\geqslant i$ for $i=1,\ldots,n$, and $n\leqslant k=\deg f$, then

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

A General Conjecture

Conjecture [Z. W. Sun, Finite Fields Appl. 2008]. If A is a finite subset of F with $|A| \geqslant n > k$ and $p(F) \neq n+1$, then

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

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

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

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

Section 2.
Snevily's Conjecture and the DKSS Conjecture

Snevily's Conjecture

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

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

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

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

Alon's Contribution

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 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, it suffices to prove

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

Obverse that

$$\begin{aligned} c =& [x_1^{k-1} \cdots x_k^{k-1}] \prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)^2 \\ =& [x_1^{k-1} \cdots x_k^{k-1}] (\det(x_j^{i-1})_{1 \leqslant i,j \leqslant k})^2 \\ =& [x_1^{k-1} \cdots x_k^{k-1}] \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \prod_{j=1}^{k} x_j^{\sigma(j)-1} \sum_{\tau \in S_k} \operatorname{sgn}(\tau) \prod_{j=1}^{k} x_j^{\tau(j)-1} \\ =& \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma') = \sum_{\sigma \in S_k} (-1)^{\binom{k}{2}} = k!(-1)^{\binom{k}{2}} \neq 0 \text{ (in } \mathbb{Z}_p). \end{aligned}$$

where $\sigma'(j) = k - \sigma(j) + 1$ for $j = 1, \ldots, n$.

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 $\mathbb{F}_{2^{\varphi(n)}}$.** Thus, it suffices to show that

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

Alternatively, one may also try to prove

$$\sum_{\sigma \in s_k} \operatorname{sgn}(\sigma) \prod_{1 \leqslant i < j \leqslant k} (a_{\sigma(j)} b_j - a_{\sigma(i)} b_i) \neq 0.$$

Remark. The condition that $|G|$ is odd can be replaced by the weaker condition that $b_1, \ldots, b_k$ have odd order (see, Z. W. Sun [J. Combin. Theory Ser. A 2003]).

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. 2008]. Let G be any additive abelian group with cyclic torsion subgroup, 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 all the sums $a_i + b_i + c_i$ $(1 \leqslant i \leqslant n)$ 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 does not hold for general abelian groups. It even fails for the Klein group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Conjecture [Z. W. Sun, Math. Res. Lett. 200]. Any $n \times n \times n$ Latin cube contains a Latin transversal.

The DKSS Conjecture

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

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

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

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

A Recent Result of Feng, Sun and Xiang

Theorem (T. Feng, Z. W. Sun & Q. Xiang, Israel J. Math., to appear). 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.

Key lemmas

Lemma 3 (Z. W. Sun, Trans. AMS 1996; Combinatorica, 2003) Let $\lambda_1, \ldots, \lambda_k$ be complex nth roots of unity. Suppose that

$$c_1\lambda_1 + \cdots + c_k\lambda_k = 0,$$

where $c_1, \ldots, c_k$ are nonnegative integers. Then $c_1 + \cdots + c_k$ can be written in the form $\sum_{p|n} px_p$, where the sum is over all prime divisors of n and the x_p are nonnegative integers.

Tools for the proof. Galois group of cyclotomic extension, Newton's identity for symmetric functions.

Recent progress on Snevily's conjecture

In 2008, Feng, Sun and Xiang noted Snevily's conjecture follows from their following conjecture.

Conjecture (Feng-Sun-Xiang, 2008) Let G be a finite abelian group, and let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ be two subsets of G with cardinality k. Let K be any field containing an element of multiplicative order $|G|$, and let $\hat{G}$ be the character group of all group homomorphisms from G to $K^* = K \setminus \{0\}$. Then there are $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j))_{1 \leqslant i,j \leqslant k}$ and $\det(\chi_i(b_j))_{1 \leqslant i,j \leqslant k}$ are both nonzero.

In 2010 Bodan Arsovski proved Snevily's conjecture fully! His paper will appear in *Israel J. Math.*

Some of Arsovski's ideas are similar to the Feng-Sun-Xiang approach to the DKSS conjecture and the Snevily conjecture. After reading Arsovski's preprint, G. Harcos, G. Károlyi and G. Kós [arXiv:1004.0253] simplified Arsovski's proof by **showing the Feng-Sun-Xiang conjecture**.

Section 3.
Some Other Conjectures

Another Conjecture of Snevily

Hall's Theorem [Proc. AMS, 1952]. Let $G = \{a_1, \ldots, a_n\}$ be an additive abelian group of order n and let $b_1, \ldots, b_n \in G$. Then there is a permutation $\pi \in S_n$ such that $a_1 + b_{\pi(1)}, \ldots, a_n + b_{\pi(n)}$ are distinct (i.e., $\{a_1 + b_{\pi(1)}, \ldots, a_n + b_{\pi(n)}\} = G$) if and only if $b_1 + \cdots + b_n = 0$.

A Conjecture of Snevily [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.

Bialostocki's conjecture for zero-sum sequences

Bialostocki's Conjecture [Integers 7(2007)]. Let n be a positive *even* integer, and let $a_1, \ldots, a_n$ and $w_1, \ldots, w_n$ be integers satisfying $\sum_{k=1}^{n} a_k \equiv \sum_{k=1}^{n} w_k \equiv 0 \pmod{n}$. Then there is a permutation $\sigma \in S_n$ such that $\sum_{k=1}^{n} w_k a_{\sigma(k)} \equiv 0 \pmod{n}$.

S. Guo and Z. W. Sun [Acta Arith. 140(2009)]. The conjecture holds if $w_1, \ldots, w_n$ form an arithmetic progression with even common difference.

The proof uses the following well-known theorem

Erdős-Ginzburgh-Ziv Theorem. For $a_1, \ldots, a_{2n-1} \in \mathbb{Z}$ there is an $I \subseteq [1, 2n-1]$ with $|I| = n$ such that $\sum_{i \in I} a_i \equiv 0 \pmod{n}$.

A new conjecture in combinatorial number theory

Let $m_1, \ldots, m_{n-1} \in \mathbb{Z}$. Motivated by applications of covering systems, in May 2004 I investigated when there is a permutation $\pi \in S_{n-1}$ such that n divides *none* of $\pi(1)m_1, \ldots, \pi(n-1)m_{n-1}$. If there exists such a permutation π, then for any positive divisor d of n, we have

$$|\{0 < s < n : \ m_s \not\equiv 0 \pmod{d}\}| \geqslant d - 1.$$

For, if $\pi(s)$ is a multiple of n/d, then $d \nmid m_s$. I guessed that this necessary condition is also sufficient. Namely, I have the following conjecture which was formulated by me on May 1, 2004.

Conjecture [Z. W. Sun, 2004]. Let $m_1, \ldots, m_{n-1}$ be integers such that

$$|\{1 \leqslant s \leqslant n-1 : \ d \nmid m_s\}| \geqslant d - 1 \ \text{ for any divisor } d \text{ of } n.$$

Then there is a permutation $\pi \in S_{n-1}$ such that

$$\pi(s)m_s \not\equiv 0 \pmod{n} \quad \text{for all } s = 1, \ldots, n-1.$$

What has been done

I have proved (a)⇒(b)⇒(c), where (a),(b),(c) are as follows:

(a) $\gcd(m_s, n) \leqslant s$ for all $s = 1, \ldots, n-1$.

(b) $\pi(1)m_1, \ldots, \pi(n-1)m_{n-1} \not\equiv 0 \pmod{n}$ for some $\pi \in S_{n-1}$.

(c) $\{\sum_{i\in I} m_i : \ I \subseteq [1, n-1]\}$ contains a complete system of residues modulo n.

My former students Hao Pan and Song Guo also had some partial results.

But I want to see a complete solution of the conjecture.

I made the conjecture public via a message to Number Theory List (Nov. 2009), please consult

`http://listserv.nodak.edu/cgi-bin/wa.exe?A1=ind0911&L=nmbrthry`

Thank you!