Jiangsu University (Nov. 24, 2017)
and Shandong University (Dec. 1, 2017)
and Hunan University (Dec. 10, 2017)
and Southwest University (April 8, 2019)

On Snevily's Conjecture and Related Topics

Zhi-Wei Sun

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

April 8, 2019

Abstract

Let G be a finite abelian group of odd order. In 1999 H. S. Snevily conjectured that for any two subsets A and B of G with $|A| = |B| = n$ there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A and a numbering $\{b_i\}_{i=1}^n$ of the elements of B such that $a_1 + b_1, \ldots, a_n + b_n$ are pairwise distinct. In this talk we first review the initial progress on this conjecture via Alon's Combinatorial Nullstellensatz, and also the Feng-Sun-Xiang work on the related Dasgupta-Karolyi-Serra-Szegedy conjecture via characters of abelian groups. Finally we talk about B. Arsovski's elegant solution of the Snevily conjecture and pose a new conjecture on finite abelian groups.

Part A.
Hall's theorem and two conjectures of Snevily

Cramer's conjecture

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

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

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

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

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

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

Hall's theorem

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

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

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

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

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

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

and hence n is *odd*.

A conjecture of Snevily

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

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

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

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

Latin transversal

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

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

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

Another Conjecture of Snevily

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

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

Jäger-Alon-Tarsi Conjecture

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

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

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

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

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

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.

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 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

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

For $\sigma \in S_k$ let $\varepsilon(\sigma)$ be the sign of σ which takes 1 or -1 according as the permutation σ is even or odd.
Recall that

$$\det(a_{ij})_{1\leqslant i,j\leqslant k} = \sum_{\sigma\in S_k} \varepsilon(\sigma) \prod_{i=1}^{k} a_{i,\sigma(i)},\ \mathrm{per}(a_{ij})_{1\leqslant i,j\leqslant k} = \sum_{\sigma\in S_k} \prod_{i=1}^{k} a_{i,\sigma(i)}.$$

Now we have

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

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

An extension of Alon's result by Hou and Sun

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

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

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

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

Snevily's Conjecture for cyclic groups

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

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

Their key observation is that **a cyclic group of odd order n can be viewed as a subgroup of the multiplicative group of the finite field $\mathbb{F}_{2^{\varphi(n)}}$.** 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.

Comuting c

For $\sigma \in S_k$ let $\varepsilon(\sigma)$ be the sign of σ. Then

$$\prod_{1\leqslant i<j\leqslant k}(x_j - x_i)(b_j x_j - b_i x_i)$$

$$=(-1)^{\binom{k}{2}}|x_i^{k-j}|_{1\leqslant i,j\leqslant k}|b_i^{j-1}x_i^{j-1}|_{1\leqslant i,j\leqslant k}$$

$$=(-1)^{\binom{k}{2}}\sum_{\sigma\in S_k}\varepsilon(\sigma)\prod_{i=1}^{k}x_i^{k-\sigma(i)}\sum_{\tau\in S_k}\varepsilon(\tau)\prod_{i=1}^{k}b_i^{\tau(i)-1}x_i^{\tau(i)-1}.$$

Therefore

$$(-1)^{\binom{k}{2}}c=\sum_{\sigma\in S_k}\varepsilon(\sigma)^2\prod_{i=1}^{k}b_i^{\sigma(i)-1}=\mathrm{per}((b_i^{j-1})_{1\leqslant i,j\leqslant k})$$

$$=\sum_{\sigma\in S_k}\varepsilon(\sigma)\prod_{i=1}^{k}b_i^{\sigma(i)-1}\quad(\text{because ch}(F)=2)$$

$$=|b_j^{i-1}|_{1\leqslant i,j\leqslant k}=\prod_{1\leqslant i<j\leqslant k}(b_j-b_i)\neq 0\ (\text{Vandermonde}).$$

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. Let $A = \{1, \ldots, k\}$. For $x_i, x_j \in A$, since

$$|x_i - x_j| \leqslant k - 1 \leqslant \frac{n-1}{2} < \frac{n}{2},$$

we have

$$\begin{aligned} & x_i + a_i \not\equiv x_j + a_j \pmod{n} \\ \iff & x_j - x_i \not\equiv a_i - a_j \pmod{n} \\ \iff & x_j - x_i \neq r_{ij} \end{aligned}$$

where r_{ij} denotes the residue of $a_i - a_j$ in the interval $(-n/2, n/2]$.

Continue the proof

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

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

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

My related work

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

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

and

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

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

My related work

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

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

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

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

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

Part B.
The DKSS technique and the DKSS conjecture

A new technique of DKSS

DKSS found a new technique which allows them to prove Snevily's conjecture for cyclic groups of odd order **without use of the Combinatorial Nullstellensatz**.

Let F a field of characteristic 2 and let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ be two subsets of $F^* = F \setminus \{0\}$ with cardinality k. To show that there exists $\sigma \in S_k$ such that $a_{\sigma(1)}b_1, \ldots, \ldots, a_{\sigma(k)}b_k$ are distinct, we try to prove that

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

A new technique of DKSS

$$
\begin{aligned}
\Sigma &= \sum_{\sigma\in S_k} \varepsilon(\sigma)|(a_{\sigma(j)}b_j)^{i-1}|_{1\leqslant i,j\leqslant k} \\
&= \sum_{\sigma\in S_k} \varepsilon(\sigma) \sum_{\tau\in S_k} \varepsilon(\tau) \prod_{i=1}^{k} (a_{\sigma(\tau(i))}b_{\tau(i)})^{i-1} \\
&= \sum_{\tau\in S_k} \prod_{i=1}^{k} b_{\tau(i)}^{i-1} \sum_{\sigma\in S_k} \varepsilon(\sigma\tau) \prod_{i=1}^{k} a_{\sigma\tau(i)}^{i-1} \\
&= \sum_{\tau\in S_k} \varepsilon(\tau) \prod_{i=1}^{k} b_{\tau(i)}^{i-1} \sum_{\pi\in S_k} \varepsilon(\pi) \prod_{i=1}^{k} a_{\pi(i)}^{i-1} \quad (\mathrm{ch}(F)=2) \\
&= |b_j^{i-1}|_{1\leqslant i,j\leqslant k} \times |a_j^{i-1}|_{1\leqslant i,j\leqslant k} \\
&= \prod_{1\leqslant i<j\leqslant k} (b_j - b_i) \times \prod_{1\leqslant i<j\leqslant k} (a_j - a_i) \neq 0.
\end{aligned}
$$

An extension by Sun

Lemma [Z. W. Sun, Math. Res. Lett., 15(2008)] Let R be a commutative ring with identity, and let $a_{ij} \in R$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$, where $m \in \{3, 5, \ldots\}$. The we have the identity

$$\sum_{\sigma_1,\ldots,\sigma_{m-1}\in S_n} \varepsilon(\sigma_1 \cdots \sigma_{m-1}) \prod_{1\leqslant i<j\leqslant n} \left(a_{mj} \prod_{s=1}^{m-1} a_{s\sigma_s(j)} - a_{mi} \prod_{s=1}^{m-1} a_{s\sigma_s(i)} \right)$$
$$= \prod_{1\leqslant i<j\leqslant n} (a_{1j} - a_{1i}) \cdots (a_{mj} - a_{mi}).$$

With helps of this lemma and Dirichlet's unit theorem we can prove the following result.

Theorem [Z. W. Sun, Math. Res. Lett., 15(2008)] Let G be any additive abelian group with cyclic torsion subgroup, and let $A_1, \ldots, A_m$ be arbitrary subsets of G with cardinality $n \in \mathbb{Z}^+$, where m is odd. Then the elements of A_i $(1 \leqslant i \leqslant m)$ can be listed in a suitable order $a_{i1}, \ldots, a_{in}$, so that all the sums $\sum_{i=1}^{m} a_{ij}$ $(1 \leqslant j \leqslant n)$ are distinct.

Latin transversal in a Latin cube

Recall that a line of an $n \times n$ matrix is a row or column of the matrix. We define a line of an $n \times n \times n$ cube in a similar way. A *Latin cube* over a set S of cardinality n is an $n \times n \times n$ cube whose entries come from the set S and no line of which contains a repeated element. A *transversal* of an $n \times n \times n$ cube is a collection of n cells no two of which lie in the same line. A *Latin transversal* of a cube is a transversal whose cells contain no repeated element.

Corollary Let N be any positive integer. For the $N \times N \times N$ Latin cube over $\mathbb{Z}/N\mathbb{Z}$ formed by the Cayley addition table, each $n \times n \times n$ subcube with $n \leqslant N$ contains a Latin transversal.

Conjecture (Z. W. Sun [Math. Res. Lett. 15(2008)]) Every $n \times n \times n$ 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., 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.

Below I'll introduce the work of Feng-Sun-Xiang by avoiding exterior algebra.

Characterize the distinction of elements

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

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

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

where K is a field having an element of multiplicative order $|G|$. It is well known that $\hat{G} \cong G$.

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 $\det(\chi_i(a_j))_{1 \leq i,j \leq k} \neq 0$.

Proof. If $a_s = a_t$ for some $1 \leq s < t \leq k$, then for any $\chi_1, \ldots, \chi_k \in \hat{G}$ the determinant $\det(\chi_i(a_j))_{1 \leq i,j \leq k}$ vanishes since the sth column and tth column of the matrix $(\chi_i(a_j))_{1 \leq i,j \leq k}$ are identical.

Continue the proof

Now suppose that $a_1, \ldots, a_k$ are distinct. If the characteristic of K is a prime p dividing $|G|$, then

$$(x^{|G|/p} - 1)^p = x^{|G|} - 1 \quad \text{for all } x \in K,$$

which contradicts the assumption that K contains an element of multiplicative order $|G|$. So we have $|G|1 \neq 0$, where 1 is the identity of the field K. It is well known that

$$\sum_{\chi \in \hat{G}} \chi(a) = \begin{cases} 0, & \text{if } a \in G \setminus \{e\}, \\ |G|1, & \text{if } a = e. \end{cases}$$

To show that there are $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j))_{1 \leq i,j \leq k} \neq 0$, we make the following observation.

Continue the proof

$$\sum_{\chi_1,\ldots,\chi_k\in\hat{G}} \chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1})\det(\chi_i(a_j))_{1\le i,j\le k}$$

$$= \sum_{\chi_1,\ldots,\chi_k\in\hat{G}} \chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1})\sum_{\pi\in S_k}\varepsilon(\pi)\prod_{i=1}^{k}\chi_i(a_{\pi(i)})$$

$$= \sum_{\chi_1,\ldots,\chi_k\in\hat{G}}\sum_{\pi\in S_k}\varepsilon(\pi)\prod_{i=1}^{k}\chi_i(a_{\pi(i)}a_i^{-1})$$

$$= \sum_{\pi\in S_k}\varepsilon(\pi)\prod_{i=1}^{k}\sum_{\chi_i\in\hat{G}}\chi_i(a_{\pi(i)}a_i^{-1})$$

$$= \varepsilon(I)\prod_{i=1}^{k}(|G|1) = (|G|1)^k \neq 0,$$

where I is the identity permutation in S_k.

A Remark

Remark If we apply Lemma 1 with $k = |G|$ then we obtain the following classical result: The matrix $T = \big(\chi(g)\big)_{\chi \in \hat{G},\, g \in G}$ is nonsingular; in other words, all the characters in $\hat{G}$ are linearly independent over the field K. It is well known that all the characters in $\hat{G}$ actually form a basis of the vector space

$$K^G = \{f : \ f \text{ is a function from } G \text{ to } K\}$$

over the field K.

Another Lemma

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.

Proof. By Lemma 1 it suffice to show that $\det(\chi_i(a_j b_{\pi(j)}))_{1\leqslant i,j\leqslant k} \neq 0$ for some $\pi \in S_k$. Note that

$$\begin{aligned}
&\sum_{\pi\in S_k} \det(\chi_i(a_j b_{\pi(j)}))_{1\leqslant i,j\leqslant k} \\
=&\sum_{\pi\in S_k}\sum_{\sigma\in S_k} \varepsilon(\sigma)\prod_{i=1}^{k}\chi_i(a_{\sigma(i)}b_{\pi(\sigma(i))}) \\
=&\sum_{\sigma\in S_k} \varepsilon(\sigma)\prod_{i=1}^{k}\chi_i(a_{\sigma(i)})\sum_{\pi\in S_k}\prod_{i=1}^{k}\chi_i(b_{\pi\sigma(i)}) \\
=&\det(\chi_i(a_j))_{1\leqslant i,j\leqslant k}\mathrm{per}(\chi_i(b_j))_{1\leqslant i,j\leqslant k} \neq 0.
\end{aligned}$$

One more lemma

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.

Corollary. Let p be a prime and let $a \in \mathbb{Z}^+$. If $\lambda_1, \ldots \lambda_k$ are p^ath roots of unity with $\lambda_1 + \cdots + \lambda_k = 0$, then $k \equiv 0 \pmod{p}$.

Proof of the DKSS conjecture for abelian p-groups

Let G be an abelian p-group with $|G| = p^a > 1$ and let $a_1, \ldots, a_k$ be distinct elements of G with $k < p$. Let $b_1, \ldots, b_k$ be a sequence of (not necessarily distinct) elements of G. Let $\hat{G}$ be the group of all complex-valued characters of G.

As $a_1, \ldots, a_k$ are distinct, by Lemma 1 there are $\chi_1, \ldots, \chi_k \in \hat{G}$ such that $\det(\chi_i(a_j))_{1 \leqslant i,j \leqslant k} \neq 0$. Since all those $\chi_i(b_j)$ are p^ath roots of unity and $|S_k| = k! \not\equiv 0 \pmod{p}$, by Lemma 3 we have

$$\operatorname{per}(\chi_i(b_j))_{1 \leqslant i,j \leqslant k} = \sum_{\pi \in S_k} \prod_{i=1}^{k} \chi_i(b_{\pi(i)}) \neq 0.$$

Applying Lemma 2 we see that for some $\pi \in S_k$ the products $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct!

Open Problem

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

In particular,

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

Part C.
Final Solution of Snevily's Conjecture

A conjecture implying Snevily's conjecture

Conjecture (Feng, Sun and Xiang, 2009) Let G be a finite abelian group, and let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_k\}$ be two k-subsets of G. 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 $\det(\chi_i(a_j))_{1\le i,j\le k}$ and $\det(\chi_i(b_j))_{1\le i,j\le k}$ are both nonzero.

Remark. When G is cyclic, we may take $\chi_i = \chi^i$ for $i = 1, \ldots, k$, where χ is a generator of $\hat{G}$. Then the two determinants $\det(\chi_i(a_j))_{1\le i,j\le k}$ and $\det(\chi_i(b_j))_{1\le i,j\le k}$ in the above conjecture are both nonzero since they are Vandermonde determinants. Therefore the conjecture is true for cyclic groups.

Chebotarëv's Theorem

When G is a cyclic group of prime order and K is the complex field $\mathbb{C}$, for any distinct

$$\chi_1, \ldots, \chi_k \in \hat{G}$$

and distinct

$$a_1, \ldots, a_k \in G$$

we have

$$\det(\chi_i(a_j))_{1 \leq i,j \leq k} \neq 0$$

by the Chebotarëv theorem

See also Terence Tao [Math. Res. Lett. 12(2005)]).

This is stronger than what the above conjecture asserts.

A Result of Feng, Sun and Xiang

Theorem (FSX) (i) The conjecture of FSX implies Snevily's conjecture.

(ii) Let $G, A, B, \hat{G}$ be as in the conjecture of FSX. Assume that there is a $\pi \in S_k$ such that $C = \{a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}\}$ is a k-set with $\{a_1 b_{\tau(1)}, \ldots, a_k b_{\tau(k)}\} \neq C$ for all $\tau \in S_k \setminus \{\pi\}$. Then there are $\chi_1, \ldots, \chi_k \in \hat{G}$ such that

$$\det(\chi_i(a_j))_{1\leq i,j\leq k} \det(\chi_i(b_j))_{1\leq i,j\leq k} \neq 0.$$

Also, there are $\chi_1, \ldots, \chi_k \in \hat{G}$ such that

$$\det(\chi_i(a_j))_{1\leq i,j\leq k} \mathrm{per}(\chi_i(b_j))_{1\leq i,j\leq k} \neq 0,$$

and there are $\psi_1, \ldots, \psi_k \in \hat{G}$ such that

$$\mathrm{per}(\psi_i(a_j))_{1\leq i,j\leq k} \mathrm{per}(\psi_i(b_j))_{1\leq i,j\leq k} \neq 0.$$

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 conditions in part (ii) of the above result of FSX.

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

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

and

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

are different.

Motivated by Arsovski's solution to Snevily's conjecture, G. Harcos, G. Károlyi, G. Kós [arxiv:1004.0253] confirmed the conjecture of FSX.

Proof of Arsovski's Combinatorial Lemma

The lemma is trivial for $k = 1$.

For $k = 2$ we may just let π be the identity of $S_k = S_2$ since the multi-sets $\{a_1 b_1, a_2 b_2\}$ and $\{a_1 b_2, a_2 b_1\}$ are different.

Now let $k > 2$ and assume that the lemma holds for smaller values of k. Take $g = a_1 b_1$, and set

$$I = \{1 \leqslant i \leqslant k : \ a_i b_j = g \text{ for some } 1 \leqslant j \leqslant k\}$$

and $I' = \{1, \ldots, k\} \setminus I$. For each $i \in I$, let $\pi(i)$ be the unique $j \in \{1, \ldots, k\}$ with $a_i b_j = g$. Clearly, all those $\pi(i)$ with $i \in I$ are distinct. If $I = \{1, \ldots, k\}$, then

$$a_1 b_{\pi(1)} = \ldots = a_k b_{\pi(k)} = g$$

and the two multi-sets $\{a_i b_{\sigma(i)} : \ i = 1, \ldots, k\}$ and $\{a_i b_{\pi(i)} : \ i = 1, \ldots, k\}$ are different for any $\sigma \in S_k \setminus \{\pi\}$.

Proof of Arsovski's Combinatorial Lemma (continued)

Now let $I' \neq \emptyset$. By the induction hypothesis to the $(k - |I|)$-subsets

$$A' = \{a_i : \ i \in \bar{I}\} \text{ and } B' = \{b_j : \ j \in \{1, \ldots, k\} \setminus \{\pi(i) : \ i \in I\}\},$$

there is a permutation π' on I' such that for any other permutation σ' on I' the multi-sets $\{a_i b_{\pi'(i)} : \ i \in I'\}$ and $\{a_i b_{\sigma'(i)} : \ i \in \bar{I}\}$ are different.

Let $\pi(i) = \pi'(i)$ for all $i \in I'$. Then $\pi \in S_k$. Suppose that σ is a permutation in S_k with the two multi-sets $\{a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}\}$ and $\{a_1 b_{\sigma(1)}, \ldots, a_k b_{\sigma(k)}\}$ equal. As g appears in the first multi-set exactly $|I|$ times, it also appears in the second multi-set exactly $|I|$ times. So $\sigma(i) = \pi(i)$ for all $i \in I$. Since the muti-sets $\{a_i b_{\pi'(i)} : \ i \in I'\}$ and $\{a_i b_{\sigma(i)} : \ i \in I'\}$ are equal, $\sigma(i) = \pi'(i)$ for all $i \in I'$. Therefore $\sigma = \pi$. This concludes the proof.

Arsovski's proof of Snevily's conjecture

Let F be a field of characteristic 2 containing an element of multiplicative order $m = |G|$ and consider its purely transcendental extension $K = F(t_1, \ldots, t_m)$. The character group

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

is isomorphic to G, and the characters in $\hat{G}$ form a basis of the vector space $V := \{\text{maps from } G \text{ to } K\}$ over the field K.

Write $G = \{g_1, \ldots, g_m\}$ and define $f(g_i) = t_i$ for $i = 1, \ldots, m$. By Arsovski's combinatorial lemma, there is a permutation $\pi \in S_k$ such that for any $\sigma \in S_k \setminus \{\pi\}$ the two multi-sets $\{a_i b_{\pi(i)} : \ i = 1, \ldots, k\}$ and $\{a_i b_{\sigma(i)} : \ i = 1, \ldots, k\}$ are different.

Suppose that each g_j $(1 \leqslant j \leqslant m)$ occurs in the multi-set $\{a_i b_{\pi(i)} : \ i = 1, \ldots, k\}$ exactly k_j times. Then

$$D =: \det(f(a_i b_j))_{1 \leqslant i,j \leqslant n} \neq 0$$

since its expansion contains the monomial $t_1^{k_1} \ldots t_m^{k_m}$ only once.

Arsovski's proof of Snevily's conjecture (continued)

Write $\hat{G} = \{\chi_1, \ldots, \chi_m\}$ and $f = c_1\chi_1 + \ldots + c_m\chi_m$ with $c_1, \ldots, c_m \in K$. Then

$$D = \det(\Sigma_{s=1}^{m} c_s \chi_s(a_i b_j)) = \sum_{s_1=1}^{m} \ldots \sum_{s_k=1}^{m} \det(c_{s_i} \chi_{s_i}(a_i b_j))$$

$$= \sum_{\substack{1 \leqslant s_1, \ldots, s_k \leqslant m \\ \text{distinct}}} \det(c_{s_i} \chi_{s_i}(a_i b_j))$$

$$= \sum_{1 \leqslant s_1 < \ldots < s_k \leqslant m} \sum_{\sigma \in S_k} \det(c_{s_{\sigma(i)}} \chi_{s_{\sigma(i)}}(a_i b_j))$$

$$= \sum_{1 \leqslant s_1 < \ldots < s_k \leqslant m} \sum_{\sigma \in S_k} \sum_{\tau \in S_k} \varepsilon(\tau) \prod_{i=1}^{k} c_{s_{\sigma(i)}} \chi_{s_{\sigma(i)}}(a_i b_{\tau(i)})$$

$$= \sum_{1 \leqslant s_1 < \ldots < s_k \leqslant m} c_{s_1} \cdots c_{s_k} \sum_{\tau \in S_k} \varepsilon(\tau) \sum_{\sigma \in S_k} \prod_{i=1}^{k} \chi_{s_{\sigma(i)}}(a_i b_{\tau(i)}).$$

Arsovski's proof of Snevily's conjecture (continued)

Recall that K is of characteristic 2. Thus

$$D = \sum_{1 \leqslant s_1 < \ldots < s_k \leqslant m} c_{s_1} \cdots c_{s_k} \sum_{\tau \in S_k} \det(\chi_{s_j}(a_i b_{\tau(i)}).$$

Since $D \neq 0$, for some $1 \leqslant s_1 < \ldots < s_k \leqslant m$ and $\tau \in S_k$ we have

$$\det(\chi_{s_j}(a_i b_{\tau(i)}) \neq 0$$

and hence $a_1 b_{\tau(1)}, \ldots, a_k b_{\tau(k)}$ are distinct.

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."

A conjecture for general abelian groups

Conjecture (Sun, 2013-09-04). Let G be a finite abelian group. If G is cyclic or G contains no involution (i.e., elemnt of order 2), then for any finite subset A of G with $|A| = n > 3$, there is a numbering $a_1, \ldots, a_n$ of all the n elements of A such that

$$a_1+a_2+a_3,\ a_2+a_3+a_4,\ \ldots,\ a_{n-2}+a_{n-1}+a_n,\ a_{n-1}+a_n+a_1,\ a_n+a_1+a_2$$

are pairwise distinct.

Remark. For a finite abelian group $G = \{a_1, a_2, \ldots, a_n\}$, it is easy to see that $2(a_1 + \cdots + a_n) = 0$.

Theorem (Sun, 2013-09-19). The conjecture holds for any *torsion-free* abelian group G.

Remark. (1) I became too tired and ill immediately after I spent the whole day to finish the proof of this theorem.
(2) The conjecture is even open for cyclic groups of prime orders.

Thank you!