On the DKSS Technique and the DKSS Conjecture

Zhi-Wei Sun

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

Feb. 4, 2010

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!**

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

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 $j = 1, \ldots, k$.

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

$$\prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)(b_j x_j - b_i x_i)$$
$$=(-1)^{\binom{n}{2}} |x_i^{k-j}|_{1 \leqslant i,j \leqslant k} |b_i^{j-1} x_i^{j-1}|_{1 \leqslant i,j \leqslant k}$$
$$=(-1)^{\binom{n}{2}} \sum_{\sigma \in S_k} \varepsilon(\sigma) \prod_{i=1}^{k} x_i^{k-\sigma(i)} \sum_{\tau \in S_k} \varepsilon(\tau) \prod_{i=1}^{k} b_i^{\tau(i)-1} x_i^{\tau(i)-1}.$$

Therefore

$$(-1)^{\binom{k}{2}} c = \sum_{\sigma \in S_k} \varepsilon(\sigma)^2 \prod_{i=1}^{k} b_i^{\sigma(i)-1} = \mathrm{per}((b_i^{j-1})_{1 \leqslant i,j \leqslant k})$$
$$= \sum_{\sigma \in S_k} \varepsilon(\sigma) \prod_{i=1}^{k} b_i^{\sigma(i)-1} \quad \text{(because } \mathrm{ch}(F) = 2\text{)}$$
$$=|b_j^{i-1}|_{1 \leqslant i,j \leqslant k} = \prod_{1 \leqslant i < j \leqslant k} (b_j - b_i) \neq 0 \text{ (Vandermonde).}$$

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

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

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 $j = 1, \ldots, k$.

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 $B = \{b_1, \ldots, k\}$ 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., 115(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

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

Via this lemma we can give a simple proof of the following result.

Theorem [Z. W. Sun, Math. Res. Lett., 115(2008)] Let F be a field and let $m > 0$ be an odd integer. Suppose that $A_1, \ldots, A_m$ are subsets of F with cardinality $n \in \mathbb{Z}^+$. 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 products $\prod_{i=1}^m a_{ij}$ $(1 \leqslant j \leqslant n)$ are distinct.

The DKSS Conjecture

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

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

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

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

A 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.

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

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

$$\begin{aligned}
&\sum_{\chi_1,\ldots,\chi_k\in\hat{G}} \chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1})\det(\chi_i(a_j))_{1\le i,j\le k}\\
=&\sum_{\chi_1,\ldots,\chi_k\in\hat{G}} \chi_1(a_1^{-1})\cdots\chi_k(a_k^{-1})\sum_{\pi\in S_k}\varepsilon(\pi)\prod_{i=1}^{k}\chi_i(a_{\pi(i)})\\
=&\sum_{\chi_1,\ldots,\chi_k\in\hat{G}}\sum_{\pi\in S_k}\varepsilon(\pi)\prod_{i=1}^{k}\chi_i(a_{\pi(i)}a_i^{-1})\\
=&\sum_{\pi\in S_k}\varepsilon(\pi)\prod_{i=1}^{k}\sum_{\chi_i\in\hat{G}}\chi_i(a_{\pi(i)}a_i^{-1})\\
=&\varepsilon(I)\prod_{i=1}^{k}(|G|1)=(|G|1)^k\neq 0,
\end{aligned}$$

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

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

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

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

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 $\mathbb{Z}/n\mathbb{Z}$?

Thank you!