# Exterior Algebras and Two Conjectures about Finite Abelian Groups

Qing Xiang
joint work with Tao Feng and Zhi-Wei Sun

University of Delaware
Newark, DE 19716
xiang@math.udel.edu

IPM20, May 18, 2009

# The Statement of the Conjecture

Snevily's Conjecture on Latin Transversals (1999).

Let $G$ be a multiplicatively written abelian group of odd order, and let $A = \{a_1, \ldots, a_k\}$, $B = \{b_1, \ldots, b_k\}$ be two subsets of $G$ of size $k$. Then there is a permutation $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct.

# Some Remarks

**Remarks.** (1) The condition that $G$ has odd order is needed. Let $|G|$ be even, $g$ be an element of order 2, and let $A = \{1, g\} = B$. Then for $\pi = \mathrm{id}$, we have $a_1 b_{\pi(1)} = a_2 b_{\pi(2)} = 1$, and for $\pi = (12)$, we have $a_1 b_{\pi(1)} = a_2 b_{\pi(2)} = g$.

(2) The conjecture first appeared in "The Cayley addition table of $\mathbb{Z}_n$" (Snevily), American Math. Monthly (106) 1999, 584–585. The whole Section 9.3 in the book "Additive Combinatorics" (Tao and Vu) is devoted to Snevily's conjecture.

# Motivation

- Complete mappings

A *complete mapping* for a multiplicatively written group $G$ is a bijection $\phi : G \to G$ such that the map $x \mapsto x\phi(x)$ is also a bijection.

- The Hall-Paige Conjecture (1955)

If $G$ is a finite group and the Sylow 2-subgroups of $G$ are either trivial or noncyclic, then $G$ has a complete mapping.

# Motivation, continued

**Remark.** If a finite group $G$ has a complete mapping, then the Sylow 2-subgroups of $G$ are either trivial or noncyclic.

Call a collection of $k$ cells from a $k \times k$ matrix a *transversal* if no two of the $k$ cells are on a line (row or column). A transversal is called *Latin* if no two of its cells contain the same symbol.

$$\begin{matrix} \underline{1} & 2 & 3 & 4 & 5 \\ 2 & 1 & \underline{4} & 5 & 3 \\ 3 & \underline{5} & 1 & 2 & 4 \\ 4 & 3 & 5 & 1 & \underline{2} \\ 5 & 4 & 2 & \underline{3} & 1 \end{matrix}$$

# Motivation, continued

The multiplication table of any finite group $G$ is a Latin square.

Let $G$ be a finite group. Then the multiplication table of $G$ has a Latin transversal if and only if $G$ has a complete mapping.

Therefore, the Hall-Paige conjecture is about existence of Latin transversals in the multiplication table of a finite group.

# Motivation, continued

**Snevily's Conjecture** (restated)

Let $G$ be an abelian group of odd order. Then any $k \times k$ submatrix of the multiplication table of $G$ has a Latin transversal.

# Hall-Paige

**The Hall-Paige Conjecture is proved.**

(1) Early work by Hall and Paige

(2) A. B. Evans, Michael Aschbacher, F. Dalla Volta and N. Gavioli

(3) Stewart Wilcox (preprint): Any minimal counterexample to the Hall-Paige conjecture must be a simple group. Furthermore, Wilcox showed that any minimal counterexample to the Hall-Paige conjecture must be a sporadic simple group.

(4) A. B. Evans (J. Algebra, Jan. 2009), John Bray (preprint).

# Known results on Snevily's conjecture

**Theorem.** (Alon, 2000) Let $G$ be a cyclic group of prime order $p$. Let $k < p$ be a positive integer. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a $k$-subset of $G$ and $b_1, b_2, \ldots, b_k$ be (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.** The proof uses the Combinatorial Nullstellensatz which is stated below.

# Combinatorial Nullstellensatz

**Theorem.** (Combinatorial Nullstellensatz) Let $F$ be an arbitrary field, let $P \in F[x_1, x_2, \ldots, x_n]$ be a polynomial of degree $d$ which has a nonzero coefficient at $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ $(d_1 + d_2 + \cdots + d_n = d)$, and let $S_1, S_2, \ldots, S_n$ be subsets of $F$ such that $|S_i| > d_i$ for all $1 \leq i \leq n$. Then there exist $t_1 \in S_1, t_2 \in S_2, \ldots, t_n \in S_n$ such that $P(t_1, t_2, \ldots, t_n) \neq 0$.

# Known results, continued

**Theorem.** (Dasgupta, G. Károlyi, O. Serra and B. Szegedy, 2001) Snevily's conjecture holds for cyclic groups of odd order.

**Theorem.** (Dasgupta, G. Károlyi, O. Serra and B. Szegedy, 2001) Let $p$ be a prime and let $\alpha$ be a positive integer. Let $G$ be the cyclic group $\mathbb{Z}_{p^\alpha}$ or the elementary abelian $p$-group $\mathbb{Z}_p^\alpha$. 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 $G$, where $k < p$. Then for some $\pi \in S_k$, $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct.

# The DKSS conjecture

**The DKSS Conjecture.**

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.

# New results and their proofs

**Theorem 1.** (F-S-X) The DKSS conjecture is true for all abelian $p$-groups.

That is: Let $p$ be a prime. Assume that $G$ is an abelian $p$-group, and $k$ is a positive integer such that $k < p$. Let $A = \{a_1, \ldots, a_k\}$ be a $k$-subset of $G$, and $b_1, b_2, \ldots, b_k$ be (not necessarily distinct) elements of $G$. Then $\exists$ a $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct.

# New results and their proofs

Theorem 1 can be slightly generalized.

**Definition.** Let $k$ and $n > 1$ be positive integers. We say that $n$ is *$k$-large* if the smallest prime divisor of $n$ is greater than $k$ and any other prime divisor of $n$ is greater than $k!$.

# New results and their proofs

**Theorem 2.** (F-S-X) Let $G$ be a finite abelian group. Let $A = \{a_1, \ldots, a_k\}$ be a $k$-subset of $G$, and $b_1, \ldots, b_k$ be (not necessarily distinct) elements of $G$. Suppose that either $A$ or $B = \{b_1, \ldots, b_k\}$ is contained a subgroup $H$ of $G$ and $|H|$ is $k$-large. Then there exists a permutation $\pi \in S_k$ such that $a_1 b_{\pi(1)}, \ldots, a_k b_{\pi(k)}$ are distinct.

Note that if $k$ is a positive integer and $p$ is a prime such that $p > k$, then for every integer $\alpha \geq 1$, $p^\alpha$ is certainly $k$-large. Hence Theorem 1 is a special case of Theorem 2.

# New results and their proofs

- Exterior powers

Let $F$ be any field, and let $V$ be an $n$-dimensional vector space over $F$.

The exterior power $\bigwedge^k V$ can be constructed as the quotient space of $V^{\otimes k}$ (the $k$-th tensor power) by the subspace generated by all those $v_1 \otimes v_2 \otimes \cdots \otimes v_k$ with two of the $v_i$ equal. We naturally identify $\bigwedge^0 V = F$ and $\bigwedge^1 V = V$. The *exterior algebra* of $V$, denoted by $E(V)$, is the algebra $\oplus_{k\geq 0} \bigwedge^k(V)$, with respect to the wedge product '$\wedge$'.

Note that $\dim(\bigwedge^k V) = \binom{n}{k}$ and $\dim(E(V)) = 2^n$.

# New results and their proofs

- Skew derivations

A *skew derivation* on $E(V)$ is an $F$-homomorphism $\Delta : E(V) \to E(V)$ such that

$$\Delta(xy) = (\Delta x)y + (-1)^k x(\Delta y),$$

for all $x \in \bigwedge^k V$ and $y \in E(V)$.

# New results and their proofs

**Lemma.** Let $G$ be a finite abelian group. Let $\hat{G}$ denote the group of characters from $G$ to $K^* = K \setminus \{0\}$, where $K$ is a field containing a primitive $|G|$-th root of unity. Let $a_1, \dots, a_k, b_1, \dots, b_k \in G$ and $\chi_1, \dots, \chi_k \in \hat{G}$. Let

$$M_A = (\chi_i(a_j))_{1 \le i,j \le k}, \quad M_B = (\chi_i(b_j))_{1 \le i,j \le k}.$$

Suppose that both $\det(M_A)$ and $\mathrm{per}(M_B)$ are nonzero. Then there is $\pi \in S_k$ such that the products $a_1 b_{\pi(1)}, \dots, a_k b_{\pi(k)}$ are distinct.

# New results and their proofs

$V = K[G]$: $|G|$-dimensional vector space over $K$.

For any $\pi \in S_k$ we set

$$Q_\pi := a_1 b_{\pi(1)} \wedge \cdots \wedge a_k b_{\pi(k)} \in \bigwedge^k V.$$

**Goal.** Prove that $\exists\ \pi \in S_k$ such that $Q_\pi \neq 0$.

Consider $\sum_{\pi \in S_k} Q_\pi$. If one can show that this sum is nonzero, then there exists one summand which is nonzero.

# New results and their proofs

Apply skew derivations $\Delta_{\chi_i}$, $(\chi_i \in \hat{G})$, $1 \leq i \leq k$, to the above sum, we get

$$(\Delta_{\chi_1} \circ \cdots \circ \Delta_{\chi_k})\left(\sum_{\pi \in S_k} Q_\pi\right) = (-1)^{k(k-1)/2}\,\mathrm{det}(M_A)\mathrm{per}(M_B).$$

# New results and their proofs

Using this lemma, together with some (elementary) algebraic number theory, we can prove Theorem 1 (F-S-X) mentioned above.

**Proof of Theorem 1.** Let $|G| = p^\alpha$, and $K = \mathbb{Q}(\xi_{p^\alpha})$, where $\xi_{p^\alpha}$ is a complex primitive $p^\alpha$-th of unity. Then one can certainly find complex characters $\chi_1, \chi_2, \ldots, \chi_k$ such that $\det(M_A) \neq 0$ (by orthogonality of characters). Now using the same $\chi_1, \chi_2, \ldots, \chi_k$ to construct $M_B$. We need to show that $\mathrm{Per}(M_B) \neq 0$.

Let us consider $\mathrm{Per}(M_B)$ modulo the **prime** ideal $(1 - \xi_{p^\alpha})$. We have

$$\mathrm{Per}(M_B) \equiv k! \pmod{(1 - \xi_{p^\alpha})}.$$

Note that $\mathbb{Z}[\xi_{p^\alpha}]/(1 - \xi_{p^\alpha})$ is isomorphic to the finite field $\mathbb{Z}/p\mathbb{Z}$. Since $k < p$, we see that $k!$ is nonzero in $\mathbb{Z}/p\mathbb{Z}$. Hence $\mathrm{Per}(M_B) \neq 0$.

# A new conjecture

**Conjecture.** (F-S-X) Let $G$ be a finite abelian group, and let $A = \{a_1, \ldots, a_k\}$, $B = \{b_1, \ldots, b_k\}$ be two $k$-subsets of $G$. Let $K$ be an arbitrary 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.

**Remarks.** (1). The validity of this conjecture implies that of the Snevily conjecture. This can be seen by using characters from $G$ to $K^*$, where $K$ is a field of characteristic 2.

2. The conjecture holds when $G$ is cyclic (Vandermonde determinants). Therefore we have a new proof of the DKSS theorem stating that the Snevily's conjecture is true for all odd order cyclic groups.