J. Combin. Theory Ser. A 103(2003), no.2, 288–301.

ON SNEVILY'S CONJECTURE AND RESTRICTED SUMSETS

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093
The People's Republic of China
E-mail: zwsun@nju.edu.cn
Homepage: http://pweb.nju.edu.cn/zwsun

Abstract. Let G be an additive abelian group whose finite subgroups are all cyclic. Let $A_1, \ldots, A_n$ $(n > 1)$ be finite subsets of G with cardinality $k > 0$, and let $b_1, \ldots, b_n$ be pairwise distinct elements of G with odd order. We show that for every positive integer $m \leqslant (k-1)/(n-1)$ there are more than $(k-1)n-(m+1)\binom{n}{2}$ sets $\{a_1, \ldots, a_n\}$ such that $a_1 \in A_1, \ldots, a_n \in A_n$, and both $a_i \neq a_j$ and $ma_i + b_i \neq ma_j + b_j$ (or both $ma_i \neq ma_j$ and $a_i + b_i \neq a_j + b_j$) for all $1 \leqslant i < j \leqslant n$. This extends a recent result of Dasgupta, Károlyi, Serra and Szegedy on Snevily's conjecture. Actually stronger results on sumsets with polynomial restrictions are obtained in this paper.

1. Introduction

In 1999 Snevily [Sn] posed the following conjecture.

Snevily's Conjecture. *Let G be an additive abelian group with $|G|$ odd. Let A and B be subsets of G with cardinality $n > 0$. Then 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.*

Using the polynomial method of Alon, Nathanson and Ruzsa (see, e.g. [ANR], [A1] and [N]), Alon [A2] proved that the above conjecture holds when $|G|$ is an odd prime. In 2001 Dasgupta, Károlyi, Serra and Szegedy [DKSS] confirmed Snevily's conjecture for any cyclic group with odd order.

In this paper we will show the following result in this direction.

2000 *Mathematics Subject Classification.* Primary 11B75; Secondary 05A05, 11C20, 11P70, 12E05, 20D60.

Supported by the Teaching and Research Award Program for Outstanding Young Teachers in Higher Education Institutions of MOE, and the National Natural Science Foundation of the People's Republic of China.

Theorem 1.1. *Let G be an additive abelian group whose finite subgroups are all cyclic. Let $A_1,\ldots,A_n$ $(n>1)$ be finite subsets of G with cardinality $k\geqslant n$, and let $b_1,\ldots,b_n$ be elements of G. Let m be any positive integer not exceeding $(k-1)/(n-1)$.*

(i) *If $b_1,\ldots,b_n$ are pairwise distinct, then 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) *The sets*

$$\{\{a_1,\ldots,a_n\}\colon a_i\in A_i,\ a_i\neq a_j \text{ and } ma_i+b_i\neq ma_j+b_j \text{ if } i\neq j\} \quad (1.1)$$

and

$$\{\{a_1,\ldots,a_n\}\colon a_i\in A_i,\ ma_i\neq ma_j \text{ and } a_i+b_i\neq a_j+b_j \text{ if } i\neq j\} \quad (1.2)$$

have more than $(k-1)n-(m+1)\binom{n}{2}\geqslant(m-1)\binom{n}{2}$ elements, provided that $b_1,\ldots,b_n$ are pairwise distinct and of odd order, or they have finite order and $n!$ cannot be written in the form $\sum_{p\in P}px_p$ where all the x_p are nonnegative integers and P is the set of primes dividing one of the orders of $b_1,\ldots,b_n$.

Remark 1.1. When G is a cyclic group with $|G|$ being odd or a prime power, our Theorem 1.1 (ii) in the case $k=n$ and $m=1$, yields Theorems 1 and 2 of [DKSS] respectively. In our opinion, the condition that all finite subgroups of G are cyclic might be omitted from Theorem 1.1.

We will deduce Theorem 1.1 from our stronger results on sumsets with polynomial restrictions. (As for sumsets of subsets of $\mathbb{Z}$ with linear restrictions, the reader may consult [Su2].)

Let F be a field. We use $\mathrm{ch}(F)$ to denote the additive order of the multiplicative identity of F and call it the *characteristic* of F. (When $\mathrm{ch}(F)=\infty$, some mathematicians regard the characteristic of F as zero.) There are several recent results ([DH], [ANR], [HS], [LS], [PS]) concerning various restricted sumsets of $A_1,\ldots,A_n\subseteq F$. For example, Corollary 1 of [HS] in the case $m=1$ can be stated as follows:

Let $k\geqslant n\geqslant 1$ be integers, and F be a field with $\mathrm{ch}(F)$ *greater than n and $(k-n)n$. Let $A_1,\ldots,A_n$ be subsets of F with cardinality k, and $b_1,\ldots,b_n$ be elements of F. Then the sumset*

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

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

When F is a finite field of order p^α (where p is a prime and α is a positive integer), the additive group of F is isomorphic to the direct sum of α copies of the additive cyclic group $\mathbb{Z}/p\mathbb{Z}$, and the above result in the case $k = n$ was also found by Dasgupta et al. ([DKSS]) who followed Alon's approach in [A2].

Let R be any commutative ring with identity. For $P(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$, we simply write $[x_1^{i_1} \cdots x_n^{i_n}]P(x_1, \dots, x_n)$ for the coefficient of the monomial $x_1^{i_1} \cdots x_n^{i_n}$ in $P(x_1, \dots, x_n)$. For a matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ with entries in R, we use $\det(A)$ or $|a_{ij}|_{1 \leqslant i,j \leqslant n}$ to denote the determinant of A, and define the *permanent* of A by

$$\operatorname{per}(A) = \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \tag{1.3}$$

where S_n is the symmetric group of all the permutations on $\{1, \dots, n\}$.

By studying certain coefficients of some related polynomials in the next section, we are able to prove the following main theorems in Section 3.

Theorem 1.2. *Let k, m, n be positive integers with $k > m(n-1)$, and let $A_1, \dots, A_n$ be subsets of a field F with cardinality k. Let $K = (k-1)n - m\binom{n}{2}$ and $P_1(x), \dots, P_n(x) \in F[x]$ have degree m.*

(i) *If $\operatorname{ch}(F) > K$ and all the $b_i = [x^m]P_i(x)$ $(i = 1, \dots, n)$ are pairwise distinct, then $|S| \geqslant K + 1$ where*

$$S = \left\{ \sum_{i=1}^{n} a_i \colon a_1 \in A_1, \dots, a_n \in A_n,\ \text{and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j \right\}. \tag{1.4}$$

(ii) *If $\operatorname{ch}(F) > K - \binom{n}{2}$ and the permanent of $B = (b_j^{i-1})_{1 \leqslant i,j \leqslant n}$ does not vanish, then $|T| \geqslant K - \binom{n}{2} + 1$ where*

$$T = \left\{ \sum_{i=1}^{n} a_i \colon a_i \in A_i,\ a_i \neq a_j \text{ and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j \right\}. \tag{1.5}$$

(iii) *We have $\operatorname{per}(B) \neq 0$, if F is the complex field $\mathbb{C}$, $b_1, \dots, b_n$ are qth roots of unity, and $n!$ does not belong to the set*

$$D(q) = \left\{ \sum_{p \mid q} p x_p \colon x_p \in \{0, 1, 2, \dots\} \text{ for any prime divisor } p \text{ of } q \right\}. \tag{1.6}$$

Remark 1.2. Let $b_1, \dots, b_n$ be pairwise distinct elements of a field F, and let B be the Vandermonde matrix $(b_j^{i-1})_{1 \leqslant i,j \leqslant n}$. If $\operatorname{ch}(F) = 2$, then

$$\operatorname{per}(B) = \det(B) = \prod_{1 \leqslant i < j \leqslant n} (b_j - b_i) \neq 0$$

as observed by Dasgupta et al. [DKSS]. If $F = \mathbb{C}$, $\mathrm{per}(B) = 0$ and all the b_i are qth roots of unity, then $\prod_{1\leqslant i<j\leqslant n}(1-b_i/b_j) = 2\omega$ for some algebraic integer $\omega \in E = \mathbb{Q}(e^{2\pi i/q})$ and hence q must be even (otherwise the norms of those $1 - b_i/b_j$ $(1 \leqslant i < j \leqslant n)$ with respect to the field extension $E/\mathbb{Q}$ would be odd); this fact is also due to Dasgupta et al. [DKSS].

Concerning the sumset S given by (1.4), there is another result due to Liu and Sun [LS]: *Let F be a field and $P_1(x), \ldots, P_n(x) \in F[x]$ be monic and of degree $m > 0$. Let $A_1, \ldots, A_n$ be finite subsets of F with $k = |A_n| > m(n-1)$ and $|A_{i+1}| - |A_i| \in \{0, 1\}$ for all $i = 1, \ldots, n-1$. If $L = (k-1)n - (m+1)\binom{n}{2} < \mathrm{ch}(F)$, then $|S| \geqslant L + 1$.*

Theorem 1.3. *Let $A_1, \ldots, A_n$ be finite subsets of a field F with $0 < k_1 = |A_1| \leqslant \ldots \leqslant k_n = |A_n|$, and let $P_1(x), \ldots, P_n(x) \in F[x]$ be monic and of degree m where*

$$m > k_n - k_1 \text{ and } k_n > m(n-1). \tag{1.7}$$

(i) *We have $L = \sum_{i=1}^{n}(k_i - 1) - (m+1)\binom{n}{2} \geqslant 0$. If $\mathrm{ch}(F) > L!n!$, then $|T| \geqslant L + 1$ where T is as in* (1.5).

(ii) *When $k_1 = \ldots = k_n = k$ and $\mathrm{ch}(F) > L$, we have $|T| \geqslant L \geqslant (m-1)\binom{n}{2}$, and $|T| = L$ only if $k = n \geqslant \mathrm{ch}(F) > m = 1$ or $\mathrm{ch}(F) = m = n = 2 < k = 3$.*

As for Theorem 1.3 (ii), the following example shows that $|T| = L$ may happen in the exceptional cases.

Example 1.1. (i) Let F be a field of prime characteristic p. Let $b_1 = 0$ and $b_2 = \ldots = b_p = b \in F \setminus \{0\}$. Set $A_1 = \ldots = A_p = \{0, b, \ldots, (p-1)b\}$. Suppose that $a_1 \in A_1, \ldots, a_p \in A_p$ and $a_1, \ldots, a_p$ are pairwise distinct. Then $a_1 + b_1, \ldots, a_p + b_p$ cannot be pairwise distinct. In fact, if $a_1 - b = a_i$ where $1 < i \leqslant p$, then $a_1 + b_1 = a_1 = a_i + b_i$.

(ii) Let F be a field of order 4 with identity 1. Let $a \in F \setminus \{0, 1\}$. Since $a^3 = 1$ and $a \neq 1$, we have $a^2 + a + 1 = 0$. If a_1, a_2 are distinct elements of $\{0, 1, a\}$ and $a_1^2 + a_1 \neq a_2^2 + a_2 + 1$, then $\{a_1, a_2\} \neq \{0, a\}, \{1, a\}$ and hence $a_1 + a_2 = 0 + 1$.

The following example indicates that the condition $k_n > m(n-1)$ in Theorem 1.3 cannot be replaced by $k_n \geqslant m(n-1)$.

Example 1.2. Let m and n be positive integers. Let F be a finite field with $|F| = p^{\varphi(m)} > m(n-1)$, where p is a prime not dividing m and φ is Euler's totient function. As $m \mid p^{\varphi(m)} - 1$, the cyclic group $F^* = F \setminus \{0\}$ contains an element γ of order m. Since $|\{a^m \colon a \in F^*\}| = |F^*|/m \geqslant n-1$, there are $c_1, \ldots, c_{n-1} \in F^*$ such that $c_1^m, \ldots, c_{n-1}^m$ are pairwise distinct. Clearly the set $A = \{c_i\gamma^j \colon 0 < i < n,\ 0 \leqslant j < m\}$ has cardinality $m(n-1)$. If $a_1, \ldots, a_n \in A$, then $\{a_1^m, \ldots, a_n^m\} \subseteq \{c_1^m, \ldots, c_{n-1}^m\}$ and so $a_1^m, \ldots, a_n^m$ cannot be pairwise distinct.

Now we give one more theorem.

Theorem 1.4. *Let F be a field, $b_1,\ldots,b_n \in F$ and $c_{ij} \in F$ for all $1 \leqslant i < j \leqslant n$. Let $P_1(x),\ldots,P_n(x) \in F[x]$ be monic and of degree $m > 0$, and let $A_1,\ldots,A_n$ be subsets of F with cardinality $k > m(n-1)$. Set $B = (b_j^{i-1})_{1\leqslant i,j\leqslant n}$ and*

$$C = \Big\{ \sum_{i=1}^n a_i\colon a_i \in A_i,\ P_i(a_i) \neq P_j(a_j) \text{ and } a_ib_i - a_jb_j \neq c_{ij} \text{ if } i<j \Big\}. \tag{1.8}$$

(i) *If* $\mathrm{ch}(F) > (k-1)n - (m+1)\binom{n}{2}$ *and* $\mathrm{per}(B) \neq 0$*, then* $|C| > (k-1)n - (m+1)\binom{n}{2} \geqslant (m-1)\binom{n}{2}$.

(ii) *If* $\mathrm{ch}(F) = 2$*,* $m = 1$*,* $k = n+1$ *and* $b_1,\ldots,b_n$ *are pairwise distinct, then we have* $|C| \geqslant n+1$.

(iii) *Suppose that F is the complex field and $b_1,\ldots,b_n$ are qth roots of unity. If $n! \notin D(q)$ where $D(q)$ is as in (1.6), or q is odd and $b_1,\ldots,b_n$ are pairwise distinct, then $|C| \geqslant (k-1)n - (m+1)\binom{n}{2} + 1$.*

Corollary 1.1 ([DKSS]). *Let F be a field of characteristic 2, and let A and $B = \{b_1,\ldots,b_n\}$ be subsets of F with cardinality n. Then there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A such that $a_1b_1,\ldots,a_nb_n$ are pairwise distinct.*

Proof. If $A = F$ then we may simply take $a_i = b_i$ because $b_1^2,\ldots,b_n^2$ are pairwise distinct. If $a \in F \setminus A$, then we may apply Theorem 1.4 (ii) with $A_1 = \ldots = A_n = A \cup \{a\}$. □

For an odd integer $n > 0$, the multiplicative group of the finite field F with $|F| = 2^{\varphi(n)}$ has a cyclic subgroup of order n. This observation of Dasgupta et al. indicates that Corollary 1.1 implies the truth of Snevily's conjecture for any cyclic group of odd order.

Later we will deduce Theorem 1.1 from Theorems 1.2 and 1.4.

2. Auxiliary Results

For convenience we set $\mathbb{N} = \{0,1,2,\ldots\}$, $\mathbb{Z}^+ = \{1,2,3,\ldots\}$ and $(x)_n = \prod_{0\leqslant j<n}(x-j)$ for $n \in \mathbb{N}$. (An empty product is regarded as 1.) For $\sigma \in S_n$ we let $\varepsilon(\sigma)$ take 1 or -1 according to whether $\sigma \in S_n$ is even or odd.

Theorem 2.1. *Let R be a commutative ring with identity, and let $a_{i,j} \in R$ for all $i,j = 1,\ldots,n$. Let $k_1,\ldots,k_n,m_1,\ldots,m_n$ be nonnegative integers with $M = \sum_{i=1}^n m_i + \delta\binom{n}{2} \leqslant \sum_{i=1}^n k_i$ where $\delta \in \{0,1\}$. Then*

$$[x_1^{k_1}\cdots x_n^{k_n}]|a_{i,j}x_j^{m_i}|_{1\leqslant i,j\leqslant n} \prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{\delta} \cdot \Big(\sum_{s=1}^n x_s\Big)^{\sum_{i=1}^n k_i - M}$$
$$= \begin{cases} \sum_{\sigma\in S_n,\ D_\sigma\subseteq\mathbb{N}} \varepsilon(\sigma)N_\sigma \prod_{i=1}^n a_{i,\sigma(i)} & \text{if } \delta = 0, \\ \sum_{\sigma\in T_n} \varepsilon(\sigma')N_\sigma \prod_{i=1}^n a_{i,\sigma(i)} & \text{if } \delta = 1, \end{cases}$$

where

$$\begin{aligned}D_\sigma =&\{k_{\sigma(1)}-m_1,\ldots,k_{\sigma(n)}-m_n\},\\ T_n =&\{\sigma\in S_n\colon D_\sigma\subseteq\mathbb{N} \text{ and } |D_\sigma|=n\},\\ N_\sigma =&\frac{(k_1+\ldots+k_n-M)!}{\prod_{i=1}^n\prod_{\substack{0\leqslant j<k_{\sigma(i)}-m_i\\ j\notin D_\sigma \text{ if } \delta=1}}(k_{\sigma(i)}-m_i-j)}\in\mathbb{Z}^+,\end{aligned}$$

and σ' *(with* $\sigma\in T_n$*) is the unique permutation in* S_n *such that*

$$0\leqslant k_{\sigma(\sigma'(1))}-m_{\sigma'(1)}<\ldots<k_{\sigma(\sigma'(n))}-m_{\sigma'(n)}.$$

Proof. Write

$$\begin{aligned}P(x_1,\ldots,x_n) =&|a_{i,j}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^\delta\\ =&\sum_{\substack{i_1,\ldots,i_n\in\mathbb{N}\\ i_1+\ldots+i_n=M}}c_{i_1,\ldots,i_n}x_1^{i_1}\cdots x_n^{i_n}\end{aligned}$$

where $c_{i_1,\ldots,i_n}\in R$. And let $c=[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\ldots,x_n)(x_1+\ldots+x_n)^K$ where $K=k_1+\ldots+k_n-M$. Clearly

$$\begin{aligned}c =&[x_1^{k_1}\ldots x_n^{k_n}]P(x_1,\ldots,x_n)\sum_{\substack{j_1,\ldots,j_n\in\mathbb{N}\\ j_1+\ldots+j_n=K}}\frac{K!}{j_1!\cdots j_n!}x_1^{j_1}\cdots x_n^{j_n}\\ =&\sum_{\substack{0\leqslant i_1\leqslant k_1,\ldots,0\leqslant i_n\leqslant k_n\\ i_1+\ldots+i_n=M}}\frac{K!}{(k_1-i_1)!\cdots(k_n-i_n)!}c_{i_1,\ldots,i_n}.\end{aligned}$$

It is well known that

$$\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)=|x_j^{i-1}|_{1\leqslant i,j\leqslant n}=\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^n x_j^{\sigma(j)-1}.$$

In the case $\delta=1$, we have

$$\begin{aligned}P(x_1,\ldots,x_n)=&\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^n x_j^{\sigma(j)-1}\times\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{j=1}^n a_{\tau(j),j}x_j^{m_{\tau(j)}}\\ =&\sum_{\sigma\in S_n}\varepsilon(\sigma)\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{j=1}^n a_{\tau(j),j}x_j^{\sigma(j)-1+m_{\tau(j)}}\end{aligned}$$

and hence

$$\begin{aligned}
c =& \sum_{\substack{\sigma,\tau\in S_n\\ \sigma(j)-1+m_{\tau(j)}\leqslant k_j\\ \text{for } j=1,\dots,n}} \varepsilon(\sigma)\varepsilon(\tau)\frac{K!}{\prod_{j=1}^n(k_j-(\sigma(j)-1+m_{\tau(j)}))!}\prod_{j=1}^n a_{\tau(j),j}\\
=& \sum_{\substack{\sigma,\tau\in S_n\\ \sigma(j)-1+m_{\tau(j)}\leqslant k_j\\ \text{for } j=1,\dots,n}} \varepsilon(\sigma)\varepsilon(\tau)\frac{K!\prod_{j=1}^n(k_j-m_{\tau(j)})_{\sigma(j)-1}}{\prod_{j=1}^n(k_j-m_{\tau(j)})!}\prod_{j=1}^n a_{\tau(j),j}\\
=& \sum_{\substack{\tau\in S_n\\ m_{\tau(j)}\leqslant k_j\\ \text{for } j=1,\dots,n}} \varepsilon(\tau)\frac{K!\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^n(k_j-m_{\tau(j)})_{\sigma(j)-1}}{\prod_{j=1}^n(k_j-m_{\tau(j)})!}\prod_{j=1}^n a_{\tau(j),j}\\
=& \sum_{\substack{\tau\in S_n\\ m_{\tau(j)}\leqslant k_j\\ \text{for } j=1,\dots,n}} \varepsilon(\tau)\frac{K!|(k_j-m_{\tau(j)})_{i-1}|_{1\leqslant i,j\leqslant n}}{\prod_{j=1}^n(k_j-m_{\tau(j)})!}\prod_{j=1}^n a_{\tau(j),j}.
\end{aligned}$$

Similarly, if $\delta = 0$ then

$$\begin{aligned}
c =& \sum_{\substack{\tau\in S_n\\ m_{\tau(j)}\leqslant k_j\\ \text{for } j=1,\dots,n}} \varepsilon(\tau)\frac{K!}{\prod_{j=1}^n(k_j-m_{\tau(j)})!}\prod_{j=1}^n a_{\tau(j),j}\\
=& \sum_{\substack{\sigma\in S_n\\ D_\sigma\subseteq\mathbb{N}}} \varepsilon(\sigma)\frac{K!}{\prod_{i=1}^n(k_{\sigma(i)}-m_i)!}\prod_{i=1}^n a_{i,\sigma(i)}
\end{aligned}$$

as desired.

Since $x^r = (x)_r + \sum_{0\leqslant t<r} S(r,t)(x)_t$ for $r = 0, 1, \dots, n-1$ where $S(r,t)$ are Stirling numbers of the second kind, for $\tau \in S_n$ we have

$$\begin{aligned}
&|(k_j-m_{\tau(j)})_{i-1}|_{1\leqslant i,j\leqslant n} = |(k_j-m_{\tau(j)})^{i-1}|_{1\leqslant i,j\leqslant n}\\
=& \prod_{1\leqslant s<t\leqslant n}\big(k_t-m_{\tau(t)}-(k_s-m_{\tau(s)})\big)\\
=&(-1)^{|\{1\leqslant s<t\leqslant n:\ \tau(s)>\tau(t)\}|}\prod_{\substack{1\leqslant s,t\leqslant n\\ \tau(s)<\tau(t)}}\big(k_t-m_{\tau(t)}-(k_s-m_{\tau(s)})\big)\\
=&\varepsilon(\tau)\prod_{1\leqslant i<j\leqslant n}\big(k_{\tau^{-1}(j)}-m_j-(k_{\tau^{-1}(i)}-m_i)\big).
\end{aligned}$$

Therefore, if $\delta=1$ then

$$\begin{aligned}
c=&\sum_{\substack{\sigma\in S_n\\ D_\sigma\subseteq\mathbb{N}}}\frac{K!\prod_{1\leqslant i<j\leqslant n}(k_{\sigma(j)}-m_j-(k_{\sigma(i)}-m_i))}{\prod_{i=1}^n(k_{\sigma(i)}-m_i)!}\prod_{i=1}^n a_{i,\sigma(i)}\\
=&\sum_{\sigma\in T_n}\frac{K!\varepsilon(\sigma')\prod_{u,v\in D_\sigma,\ u<v}(v-u)}{\prod_{i=1}^n\prod_{0\leqslant j<k_{\sigma(i)}-m_i}(k_{\sigma(i)}-m_i-j)}\prod_{i=1}^n a_{i,\sigma(i)}\\
=&\sum_{\sigma\in T_n}\varepsilon(\sigma')N_\sigma\prod_{i=1}^n a_{i,\sigma(i)}.
\end{aligned}$$

By the above we also have $N_\sigma\in\mathbb{Z}^+$ for all those $\sigma\in T_n$.

The proof of Theorem 2.1 is now complete. □

Corollary 2.1. *Let R be a commutative ring with identity, and let $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ be a matrix with all the a_{ij} in R. Let $k,m_1,\ldots,m_n$ be nonnegative integers with $m_1\leqslant\ldots\leqslant m_n\leqslant k$.*

(i) *We have*

$$\begin{aligned}
&[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}(x_1+\ldots+x_n)^{kn-\sum_{i=1}^n m_i}\\
&=\frac{(kn-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n(k-m_i)!}\det(A).
\end{aligned}\tag{2.1}$$

(ii) *If $m_1<\ldots<m_n$ then*

$$\begin{aligned}
&[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\cdot\left(\sum_{s=1}^n x_s\right)^{kn-\binom n2-\sum_{i=1}^n m_i}\\
&=(-1)^{\binom n2}\frac{(kn-\binom n2-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n\prod_{\substack{m_i<j\leqslant k\\ j\neq m_{i+1},\ldots,m_n}}(j-m_i)}\mathrm{per}(A).
\end{aligned}$$

Proof. Let $\delta\in\{0,1\}$, and suppose that $m_1<\ldots<m_n$ if $\delta=1$. Then $K=kn-\sum_{i=1}^n m_i-\delta\binom n2\geqslant 0$. Set

$$c=[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^\delta\cdot(x_1+\ldots+x_n)^K.$$

By Theorem 2.1, if $\delta=0$ then $c=(K!/\prod_{i=1}^n(k-m_i)!)\det(A)$. In the case $\delta=1$ we should have

$$\begin{aligned}
c=&\frac{K!}{\prod_{i=1}^n\prod_{\substack{0\leqslant r<k-m_i\\ k-r\neq m_{i+1},\ldots,m_n}}(k-m_i-r)}\sum_{\sigma\in S_n}\varepsilon(\sigma')\prod_{i=1}^n a_{i,\sigma(i)}\\
=&\frac{K!}{\prod_{i=1}^n\prod_{\substack{m_i<j\leqslant k\\ j\neq m_{i+1},\ldots,m_n}}(j-m_i)}(-1)^{\binom n2}\mathrm{per}(A).
\end{aligned}$$

This completes the proof. □

Corollary 2.2. *Let $k_1,\ldots,k_n,m_1,\ldots,m_n$ be nonnegative integers with*

$$k_1-m_1>\ldots>k_n-m_n\geqslant 0 \tag{2.2}$$

and

$$\min_{1\leqslant i<n}(m_{i+1}-m_i)\geqslant \max_{1\leqslant i\leqslant n}k_i-\min_{1\leqslant i\leqslant n}k_i. \tag{2.3}$$

Let $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ be a matrix with $a_{ij}\in\mathbb{N}$ and $\prod_{i=1}^m a_{ii}\neq 0$. Put $L=\sum_{i=1}^n(k_i-m_i)-\binom{n}{2}$. Then, for the coefficient c of $x_1^{k_1}\cdots x_n^{k_n}$ in the polynomial

$$|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\cdot(x_1+\ldots+x_n)^L,$$

we have $0<(-1)^{n(n-1)/2}c\leqslant L!\mathrm{per}(A)$.

Proof. In view of (2.3), if $\sigma\in S_n$ then

$$k_{\sigma(1)}-m_1\geqslant k_{\sigma(2)}-m_2\geqslant\ldots\geqslant k_{\sigma(n)}-m_n.$$

Thus, for any $\sigma\in T_n$ we have $\varepsilon(\sigma')=(-1)^{\binom{n}{2}}$ because $\sigma'(i)=n-i+1$ for $i=1,\ldots,n$. Observe that T_n contains the identity of S_n and $N_\sigma\leqslant L!$ for all $\sigma\in T_n$. Therefore $(-1)^{\binom{n}{2}}c=\sum_{\sigma\in T_n}N_\sigma\prod_{i=1}^n a_{i,\sigma(i)}$ is a positive integer not larger than $L!\mathrm{per}(A)$. We are done. □

Theorem 2.2. *Let R be a commutative ring with identity, and let $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ be a matrix with all the a_{ij} in R. Let $k,l_1,\ldots,l_n,m_1,\ldots,m_n$ be nonnegative integers with $K=kn-\sum_{i=1}^n(l_i+m_i)\geqslant 0$. Then*

$$\begin{aligned}&[x_1^k\cdots x_n^k]|a_{ij}x_j^{l_i}|_{1\leqslant i,j\leqslant n}|x_j^{m_i}|_{1\leqslant i,j\leqslant n}(x_1+\ldots+x_n)^K\\ =&[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}|x_j^{l_i}|_{1\leqslant i,j\leqslant n}(x_1+\ldots+x_n)^K.\end{aligned} \tag{2.4}$$

Proof. Let c_1 and c_2 denote the left-hand side and the right-hand side of (2.4) respectively. Observe that

$$\begin{aligned}c_1=&[x_1^k\cdots x_n^k]\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^n(a_{\sigma(j),j}x_j^{l_{\sigma(j)}})\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{j=1}^n x_j^{m_{\tau(j)}}\cdot\left(\sum_{s=1}^n x_s\right)^K\\ =&\sum_{\substack{\sigma,\tau\in S_n\\ l_{\sigma(j)}+m_{\tau(j)}\leqslant k\\ \text{for } j=1,\ldots,n}}\varepsilon(\sigma)\varepsilon(\tau)\left[\prod_{j=1}^n x_j^{k-l_{\sigma(j)}-m_{\tau(j)}}\right](x_1+\ldots+x_n)^K\prod_{j=1}^n a_{\sigma(j),j}\\ =&\sum_{\substack{\sigma,\tau\in S_n\\ l_{\sigma(j)}+m_{\tau(j)}\leqslant k\\ \text{for } j=1,\ldots,n}}\varepsilon(\sigma)\varepsilon(\tau)\frac{K!}{\prod_{j=1}^n(k-l_{\sigma(j)}-m_{\tau(j)})!}\prod_{j=1}^n a_{\sigma(j),j}.\end{aligned}$$

Similarly,

$$c_2=\sum_{\substack{\sigma,\tau\in S_n\\ m_{\sigma(j)}+l_{\tau(j)}\leqslant k\\ \text{for } j=1,\ldots,n}}\varepsilon(\sigma)\varepsilon(\tau)\frac{K!}{\prod_{j=1}^n(k-m_{\sigma(j)}-l_{\tau(j)})!}\prod_{j=1}^n a_{\sigma(j),j}.$$

If $l_i>k$ for some $i=1,\ldots,n$, then both c_1 and c_2 vanish. Now suppose that $k\geqslant\max_{1\leqslant i\leqslant n}l_i$. Then

$$\begin{aligned}c_1=&\sum_{\sigma,\tau\in S_n}\varepsilon(\sigma)\varepsilon(\tau)\frac{K!\prod_{j=1}^n(k-l_{\sigma(j)})_{m_{\tau(j)}}}{\prod_{j=1}^n(k-l_{\sigma(j)})!}\prod_{j=1}^n a_{\sigma(j),j}\\ =&\sum_{\sigma\in S_n}\varepsilon(\sigma)\frac{K!\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{j=1}^n(k-l_{\sigma(j)})_{m_{\tau(j)}}}{(k-l_1)!\cdots(k-l_n)!}\prod_{j=1}^n a_{\sigma(j),j}\end{aligned}$$

and

$$\begin{aligned}c_2=&\sum_{\sigma,\tau\in S_n}\varepsilon(\sigma)\varepsilon(\tau)\frac{K!\prod_{j=1}^n(k-l_{\tau(j)})_{m_{\sigma(j)}}}{\prod_{j=1}^n(k-l_{\tau(j)})!}\prod_{j=1}^n a_{\sigma(j),j}\\ =&\sum_{\sigma\in S_n}\varepsilon(\sigma)\frac{K!\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{j=1}^n(k-l_{\tau(j)})_{m_{\sigma(j)}}}{(k-l_1)!\cdots(k-l_n)!}\prod_{j=1}^n a_{\sigma(j),j}.\end{aligned}$$

Note that

$$\begin{aligned}&\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{j=1}^n(k-l_{\sigma(j)})_{m_{\tau(j)}}\\ =&\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{i=1}^n(k-l_{\sigma\tau^{-1}(i)})_{m_i}=\varepsilon(\sigma)|(k-l_j)_{m_i}|_{1\leqslant i,j\leqslant n}\\ =&\varepsilon(\sigma)\sum_{\tau\in S_n}\varepsilon(\tau\sigma^{-1})\prod_{i=1}^n(k-l_{\tau\sigma^{-1}(i)})_{m_i}=\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{j=1}^n(k-l_{\tau(j)})_{m_{\sigma(j)}}.\end{aligned}$$

So we have $c_1=c_2$. □

3. Proof of Theorems 1.1–1.4

Theorem 1.2 of [A1] implies the following basic lemma.

Lemma 3.1 ([A1, Theorem 4.1; ANR, Theorem 2.1])**.** *Let $A_1,\ldots,A_n$ be finite subsets of a field F with $k_i=|A_i|>0$ for $i=1,\ldots,n$. Let $P(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]\setminus\{0\}$ and $\deg P\leqslant\sum_{i=1}^n(k_i-1)$. If*

$$[x_1^{k_1-1}\cdots x_n^{k_n-1}]P(x_1,\ldots,x_n)(x_1+\ldots+x_n)^{\sum_{i=1}^n(k_i-1)-\deg P}\neq0,$$

then

$$|\{a_1+\ldots+a_n\colon a_i\in A_i,\ P(a_1,\ldots,a_n)\neq 0\}|\geqslant\sum_{i=1}^n(k_i-1)-\deg P+1.$$

Proof of Theorem 1.2. Applying Corollary 2.1 we find that

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}]\prod_{1\leqslant i<j\leqslant n}(P_j(x_j)-P_i(x_i))\cdot(x_1+\ldots+x_n)^K\\=&[x_1^{k-1}\cdots x_n^{k-1}]|b_j^{i-1}x_j^{(i-1)m}|_{1\leqslant i,j\leqslant n}(x_1+\ldots+x_n)^K\\=&\frac{K!}{\prod_{i=1}^n(k-1-(i-1)m)!}|b_j^{i-1}|_{1\leqslant i,j\leqslant n}\\=&\frac{K!}{\prod_{r=0}^{n-1}(k-1-rm)!}\prod_{1\leqslant i<j\leqslant n}(b_j-b_i)\end{aligned}$$

and

$$\begin{aligned}&\left[\prod_{s=1}^n x_s^{k-1}\right]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(P_j(x_j)-P_i(x_i))\cdot(x_1+\ldots+x_n)^{K-\binom n2}\\=&\left[\prod_{s=1}^n x_s^{k-1}\right]|b_j^{i-1}x_j^{(i-1)m}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\cdot(x_1+\ldots+x_n)^{K-\binom n2}\\=&(-1)^{\binom n2}\frac{(K-\binom n2)!}{\prod_{i=1}^n\prod_{\substack{(i-1)m<j\leqslant k-1\\ j/m\neq i,\ldots,n-1}}(j-(i-1)m)}\mathrm{per}(B).\end{aligned}$$

In view of Lemma 3.1 we have parts (i) and (ii) of Theorem 1.2.

Now suppose that F is the complex field and $b_1,\ldots,b_n$ are qth roots of unity. Then $\mathrm{per}(B)=\sum_{\sigma\in S_n}b_\sigma$ where $b_\sigma=\prod_{i=1}^n b_i^{\sigma(i)-1}$ is a qth root of unity. For any integer t relatively prime to q, the cyclotomic field $\mathbb{Q}(e^{2\pi i/q})$ has an automorphism ρ_t with $\rho_t(e^{2\pi i/q})=e^{2\pi it/q}$ and therefore

$$\sum_{\sigma\in S_n}b_\sigma^t=\sum_{\sigma\in S_n}\rho_t(b_\sigma)=\rho_t(\mathrm{per}(B)).$$

If $\mathrm{per}(B)=0$, then $\sum_{\sigma\in S_n}b_\sigma^t=0$ for all those $t\in\mathbb{Z}$ divisible by none of the prime divisors of q, and thus $n!=|S_n|\in D(q)$ by Lemma 9 of [Su1]. This proves part (iii) of Theorem 1.2. □

Proof of Theorem 1.3. (i) As $m>k_n-k_1\geqslant k_{i+1}-k_i$ for $i=1,\ldots,n-1$, we have

$$k_1-1>k_2-1-m>\ldots>k_n-1-(n-1)m\geqslant 0.$$

Thus $\sum_{i=1}^n(k_i-1-(i-1)m)\geqslant\sum_{i=0}^{n-1}i$ and hence $L\geqslant 0$. Let

$$l=[x_1^{k_1-1}\cdots x_n^{k_n-1}]|x_j^{(i-1)m}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\cdot(x_1+\ldots+x_n)^L.$$

Then $0<(-1)^{n(n-1)/2}l\leqslant L!n!$ by Corollary 2.2. Observe that

$$[x_1^{k_1-1}\cdots x_n^{k_n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(P_j(x_j)-P_i(x_i))\cdot(x_1+\ldots+x_n)^L$$

coincides with le where e is the identity of the field F. If $\mathrm{ch}(F)>L!n!$, then $le\neq 0$ and hence $|T|\geqslant L+1$ by Lemma 3.1.

(ii) It is clear that

$$L\geqslant m(n-1)n-(m+1)\binom{n}{2}=(m-1)\binom{n}{2}=\frac{(m-1)(n-1)}{2}n.$$

If $k_1=\ldots=k_n=k$ and $n\geqslant\mathrm{ch}(F)>L$, then $k-1=m(n-1)$ and $(m-1)(n-1)<2$, thus $m=1$ and $k=n\geqslant\mathrm{ch}(F)$ (in this case $L=0$), or $m=n=2=\mathrm{ch}(F)$ and $k=3$ (in this case $L=1$).

In light of Theorem 1.2(ii) and the above, it suffices to deduce a contradiction under the conditions $\mathrm{ch}(F)=m=n=2$, $k_1=k_2=3$ and $T=\emptyset$. Let a,b,c be the three elements of A_1. If $d\in A_2\setminus A_1$, then $P_1(x)-P_2(d)=0$ for $x=a,b,c$, which is absurd since $\deg P_1(x)=2$. Therefore $A_2\subseteq A_1$ and hence $A_2=A_1=\{a,b,c\}$. As $T=\emptyset$ we have $P_1(a)=P_2(b)=P_1(c)=P_2(a)=P_1(b)$, thus $P_1(x)=P_2(a)$ for $x=a,b,c$, which also leads to a contradiction.

The proof of Theorem 1.3 is now complete. □

Proof of Theorem 1.4. Note that $L=(k-1)n-(m+1)\binom{n}{2}\geqslant(m-1)\binom{n}{2}$. In view of Theorem 2.2 and Corollary 2.1 (ii),

$$\begin{aligned}&\left[\prod_{i=1}^n x_i^{k-1}\right]\prod_{1\leqslant i<j\leqslant n}(P_j(x_j)-P_i(x_i))(b_jx_j-b_ix_i+c_{ij})\cdot\left(\sum_{s=1}^n x_s\right)^L\\&=\left[\prod_{i=1}^n x_i^{k-1}\right]|x_j^{(i-1)m}|_{1\leqslant i,j\leqslant n}|b_j^{i-1}x_j^{i-1}|_{1\leqslant i,j\leqslant n}\left(\sum_{s=1}^n x_s\right)^L\\&=(-1)^{\binom{n}{2}}(N\mathrm{per}(B))\end{aligned}$$

where

$$N=\frac{L!}{\prod_{i=1}^n\prod_{\substack{(i-1)m<j\leqslant k-1\\ j/m\neq i,\ldots,n-1}}(j-(i-1)m)}.$$

If $\mathrm{ch}(F)>L$ and $\mathrm{per}(B)\neq 0$, then $N\mathrm{per}(B)\neq 0$ and hence $|C|>L$ by Lemma 3.1. This proves part (i).

When $\mathrm{ch}(F)=2,\ m=1,\ k=n+1$ and $b_1,\ldots,b_n$ are pairwise distinct, we have

$$\begin{aligned} N\mathrm{per}(B) =& \frac{n!}{\prod_{i=1}^{n}\prod_{\substack{i-1<j\leqslant n\\ j\neq i,\ldots,n-1}}(j-(i-1))}\mathrm{per}(B)\\ =&\mathrm{per}(B)=\det(B)=\prod_{1\leqslant i<j\leqslant n}(b_j-b_i)\neq 0\end{aligned}$$

and hence $|C|\geqslant L+1=n+1$. So part (ii) also holds.

Combining part (i) with Theorem 1.2 (iii) and Remark 1.2, we obtain part (iii) of Theorem 1.4. □

Proof of Theorem 1.1. Let H be the subgroup of G generated by the finite set $A_1\cup\ldots\cup A_n\cup\{b_1,\ldots,b_n\}$. By the structure theorem for finitely generated abelian groups, H is isomorphic to the direct sum $\mathrm{Tor}(H)\oplus\mathbb{Z}^r$ for some $r\in\mathbb{N}$, where $\mathrm{Tor}(H)=\{a\in H\colon \text{the order of } a \text{ is finite}\}$ is a finite subgroup of G and hence cyclic. Let $h=|\mathrm{Tor}(H)|$ and choose an even integer $h'>2$ so that $h\mid h'$ and $\varphi(h')/2\geqslant r+1$. By Dirichlet's unit theorem (cf. [H, Theorem 100]), the unit group $U_{h'}$ of the ring $\mathbb{Z}[e^{2\pi i/h'}]$ is isomorphic to $(\mathbb{Z}/h'\mathbb{Z})\oplus\mathbb{Z}^{\varphi(h')/2-1}$. Thus we can identify the additive group H with a subgroup of the multiplicative group $U_{h'}$. So, without loss of generality, we may simply let G be the multiplicative group $\mathbb{C}^*=\mathbb{C}\setminus\{0\}$. (There is an alternate way to embed H into the group $\mathbb{C}^*$: Take any minimal basis $c_0,\ldots,c_r$ of H where c_0 is a torsion element of order h. Then map c_0 to $e^{2\pi i/h}$ and $c_1,\ldots,c_r$ onto any set of r algebraically independent elements of the uncountable unit circle $\{e^{2\pi i\theta}\colon 0\leqslant\theta<1\}$. Clearly the map can be extended in a unique way to an embedding of H into the multiplicative group $\mathbb{C}^*$.)

(i) If $b_1,\ldots,b_n\in\mathbb{C}^*$ are pairwise distinct, then by Theorem 1.2 the sumset

$$\{a_1+\ldots+a_n\colon a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } a_i^m b_i\neq a_j^m b_j \text{ if } i\neq j\}$$

has at least $(k-1)n-m\binom{n}{2}+1$ elements.

(ii) Now let us work under the conditions of Theorem 1.1 (ii). If $b_1,\ldots,b_n\in\mathbb{C}^*$ are of finite order, then they are qth roots of unity where q is the least common multiple of the multiplicative orders of $b_1,\ldots,b_n$. By Remark 1.2 and Theorems 1.2 and 1.4, both

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

and

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

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

So far we have completed the proof of Theorem 1.1. □

Acknowledgments. The author thanks Prof. N. Alon for sending the paper [DKSS] and the referees for their helpful comments.

References

[A1] N. Alon, *Combinatorial Nullstellenstaz*, Combin. Probab. Comput. **8** (1999), 7–29.

[A2] N. Alon, *Additive Latin transversals*, Israel J. Math. **117** (2000), 125–130.

[ANR] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, J. Number Theory **56** (1996), 404–417.

[DKSS] S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, *Transversals of additive Latin squares*, Israel J. Math. **126** (2001), 17–28.

[DH] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. **26** (1994), 140–146.

[H] E. Hecke, *Lectures on the Theory of Algebraic Numbers* (Graduate texts in math.; 77), Springer-Verlag, New York, 1981, pp. 108–116.

[HS] Q. H. Hou and Z. W. Sun, *Restricted sums in a field*, Acta Arith. **102** (2002), 239–249.

[LS] J. X. Liu and Z. W. Sun, *Sums of subsets with polynomial restrictions*, J. Number Theory **97** (2002), 301–304.

[N] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets* (Graduate texts in math.; 165), Springer-Verlag, New York, 1996, pp. 98–107.

[PS] H. Pan and Z. W. Sun, *A lower bound for* $|\{a+b\colon a\in A,\ b\in B,\ P(a,b)\neq 0\}|$, J. Combin. Theory Ser. A **100** (2002), 387–393.

[Sn] H. S. Snevily, *The Cayley addition table of* $\mathbb{Z}_n$, Amer. Math. Monthly **106** (1999), 584–585.

[Su1] Z. W. Sun, *Covering the integers by arithmetic sequences II*, Trans. Amer. Math. Soc. **348** (1996), 4279–4320.

[Su2] Z. W. Sun, *Restricted sums of subsets of* $\mathbb{Z}$, Acta Arith. **99** (2001), 41–60.