Math. Res. Lett. **15** (2008), *no.* 6, 1263–1276

AN ADDITIVE THEOREM AND RESTRICTED SUMSETS

Zhi-Wei Sun

Abstract. Let G be any additive abelian group with cyclic torsion subgroup, and let A, B and C be finite subsets of G with cardinality $n > 0$. We show that there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A, a numbering $\{b_i\}_{i=1}^n$ of the elements of B and a numbering $\{c_i\}_{i=1}^n$ of the elements of C, such that all the sums $a_i + b_i + c_i$ $(1 \leqslant i \leqslant n)$ are (pairwise) distinct. Consequently, each subcube of the Latin cube formed by the Cayley addition table of $\mathbb{Z}/N\mathbb{Z}$ contains a Latin transversal. This additive theorem is an essential result which can be further extended via restricted sumsets in a field.

1. Introduction

In 1999 Snevily [Sn] raised the following beautiful conjecture in additive combinatorics which is currently an active area of research.

Snevily's Conjecture. *Let G be an additive abelian group with $|G|$ odd. Let A and B be subsets of G with cardinality $n \in \mathbb{Z}^+ = \{1, 2, 3, \dots\}$. 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 the sums $a_1 + b_1, \dots, a_n + b_n$ are (pairwise) distinct.*

When $|G|$ is an odd prime, this conjecture was proved by Alon [A2] via the polynomial method rooted in Alon and Tarsi [AT], and developed by Alon, Nathanson and Ruzsa [ANR] (see also [N, pp. 98-107] and [TV, pp. 329-345]) and refined by Alon [A1] in 1999. In 2001 Dasgupta, Károlyi, Serra and Szegedy [DKSS] confirmed Snevily's conjecture for any cyclic group of odd order. In 2003 Sun [Su3] obtained some further extensions of the Dasgupta-Károlyi-Serra-Szegedy result via restricted sums in a field.

In Snevily's conjecture the abelian group is required to have odd order. (An abelian group of even order has an element g of order 2 and hence we don't have the described result for $A = B = \{0, g\}$.) For a general abelian group G with its torsion subgroup $\mathrm{Tor}(G) = \{a \in G : a \text{ has a finite order}\}$ cyclic, if we make no hypothesis on the order of G, what additive properties can we impose on several finite subsets of G with cardinality n? In this direction we establish the following new theorem of additive nature.

Received by the editors February 23, 2007.

2000 *Mathematics Subject Classification.* Primary 11B75; Secondary 05A05, 05B15, 05E99, 11C08, 11P99, 15A15, 20D60, 20K99.

Supported by the National Science Fund (grant 10425103) for Distinguished Young Scholars in China.

Theorem 1.1. *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. In other words, for a certain subset A_{m+1} of G with $|A_{m+1}|=n$, there is a matrix $(a_{ij})_{1\leqslant i\leqslant m+1,\,1\leqslant j\leqslant n}$ such that $\{a_{i1},\ldots,a_{in}\}=A_i$ for all $i=1,\ldots,m+1$ and the column sum $\sum_{i=1}^{m+1}a_{ij}$ vanishes for every $j=1,\ldots,n$.*

Remark 1.1. Theorem 1.1 in the case $m=3$ is essential; the result for $m=5,7,\ldots$ can be obtained by repeated use of the case $m=3$.

Example 1.1. In Theorem 1.1 the condition $2\nmid m$ is indispensable. Let G be an additive cyclic group of even order n. Then G has a unique element g of order 2 and hence $a\neq -a$ for all $a\in G\setminus\{0,g\}$. Thus $\sum_{a\in G}a=0+g=g$. For each $i=1,\ldots,m$ let $a_{i1},\ldots,a_{in}$ be a list of the n elements of G. If those $\sum_{i=1}^m a_{ij}$ with $1\leqslant j\leqslant n$ are distinct, then

$$\sum_{a\in G}a=\sum_{j=1}^n\sum_{i=1}^m a_{ij}=\sum_{i=1}^m\sum_{j=1}^n a_{ij}=m\sum_{a\in G}a,$$

hence $(m-1)g=(m-1)\sum_{a\in G}a=0$ and therefore m is odd.

Example 1.2. The group G in Theorem 1.1 cannot be replaced by an arbitrary abelian group. To illustrate this, we look at the Klein quaternion group

$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}=\{(0,0),(0,1),(1,0),(1,1)\}$$

and its subsets

$$A_1=\{(0,0),(0,1)\},\ A_2=\{(0,0),(1,0)\},\ A_3=\cdots=A_m=\{(0,0),(1,1)\},$$

where $m\geqslant 3$ is odd. For $i=1,\ldots,m$ let a_i,a_i' be a list of the two elements of A_i, then

$$\sum_{i=1}^m(a_i+a_i')=(0,1)+(1,0)+(m-2)(1,1)=(0,0)$$

and hence $\sum_{i=1}^m a_i=-\sum_{i=1}^m a_i'=\sum_{i=1}^m a_i'$.

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 1.1. *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.*

Proof. Just apply Theorem 1.1 with $G=\mathbb{Z}/N\mathbb{Z}$ and $m=3$. □

In 1967 Ryser [R] conjectured that every Latin square of odd order has a Latin transversal. Another conjecture of Brualdi (cf. [D], [DK, p. 103] and [EHNS]) states that every Latin square of order n has a partial Latin transversal of size $n-1$. These and Corollary 1.1 suggest that our following conjecture might be reasonable.

Conjecture 1.1. *Every $n \times n \times n$ Latin cube contains a Latin transversal.*

Note that Conjecture 1.1 does not imply Theorem 1.1 since an $n \times n \times n$ subcube of a Latin cube might have more than n distinct entries.

Corollary 1.2. *Let G be any additive abelian group with cyclic torsion subgroup, and let $A_1, \ldots, A_m$ be subsets of G with cardinality $n \in \mathbb{Z}^+$, where m is even. Suppose that all the elements of A_m have odd order. 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.*

Proof. As $m-1$ is odd, by Theorem 1.1 the elements of A_i $(1 \leqslant i \leqslant m-1)$ can be listed in a suitable order $a_{i1}, \ldots, a_{in}$, such that all the sums $s_j = \sum_{i=1}^{m-1} a_{ij}$ $(1 \leqslant j \leqslant n)$ are distinct. Since all the elements of A_m have odd order, by [Su3, Theorem 1.1(ii)] there is a numbering $\{a_{mj}\}_{j=1}^{n}$ of the elements of A_m such that all the sums $s_j + a_{mj} = \sum_{i=1}^{m} a_{ij}$ $(1 \leqslant j \leqslant n)$ are distinct. We are done. □

As an essential result, Theorem 1.1 might have various potential applications in additive number theory and combinatorial designs.

We can extend Theorem 1.1 via restricted sumsets in a field. The additive order of the multiplicative identity of a field F is either infinite or a prime; we call it the *characteristic* of F and denote it by $\mathrm{ch}(F)$. The reader is referred to [DH], [ANR], [Su2], [HS], [LS], [PS1], [Su3], [SY] and [PS2] for various results on restricted sumsets of the type

$$\{a_1 + \cdots + a_n : \ a_1 \in A_1, \ldots, a_n \in A_n \text{ and } P(a_1, \ldots, a_n) \neq 0\},$$

where $A_1, \ldots, A_n \subseteq F$ and $P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$.

For a finite sequence $\{A_i\}_{i=1}^{n}$ of sets, if $a_1 \in A_1, \ldots, a_n \in A_n$ and $a_1, \ldots, a_n$ are distinct, then the sequence $\{a_i\}_{i=1}^{n}$ is called a *system of distinct representives* (SDR) of $\{A_i\}_{i=1}^{n}$. This concept plays an important role in combinatorics and a celebrated theorem of Hall tells us when $\{A_i\}_{i=1}^{n}$ has an SDR (see, e.g., [Su1]). Most results in our paper involve SDRs of several subsets of a field.

Now we state our second theorem which is much more general than Theorem 1.1.

Theorem 1.2. *Let h, k, l, m, n be positive integers satisfying*

$$k - 1 \geqslant m(n-1) \quad \text{and} \quad l - 1 \geqslant h(n-1). \tag{1.1}$$

Let F be a field with $\mathrm{ch}(F) > \max\{K, L\}$, where

$$K = (k-1)n - (m+1)\binom{n}{2} \text{ and } L = (l-1)n - (h+1)\binom{n}{2}. \tag{1.2}$$

Assume that $c_1, \ldots, c_n \in F$ are distinct and $A_1, \ldots, A_n, B_1, \ldots, B_n$ are subsets of F with

$$|A_1| = \cdots = |A_n| = k \text{ and } |B_1| = \cdots = |B_n| = l. \tag{1.3}$$

Let $P_1(x), \ldots, P_n(x), Q_1(x), \ldots, Q_n(x) \in F[x]$ be monic polynomials with $\deg P_i(x) = m$ and $\deg Q_i(x) = h$ for $i = 1, \ldots, n$. Then, for any $S, T \subseteq F$ with $|S| \leqslant K$

and $|T| \leqslant L$, *there exist* $a_1 \in A_1, \dots, a_n \in A_n, b_1 \in B_1, \dots, b_n \in B_n$ *such that* $a_1 + \dots + a_n \notin S$, $b_1 + \dots + b_n \notin T$, *and also*

$$a_ib_ic_i \neq a_jb_jc_j,\ P_i(a_i) \neq P_j(a_j),\ Q_i(b_i) \neq Q_j(b_j) \quad \text{if } 1 \leqslant i < j \leqslant n. \tag{1.4}$$

Remark 1.2. If h, k, l, m, n are positive integers satisfying (1.1), then the integers K and L given by (1.2) are nonnegative since

$$K \geqslant m(n-1)n - (m+1)\binom{n}{2} = (m-1)\binom{n}{2} \text{ and } L \geqslant (h-1)\binom{n}{2}.$$

From Theorem 1.2 we can deduce the following extension of Theorem 1.1.

Theorem 1.3. *Let* G *be an additive abelian group with cyclic torsion subgroup. Let* h, k, l, m, n *be positive integers satisfying* (1.1). *Assume that* $c_1, \dots, c_n \in G$ *are distinct, and* $A_1, \dots, A_n, B_1, \dots, B_n$ *are subsets of* G *with* $|A_1| = \dots = |A_n| = k$ *and* $|B_1| = \dots = |B_n| = l$. *Then, for any sets* S *and* T *with* $|S| \leqslant (k-1)n - (m+1)\binom{n}{2}$ *and* $|T| \leqslant (l-1)n - (h+1)\binom{n}{2}$, *there are* $a_1 \in A_1, \dots, a_n \in A_n, b_1 \in B_1, \dots, b_n \in B_n$ *such that* $\{a_1, \dots, a_n\} \notin S$, $\{b_1, \dots, b_n\} \notin T$, *and also*

$$a_i + b_i + c_i \neq a_j + b_j + c_j,\ ma_i \neq ma_j,\ hb_i \neq hb_j \quad \text{if } 1 \leqslant i < j \leqslant n. \tag{1.5}$$

Proof. Let H be the subgroup of G generated by the finite set

$$A_1 \cup \dots \cup A_n \cup B_1 \cup \dots \cup B_n \cup \{c_1, \dots, c_n\}.$$

Since $\mathrm{Tor}(H)$ is cyclic and finite, as in the proof of [Su3, Theorem 1.1] we can identify the additive group H with a subgroup of the multiplicative group $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$, where $\mathbb{C}$ is the field of complex numbers. So, without loss of generality, below we simply view G as the multiplicative group $\mathbb{C}^*$.

Let S and T be two sets with $|S| \leqslant (k-1)n - (m+1)\binom{n}{2}$ and $|T| \leqslant (l-1)n - (h+1)\binom{n}{2}$. Then

$$S' = \{a_1 + \dots + a_n :\ a_1 \in A_1, \dots, a_n \in A_n,\ \{a_1, \dots, a_n\} \in S\}$$

and

$$T' = \{b_1 + \dots + b_n :\ b_1 \in B_1, \dots, b_n \in B_n,\ \{b_1, \dots, b_n\} \in T\}$$

are subsets of $\mathbb{C}$ with $|S'| \leqslant |S|$ and $|T'| \leqslant |T|$. By Theorem 1.2 with $P_i(x) = x^m$ and $Q_i(x) = x^h$ $(1 \leqslant i \leqslant n)$, there are $a_1 \in A_1, \dots, a_n \in A_n, b_1 \in B_1, \dots, b_n \in B_n$ such that $a_1 + \dots + a_n \notin S'$ (and hence $\{a_1, \dots, a_n\} \notin S$), $b_1 + \dots + b_n \notin T'$ (and hence $\{b_1, \dots, b_n\} \notin T$), and also

$$a_ib_ic_i \neq a_jb_jc_j,\ a_i^m \neq a_j^m,\ b_i^h \neq b_j^h \quad \text{if } 1 \leqslant i < j \leqslant n.$$

This concludes the proof. □

Remark 1.3. Theorem 1.1 in the case $m = 3$ is a special case of Theorem 1.3.

Here is another extension of Theorem 1.1 via restricted sumsets in a field.

Theorem 1.4. *Let k, m, n be positive integers with $k-1 \geqslant m(n-1)$, and let F be a field with* $\mathrm{ch}(F) > \max\{mn, (k-1-m(n-1))n\}$. *Assume that $c_1, \ldots, c_n \in F$ are distinct, and $A_1, \ldots, A_n, B_1, \ldots, B_n$ are subsets of F with $|A_1| = \cdots = |A_n| = k$ and $|B_1| = \cdots = |B_n| = n$. Let $S_{ij} \subseteq F$ with $|S_{ij}| < 2m$ for all $1 \leqslant i < j \leqslant n$. Then there is an SDR $\{b_i\}_{i=1}^n$ of $\{B_i\}_{i=1}^n$ such that the restricted sumset*

$$S = \{a_1 + \cdots + a_n : a_i \in A_i,\ a_i - a_j \notin S_{ij} \text{ and } a_i b_i c_i \neq a_j b_j c_j \text{ if } i < j\} \tag{1.6}$$

has at least $(k-1-m(n-1))n+1$ elements.

Now we introduce some basic notations in this paper. Let R be any commutative ring with identity. The *permanent* of a matrix $A = (a_{ij})_{1\leqslant i,j\leqslant n}$ over R is given by

$$\mathrm{per}(A) = \|a_{ij}\|_{1\leqslant i,j\leqslant n} = \sum_{\sigma\in S_n} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}, \tag{1.7}$$

where S_n is the symmetric group of all the permutations on $\{1, \ldots, n\}$. Recall that the determinant of A is defined by

$$\det(A) = |a_{ij}|_{1\leqslant i,j\leqslant n} = \sum_{\sigma\in S_n} \varepsilon(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}, \tag{1.8}$$

where $\varepsilon(\sigma)$ is 1 or -1 according as σ is even or odd. We remind the difference between the notations $|\cdot|$ and $\|\cdot\|$. For the sake of convenience, the coefficient of the monomial $x_1^{k_1} \cdots x_n^{k_n}$ in a polynomial $P(x_1, \ldots, x_n)$ over R will be denoted by $[x_1^{k_1} \cdots x_n^{k_n}]P(x_1, \ldots, x_n)$.

In the next section we are going to prove Theorem 1.1 in two different ways. Section 3 is devoted to the study of duality between determinant and permanent. On the basis of Section 3, we will show Theorem 1.2 in Section 4 via the polynomial method. In Section 5, we will present our proof of Theorem 1.4.

2. Two proofs of Theorem 1.1

Lemma 2.1. *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*

$$\begin{aligned}\sum_{\sigma_1,\ldots,\sigma_{m-1}\in S_n} &\varepsilon(\sigma_1\cdots\sigma_{m-1}) \prod_{1\leqslant i<j\leqslant n} \left(a_{mj}\prod_{s=1}^{m-1} a_{s\sigma_s(j)} - a_{mi}\prod_{s=1}^{m-1} a_{s\sigma_s(i)}\right) \\ &= \prod_{1\leqslant i<j\leqslant n} (a_{1j} - a_{1i}) \cdots (a_{mj} - a_{mi}).\end{aligned} \tag{2.1}$$

Proof. Recall that $|x_j^{i-1}|_{1\leqslant i,j\leqslant n} = \prod_{1\leqslant i<j\leqslant n}(x_j - x_i)$ (Vandermonde). Let Σ denote

the left-hand side of (2.1). Then

$$\begin{aligned}\Sigma &= \sum_{\sigma_1,\dots,\sigma_{m-1}\in S_n} \varepsilon(\sigma_1\cdots\sigma_{m-1})|(a_{1,\sigma_1(j)}\cdots a_{m-1,\sigma_{m-1}(j)}a_{mj})^{i-1}|_{1\leqslant i,j\leqslant n}\\
&= \sum_{\sigma_1,\dots,\sigma_{m-1}\in S_n} \varepsilon(\sigma_1)\times\cdots\times\varepsilon(\sigma_{m-1})\\
&\qquad \times\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{i=1}^n(a_{1,\sigma_1(\tau(i))}\cdots a_{m-1,\sigma_{m-1}(\tau(i))}a_{m,\tau(i)})^{i-1}\\
&= \sum_{\tau\in S_n}\varepsilon(\tau)^m\prod_{i=1}^n a_{m,\tau(i)}^{i-1}\times\prod_{s=1}^{m-1}\sum_{\sigma_s\in S_n}\varepsilon(\sigma_s\tau)\prod_{i=1}^n a_{s,\sigma_s\tau(i)}^{i-1}\\
&= \sum_{\tau\in S_n}\varepsilon(\tau)^m\prod_{i=1}^n a_{m,\tau(i)}^{i-1}\times\prod_{s=1}^{m-1}\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{i=1}^n a_{s,\sigma(i)}^{i-1}.\end{aligned}$$

Since m is odd, we finally have

$$\Sigma = |a_{mj}^{i-1}|_{1\leqslant i,j\leqslant n}\prod_{s=1}^{m-1}|a_{sj}^{i-1}|_{1\leqslant i,j\leqslant n} = \prod_{s=1}^{m}\prod_{1\leqslant i<j\leqslant n}(a_{sj}-a_{si}).$$

This proves (2.1). □

Remark 2.1. When $m\in\{2,4,6,\dots\}$, the right-hand side of (2.1) should be replaced by

$$\|a_{mj}^{i-1}\|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(a_{1j}-a_{1i})\cdots(a_{m-1,j}-a_{m-1,i}).$$

Definition 2.1. A subset S of a commutative ring R with identity is said to be *regular* if all those $a-b$ with $a,b\in S$ and $a\neq b$ are units (i.e., invertible elements) of R.

Theorem 2.1. *Let R be a commutative ring with identity, and let $m>0$ be odd. Then, for any regular subsets $A_1,\dots,A_m$ of R with cardinality $n\in\mathbb{Z}^+$, the elements of A_i $(1\leqslant i\leqslant m)$ can be listed in a suitable order $a_{i1},\dots,a_{in}$, so that all the products $\prod_{i=1}^m a_{ij}$ $(1\leqslant j\leqslant n)$ are distinct.*

Proof. The case $m=1$ is trivial. Below we let $m\in\{3,5,\dots\}$.

Write $A_s=\{b_{s1},\dots,b_{sn}\}$ for $s=1,\dots,m$. As all those $b_{sj}-b_{si}$ with $1\leqslant s\leqslant m$ and $1\leqslant i<j\leqslant n$ are units of R, the product

$$\prod_{1\leqslant i<j\leqslant n}(b_{1j}-b_{1i})\cdots(b_{mj}-b_{mi})$$

is also a unit of R and hence nonzero. Thus, by Lemma 2.1 there are $\sigma_1,\dots,\sigma_{m-1}\in S_n$ such that whenever $1\leqslant i<j\leqslant n$ we have

$$b_{1,\sigma_1(i)}\cdots b_{m-1,\sigma_{m-1}(i)}b_{mi}\neq b_{1,\sigma_1(j)}\cdots b_{m-1,\sigma_{m-1}(j)}b_{mj}.$$

For $1 \leqslant s \leqslant m$ and $1 \leqslant j \leqslant n$, let $a_{sj} = b_{s,\sigma_s(j)}$ if $s < m$, and $a_{sj} = b_{sj}$ if $s = m$. Then $\{a_{s1}, \dots, a_{sn}\} = A_s$, and all the products $\prod_{s=1}^m a_{sj}$ $(j = 1, \dots, n)$ are distinct. This concludes the proof. □

Proof of Theorem 1.1. As mentioned in the proof of Theorem 1.3 via Theorem 1.2, without loss of generality we may simply take G to be the multiplicative group $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. As any nonzero element of a field is a unit in the field, the desired result follows from Theorem 2.1 immediately. □

Now we turn to our second approach to Theorem 1.1.

Lemma 2.2. *Let $c_1, \dots, c_n$ be elements of a commutative ring with identity. Then we have*

$$\begin{aligned}&[x_1^{n-1} \cdots x_n^{n-1} y_1^{n-1} \cdots y_n^{n-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)(y_j - y_i)(c_j x_j y_j - c_i x_i y_i) \\ &\qquad = \prod_{1 \leqslant i < j \leqslant n} (c_j - c_i).\end{aligned} \tag{2.2}$$

Proof. Observe that

$$\begin{aligned}&\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)(y_j - y_i)(c_j x_j y_j - c_i x_i y_i) \\ =&|x_i^{j-1}|_{1 \leqslant i,j \leqslant n} |y_i^{j-1}|_{1 \leqslant i,j \leqslant n} |(c_i x_i y_i)^{j-1}|_{1 \leqslant i,j \leqslant n} \\ =& \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^n x_i^{\sigma(i)-1} \times \sum_{\tau \in S_n} \varepsilon(\tau) \prod_{i=1}^n y_i^{\tau(i)-1} \times \sum_{\lambda \in S_n} \varepsilon(\lambda) \prod_{i=1}^n (c_i x_i y_i)^{\lambda(i)-1} \\ =& \sum_{\lambda \in S_n} \varepsilon(\lambda) \prod_{i=1}^n c_i^{\lambda(i)-1} \sum_{\sigma, \tau \in S_n} \varepsilon(\sigma\tau) \prod_{i=1}^n \left(x_i^{\lambda(i)+\sigma(i)-2} y_i^{\lambda(i)+\tau(i)-2} \right).\end{aligned}$$

Thus the left-hand side of (2.2) coincides with

$$\sum_{\lambda \in S_n} \left(\varepsilon(\lambda) \prod_{i=1}^n c_i^{\lambda(i)-1} \right) \varepsilon(\bar{\lambda}\bar{\lambda}) = |c_i^{j-1}|_{1 \leqslant i,j \leqslant n} = \prod_{1 \leqslant i < j \leqslant n} (c_j - c_i),$$

where $\bar{\lambda}(i) = n + 1 - \lambda(i)$ for $i = 1, \dots, n$. We are done. □

Let us recall the following central principle of the polynomial method.

Combinatorial Nullstellensatz [A1]. *Let $A_1, \dots, A_n$ be finite subsets of a field F with $|A_i| > k_i$ for $i = 1, \dots, n$, where $k_1, \dots, k_n$ are nonnegative integers. If the total degree of $f(x_1, \dots, x_n) \in F[x_1, \dots, x_n]$ is $k_1 + \dots + k_n$ and $[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \dots, x_n)$ is nonzero, then $f(a_1, \dots, a_n) \neq 0$ for some $a_1 \in A_1, \dots, a_n \in A_n$.*

Theorem 2.2. *Let $A_1, \dots, A_n$ and $B_1, \dots, B_n$ be subsets of a field F with cardinality n. And let $c_1, \dots, c_n$ be distinct elements of F. Then there is an SDR $\{a_i\}_{i=1}^n$ of*

$\{A_i\}_{i=1}^n$ and an SDR $\{b_i\}_{i=1}^n$ of $\{B_i\}_{i=1}^n$ such that the products $a_1b_1c_1,\ldots,a_nb_nc_n$ are distinct.

Proof. As $c_1,\ldots,c_n$ are distinct, (2.2) implies that

$$[x_1^{n-1}\cdots x_n^{n-1}y_1^{n-1}\cdots y_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(y_j-y_i)(c_jx_jy_j-c_ix_iy_i)\neq 0.$$

Applying the Combinatorial Nullstellensatz, we obtain the desired result. □

Remark 2.2. When $F=\mathbb{C}$, $A_1=\cdots=A_n$ and $B_1=\cdots=B_n$, Theorem 2.2 yields Theorem 1.1 with $m=3$. Note also that Theorems 1.2 and 1.4 are different extensions of Theorem 2.2.

3. Duality between determinant and permanent

Let us first summarize Theorem 2.1 and Corollary 2.1 of Sun [Su3] in the following theorem.

Theorem 3.1 (Sun [Su3])**.** *Let R be a commutative ring with identity, and let $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ be a matrix over R.*

(i) *Let $k_1,\ldots,k_n,m_1,\ldots,m_n\in\mathbb{N}=\{0,1,2,\ldots\}$ 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*

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

where

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

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

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

(ii) *Let $k,m_1,\ldots,m_n\in\mathbb{N}$ with $m_1\leqslant\cdots\leqslant m_n\leqslant k$. Then*

$$\begin{aligned}&[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^{kn-\sum_{i=1}^n m_i}\\&\quad=\frac{(kn-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n(k-m_i)!}\det(A).\end{aligned}\tag{3.1}$$

In the case $m_1 < \cdots < m_n$, we also have

$$\begin{aligned}&[x_1^k \cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\times\left(\sum_{s=1}^n x_s\right)^{kn-\binom{n}{2}-\sum_{i=1}^n m_i}\\ &=(-1)^{\binom{n}{2}}\frac{(kn-\binom{n}{2}-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n\prod_{\substack{m_i<j\leqslant k\\ j\notin\{m_s:\, i<s\leqslant n\}}}(j-m_i)}\mathrm{per}(A).\end{aligned}\tag{3.2}$$

In view of the minor difference between the definitions of determinant and permanent, by modifying the proof of the above result in [Su3] slightly we get the following dual of Theorem 3.1.

Theorem 3.2. *Let R be a commutative ring with identity, and let $A = (a_{ij})_{1\leqslant i,j\leqslant n}$ be a matrix over R.*

(i) *Let $k_1, m_1, \ldots, k_n, m_n \in \mathbb{N}$ 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*

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

where D_σ, T_n, N_σ and σ' are as in Theorem 3.1(i)*.*

(ii) *Let $k, m_1, \ldots, m_n \in \mathbb{N}$ with $m_1 \leqslant \cdots \leqslant m_n \leqslant k$. Then*

$$\begin{aligned}&[x_1^k\cdots x_n^k]\|a_{ij}x_j^{m_i}\|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^{kn-\sum_{i=1}^n m_i}\\ &=\frac{(kn-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n(k-m_i)!}\mathrm{per}(A).\end{aligned}\tag{3.3}$$

In the case $m_1 < \cdots < m_n$, we also have

$$\begin{aligned}&[x_1^k \cdots x_n^k]\|a_{ij}x_j^{m_i}\|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\times\left(\sum_{s=1}^n x_s\right)^{kn-\binom{n}{2}-\sum_{i=1}^n m_i}\\ &=(-1)^{\binom{n}{2}}\frac{(kn-\binom{n}{2}-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n\prod_{\substack{m_i<j\leqslant k\\ j\notin\{m_s:\, i<s\leqslant n\}}}(j-m_i)}\det(A).\end{aligned}\tag{3.4}$$

Remark 3.1. Part (ii) of Theorem 3.2 follows from the first part.

Theorem 3.3. *Let R be a commutative ring with identity, and let $a_{ij} \in R$ for all $i, j = 1, \ldots, n$. Let $k, l_1, \ldots, l_n, m_1, \ldots, m_n \in \mathbb{N}$ with $N = kn - \sum_{i=1}^n (l_i + m_i) \geqslant 0$.*

(i) (Sun [Su3, Theorem 2.2]) *There holds the identity*

$$\begin{aligned}&[x_1^k\cdots x_n^k]|a_{ij}x_j^{l_i}|_{1\leqslant i,j\leqslant n}\,|x_j^{m_i}|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N\\ =&[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\,|x_j^{l_i}|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N.\end{aligned}\tag{3.5}$$

(ii) *We also have the following symmetric identities:*

$$\begin{aligned}&[x_1^k\cdots x_n^k]\|a_{ij}x_j^{l_i}\|_{1\leqslant i,j\leqslant n}\,|x_j^{m_i}|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N\\ =&[x_1^k\cdots x_n^k]\|a_{ij}x_j^{m_i}\|_{1\leqslant i,j\leqslant n}\,|x_j^{l_i}|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N,\end{aligned}\tag{3.6}$$

$$\begin{aligned}&[x_1^k\cdots x_n^k]|a_{ij}x_j^{l_i}|_{1\leqslant i,j\leqslant n}\,\|x_j^{m_i}\|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N\\ =&[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}\,\|x_j^{l_i}\|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N,\end{aligned}\tag{3.7}$$

and

$$\begin{aligned}&[x_1^k\cdots x_n^k]\|a_{ij}x_j^{l_i}\|_{1\leqslant i,j\leqslant n}\,\|x_j^{m_i}\|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N\\ =&[x_1^k\cdots x_n^k]\|a_{ij}x_j^{m_i}\|_{1\leqslant i,j\leqslant n}\,\|x_j^{l_i}\|_{1\leqslant i,j\leqslant n}\,(x_1+\cdots+x_n)^N.\end{aligned}\tag{3.8}$$

Theorem 3.3(ii) can be proved by modifying the proof of [Su3, Theorem 2.2] slightly.

4. Proof of Theorem 1.2

Lemma 4.1. *Let h,k,l,m,n be positive integers satisfying* (1.1)*. Let $c_1,\ldots,c_n$ be elements of a commutative ring R with identity, and let $P(x_1,\ldots,x_n,y_1,\ldots,y_n)$ denote the polynomial*

$$\prod_{1\leqslant i<j\leqslant n}(c_jx_jy_j-c_ix_iy_i)(x_j^m-x_i^m)(y_j^h-y_i^h)\times(x_1+\cdots+x_n)^K(y_1+\cdots+y_n)^L,$$

where K and L are given by (1.2)*. Then*

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}y_1^{l-1}\cdots y_n^{l-1}]P(x_1,\ldots,x_n,y_1,\ldots,y_n)\\ &\qquad=\frac{K!L!}{N}\prod_{1\leqslant i<j\leqslant n}(c_j-c_i),\end{aligned}\tag{4.1}$$

where

$$N=(hm)^{-\binom n2}\prod_{r=0}^{n-1}\frac{(k-1-rm)!(l-1-rh)!}{(r!)^2}\in\mathbb{Z}^+.\tag{4.2}$$

Proof. In view of Theorem 3.3(i) and Theorem 3.1(ii),

$$\begin{aligned}&[y_1^{l-1}\cdots y_n^{l-1}]\prod_{1\leqslant i<j\leqslant n}(c_jx_jy_j-c_ix_iy_i)(y_j^h-y_i^h)\times(y_1+\cdots+y_n)^L\\ =&[y_1^{l-1}\cdots y_n^{l-1}]|(c_jx_j)^{i-1}y_j^{i-1}|_{1\leqslant i,j\leqslant n}|y_j^{(i-1)h}|_{1\leqslant i,j\leqslant n}(y_1+\cdots+y_n)^L\\ =&[y_1^{l-1}\cdots y_n^{l-1}]|(c_jx_j)^{i-1}y_j^{(i-1)h}|_{1\leqslant i,j\leqslant n}|y_j^{i-1}|_{1\leqslant i,j\leqslant n}(y_1+\cdots+y_n)^L\\ =&(-1)^{\binom n2}\frac{L!}{L_0}\|(c_jx_j)^{i-1}\|_{1\leqslant i,j\leqslant n},\end{aligned}$$

where

$$L_0 = \prod_{i=1}^{n} \prod_{\substack{(i-1)h<j\leqslant l-1 \\ j/h\notin\{s\in\mathbb{Z}:\, i\leqslant s<n\}}} (j-(i-1)h) = \prod_{i=1}^{n} \frac{(l-1-(i-1)h)!}{\prod_{0<j\leqslant n-i}(jh)}$$
$$= \prod_{i=1}^{n} \frac{(l-1-(i-1)h)!}{(n-i)!h^{n-i}} = h^{-\binom{n}{2}} \prod_{r=0}^{n-1} \frac{(l-1-rh)!}{r!}.$$

Thus, with helps of Theorem 3.3(ii) and Theorem 3.2(ii), we have

$$\begin{aligned}
&(-1)^{\binom{n}{2}}[x_1^{k-1}\cdots x_n^{k-1}y_1^{l-1}\cdots y_n^{l-1}]P(x_1,\dots,x_n,y_1,\dots,y_n)\\
=&[x_1^{k-1}\cdots x_n^{k-1}]\frac{L!}{L_0}\|(c_jx_j)^{i-1}\|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j^m-x_i^m)\times\left(\sum_{s=1}^n x_s\right)^K\\
=&\frac{L!}{L_0}[x_1^{k-1}\cdots x_n^{k-1}]\|c_j^{i-1}x_j^{i-1}\|_{1\leqslant i,j\leqslant n}|x_j^{(i-1)m}|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^K\\
=&\frac{L!}{L_0}[x_1^{k-1}\cdots x_n^{k-1}]\|c_j^{i-1}x_j^{(i-1)m}\|_{1\leqslant i,j\leqslant n}|x_j^{i-1}|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^K\\
=&\frac{L!}{L_0}(-1)^{\binom{n}{2}}\frac{K!}{K_0}|c_j^{i-1}|_{1\leqslant i,j\leqslant n}=(-1)^{\binom{n}{2}}\frac{K!L!}{K_0L_0}\prod_{1\leqslant i<j\leqslant n}(c_j-c_i),
\end{aligned}$$

where

$$K_0 = \prod_{i=1}^{n} \prod_{\substack{(i-1)m<j\leqslant k-1 \\ j/m\notin\{s\in\mathbb{Z}:\, i\leqslant s<n\}}} (j-(i-1)m) = m^{-\binom{n}{2}} \prod_{r=0}^{n-1} \frac{(k-1-rm)!}{r!}. \tag{4.3}$$

Therefore (4.1) holds with $N = K_0L_0 \in \mathbb{Z}^+$. □

Proof of Theorem 1.2. Let $f(x_1,\dots,x_n,y_1,\dots,y_n)$ denote the polynomial

$$\begin{aligned}
&\prod_{1\leqslant i<j\leqslant n}(P_j(x_j)-P_i(x_i))(Q_j(y_j)-Q_i(y_i))(c_jx_jy_j-c_ix_iy_i)\\
&\times(x_1+\cdots+x_n)^{K-|S|}\prod_{a\in S}(x_1+\cdots+x_n-a)\\
&\times(y_1+\cdots+y_n)^{L-|T|}\prod_{b\in T}(y_1+\cdots+y_n-b).
\end{aligned}$$

Then

$$\deg f \leqslant (m+h+2)\binom{n}{2}+|K|+|L| = (k-1+l-1)n = \sum_{i=1}^{n}(|A_i|-1+|B_i|-1).$$

Since $\mathrm{ch}(F) > \max\{K, L\}$ and $\prod_{1\leqslant i<j\leqslant n}(c_j - c_i) \neq 0$, in view of Lemma 4.1 we have

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}y_1^{l-1}\cdots y_n^{l-1}]f(x_1,\dots,x_n,y_1,\dots,y_n)\\=&[x_1^{k-1}\cdots x_n^{k-1}y_1^{l-1}\cdots y_n^{l-1}]P(x_1,\dots,x_n,y_1,\dots,y_n)\neq 0,\end{aligned}$$

where $P(x_1,\dots,x_n,y_1,\dots,y_n)$ is defined as in Lemma 4.1. Applying the Combinatorial Nullstellensatz we find that $f(a_1,\dots,a_n,b_1,\dots,b_n) \neq 0$ for some $a_1 \in A_1,\dots,a_n \in A_n, b_1 \in B_1,\dots,b_n \in B_n$. Thus (1.4) holds, and also $a_1+\cdots+a_n \notin S$ and $b_1+\cdots+b_n \notin T$. We are done. □

5. Proof of Theorem 1.4

Non-vanishing permanents are useful in combinatorics. For example, Alon's permanent lemma [A1] states that, if $A = (a_{ij})_{1\leqslant i,j\leqslant n}$ is a matrix over a field F with $\mathrm{per}(A) \neq 0$, and $X_1,\dots,X_n$ are subsets of F with cardinality 2, then for any $b_1,\dots,b_n \in F$ there are $x_1 \in X_1,\dots,x_n \in X_n$ such that $\sum_{j=1}^n a_{ij}x_j \neq b_i$ for all $i = 1,\dots,n$.

In contrast with [Su3, Theorem 1.2(ii)], we have the following auxiliary result.

Theorem 5.1. *Let $A_1,\dots,A_n$ be finite subsets of a field F with $|A_1| = \cdots = |A_n| = k$, and let $P_1(x),\dots,P_n(x) \in F[x]$ have degree at most $m \in \mathbb{Z}^+$ with $[x^m]P_1(x),\dots,[x^m]P_n(x)$ distinct. Suppose that $k-1 \geqslant m(n-1)$ and $\mathrm{ch}(F) > (k-1)n-(m+1)\binom{n}{2}$. Then the restricted sumset*

$$C=\left\{\sum_{i=1}^n a_i:\ a_i\in A_i,\ a_i\neq a_j \text{ for } i\neq j,\ \text{and } \|P_j(a_j)^{i-1}\|_{1\leqslant i,j\leqslant n}\neq 0\right\}\tag{5.1}$$

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

Proof. Assume that $|C| \leqslant K = (k-1)n-(m+1)\binom{n}{2}$. Clearly the polynomial

$$\begin{aligned}f(x_1,\dots,x_n):=&\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\times\|P_j(x_j)^{i-1}\|_{1\leqslant i,j\leqslant n}\\&\times\prod_{c\in C}(x_1+\cdots+x_n-c)\times(x_1+\cdots+x_n)^{K-|C|}\end{aligned}$$

has degree not exceeding $(k-1)n = \sum_{i=1}^n(|A_i|-1)$. Since $\mathrm{ch}(F)$ is greater than K, and those $b_i = [x^m]P_i(x)$ with $1 \leqslant i \leqslant n$ are distinct, with the help of Theorem 3.2(ii) we have

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}]f(x_1,\dots,x_n)\\=&[x_1^{k-1}\cdots x_n^{k-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\times\|b_j^{i-1}x_j^{(i-1)m}\|_{1\leqslant i,j\leqslant n}\left(\sum_{s=1}^n x_s\right)^K\\=&(-1)^{\binom{n}{2}}\frac{K!}{K_0}|b_j^{i-1}|_{1\leqslant i,j\leqslant n}=(-1)^{\binom{n}{2}}\frac{K!}{K_0}\prod_{1\leqslant i<j\leqslant n}(b_j-b_i)\neq 0,\end{aligned}$$

where K_0 is given by (4.3). Thus, by the Combinatorial Nullstellensatz, $f(a_1,\dots,a_n) \neq 0$ for some $a_1 \in A_1,\dots,a_n \in A_n$. Clearly $\sum_{i=1}^n a_i \in C$ if $\|P_j(a_j)^{i-1}\|_{1\leqslant i,j\leqslant n} \neq 0$ and $a_i \neq a_j$ for all $1 \leqslant i < j \leqslant n$. So we also have $f(a_1,\dots,a_n) = 0$ by the definition of $f(x_1,\dots,x_n)$. The contradiction ends our proof. □

Corollary 5.1. *Let $A_1,\dots,A_n$ and $B=\{b_1,\dots,b_n\}$ be subsets of a field with cardinality n. Then there is an SDR $\{a_i\}_{i=1}^n$ of $\{A_i\}_{i=1}^n$ such that the permanent $\|(a_jb_j)^{i-1}\|_{1\leqslant i,j\leqslant n}$ is nonzero.*

Proof. Simply apply Theorem 5.1 with $k=n$ and $P_j(x)=b_jx$ for $j=1,\dots,n$. $\square$

Lemma 5.1. *Let $k,m,n\in\mathbb{Z}^+$ with $k-1\geqslant m(n-1)$. Then*

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{2m-1}(x_jy_j-x_iy_i)\times\left(\sum_{s=1}^n x_s\right)^N\\ =&(-1)^{m\binom{n}{2}}\frac{(mn)!N!}{(m!)^n n!}\prod_{r=0}^{n-1}\frac{(rm)!}{(k-1-rm)!}\times\|y_j^{i-1}\|_{1\leqslant i,j\leqslant n},\end{aligned}\tag{5.2}$$

where $N=(k-1-m(n-1))n$.

Proof. Since both sides of (5.2) are polynomials in $y_1,\dots,y_n$, it suffices to show that (5.2) with $y_1,\dots,y_n$ replaced by $a_1,\dots,a_n\in\mathbb{C}$ always holds.

By Lemma 2.1 and (2.6) of [SY], we have

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{2m-1}(a_jx_j-a_ix_i)\times\left(\sum_{s=1}^n x_s\right)^N\\ =&\frac{N!}{((k-1)!)^n}(-1)^{m\binom{n}{2}}\frac{m!(2m)!\cdots(nm)!}{(m!)^n n!}\|a_j^{i-1}\|_{1\leqslant i,j\leqslant n}\prod_{0<r<n}\prod_{s=1}^{rm}(k-s)\\ =&(-1)^{m\binom{n}{2}}\frac{(mn)!N!}{(m!)^n n!}\|a_j^{i-1}\|_{1\leqslant i,j\leqslant n}\prod_{r=0}^{n-1}\frac{(rm)!}{(k-1-rm)!}.\end{aligned}$$

This concludes the proof. $\square$

Proof of Theorem 1.4. Since $c_1,\dots,c_n$ are distinct and $|B_1|=\dots=|B_n|=n$, by Corollary 5.1 there is an SDR $\{b_i\}_{i=1}^n$ of $\{B_i\}_{i=1}^n$ such that $\|(b_jc_j)^{i-1}\|_{1\leqslant i,j\leqslant n}\neq 0$.

Suppose that $|S|\leqslant N=(k-1-m(n-1))n$. We want to derive a contradiction. Let $f(x_1,\dots,x_n)$ denote the polynomial

$$\begin{aligned}&\prod_{1\leqslant i<j\leqslant n}\left((b_jc_jx_j-b_ic_ix_i)(x_j-x_i)^{2m-1-|S_{ij}|}\prod_{c\in S_{ij}}(x_j-x_i+c)\right)\\ &\qquad\times(x_1+\dots+x_n)^{N-|S|}\prod_{a\in S}(x_1+\dots+x_n-a).\end{aligned}$$

Then

$$\deg f\leqslant 2m\binom{n}{2}+N=(k-1)n=\sum_{i=1}^n(|A_i|-1).$$

With the help of Lemma 5.1, we have

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}]f(x_1,\dots,x_n)\\ =&[x_1^{k-1}\cdots x_n^{k-1}](x_1+\dots+x_n)^N\prod_{1\leqslant i<j\leqslant n}(b_jc_jx_j-b_ic_ix_i)(x_j-x_i)^{2m-1}\\ =&(-1)^{m\binom{n}{2}}\frac{(mn)!N!}{(m!)^n n!}\prod_{r=0}^{n-1}\frac{(rm)!}{(k-1-rm)!}\times\|(b_jc_j)^{i-1}\|_{1\leqslant i,j\leqslant n}\neq 0\end{aligned}$$

since $\mathrm{ch}(F) > \max\{mn, N\}$. By the Combinatorial Nullstellensatz, there are $a_1 \in A_1, \ldots, a_n \in A_n$ such that $f(a_1, \ldots, a_n) \neq 0$. On the other hand, we do have $f(a_1, \ldots, a_n) = 0$, because $a_1 + \cdots + a_n \in S$ if $a_i - a_j \notin S_{ij}$ and $a_i b_i c_i \neq a_j b_j c_j$ for all $1 \leqslant i < j \leqslant n$. So we get a contradiction. $\square$

References

[A1] N. Alon, *Combinatorial Nullstellensatz*, 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.

[AT] N. Alon and M. Tarsi, *A nowhere-zero point in linear mappings*, Combinatorica **9** (1989), 393–395.

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

[DK] J. Dénes and A. D. Keedwell, *Latin Squares and their Applications*, Academic Press, New York, 1974.

[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.

[D] A. A. Drisko, *Transversals in row-Latin rectangles*, J. Combin. Theory Ser. A **84** (1998), 181–195.

[EHNS] P. Erdős, D. R. Hickerson, D. A. Norton and S. K. Stein, *Has every latin square of order n a partial latin transversal of size $n-1$?* Amer. Math. Monthly **95** (1988), 428–430.

[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, New York, 1996.

[PS1] 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.

[PS2] H. Pan and Z. W. Sun, *Restricted sumsets and a conjecture of Lev*, Israel J. Math. **154** (2006), 21–28.

[R] H. J. Ryser, *Neuere Probleme der Kombinatorik*, in: Vorträge über Kombinatorik (Oberwolfach, 1967), Mathematiches Forschungsinstitut, Oberwolfach, 1968, pp. 69–91.

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

[Su1] Z. W. Sun, *Hall's theorem revisited*, Proc. Amer. Math. Soc. **129** (2001), 3129–3131.

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

[Su3] Z. W. Sun, *On Snevily's conjecture and restricted sumsets*, J. Combin. Theory Ser. A **103** (2003), 288–301.

[SY] Z. W. Sun and Y. N. Yeh, *On various restricted sumsets*, J. Number Theory **114** (2005), 209–220.

[TV] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zwsun@nju.edu.cn *Homepage*: http://math.nju.edu.cn/∼zwsun

State Key Laboratory of Novel Software Technology, Nanjing University, Nanjing 210093, People's Republic of China