ACTA ARITHMETICA
102.3 (2002)

Restricted sums in a field

by

QING-HU HOU (Tianjin) and ZHI-WEI SUN (Nanjing)

1. Introduction. Let $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ stand for the field of all residue classes modulo prime p. In 1964 P. Erdős and H. Heilbronn (cf. [EH] and [Gu]) conjectured that for each nonempty subset A of $\mathbb{Z}_p$ there are at least $\min\{p, 2|A|-3\}$ residue classes modulo p that can be written as the sum of two distinct elements of A. This had been open for thirty years until J. A. Dias da Silva and Y. O. Hamidoune [DH] proved the following result with the help of the representation theory of symmetric groups.

THE DIAS DA SILVA–HAMIDOUNE THEOREM. *Let F be any field and n a positive integer. Then for any finite subset A of F we have*

$$|n^\wedge A| \geq \min\{p(F), n|A| - n^2 + 1\}, \tag{1.1}$$

where $n^\wedge A$ denotes the set of all sums of n distinct elements of A, and $p(F)$ represents the additive order of the multiplicative identity of F.

Let F be a field and e be its multiplicative identity. If e has a finite order as an element of the additive group of F, then the order $p(F)$ is a prime and is called the *characteristic* of F; otherwise, $p(F)$ is $+\infty$ and the characteristic of F is usually said to be 0.

In 1995–1996, N. Alon, M. B. Nathanson and I. Z. Ruzsa [ANR1, ANR2] invented a polynomial method to obtain results similar to the Dias da Silva–Hamidoune theorem.

By means of the polynomial method and the determination of certain coefficients in a polynomial in product form, we obtain

THEOREM 1.1. *Let k, m be nonnegative integers and n a positive integer. Let F be a field of characteristic p where p is zero or a prime with p/n greater than m and $k + m - mn - 1$. Let $A_1, \ldots, A_n$ be subsets of F with*

2000 *Mathematics Subject Classification*: Primary 11B75; Secondary 05A05, 11C08.

The second author is responsible for all the communications, and 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 P.R. China.

cardinality k. *For any* $i, j = 1, \ldots, n$ *with* $i \neq j$, *let* $S_{ij} \subseteq F$ *and* $|S_{ij}| \leq m$. *Then, for the set*

$$C = \{a_1 + \ldots + a_n : a_1 \in A_1, \ldots, a_n \in A_n,\ a_i - a_j \notin S_{ij} \text{ if } i \neq j\}, \tag{1.2}$$

we have

$$|C| \geq (k + m - mn - 1)n + 1. \tag{1.3}$$

REMARK 1.1. In the case $m = 0$, the result also follows from the well known Cauchy–Davenport theorem (cf. Theorem 2.2 of [N]) which asserts that for any finite nonempty subsets A and B of a field F we have $|A+B| \geq \min\{p(F), |A|+|B|-1\}$. When $m = 1$ and $S_{ij} = \{0\}$, the set C given by (1.2) coincides with $n^\wedge A$ if $A_1 = \ldots = A_n = A$. Since $(k+m-mn-1)n-(k-1) = (k-1-mn)(n-1)$, the condition $p(F) > n\max\{m, k+m-mn-1\}$ implies that $k \leq p(F)$. If the condition $p(F) > (k+m-mn-1)n$ in Theorem 1.1 is violated, then $k'+m-mn-1 = [(p(F)-1)/n]$ for some $0 < k' < k$ (where $[\alpha]$ denotes the greatest integer not exceeding the real number α), thus for a certain $C' \subseteq C$ we have

$$|C| \geq |C'| \geq (k' + m - mn - 1)n + 1 = n\left[\frac{p(F) - 1}{n}\right] + 1.$$

For convenience we now set

$$\mathbb{N} = \{0, 1, 2, \ldots\} \quad \text{and} \quad \mathbb{Z}^+ = \{1, 2, 3, \ldots\}.$$

If $k, l \in \mathbb{Z}$ then we put

$$[k, l) = \{x \in \mathbb{Z} : k \leq x < l\} \quad \text{and} \quad [k, l] = \{x \in \mathbb{Z} : k \leq x \leq l\}.$$

The following example shows that the lower bound in (1.3) can be attained if it is positive.

EXAMPLE 1.1. Let F be a field and e be its multiplicative identity. Let $k, m \in \mathbb{N}$, $n \in \mathbb{Z}^+$ and $m(n-1) < k \leq p(F)$. Set $A_1 = \ldots = A_n = \{xe : x \in [0, k)\}$, $S = \{xe : x \in [0, m)\}$ and

$$C = \{a_1 + \ldots + a_n : a_1 \in A_1, \ldots, a_n \in A_n,\ a_i - a_j \notin S \text{ if } i \neq j\}.$$

Then $|A_1| = \ldots = |A_n| = k$, $|S| \leq m$ and $C = \{xe : x \in I\}$ where

$$I = \{a_1 + \ldots + a_k : a_1, \ldots, a_k \in [0, k),\ |a_i - a_j| \geq m \text{ whenever } i \neq j\}.$$

Observe that I is the union of the following intervals:

$$0 + m + 2m + \ldots + (n-3)m + (n-2)m + [(n-1)m, k-1],$$
$$0 + m + 2m + \ldots + (n-3)m + [(n-2)m, k-1-m] + k - 1,$$
$$\cdots\cdots\cdots$$
$$[0, k-1-(n-1)m] + (k-1-(n-2)m) + \ldots + (k-1-m) + (k-1).$$

Therefore

$$I=\Big[\sum_{r=0}^{n-1}rm,\sum_{r=0}^{n-1}(k-1-rm)\Big]=\Big[\frac{mn(n-1)}{2},(k-1)n-\frac{mn(n-1)}{2}\Big]$$

and $|I|=(k+m-mn-1)n+1$. So $|C|=\min\{p(F),(k+m-mn-1)n+1\}$.

COROLLARY 1.1. *Let $k\in\mathbb{N}$, $m,n\in\mathbb{Z}^+$ and $k>m(n-1)$. Let F be a field with $p(F)>n\max\{m,k-1-m(n-1)\}$, and $A_1,\dots,A_n$ be subsets of F with cardinality k. Let $b_1,\dots,b_n\in F$, $0\in S\subseteq F$ and $|S|=m$. Then the set*

$$\{a_1+\ldots+a_n: a_i\in A_i,\ a_i\neq a_j \text{ and } a_i+b_i-(a_j+b_j)\notin S \text{ if } i\neq j\} \tag{1.4}$$

is nonempty, and its cardinality is greater than $(k-1-m(n-1))n$.

Proof. For $1\le i<j\le n$ we put

$$S_{ij}=\{0\}\cup\{x-b_i+b_j: x\in S\setminus\{0\}\}\quad\text{and}\quad S_{ji}=\{x-b_j+b_i: x\in S\}.$$

Applying Theorem 1.1 we immediately get the required result. ■

REMARK 1.2. The fact that (1.4) is nonempty under the assumptions of Corollary 1.1 was realized by Alon [A2] in the case $F=\mathbb{Z}_p$ with p being a prime. In the special case $k=n$, $m=1$ and $S=\{0\}$, the result implies that for any odd prime p and subsets A,B of $\mathbb{Z}_p$ with cardinality n, there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A and a numbering $\{b_i\}_{i=1}^n$ of those in B such that the sums $a_1+b_1,\dots,a_n+b_n$ are distinct. In fact, H. S. Snevily [Sn] even conjectured that the above $\mathbb{Z}_p$ can be replaced by any abelian group whose order is odd.

Let us end this section with a conjecture posed by the second author.

CONJECTURE 1.1. *Let F be any field, and $A_1,\dots,A_n$ be subsets of F which are finite and nonempty. For $1\le i<j\le n$ let S_{ij} and S_{ji} be finite subsets of F with $|S_{ij}|\equiv|S_{ji}|\pmod 2$. Then, for the set C given by (1.2), we have*

$$|C|\ge\min\Big\{p(F),\sum_{i=1}^n|A_i|-\sum_{1\le i<j\le n}(|S_{ij}|+|S_{ji}|)-n+1\Big\}. \tag{1.5}$$

The conjecture is open even when F is the rational field $\mathbb{Q}$; the reader may consult [Su] for related results.

2. Two auxiliary propositions

PROPOSITION 2.1. *Let $A_1,\dots,A_n$ be finite subsets of a field F with $|A_i|\ge k_i$ for $i\in[1,n]$ where $k_1,\dots,k_n\in\mathbb{Z}^+$. Let $\lambda(x_1,\dots,x_n),\mu(x_1,\dots,x_n)\in F[x_1,\dots,x_n]$ and $\deg\mu>0$. Put*

$$C=\{\mu(a_1,\dots,a_n): a_1\in A_1,\dots,a_n\in A_n,\ \lambda(a_1,\dots,a_n)\neq 0\}. \tag{2.1}$$

Then there is no $\omega(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$ *such that*

$$\lambda(x_1,\ldots,x_n)\omega(x_1,\ldots,x_n)\mu(x_1,\ldots,x_n)^{|C|}$$

is of degree $\sum_{i=1}^n(k_i-1)$ *and the coefficient of* $x_1^{k_1-1}\ldots x_n^{k_n-1}$ *is nonzero.*

Proof. Suppose that such an $\omega(x_1,\ldots,x_n)$ exists. Write

$$f(x_1,\ldots,x_n)=\lambda(x_1,\ldots,x_n)\omega(x_1,\ldots,x_n)\prod_{c\in C}(\mu(x_1,\ldots,x_n)-c).$$

Then $\deg f=\sum_{i=1}^n(k_i-1)$, and the coefficient of $\prod_{i=1}^n x_i^{k_i-1}$ in f is nonzero. By Theorem 1.2 of [A1], 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, by the very definition of C, $f(a_1,\ldots,a_n)=0$ for all $a_1\in A_1,\ldots,a_n\in A_n$. So we get a contradiction. ■

PROPOSITION 2.2. *Let* k,m,n *be integers with* $m\geq 0$, $n>1$ *and* $k>m(n-1)$. *Then the coefficient of* $x_1^{k-1}\ldots x_n^{k-1}$ *in*

$$\prod_{1\leq i<j\leq n}(x_i-x_j)^{2m}(x_1+\ldots+x_n)^{n(k+m-mn-1)}$$

coincides with

$$(-1)^{mn(n-1)/2}\frac{((k+m-mn-1)n)!}{(m!)^n}\prod_{j=1}^n\frac{(jm)!}{(k-1-(j-1)m)!}. \tag{2.2}$$

To prove this proposition is the main difficulty in our paper; the proof will be presented in the next section.

Now we deduce Theorem 1.1 from Propositions 2.1 and 2.2.

Proof of Theorem 1.1. As $|F|\geq p(F)>mn\geq m$, we can extend each S_{ij} $(i\neq j)$ to a subset of F with cardinality m. Without any loss of generality, we may assume that all the S_{ij} have cardinality m.

Let $l=k+m-mn-1$. The case $l<0$ or $n=1$ is trivial. Below we handle the case $l\geq 0$ and $n\geq 2$.

Suppose on the contrary that $|C|\leq ln$. Put

$$\lambda(x_1,\ldots,x_n)=\prod_{1\leq i<j\leq n}\prod_{c_{ij}\in S_{ij}}(x_i-x_j-c_{ij})\prod_{c_{ji}\in S_{ji}}(x_i-x_j+c_{ji}),$$
$$\mu(x_1,\ldots,x_n)=x_1+\ldots+x_n,$$
$$\omega(x_1,\ldots,x_n)=(x_1+\ldots+x_n)^{ln-|C|}.$$

Then (2.1) holds. For

$$f(x_1,\ldots,x_n)=\lambda(x_1,\ldots,x_n)\omega(x_1,\ldots,x_n)\mu(x_1,\ldots,x_n)^{|C|},$$

the total degree is $mn(n-1)+ln = n(k-1) = \sum_{i=1}^n(|A_i|-1)$ and the coefficient of $x_1^{k-1}\dots x_n^{k-1}$ in $f(x_1,\dots,x_n)$ is the same as that in

$$\prod_{1\le i<j\le n}(x_i-x_j)^{2m}(x_1+\dots+x_n)^{ln}\in F[x_1,\dots,x_n].$$

By Proposition 2.2, the coefficient of $x_1^{k-1}\dots x_n^{k-1}$ should be he where e is the (multiplicative) identity of F and

$$h=(-1)^{mn(n-1)/2}\frac{(ln)!}{(m!)^n}\prod_{j=1}^n\frac{(jm)!}{(k-1-(j-1)m)!}\in\mathbb{Z}\setminus\{0\}.$$

In view of Proposition 2.1, we should have $he=0$. So, p is a prime dividing h. Since p is greater than mn and ln, we have $h\not\equiv 0 \pmod p$ and a contradiction follows. ■

3. Proof of Proposition 2.2. For $k=0,1,2,\dots$ we let

$$(x)_k=\prod_{j\in[0,k)}(x-j).$$

(The empty product is regarded as 1.) For $f(x_1,\dots,x_n)\in\mathbb{Q}[x_1,\dots,x_n]$, by coeff $[x_1^{i_1}\dots x_n^{i_n}]$ in $f(x_1,\dots,x_n)$ we mean the coefficient of the monomial $x_1^{i_1}\dots x_n^{i_n}$ in the polynomial $f(x_1,\dots,x_n)$.

Let $m\ge 0$ and $n>1$ be integers. Write

$$f_m(x_1,\dots,x_n)=\prod_{1\le i<j\le n}(x_i-x_j)^{2m}=\sum_{j_1,\dots,j_n}f^{(m)}_{j_1,\dots,j_n}x_1^{j_1}\dots x_n^{j_n}.$$

For any integer $k>m(n-1)$, clearly

$$\begin{aligned}
&\text{coeff }[x_1^{k-1}\dots x_n^{k-1}]\text{ in }f_m(x_1,\dots,x_n)(x_1+\dots+x_n)^{n(k-1-m(n-1))}\\
&=\sum_{\substack{j_1,\dots,j_n\in[0,k)\\ j_1+\dots+j_n=mn(n-1)}}f^{(m)}_{j_1,\dots,j_n}\frac{((k+m-mn-1)n)!}{(k-1-j_1)!\dots(k-1-j_n)!}\\
&=\frac{((k+m-mn-1)n)!}{((k-1)!)^n}\sum_{\substack{j_1,\dots,j_n\in[0,k)\\ j_1+\dots+j_n=mn(n-1)}}f^{(m)}_{j_1,\dots,j_n}(k-1)_{j_1}\dots(k-1)_{j_n}\\
&=\frac{((k+m-mn-1)n)!}{((k-1)!)^n}\mathcal{L}(f_m)(k-1),
\end{aligned}$$

where $\mathcal{L}:\mathbb{Q}[x_1,\dots,x_n]\to\mathbb{Q}[x]$ is the linear operator given by

$$\mathcal{L}(x_1^{j_1}\dots x_n^{j_n})=(x)_{j_1}\dots(x)_{j_n}. \tag{3.1}$$

Thus the main problem is to determine $\mathcal{L}(f_m)$.

LEMMA 3.1. *Let m be any positive integer. Then*

$$(x)_0(x)_m\dots(x)_{(n-1)m}\,|\,\mathcal{L}(f_m). \tag{3.2}$$

Proof. Observe that

$$(x)_0(x)_m\dots(x)_{(n-1)m}=\prod_{q=0}^{n-1}\prod_{r=0}^{m-1}(x-(qm+r))^{n-1-q}$$

because $\{j\in[0,n): jm-1\ge qm+r\}=[q+1,n)$ has cardinality $n-1-q$. So it suffices to show that $(x-l)^{n-1-[l/m]}\,|\,\mathcal{L}(f_m)$ for any $l=0,1,\dots,mn-1$.

Let $j_1,\dots,j_n$ be nonnegative integers with $f^{(m)}_{j_1,\dots,j_n}\neq 0$. In order to prove that $\mathcal{L}(x_1^{j_1}\dots x_n^{j_n})=(x)_{j_1}\dots(x)_{j_n}$ is divisible by $(x-l)^{n-1-[l/m]}$, we only need to show that

$$|\{1\le i\le n: j_i>l\}|\ge n-1-\left[\frac{l}{m}\right],\ \text{i.e.}\ |\{1\le i\le n: j_i\le l\}|\le 1+\left[\frac{l}{m}\right].$$

Let $I=\{1\le i\le n: j_i\le l\}\neq\emptyset$. The polynomial $\prod_{i,j\in I,\,i<j}(x_i-x_j)^{2m}$ divides $f_m(x_1,\dots,x_n)$ and each monomial in it has degree $2m\binom{|I|}{2}=m|I|(|I|-1)$. Since $f^{(m)}_{j_1,\dots,j_n}\neq 0$, we have $\sum_{i\in I}j_i\ge m|I|(|I|-1)$ and hence $l\ge j_i\ge m(|I|-1)$ for some $i\in I$. Therefore $|I|\le 1+[l/m]$. This concludes the proof. ∎

LEMMA 3.2. *Let $g(x_1,\dots,x_n)\in\mathbb{Q}[x_1,\dots,x_n]$ and $1\le s<t\le n$. Then*

$$\mathcal{L}((x_s-x_t)g(x_1,\dots,x_n))=\mathcal{L}\biggl(x_t\frac{\partial g(x_1,\dots,x_n)}{\partial x_t}\biggr)-\mathcal{L}\biggl(x_s\frac{\partial g(x_1,\dots,x_n)}{\partial x_s}\biggr).$$

Proof. For any nonnegative integers $j_1,\dots,j_n$, we have

$$\begin{aligned}\mathcal{L}((x_s-x_t)x_1^{j_1}\dots x_n^{j_n})&=\prod_{\substack{i=1\\ i\neq s,t}}^{n}(x)_{j_i}\cdot((x)_{j_s+1}(x)_{j_t}-(x)_{j_s}(x)_{j_t+1})\\&=(x)_{j_1}\dots(x)_{j_n}(x-j_s-x+j_t)=j_t(x)_{j_1}\dots(x)_{j_n}-j_s(x)_{j_1}\dots(x)_{j_n}\\&=\mathcal{L}\biggl(x_t\frac{\partial(x_1^{j_1}\dots x_n^{j_n})}{\partial x_t}\biggr)-\mathcal{L}\biggl(x_s\frac{\partial(x_1^{j_1}\dots x_n^{j_n})}{\partial x_s}\biggr).\end{aligned}$$

Write $g(x_1,\dots,x_n)=\sum_{j_1,\dots,j_n}g_{j_1,\dots,j_n}x_1^{j_1}\dots x_n^{j_n}$ where $g_{j_1,\dots,j_n}\in\mathbb{Q}$. Then, by the above,

$$\begin{aligned}
&\mathcal{L}((x_s - x_t)g(x_1, \ldots, x_n)) \\
&\quad= \sum_{j_1,\ldots,j_n} g_{j_1,\ldots,j_n}\mathcal{L}((x_s - x_t)x_1^{j_1}\ldots x_n^{j_n}) \\
&\quad= \mathcal{L}\Big(\sum g_{j_1,\ldots,j_n} x_t \frac{\partial(x_1^{j_1}\ldots x_n^{j_n})}{\partial x_t}\Big) - \mathcal{L}\Big(\sum g_{j_1,\ldots,j_n} x_s \frac{\partial(x_1^{j_1}\ldots x_n^{j_n})}{\partial x_s}\Big) \\
&\quad= \mathcal{L}\Big(x_t \frac{\partial g(x_1, \ldots, x_n)}{\partial x_t}\Big) - \mathcal{L}\Big(x_s \frac{\partial g(x_1, \ldots, x_n)}{\partial x_s}\Big). \blacksquare
\end{aligned}$$

LEMMA 3.3. *Let $\Delta \neq \emptyset$ be a finite multi-set whose elements are ordered pairs in the form (i,j) with $1 \le i < j \le n$. Let $g(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ and $1 \le r \le n$. Then*

$$\frac{\partial}{\partial x_r}\Big(g(x_1, \ldots, x_n) \prod_{(i,j)\in\Delta} (x_i - x_j)\Big) = \sum_{(s,t)\in\Delta} \frac{g_{s,t}(x_1, \ldots, x_n)}{x_s - x_t} \prod_{(i,j)\in\Delta} (x_i - x_j)$$

where $g_{s,t}(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ and $\deg g_{s,t} \le \deg g$.

Proof. Let (u,v) be any element of Δ. Then

$$\begin{aligned}
&\frac{\partial}{\partial x_r}\Big(g(x_1, \ldots, x_n) \prod_{(i,j)\in\Delta} (x_i - x_j)\Big) \\
&\quad= \frac{\partial g(x_1, \ldots, x_n)}{\partial x_r} \prod_{(i,j)\in\Delta} (x_i - x_j) + g(x_1, \ldots, x_n)\frac{\partial}{\partial x_r} \prod_{(i,j)\in\Delta} (x_i - x_j) \\
&\quad= \Big(\frac{\partial g(x_1, \ldots, x_n)}{\partial x_r}(x_u - x_v)\Big) \frac{\prod_{(i,j)\in\Delta}(x_i - x_j)}{x_u - x_v} \\
&\qquad + g(x_1, \ldots, x_n) \sum_{(s,t)\in\Delta} \frac{\partial(x_s - x_t)}{\partial x_r} \cdot \frac{\prod_{(i,j)\in\Delta}(x_i - x_j)}{x_s - x_t}.
\end{aligned}$$

Clearly $\deg g$ is not less than the degrees of those $g(x_1, \ldots, x_n)\frac{\partial(x_s - x_t)}{\partial x_r}$ (where $(s,t) \in \Delta$) and $\frac{\partial g(x_1,\ldots,x_n)}{\partial x_r}(x_u - x_v)$. So the desired result follows. ■

Combining Lemmas 3.2 and 3.3 we have

LEMMA 3.4. *Let m be a nonnegative integer and Δ a multi-set with elements in the form (i,j) $(1 \le i < j \le n)$ and $|\Delta|$ equal to $2m$. Then for any $g(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ we have*

$$\deg \mathcal{L}\Big(g(x_1, \ldots, x_n) \prod_{(i,j)\in\Delta} (x_i - x_j)\Big) \le \deg g + m. \tag{3.3}$$

Proof. We use induction on m. The case $m=0$ is trivial, so we proceed to the induction step.

Assume $m\in\mathbb{Z}^+$. Let (s,t) be any element in Δ and Δ' denote the multi-set Δ with one (s,t) omitted. By Lemmas 3.2 and 3.3,

$$\mathcal{L}\Big(g(x_1,\dots,x_n)\prod_{(i,j)\in\Delta}(x_i-x_j)\Big) = \mathcal{L}\bigg(x_t\frac{\partial(g(x_1,\dots,x_n)\prod_{(i,j)\in\Delta'}(x_i-x_j))}{\partial x_t}\bigg) - \mathcal{L}\bigg(x_s\frac{\partial(g(x_1,\dots,x_n)\prod_{(i,j)\in\Delta'}(x_i-x_j))}{\partial x_s}\bigg)$$

can be written in the form

$$\mathcal{L}\bigg(\sum_{(u,v)\in\Delta'}\frac{g_{uv}(x_1,\dots,x_n)}{x_u-x_v}\prod_{(i,j)\in\Delta'}(x_i-x_j)\bigg) = \sum_{(u,v)\in\Delta'}\mathcal{L}\bigg(\frac{g_{uv}(x_1,\dots,x_n)}{x_u-x_v}\prod_{(i,j)\in\Delta'}(x_i-x_j)\bigg)$$

where $g_{uv}(x_1,\dots,x_n)\in\mathbb{Q}[x_1,\dots,x_n]$ and $\deg g_{uv}\le\deg g+1$. Choose $(u,v)\in\Delta'$ so that $\deg\mathcal{L}\big(\frac{g_{uv}(x_1,\dots,x_n)}{x_u-x_v}\prod_{(i,j)\in\Delta'}(x_i-x_j)\big)$ is maximal. Let Δ'' be the multi-set Δ' with one (u,v) deleted. Then $|\Delta''|=2(m-1)$ and

$$\deg\mathcal{L}\Big(g(x_1,\dots,x_n)\prod_{(i,j)\in\Delta}(x_i-x_j)\Big) \le \deg\mathcal{L}\Big(g_{uv}(x_1,\dots,x_n)\prod_{(i,j)\in\Delta''}(x_i-x_j)\Big).$$

By the induction hypothesis,

$$\deg\mathcal{L}\Big(g_{uv}(x_1,\dots,x_n)\prod_{(i,j)\in\Delta''}(x_i-x_j)\Big)\le\deg g_{uv}+(m-1)\le\deg g+m.$$

So we have (3.3). ∎

LEMMA 3.5. *Let $m\ge0$ and $n>1$ be integers. Then*

$$\text{coeff }[x_1^{m(n-1)}\dots x_n^{m(n-1)}]\text{ in }\prod_{1\le i<j\le n}(x_i-x_j)^{2m} = (-1)^{mn(n-1)/2}\frac{(mn)!}{(m!)^n}. \tag{3.4}$$

Proof. Let $m_1,\dots,m_n\in\mathbb{N}$. When we expand $\prod_{1\le i,j\le n,\,i\ne j}(1-x_i/x_j)^{m_j}$ as a Laurent polynomial in $x_1,\dots,x_n$ (i.e., negative exponents allowed), the constant term is the multinomial coefficient $(\sum_{i=1}^n m_i)!/\prod_{i=1}^n(m_i!)$. This result was conjectured by F. J. Dyson [D] in 1962. An elegant proof given by I. J. Good [Go] in 1970 uses the Lagrange interpolation formula. D. Zeilberger [Z] gave a combinatorial proof of Dyson's conjecture in the following equivalent form:

$$\text{coeff } [x_1^{m_1(n-1)} \dots x_n^{m_n(n-1)}] \text{ in } \prod_{1 \le i < j \le n} (x_i - x_j)^{m_i + m_j} = (-1)^{\sum_{j=1}^n (j-1)m_j} \frac{(m_1 + \dots + m_n)!}{m_1! \dots m_n!}.$$

Taking $m_1 = \dots = m_n = m$ in the above equality, we get (3.4). ∎

Now we are ready to prove

THEOREM 3.1. *Let* $f(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)^{2m}$ *where* $m \in \mathbb{N}$ *and* $n > 1$*. Then*

$$\mathcal{L}(f) = (-1)^{mn(n-1)/2} \frac{m!(2m)! \dots (nm)!}{(m!)^n} (x)_0 (x)_m \dots (x)_{(n-1)m}. \tag{3.5}$$

Proof. By Lemma 3.1, there exists a $g(x) \in \mathbb{Q}[x]$ such that

$$\mathcal{L}(f) = (x)_0 (x)_m \dots (x)_{(n-1)m} g(x).$$

Note that $\deg \prod_{j=0}^{n-1} (x)_{jm} = \sum_{j=0}^{n-1} jm = mn(n-1)/2$. By Lemma 3.4, $\deg \mathcal{L}(f) \le \deg 1 + m\binom{n}{2}$. So $g(x)$ is a constant $c \in \mathbb{Q}$. As we mentioned at the beginning of this section,

$$\text{coeff } [x_1^{mn-m} \dots x_n^{mn-m}] \text{ in } f(x_1, \dots, x_n) = \frac{((mn - m + m - mn)n)!}{((mn-m)!)^n} \mathcal{L}(f)(mn - m).$$

In view of Lemma 3.5, we have

$$c \prod_{j=0}^{n-1} (mn - m)_{jm} = \mathcal{L}(f)(mn - m) = ((mn-m)!)^n \cdot (-1)^{mn(n-1)/2} \frac{(mn)!}{(m!)^n},$$

i.e.,

$$c = (-1)^{mn(n-1)/2} \frac{(mn)!}{(m!)^n} \prod_{j=0}^{n-1} (mn - m - jm)! = (-1)^{mn(n-1)/2} \frac{\prod_{i=1}^n (im)!}{(m!)^n}.$$

This ends the proof. ∎

Proof of Proposition 2.2. Let $f(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)^{2m}$. By Theorem 3.1, we have

$$\mathcal{L}(f)(k-1) = (-1)^{mn(n-1)/2} \frac{m!(2m)! \dots (nm)!}{(m!)^n} \prod_{i=0}^{n-1} (k-1)_{im}.$$

Thus

$$\begin{aligned}&\text{coeff }[x_1^{k-1}\dots x_n^{k-1}] \text{ in } f(x_1,\dots,x_n)(x_1+\dots+x_n)^{(k-1-m(n-1))n}\\&\quad=\frac{((k+m-mn-1)n)!}{((k-1)!)^n}\mathcal{L}(f)(k-1)\\&\quad=\frac{((k+m-mn-1)n)!}{((k-1)!)^n}(-1)^{mn(n-1)/2}\frac{\prod_{j=1}^n(jm)!}{(m!)^n}\prod_{j=1}^n(k-1)_{(j-1)m}\\&\quad=(-1)^{mn(n-1)/2}\frac{\prod_{j=1}^n(jm)!}{(m!)^n}\cdot\frac{((k+m-mn-1)n)!}{\prod_{j=1}^n(k-1-(j-1)m)!}.\end{aligned}$$

We are done. ∎

Acknowledgements. The authors are indebted to Prof. N. Alon for his comments and the referee for his suggestions. The work was done during the second author's visit to the Center for Combinatorics at Nankai University; he thants Prof. William Y. C. Chen for the invitation and the Center for its support.

References

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

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

[ANR1] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *Adding distinct congruence classes modulo a prime*, Amer. Math. Monthly 102 (1995), 250–255.

[ANR2] —, —, —, *The polynomial method and restricted sums of congruence classes*, J. Number Theory 56 (1996), 404–417.

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

[D] F. J. Dyson, *Statistical theory of the energy levels of complex systems I*, J. Math. Phys. 3 (1962), 140–156.

[EH] P. Erdős and H. Heilbronn, *On the addition of residue classes mod p*, Acta Arith. 9 (1964), 149–159.

[Go] I. J. Good, *Short proof of a conjecture of Dyson*, J. Math. Phys. 11 (1970), 1884.

[Gu] R. K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer, New York, 1994, 129–131.

[N] M. B. Nathanson, *Additive Number Theory*: *Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math. 165, Springer, New York, 1996.

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

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

[Z] D. Zeilberger, *A combinatorial proof of Dyson's conjecture*, Discrete Math. 41 (1982), 317–321.

Center for Combinatorics
Nankai University
Tianjin 300071, P.R. China
E-mail: hqh@public.tpt.tj.cn

Department of Mathematics
Nanjing University
Nanjing 210093, P.R. China
E-mail: zwsun@nju.edu.cn

Received on 23.8.1999
and in revised form on 24.7.2001 (3676)