J. Number Theory 97(2002), no. 2, 301–304

SUMS OF SUBSETS WITH POLYNOMIAL RESTRICTIONS

Jian-Xin Liu and Zhi-Wei Sun

(Communicated by D. Goss)

Abstract. Let F be a field of characteristic p and let $P(x) \in F[x]$ be a polynomial of degree $m > 0$. Let $A_1, \ldots, A_n$ be finite subsets of F with $|A_n| = k > m(n-1)$ and $|A_{i+1}| - |A_i| \in \{0, 1\}$ for $i = 1, \ldots, n-1$. If $p = 0$ or $p > (k-1)n - (m+1)\binom{n}{2}$, then for the restricted sumset

$$S = \{a_1 + \ldots + a_n : a_1 \in A_1, \ldots, a_n \in A_n, \text{ and } P(a_i) \neq P(a_j) \text{ if } i \neq j\}$$

we have $|S| \geqslant 1 + (k-1)n - (m+1)\binom{n}{2}$. This extends the Erdős–Heilbronn conjecture posed in 1964 and confirmed in 1994.

1. Introduction

In 1994, using the representation theory of symmetric groups, Dias da Silva and Hamidoune ([DH]) proved the following result which was conjectured by Erdős and Heilbronn (cf. [EH]) in the case $n = 2$.

Theorem A. *Let p be a prime and let n be a positive integer. Then, for any subset A of the field $\mathbb{Z}/p\mathbb{Z}$, we have*

$$|n^{\wedge}A| \geqslant \min\{p, n|A| - n^2 + 1\}, \tag{1.1}$$

where $n^{\wedge}A$ denotes the set of all sums of n pairwise distinct elements of A.

In 1995 and 1996 Alon, Nathanson and Ruzsa [ANR1, ANR2] developed their polynomial method (see also [N]) which allowed them to show the following theorem.

Theorem B. *Let p be a prime number, and let $A_1, \ldots, A_n$ be nonempty subsets of $\mathbb{Z}/p\mathbb{Z}$ with $|A_1| < \ldots < |A_n|$ and $\sum_{i=1}^n |A_i| - n(n+1)/2 < p$. Then*

$$\left|\left\{\sum_{i=1}^n a_i : a_i \in A_i, \text{ and } a_i \neq a_j \text{ if } i \neq j\right\}\right| \geqslant \sum_{i=1}^n |A_i| - \frac{n(n+1)}{2} + 1. \tag{1.2}$$

Recent papers [Su] and [HS] are concerned with sums of subsets (of $\mathbb{Z}$ or a field) with linear restrictions. In this paper we will apply the polynomial method of Alon, Nathanson and Ruzsa to obtain the following result.

2000 *Mathematics Subject Classification.* Primary 11B75; Secondary 05A05, 11P70.

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.

Theorem 1.1. *Let k, m, n be positive integers with $k > m(n-1)$, and let F be a field of characteristic p where p is zero or greater than $K = (k-1)n - (m+1)\binom{n}{2}$. Let $A_1, \ldots, A_n$ be subsets of F for which*

$$|A_n| = k \text{ and } |A_{i+1}| - |A_i| \in \{0, 1\} \text{ for } i = 1, \ldots, n-1. \tag{1.3}$$

Let $P_1(x), \ldots, P_n(x) \in F[x]$ be monic and of degree m. Then we have

$$|\{a_1 + \ldots + a_n : a_i \in A_i, \text{ and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j\}| \geqslant K + 1. \tag{1.4}$$

Clearly our Theorem 1.1 is a partial extension of Theorems A and B. It is also related to the main result of Alon [A2] concerning a conjecture of Snevily [Sn].

Example. (i) Let k be an integer greater than $m = 2$ and F be a field of characteristic p where p is zero or an odd prime greater than $(k-1)2-(2+1)\binom{2}{2} = 2k-5$. Let $B = \{je : j \in \mathbb{Z},\ 2j \in [-k, k)\}$ where e denotes the (multiplicative) identity of F. Obviously $|B| = k$. For any $A \subseteq B$ with $|A| \in \{k-1, k\}$, we can easily verify that $|\{a + b : a \in A,\ b \in B,\ a^2 \neq b^2\}| = 2k - 4$.

(ii) The rational field has characteristic 0. Let $A = \{-3, -1, 1, 3, 5\}$ and

$$S = \{a_1 + a_2 + a_3 : a_1, a_2, a_3 \in A \text{ and } a_1^2, a_2^2, a_3^2 \text{ are distinct}\}.$$

Then $S = \{1, 3, 7, 9\}$ and $|S| = (|A| - 1)3 - (2 + 1)\binom{3}{2} + 1$.

2. Proof of Theorem 1.1

We first introduce some notations. As usual, we set $0! = 1$, $(x)_0 = 1$ and $(x)_k = \prod_{j=0}^{k-1}(x-j)$ for $k = 1, 2, 3, \ldots$. If $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ where F is a field, then we write $[x_1^{i_1} \cdots x_n^{i_n}] f(x_1, \ldots, x_n)$ for the coefficient of the monomial $x_1^{i_1} \cdots x_n^{i_n}$ in $f(x_1, \ldots, x_n)$.

The following result is one of the main tools of the polynomial method.

Lemma 2.1 ([A1, Theorem 4.1] and [ANR2, 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 $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \setminus \{0\}$ and $\deg f \leqslant \sum_{i=1}^n (k_i - 1)$. If*

$$[x_1^{k_1-1} \cdots x_n^{k_n-1}] f(x_1, \ldots, x_n)(x_1 + \ldots + x_n)^{\sum_{i=1}^n (k_i-1) - \deg f} \neq 0,$$

then

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

Although this result was formulated in [A1, ANR2] only for the field $\mathbb{Z}/p\mathbb{Z}$ (where p is a prime), it plainly remains valid in any other field.

Proof of Theorem 1.1. For $1 \leqslant i \leqslant n$ clearly $|A_n| - |A_i| \leqslant n - i$, thus we can choose $A_i' \subseteq A_i$ so that $|A_i'| = k - n + i$. Without loss of generality, we assume that $A_i' = A_i$; that is, $k_i = |A_i| = k - n + i$ for $i = 1, \ldots, n$. As the case $K < 0$ or $n = 1$ is trivial, below we suppose $K \geqslant 0$ and $n \geqslant 2$.

Let e denote the multiplicative identity of the field F, and let

$$f(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} (P_j(x_j) - P_i(x_i)).$$

Clearly, $\sum_{i=1}^n (k_i - 1) - \deg f = (k-1)n - \binom{n}{2} - \deg f = K$, and

$$[x_1^{k_1 - 1} \cdots x_n^{k_n - 1}](x_1 + \ldots + x_n)^K f(x_1, \ldots, x_n) = h e^{\binom{n}{2}},$$

where h is the coefficient of $x_1^{k-n} \ldots x_n^{k-1}$ in the polynomial

$$g(x_1, \ldots, x_n) = (x_1 + \ldots + x_n)^K \prod_{1 \leqslant i < j \leqslant n} (x_j^m - x_i^m) \in \mathbb{Z}[x_1, \ldots, x_n].$$

For a permutation $\sigma \in S_n$ of the set $\{1, \ldots, n\}$, let $\operatorname{sign}(\sigma)$ be -1 or 1 according to whether σ is odd or even. By means of Vandermonde's determinant and the multinomial theorem, $g(x_1, \ldots, x_n)$ coincides with

$$\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) x_1^{m(\sigma(1)-1)} \cdots x_n^{m(\sigma(n)-1)} \sum_{\substack{j_1, \ldots, j_n \geqslant 0 \\ j_1 + \ldots + j_n = K}} \frac{K!}{j_1! \cdots j_n!} x_1^{j_1} \cdots x_n^{j_n}.$$

Therefore

$$\begin{aligned} h =& K! \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \frac{(k - 1 - (\sigma(1) - 1)m)_{n-1}}{(k - 1 - (\sigma(1) - 1)m)!} \times \ldots \times \frac{(k - 1 - (\sigma(n) - 1)m)_0}{(k - 1 - (\sigma(n) - 1)m)!} \\ =& \frac{K!(-1)^{\binom{n}{2}}}{\prod_{i=1}^n (k - 1 - (i-1)m)!} \det \|(k - 1 - im)_j\|_{0 \leqslant i, j \leqslant n-1}. \end{aligned}$$

It is well known that $x^j = (x)_j + \sum_{0 \leqslant r < j} S(j, r)(x)_r$, where $S(j, r)$ $(0 \leqslant r < j)$ are Stirling numbers of the second kind. So

$$\begin{aligned} &\det \|(k - 1 - im)_j\|_{0 \leqslant i, j \leqslant n-1} = \det \|(k - 1 - im)^j\|_{0 \leqslant i, j \leqslant n-1} \\ =& (-1)^{\binom{n}{2}} \prod_{0 \leqslant i < j < n} (k - 1 - im - (k - 1 - jm)) \quad \text{(Vandermonde)}. \end{aligned}$$

As $(-1)^{\binom{n}{2}} \det \|(k - 1 - im)_j\|_{0 \leqslant i, j \leqslant n-1}$ divides $\prod_{i=0}^{n-1} (k - 1 - im)!$, we have $h \mid K!$ and hence $p \nmid h$.

Now it suffices to apply Lemma 2.1. $\square$

Acknowledgment. The authors are indebted to the referee for his or her helpful suggestions.

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.

[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] 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.

[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.

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

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

[N] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets* (Graduate texts in mathematics; 165), Springer-Verlag, 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.

Division of Basic Courses, Nanjing Institute of Technology, Nanjing 210013, the People's Republic of China

Department of Mathematics, Nanjing University, Nanjing 210093, the People's Republic of China. *E-mail*: zwsun@nju.edu.cn