Reported on the 2rd Cross-Strait Confer. on Graph Theory and Combin. (Taipei, 2002-06-16)

NEW RESULTS ON SUBSET SUMS

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. In this paper we give a survey of recent results on sumsets of subsets of a field with polynomial restrictions.

Let F be a field and let $F^\times$ be the multiplicative group $F\setminus\{0\}$. The additive order of the (multiplicative) identity of F is either infinite or a prime, we call it the *characteristic* of F.

Let A and B be finite subsets of the field F. Set

$$A+B=\{a+b\colon a\in A \text{ and } b\in B\}$$

and

$$A\dot{+}B=\{a+b\colon a\in A,\ b\in B,\ \text{and } a\ne b\}.$$

The theorem of Cauchy and Davenport asserts that if F is the field of residues modulo a prime p, then

$$|A+B|\ge\min\{p,\ |A|+|B|-1\}.$$

In 1964 Erdős and Heilbronn conjectured that in this case

$$|A\dot{+}A|\ge\min\{p,\ 2|A|-3\},$$

this was confirmed by Dias da Silva and Hamidoune [DH] in 1994 with the help of the representation theory of groups. In 1995–1996 Alon, Nathanson and Ruzsa [J. Number Theory 56(1996)] proposed a polynomial method to handle similar problems, they showed that if $|A| > |B| > 0$ then

$$|A \dot{+} B| \geq \min\{p,\ |A| + |B| - 2\}$$

where p is the characteristic of the field F.

The polynomial method usually yields a nontrivial conclusion provided that certain coefficient of a polynomial, related in some special way to the additive problem under considerations, does not vanish. It can be stated as follows.

Lemma 1 (Alon, Nathanson and Ruzsa)**.** *Let F be a field, and $f(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$. Let $k_1,\ldots,k_n$ be nonnegative integers such that*

$$\hat{f}(k_1,\ldots,k_n) = [x_1^{k_1}\ldots x_n^{k_n}]f(x_1,\ldots,x_n) \neq 0$$

and $\deg f = k_1 + \ldots + k_n$. Let $A_1,\ldots,A_n$ be finite subsets of F with $|A_i| > k_i$ for $i = 1,\ldots,n$. Then there are $a_1 \in A_1,\ldots,a_n \in A_n$ such that $f(a_1,\ldots,a_n) \neq 0$.

Theorem 1 [Alon, Nathanson and Ruzsa, J. Number Theory, 56(1996)**.** *Let F be a field of characteristic p, and $A_1,\ldots,A_n$ be finite nonempty subsets of F with $|A_1| < \ldots < |A_n|$. Then for the set*

$$A_1 \dot{+} \ldots \dot{+} A_n = \left\{ \sum_{i=1}^{n} a_i \colon a_i \in A_i,\ \text{and } a_i \neq a_j \text{ if } i \neq j \right\}$$

we have

$$|A_1 \dot{+} \ldots \dot{+} A_n| \geqslant \left\{ p, \sum_{i=1}^{n} |A_i| - \frac{n(n+1)}{2} + 1 \right\}.$$

The following result can be deduced from Theorem 1.

Theorem 2 [Dias da Silva & Hamidoune, Bull. London Math. Soc. 26(1994)]. *Let F be a field of characteristic p and n a positive integer. Then for any finite subset A of F we have*

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

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

Lemma 2 [Q. H. Hou and Z. W. Sun, Acta Arith. 102(2002)]. *Let k, m, n be integers with $m \geq 0$, $n > 1$ and $k > m(n-1)$. Then the coefficient of $x_1^{k-1} \cdots x_n^{k-1}$ in*

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

coincides with

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

Theorem 3 [Q. H. Hou and Z. W. Sun, Acta Arith. 102(2002)]. *Let k, m be nonnegative integers and n a positive integer. Let F be a field of characteristic p with p/n greater than m and $k+m-mn-1$. Let $A_1, \ldots, A_n$ be subsets of F with 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*

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

we have

$$|C| \geq (k+m-mn-1)n + 1.$$

Theorem 4 [J. X. Liu and Z. W. Sun, J. Number Theory 97(2002)]. *Let k, m, n be positive integers with $k > m(n-1)$, and let F be a field of characteristic p where $p > K = (k-1)n - (m+1)\binom{n}{2}$. Let $A_1, \ldots, A_n$ be subsets of F for which*

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

Let $b_1,\ldots,b_n\in F$, and $P(x)\in F[x]$ have degree m. Then we have

$$|\{a_1+\ldots+a_n\colon a_i\in A_i,\ and\ P(a_i)+b_i\neq P(a_j)+b_j\ \ if\ i\neq j\}|\geqslant K+1.$$

Theorem 5 [Z. W. Sun, J. Combin. Theory Ser. A 103(2003)]**.** *Let F be a field of characteristic p, and $A_1,\ldots,A_n$ be finite subsets of F with $0<k_1=|A_1|\leq\ldots\leq k_n=|A_n|$. Let m be a positive integer such that*

$$k_n>m(n-1)\ \ and\ m>k_n-k_1.$$

Let $b_1,\ldots,b_n\in F$, $P[x,y]\in F[x,y]$, $\deg P=m$, $[x^m]P(x,y)\neq 0$ and

$$S=\left\{\sum_{i=1}^n a_i\colon a_i\in A_i,\ \ a_i\neq a_j\ \ and\ P(a_i,b_i)\neq P(a_j,b_j)\ \ if\ i\neq j\right\}.$$

(i) *We have $K=\sum_{i=1}^n(k_i-1)-(m+1)\binom{n}{2}\geq 0$. If $p>K!n!$, then $|S|\geq K+1$.*

(ii) *When $k_1=\ldots=k_n=k$ and $p>K$, we have $|S|\geq K\geq(m-1)\binom{n}{2}$, and $|S|=K$ only if $k=n\geq p>m=1$ or $p=m=n=2<k=3$.*

Remark. Let F be a field of prime characteristic p. Let $A\subseteq F$, $|A|=n<p$ and $b_1,\ldots,b_n\in F$. By Theorem 5(ii) in the case $m=1$ and $k=n$, there is a numbering $\{a_i\}_{i=1}^n$ of the elements of A such that the sums $a_1+b_1,\ldots,a_n+b_n$ are pairwise distinct. This result was first proved by Alon [Israel J. Math. 117(2000)] in the case $F=\mathbb{Z}/p\mathbb{Z}$, it is connected with a conjecture of Snevily [Amer. Math. Monthly 106(1999)].

The following result was obtained by a somewhat constructive method.

Theorem 6 [Z. W. Sun, Acta Arith. 99(2001)]**.** *Let $A_1,\ldots,A_n$ be finite subsets of $\mathbb{Z}$, and V a set of tuples in the form (s,t,μ,ν,w) where $1\leqslant s,t\leqslant n$, $s\neq t$, $\mu,\nu\in\mathbb{Z}^*=\mathbb{Z}\setminus\{0\}$ and $w\in\mathbb{Z}$. Set*

$$C=\{a_1+\ldots+a_n:a_i\in A_i,\ \ and\ \mu a_i+\nu a_j\neq w\ \ if\ (i,j,\mu,\nu,w)\in V\}.$$

If each $V_i = \{(s,t,\mu,\nu,w) \in V : i \in \{s,t\}\}$ *has cardinality less than* $|A_i|$*, then*

$$|C| \geqslant \sum_{i=1}^{n} |A_i| - 2|V| - n + 1 = 1 + \sum_{i=1}^{n} (|A_i| - |V_i| - 1) > 0.$$

What can we say about the cardinality of the restricted sumset

$$C = \{a + b\colon a \in A,\ b \in B,\ \text{and } P(a,b) \neq 0\}$$

where $P(x,y)$ is a general polynomial over a field F? We make progress in this direction by relaxing (to some extent) the limitations of the polynomial method. Our approach allows one to draw conclusions even if no coefficients in question are known explicitly. Below we introduce the joint work with my student H. Pan.

Let E be an algebraically closed field and $P(x)$ be a polynomial over E. For $\alpha \in E$, if $(x-\alpha)^m \mid P(x)$ but $(x-\alpha)^{m+1} \nmid P(x)$, then we call m the *multiplicity* of α with respect to $P(x)$ and denote it by $m_P(\alpha)$. For any positive integer q, we set

$$N_q(P) = q|\{\alpha \in E^\times\colon m_P(\alpha) \geq q\}| - \sum_{\alpha \in E^\times} \{m_P(\alpha)\}_q$$

where $\{m\}_q$ denotes the least nonnegative residue of $m \in \mathbb{Z}$ modulo q. Note that $N_1(P)$ is the number of distinct roots in $E^\times = E \setminus \{0\}$ of the equation $P(x) = 0$. Let p be the characteristic of E, and

$$\mathcal{P}(p) = \begin{cases} \{1, p, p^2, \dots\} & \text{if } p < \infty, \\ \{1\} & \text{otherwise.} \end{cases}$$

We also define

$$N(P) = \max_{q \in \mathcal{P}(p)} q|\{\alpha \in E^\times \setminus \{-1\}\colon m_P(\alpha) \geq q\}|.$$

Clearly $N(P) \leq \sum_{\alpha \in E^\times \setminus \{-1\}} m_P(\alpha) \leq \deg P(x)$.

Let F be a field of characteristic p, and let E be the algebraic closure of F. Any $P(x) \in F[x]$ can be viewed as a polynomial over E so that $N_q(P)$ $(q = 1, 2, 3, \dots)$

and $N(P)$ are well defined. If $P(x) \in F[x]$ is irreducible and it has a repeated zero in E, then $p < \infty$ and $P(x) = f(x^p)$ for some irreducible $f(x) \in F[x]$; as $x^p - \alpha^p = (x-\alpha)^p$ for all $\alpha \in E$, by induction we find that the multiplicity of any zero of $P(x)$ belongs to $\mathcal{P}(p)$.

The key lemma of this work is the following new result.

Lemma 3 [H. Pan and Z. W. Sun, J. Combin. Theory Ser. A, 100(2002)]. *Let $P(x)$ be a polynomial over the field F of characteristic p. Suppose that there exist nonnegative integers $k < l$ such that $\hat{P}(i) = 0$ for all integers $i \in (k, l)$. Then either $x^l \mid P(x)$, or $\deg P(x) \le k$, or $N_q(P) \ge l - k$ for some $q \in \mathcal{P}(p)$.*

With helps of Lemma 3 and the polynomial method, we are able to obtain the following main result.

Theorem 7 [H. Pan and Z. W. Sun, J. Combin. Theory Ser. A 100(2002)]. *Let F be a field of characteristic p, and let A and B be two finite nonempty subsets of F. Furthermore, let $P(x, y)$ be a polynomial over F of degree $d = \deg P(x, y)$ such that for some $i \in [0, |A| - 1]$ and $j \in [0, |B| - 1]$ we have $\hat{P}(i, d - i) \ne 0$ and $\hat{P}(d - j, j) \ne 0$. Define $P_0(x, y)$ to be the homogeneous polynomial of degree d such that $P(x, y) = P_0(x, y) + R(x, y)$ for some $R(x, y) \in F[x, y]$ with $\deg R(x, y) < d$, and put $P^*(x) = P_0(x, 1)$. Then*

$$\begin{aligned} &|\{a + b\colon a \in A,\ b \in B,\ \text{and } P(a, b) \ne 0\}| \\ &\ge \min\{p - m_{P^*}(-1),\ |A| + |B| - 1 - d - N(P^*)\}. \end{aligned}$$

Corollary 1. *Let F be a field of characteristic $p \ne 2$, and let A, B and S be finite nonempty subsets of F. Then*

$$|\{a + b\colon a \in A,\ b \in B,\ \text{and } a - b \notin S\}| \ge \min\{p,\ |A| + |B| - |S| - q - 1\} \tag{6}$$

where q is the largest element of $\mathcal{P}(p)$ not exceeding $|S|$.

Corollary 2. *Let F be a field of characteristic p, and let A and B be finite nonempty subsets of F. Let $\emptyset \neq S \subseteq F^\times \times F$ and $|S| < \infty$. Then*

$$|\{a+b\colon a \in A,\ b \in B,\ \text{and } a+ub \neq v \text{ if } \langle u,v\rangle \in S\}|$$

$$\geq \min\{p - |\{v \in F\colon \langle 1,v\rangle \in S\}|,\ |A|+|B|-2|S|-1\}.$$

Recently I have some further joint work with Prof. Yeh. We are able to present a unified method to determine certain coefficients in polynomials.