Reported on the International Congress of Math. (Beijing, 2002-08-23)

SUMSETS WITH POLYNOMIAL RESTRICTIONS

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

Cyclic groups are the simplest groups in algebra. However, in combinatorial number theory there are many difficult open problems concerning cyclic groups.

Suppose that $\{a_1,\ldots,a_n\}$, $\{b_1,\ldots,b_n\}$ and $\{a_1+b_1,\ldots,a_n+b_n\}$ are complete systems of residues modulo n. Let $\sigma=0+1+\ldots+(n-1)=n(n-1)/2$. As $\sum_{i=1}^n(a_i+b_i)=\sum_{i=1}^n a_i+\sum_{i=1}^n b_i$, we have $\sigma\equiv\sigma+\sigma \pmod n$ and hence $2\nmid n$.

In 1999 Snevily [Amer. Math. Monthly] made 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 are 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.*

This conjecture is nontrivial even for the additive cyclic group $\mathbb{Z}/n\mathbb{Z}$ of residues modulo an odd integer $n>0$.

In 1964 Erdős and Heilbronn [Acta Arith.] conjectured that if $\emptyset\neq A\subseteq\mathbb{Z}/p\mathbb{Z}$ (where p is a prime) then there are at least $\min\{p,\ 2|A|-3\}$ residues modulo p that can be written as the sum of two distinct residues mod p in A. This had been open for thirty years until Dias da Silva and Hamidoune [Bull. London Math.

Soc.] confirmed it in 1994 with 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, and the method turned out to be a very powerful tool.

Using the polynomial method (already introduced in the talk of Prof. Alon), Alon [Israel J. Math. 2000] proved that Snevily's conjecture holds when G is the additive group of the field $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime.

Let F be a field. We use p_F to denote the additive order of the multiplicative identity of F, and call it the *characteristic* of F. Recently there are several interesting results concerning various restricted sumsets of $A_1, \ldots, A_n \subseteq F$. (See [Sun, Acta Arith. 2001], [Hou & Sun, Acta Arith. 2002], [Liu & Sun, J. Number Theory, 2002], [Pan & Sun, J. Combin. Theory Ser. A, 2002].)

Corollary 1 of Hou and Sun [Acta Arith. 2002] in the case $m = 1$ can be stated as follows:

Let $k \geqslant n \geqslant 1$ be integers, and F be a field with p_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

$$\{a_1 + \ldots + a_n \colon a_i \in A_i,\ a_i \neq a_j \text{ and } a_i + b_i \neq a_j + b_j \text{ if } i \neq j\} \tag{1}$$

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

In 2001 Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math.] confirmed Snevily's conjecture for any cyclic group with odd order.

Below we introduce four new theorems on restricted sumsets, which are contained in my recent paper [*On Snevily's conjecture and restricted sumsets*, to appear]. They are stronger than the existential result of Dasgupta et al.

Theorem 1 ([Sun, J. Combin. Theory Ser. A 103(2003)]). *Let F be a field with $p_F = 2$. Let $A_1, \ldots, A_n$ be subsets of F with cardinality $n+1$, and $b_1, \ldots, b_n$ be* *distinct elements of* F. *Let* $c_{ij}, d_{ij} \in F$ *for* $1 \leq i < j \leq n$. *Then the restricted sumset*

$$\{a_1 + \ldots + a_n : a_i \in A_i,\ a_i - a_j \neq c_{ij} \text{ and } a_i b_i - a_j b_j \neq d_{ij} \text{ if } i < j\} \tag{2}$$

has more than n *elements.*

Corollary 1 ([Dasgupta et al., 2001])**.** *Let* F *be a field of characteristic* 2*, and* 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 with $A_1 = \ldots = A_n = A \cup \{a\}$. $\square$

For an odd integer $n > 1$, the multiplicative group of the finite field F with $|F| = 2^{\varphi(n)}$ has a cyclic subgroup of order n (where φ is Euler's totient function). This observation of Dasgupta et al. indicates that Corollary 1 implies the truth of Snevily's conjecture for cyclic groups.

Theorem 2 ([Sun, J. Combin. Theory Ser. A 103(2003)])**.** *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 pairwise distinct elements of* G. *Let* m *be any positive integer not exceeding* $(k-1)/(n-1)$.

(i) *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) *If* $b_1, \ldots, b_n$ *are of odd orders, then*

$$\begin{aligned} &|\{\{a_1, \ldots, a_n\} : a_i \in A_i,\ a_i \neq a_j \text{ and } ma_i + b_i \neq ma_j + b_j \text{ if } i \neq j\}| \\ &\quad \geqslant (k-1)n - (m+1)\binom{n}{2} + 1 > (m-1)\binom{n}{2}. \end{aligned} \tag{3}$$

Theorem 2(ii) in the case $k = n$ and $m = 1$, also yields the main result of Dasgupta et al.

Actually Theorem 2 follows from our stronger results on sumsets with polynomial restrictions.

Theorem 3 ([Sun, J. Combin. Theory Ser. A 103(2003)]). *Let k, m, n be positive integers with $k > m(n-1)$, and let $A_1, \ldots, A_n$ be subsets of a field F with cardinality k. Let $P_1(x), \ldots, P_n(x) \in F[x]$ have degree m, and $b_1, \ldots, b_n$ be their leading coefficients respectively.*

(i) *If $K = (k-1)n - m\binom{n}{2} < p_F$ and $b_1, \ldots, b_n$ are pairwise distinct, then $|S| \geqslant K + 1$ where*

$$S = \left\{ \sum_{i=1}^{n} a_i \colon a_1 \in A_1, \ldots, a_n \in A_n, \text{ and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j \right\}. \tag{4}$$

(ii) *Suppose that F is the complex field $\mathbb{C}$ and $b_1, \ldots, b_n$ are qth roots of unity. Provided that $2 \nmid q$ and $b_1, \ldots, b_n$ are distinct, or $n!$ cannot be written as the sum of some (not necessarily distinct) prime divisors of q, we have $|T| \geqslant K - \binom{n}{2} + 1$ where*

$$T = \left\{ \sum_{i=1}^{n} a_i \colon a_i \in A_i,\ a_i \neq a_j \text{ and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j \right\}. \tag{5}$$

Theorem 4 ([Sun, J. Combin. Theory Ser. A 103(2003)]). *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*

$$m > k_n - k_1 \text{ and } k_n > m(n-1). \tag{6}$$

(i) *We have $L = \sum_{i=1}^{n}(k_i - 1) - (m+1)\binom{n}{2} \geqslant 0$. If $p_F > L!n!$, then $|T| \geqslant L + 1$ where T is as in (5).*

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

We remark that $|T| = L$ may happen in the exceptional cases. Also, the condition $k_n > m(n-1)$ cannot be replaced by $k_n \geqslant m(n-1)$.

Our tools used to obtain the above four theorems include Combinatorial Nullstellensatz posed by N. Alon, Linear Algebra and Algebraic Number Theory.