ISRAEL JOURNAL OF MATHEMATICS 154 (2006), 21–28

RESTRICTED SUMSETS AND A CONJECTURE OF LEV

BY

HAO PAN AND ZHI-WEI SUN*

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
e-mail: haopan79@yahoo.com.cn, zwsun@nju.edu.cn

ABSTRACT

Let A, B, S be finite subsets of an abelian group G. Suppose that the restricted sumset

$$C = \{a + b\colon a \in A,\ b \in B,\ \text{and } a - b \notin S\}$$

is nonempty and some $c \in C$ can be written as $a + b$ with $a \in A$ and $b \in B$ in at most m ways. We show that if G is torsion-free or elementary abelian, then $|C| \geqslant |A| + |B| - |S| - m$. We also prove that $|C| \geqslant |A| + |B| - 2|S| - m$ if the torsion subgroup of G is cyclic. In the case $S = \{0\}$ this provides an advance on a conjecture of Lev.

1. Introduction

Let A and B be finite nonempty subsets of an (additively written) abelian group G. The sumset of A and B is defined by

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

The Cauchy–Davenport theorem (cf. [N, pp. 43–48]), a basic result in additive combinatorial number theory, states that

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

* This author is responsible for communications, and supported by the National Science Fund for Distinguished Young Scholars (No. 10425103) and the Key Program of NSF (No. 10331020) in China.
Received March 27, 2005

if $G = \mathbb{Z}/p\mathbb{Z}$ with p prime. Another theorem due to Kemperman and Scherk (cf. [Sc], [Ke] and [L2]) asserts that

$$|A+B| \geqslant |A| + |B| - \min_{c \in A+B} \nu_{A,B}(c), \tag{1.1}$$

where

$$\nu_{A,B}(c) = |\{(a,b) \in A \times B \colon a+b=c\}|; \tag{1.2}$$

in particular, we have $|A+B| \geqslant |A|+|B|-1$ if some $c \in A+B$ can be uniquely written as $a+b$ with $a \in A$ and $b \in B$.

Now we define the restricted sumset

$$A \dot{+} B = \{a+b \colon a \in A,\ b \in B,\ \text{and } a \neq b\}. \tag{1.3}$$

In 1964, Erdős and Heilbronn [EH] conjectured that if $G = \mathbb{Z}/p\mathbb{Z}$ with p prime, then

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

This is much more difficult than the Cauchy–Davenport theorem concerning unrestricted sumsets. It had been open for thirty years until Dias da Silva and Hamidoune [DH] confirmed it in 1994 using representations of symmetric groups. Later Alon, Nathanson and Ruzsa [ANR1, ANR2] developed a powerful polynomial method to give a simpler proof of the Erdős–Heilbronn conjecture (see also [A2]). They showed that if $G = \mathbb{Z}/p\mathbb{Z}$ with p prime then

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

where δ is 1 or 0 according to whether $|A| = |B|$ or not. The reader may consult [HS], [K1], [K2], [L1], [LS] and [SY] for various extensions of the Erdős–Heilbronn conjecture.

Motivated by the Kemperman–Scherk theorem and the Erdős–Heilbronn conjecture, Lev [L2] proposed the following interesting conjecture.

Conjecture 1.1 (Lev): *Let G be an abelian group, and let A and B be finite nonempty subsets of G. Then we have*

$$|A \dot{+} B| \geqslant |A| + |B| - 2 - \min_{c \in A+B} \nu_{A,B}(c). \tag{1.4}$$

This conjecture is known to be true for torsion-free abelian groups and elementary abelian 2-groups. It also holds when $|G|$ is prime, or G is cyclic and $|G| \leqslant 25$. (Cf. [L2].)

Now we state our main results.

THEOREM 1.1: *Let A and B be finite nonempty subsets of a field F. Let $P(x,y) \in F[x,y]$ and*

$$C = \{a+b\colon a \in A,\ b \in B,\ \text{and } P(a,b) \neq 0\}. \tag{1.5}$$

If C is nonempty, then

$$|C| \geqslant |A| + |B| - \deg P - \min_{c \in C} \nu_{A,B}(c). \tag{1.6}$$

Remark 1.1: When $P(x,y) = 1$, (1.6) becomes (1.1).

Notice the difference between the minima in (1.4) and (1.6): as $C \subseteq A+B$ we have $\min_{c\in A+B} \nu_{A,B}(c) \leqslant \min_{c\in C} \nu_{A,B}(c)$.

THEOREM 1.2: *Let A and B be finite nonempty subsets of an abelian group G whose torsion subgroup*

$$\mathrm{Tor}(G) = \{g \in G\colon g \text{ has a finite order}\}$$

is cyclic. For $i = 1, \ldots, l$ let m_i and n_i be nonnegative integers and let $d_i \in G$. Suppose that

$$C = \{a+b\colon a \in A,\ b \in B,\ \text{and } m_i a - n_i b \neq d_i \text{ for all } i = 1, \ldots, l\} \tag{1.7}$$

is nonempty. Then

$$|C| \geqslant |A| + |B| - \sum_{i=1}^{l} (m_i + n_i) - \min_{c \in C} \nu_{A,B}(c). \tag{1.8}$$

Remark 1.2: When A and B are finite subsets of $\mathbb{Z}$, the restricted sumset in (1.7) was first studied by Sun [Su1].

From Theorems 1.1 and 1.2 we deduce the following result on difference-restricted sumsets.

THEOREM 1.3: *Let G be an abelian group, and let A, B, S be finite nonempty subsets of G with*

$$C = \{a+b\colon a \in A,\ b \in B,\ \text{and } a-b \notin S\} \neq \emptyset. \tag{1.9}$$

(i) *If G is torsion-free or elementary abelian, then*

$$|C| \geqslant |A| + |B| - |S| - \min_{c \in C} \nu_{A,B}(c). \tag{1.10}$$

(ii) *If* $\mathrm{Tor}(G)$ *is cyclic, then*

$$|C| \geqslant |A| + |B| - 2|S| - \min_{c\in C} \nu_{A,B}(c). \tag{1.11}$$

Proof: Without loss of generality we can assume that G is generated by the finite set $A \cup B \cup S$.

If $G \cong \mathbb{Z}^n$, then we can simply view G as the ring of algebraic integers in an algebraic number field K with $[K : \mathbb{Q}] = n$. If $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ where p is a prime, then G is isomorphic to the additive group of the finite field with p^n elements. Thus part (i) follows from Theorem 1.1 in the case $P(x, y) = \prod_{s\in S}(x - y - s)$.

Let $d_1, \ldots, d_l$ be all the distinct elements of S. Applying Theorem 1.2 with $m_i = n_i = 1$ for all $i = 1, \ldots, l$ we immediately get the second part. ∎

Remark 1.3: It is interesting to compare Theorem 1.3 in the case $S = \{0\}$ with Conjecture 1.1.

Concerning the set C given by (1.9), there are some known results of different types. When A, B, S are finite nonempty subsets of a field whose characteristic is an odd prime p, the authors [PS] proved that $|C| \geqslant \min\{p, |A| + |B| - |S| - q - 1\}$, where q is the largest power of p not exceeding $|S|$. By modifying Károlyi's proof of [K1, Theorem 3], we can show that if $q > 1$ is a power of a prime p, and A, B, S are subsets of $\mathbb{Z}/q\mathbb{Z}$ with $\min\{|A|, |B|\} > |S|$, then $|C| \geqslant \min\{p, |A| + |B| - 2|S| - 1\}$.

We will give a key lemma in the next section and prove Theorems 1.1 and 1.2 in Section 3. Our proofs use a version of the polynomial method.

2. Some preparations

Our basic tool is as follows.

Combinatorial Nullstellensatz ([A1, Theorem 1.1]): *Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F, and set $g_i(x) = \prod_{a\in A_i}(x - a)$ for $i = 1, \ldots, n$. Then $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ vanishes over the Cartesian product $A_1 \times \cdots \times A_n$ if and only if it can be written in the form*

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i)h_i(x_1, \ldots, x_n)$$

where $h_i(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ and $\deg h_i \leqslant \deg f - \deg g_i$.

With help of the Combinatorial Nullstellensatz, we provide a lemma for our purposes.

LEMMA 2.1: *Let A and B be finite nonempty subsets of a field F, and write*

$$\nu_i = |\{(a,b) \in A \times B: a + \lambda_i b = \mu_i\}| \tag{2.1}$$

for $i = 1, \ldots, k$ where $\lambda_i \in F \setminus \{0\}$ and $\mu_i \in F$. Let $P(x,y) \in F[x,y]$. Suppose that for any $i = 1, \ldots, k$ there are $a \in A$ and $b \in B$ with $P(a,b) \neq 0$ and $a + \lambda_i b = \mu_i$, and that for each $(a,b) \in A \times B$ with $P(a,b) \neq 0$ there is a unique $i \in \{1, \ldots, k\}$ with $a + \lambda_i b = \mu_i$. Then we have

$$k + \min\{\nu_1, \ldots, \nu_k\} \geqslant |A| + |B| - \deg P. \tag{2.2}$$

Proof: Clearly

$$f(x,y) := P(x,y) \prod_{j=1}^{k} (x + \lambda_j y - \mu_j)$$

vanishes over $A \times B$. Set $g_A(x) = \prod_{a \in A}(x - a)$ and $g_B(y) = \prod_{b \in B}(y - b)$. By the Combinatorial Nullstellensatz, there are $h_A(x,y), h_B(x,y) \in F[x,y]$ such that

$$f(x,y) = g_A(x)h_A(x,y) + g_B(y)h_B(x,y)$$

and

$$\max\{\deg g_A + \deg h_A, \deg g_B + \deg h_B\} \leqslant \deg f.$$

Fix $1 \leqslant i \leqslant k$. Write $h_B(x,y) = \sum_{s,t \geqslant 0} c_{st} x^s y^t$ where $c_{st} \in F$. Then

$$h_B(x,y) = \sum_{s,t \geqslant 0} c_{st}((x + \lambda_i y - \mu_i) + \mu_i - \lambda_i y)^s y^t = (x + \lambda_i y - \mu_i)q(x,y) + r(y),$$

where $q(x,y) \in F[x,y]$, and $r(y) = h_B(\mu_i - \lambda_i y, y)$ has degree not greater than $\deg h_B$.

Now assume that $k + \nu_i < |A| + |B| - \deg P$. We want to deduce a contradiction. Set

$$A_0 = \{a \in A: (\mu_i - a)/\lambda_i \notin B\}.$$

Obviously $|A_0| = |A| - \nu_i$ and $g_B((\mu_i - a)/\lambda_i) \neq 0$ for any $a \in A_0$. If $a \in A_0$, then

$$g_B\Big(\frac{\mu_i - a}{\lambda_i}\Big)h_B\Big(a, \frac{\mu_i - a}{\lambda_i}\Big) = f\Big(a, \frac{\mu_i - a}{\lambda_i}\Big) - g_A(a)h_A\Big(a, \frac{\mu_i - a}{\lambda_i}\Big) = 0$$

and hence

$$r\Big(\frac{\mu_i - a}{\lambda_i}\Big) = h_B\Big(a, \frac{\mu_i - a}{\lambda_i}\Big) = 0.$$

Since $\deg r \leqslant \deg f - \deg g_B < |A| - \nu_i = |A_0|$, we must have $r(y) = 0$, i.e., $h_B(x,y)$ is divisible by $x + \lambda_i y - \mu_i$. Recall that there are $a_0 \in A$ and $b_0 \in B$

such that $P(a_0, b_0) \neq 0$ and $a_0+\lambda_i b_0 = \mu_i$. Since $h_B(a_0, b_0) = 0$, the polynomial $P(a_0, y)\prod_{j=1}^k(a_0+\lambda_j y-\mu_j) = f(a_0, y) = g_B(y)h_B(a_0, y)$ is divisible by $(y-b_0)^2$. As $a_0+\lambda_j b_0 \neq \mu_j$ for any $j \neq i$, we must have $y-b_0 \mid P(a_0, y)$, which contradicts the fact that $P(a_0, b_0) \neq 0$. ∎

3. Proofs of Theorems 1.1–1.2

Proof of Theorem 1.1: Let $\mu_1, \ldots, \mu_k$ be all the distinct elements of C. Applying Lemma 2.1 with $\lambda_1 = \cdots = \lambda_k = 1$, we find that

$$|C| + \min_{c\in C} \nu_{A,B}(c) \geqslant |A| + |B| - \deg P$$

which is equivalent to (1.6). ∎

Proof of Theorem 1.2: Without loss of generality, we can assume that G is finitely generated, and furthermore that G is a subgroup of the multiplicative group of the field of complex numbers (see the proof of Theorem 1.1 of [Su2]); thus, C is the set

$$\{ab\colon a \in A, b \in B, \text{ and } a^{m_i}b^{-n_i} \neq d_i \text{ for all } i = 1, \ldots, l\}.$$

Let $-\lambda_1, \ldots, -\lambda_k$ be all the distinct elements of C, and set

$$P(x, y) = \prod_{i=1}^{l}(x^{m_i}y^{n_i} - d_i).$$

Then, for each $j \in \{1, \ldots, k\}$, there are $a \in A$ and $b \in B$ such that $a+\lambda_j b^{-1} = 0$ and $P(a, b^{-1}) \neq 0$. If $a \in A$, $b \in B$ and $P(a, b^{-1}) \neq 0$, then there is a unique $j \in \{1, \ldots, k\}$ such that $\lambda_j = -ab$ (i.e., $a + \lambda_j b^{-1} = 0$). Applying Lemma 2.1 to the sets A and $B^{-1} = \{b^{-1}\colon b \in B\}$ with $\mu_1 = \cdots = \mu_k = 0$, we obtain that

$$k + \min_{1\leqslant j\leqslant k} |\{(a, b) \in A \times B\colon a + \lambda_j b^{-1} = 0\}| \geqslant |A| + |B^{-1}| - \deg P.$$

Therefore

$$|C| + \min_{c\in C} |\{(a, b) \in A \times B\colon ab = c\}| \geqslant |A| + |B| - \sum_{i=1}^{l}(m_i + n_i)$$

as desired. ∎

ACKNOWLEDGEMENTS: The authors are indebted to the referee for his helpful comments. The revision was done during the second author's visit to the University of California at Irvine, therefore Sun would like to thank Prof. Daqing Wan for the invitation.

References

[A1] N. Alon, *Combinatorial Nullstellensatz,* Combinatorics, Probability and Computing **8** (1999), 7–29.

[A2] N. Alon, *Discrete mathematics: methods and challenges,* in *Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002),* Higher Education Press, Beijing, 2002, pp. 119–135.

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

[ANR2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes,* Journal of Number Theory **56** (1996), 404–417.

[DH] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory,* The Bulletin of the London Mathematical Society **26** (1994), 140–146.

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

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

[K1] G. Károlyi, *The Erdős–Heilbronn problem in abelian groups,* Israel Journal of Mathematics **139** (2004), 349–359.

[K2] G. Károlyi, *A compactness argument in the additive theory and the polynomial method,* Discrete Mathematics **302** (2005), 124–144.

[Ke] J. H. B. Kemperman, *On small sumsets in an abelian group,* Acta Mathematica **103** (1960), 63–88.

[L1] V. F. Lev, *Restricted set addition in groups, I. The classical setting,* Journal of the London Mathematical Society (2) **62** (2000), 27–40.

[L2] V. F. Lev, *Restricted set addition in Abelian groups: results and conjectures,* Journal de Théorie des Nombres de Bordeaux **17** (2005), 181–193.

[LS] J. X. Liu and Z. W. Sun, *Sums of subsets with polynomial restrictions,* Journal of Number Theory **97** (2002), 301–304.

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

[PS] H. Pan and Z. W. Sun, *A lower bound for* $|\{a+b\colon a \in A, b \in B, P(a,b) \neq 0\}|$, Journal of Combinatorial Theory, Series A **100** (2002), 387–393.

[Sc] P. Scherk, *Distinct elements in a set of sums,* The American Mathematical Monthly **62** (1955), 46–47.

[Su1] Z. W. Sun, *Restricted sums of subsets of $\mathbb{Z}$*, Acta Arithmetica **99** (2001), 41–60.

[Su2] Z. W. Sun, *On Snevily's conjecture and restricted sumsets,* Journal of Combinatorial Theory, Series A **103** (2003), 291–304.

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