AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **31** (2005), Pages 161–165

A conjecture on subset sums of a finite set of positive integers *

Shu-Guang Guo†

Department of Mathematics
Southeast University
Nanjing 210096, Jiangsu
P.R. CHINA
ygchen@pine.njnu.edu.cn

Abstract

Let A be a finite set of positive integers, and let $S(A)$ be the set of all nonempty sums of distinct elements of A. In this paper, a conjecture on the lower bound of $|S(A)|$ is given and a partial proof of the conjecture is obtained.

1 Introduction

Let A be a finite set of integers, and denote by $|A|$ the cardinality of A. The sumset and the restricted sumset of A are defined as

$$2A = \{a+b \,:\, a, b \in A\}, \quad 2^\wedge A = \{a+b \,:\, a, b \in A \quad \text{and} \quad a \neq b\},$$

respectively. Without loss of generality, we may assume that A has the normal form (see [5]), namely, $A \subseteq [0\,,\,l]$, $|A| = n$, $\gcd(A) = 1$ and $0, l \in A$.

It was proved by G. Freiman over 30 years ago (see [5]) that

$$|2A| \geq \min\{l, 2n-3\} + n = \begin{cases} l+n & \text{if } l \leq 2n-3, \\ 3n-3 & \text{if } l \geq 2n-2. \end{cases}$$

For $2^\wedge A$, Freiman and Lev conjectured independently (see [3]) that for $n > 7$,

$$|2^\wedge A| \geq \min\{l, 2n-5\} + n - 2 = \begin{cases} l+n-2 & \text{if } l \leq 2n-5, \\ 3n-7 & \text{if } l \geq 2n-4. \end{cases}$$

The first non-trivial result towards this problem was given by Freiman et al. [1] and was improved by Lev [3]. Very recently, Schoen [6] proved the following theorem.

* Supported by the National Natural Science Foundation of China, Grant No10201013

† Also: Department of Mathematics, Yancheng Teachers College, Yancheng 224002, Jiangsu, China

Theorem A. *Let A be a set of $n > 7$ integers such that $A \subseteq [0\,,\,l]$, $gcd(A) = 1$ and $0, l \in A$. Then*

$$|2^\wedge A| \geq \begin{cases} l+n-2 & if\ l \leq 2n-5, \\ 3n+o(n) & if\ l \geq 2n-4. \end{cases}$$

For a set A of k integers, denote by $s(A')$ the sum of the elements of a nonempty subset A' of A and the subset sums set of A is defined as

$$S(A) = \{\, s(A') \mid A' \subseteq A, A' \neq \emptyset\}.$$

For a set A of positive integers with $|A| = k > 3$, Nathanson [4], and Ilie and Salomaa [2] proved that

$$|S(A)| \geq \binom{k+1}{2}, \tag{1}$$

and the equality occurs if and only if $A = \{d, 2d, \ldots, kd\}$ for some positive integer d. Since $|S(A)|$ is invariant under scalar multiplication of A , we may freely assume that $\gcd(A) = 1$. Under the assumption, the equality in (1) occurs if and only if $A = \{1, 2, \ldots, k\}$.

The subset sums are closely related to the restricted sums. In this paper, we first give a conjecture on subset sums, which is parallel to the one on the restricted sums.

Conjecture. *Let A be a set of $k \geq 6$ positive integers such that $gcd(A) = 1$. Put $M = max(A)$. Then*

$$|S(A)| \geq \begin{cases} \frac{k(k-1)}{2} + M & if\ M \leq \frac{k^2-k+2}{2}, \\ k(k-1)+1 & if\ M \geq \frac{k^2-k+2}{2}. \end{cases}$$

This is the strongest possible assertion of this kind, as letting $A = \{1, 2, \ldots, k-1, M\}$, we get

$$|S(A)| = \begin{cases} \frac{k(k-1)}{2} + M & if\ k \leq M \leq \frac{k^2-k+2}{2}, \\ k(k-1)+1 & if\ M \geq \frac{k^2-k+2}{2}. \end{cases}$$

The condition $k \geq 6$ is necessary due to a singularity for $k = 5$: consider $A = \{1, m+2, m+3, m+4, m+5\}$ with $m \geq 2$, in which $|S(A)| = 19 < 5(5-1)+1$.

In addition, we prove following Theorem, which goes a bit further beyond (1), and is intended to be a first step in the investigation of this problem.

Theorem 1. *Let A be a set of $k \geq 5$ positive integers such that $gcd(A) = 1$. Put $M = \max(A)$. Then*

$$|S(A)| \geq \begin{cases} \frac{k(k-1)}{2} + M & if\ k \leq M \leq 2k-3, \\ \frac{k^2+3k+8}{2} + o(k) & if\ M \geq 2k-2, \end{cases} \tag{2}$$

and for $k \leq M \leq 2k-3$, the equality holds if and only if $A = \{1, 2, \cdots, k-1, M\}$.

Corollary 1. *Let A be a set of $k \geq 5$ positive integers and $l \geq 5$ negative integers. Put $M = \max(A)$ and $-m = \min(A)$. If $M \leq 2k-3$ and $m \leq 2l-3$, then*

$$|S(A)| \geq \frac{k(k-1)}{2} + \frac{l(l-1)}{2} + M + m + 1, \tag{3}$$

and the equality holds if and only if

$$A = \{1, 2, \cdots, k-1, M\}, \quad B = \{-m, -(l-1), -(l-2), \cdots, -1\}.$$

2 Proof

In order to complete the proof of Theorem 1, we need the following lemma on restricted sumsets.

Lemma 1. [5] *Let $k \geq 5$, and let A be a set of k integers. Then*

$$|2^\wedge A| \geq 2k-3,$$

and the equality holds if and only if A is an arithmetic progression.

Proof of Theorem 1. Suppose $A = \{a_1, a_2, \ldots, a_k\}$, where

$$1 \leq a_1 < a_2 < \ldots < a_k = M.$$

Let $A_k = \{0, a_1, a_2, \ldots, a_k\}$, $A_{k-2} = \{0, a_1, a_2, \ldots, a_{k-2}\}$, and

$$B_i = \{a_1 + a_i + \cdots + a_k, a_2 + a_i + \cdots + a_k, \cdots, a_{i-1} + a_i + \cdots + a_k\},$$

where $i = 2, 3, \ldots, k$. It is readily seen that

$$S(A) \supseteq (2^\wedge A_k) \cup (2^\wedge A_{k-2} + a_{k-1} + a_k) \cup \bigcup_{i=2}^{k-3} B_i, \tag{4}$$

and $2^\wedge A_k$, $2^\wedge A_{k-2} + a_{k-1} + a_k$, $B_i (i = 2, \ldots, k-3)$ are disjoint in pairs.

Case 1. $k \leq M \leq 2k-3$. Since $\gcd(A_k) = \gcd(A) = 1$ and $a_k = M \leq 2k-3 = 2(k+1)-5$, it follows from Theorem A that

$$|2^\wedge A_k| \geq M + (k+1) - 2 = M + k - 1. \tag{5}$$

By Lemma 1 we have

$$|2^\wedge A_{k-2} + a_{k-1} + a_k| = |2^\wedge A_{k-2}| \geq 2(k-1) - 3 = 2k - 5. \tag{6}$$

Therefore

$$|S(A)| \geq |(2^\wedge A_k)| + |(2^\wedge A_{k-2} + a_{k-1} + a_k)| + |\bigcup_{i=2}^{k-3} B_i|$$

$$\geq M + k - 1 + 2k - 5 + \frac{(k-4)(k-3)}{2} = \frac{k(k-1)}{2} + M. \tag{7}$$

Now suppose that the equality in (7) holds. Then all inequalities in the above argument must be equalities. In particular, we have from (6) that

$$|2^\wedge A_{k-2}| = 2(k-1) - 3.$$

It follows from Lemma 1 that A_{k-2} is an arithmetic progression. Since $k-2 \leq a_{k-2} \leq M-2 \leq 2k-5$, we have $\gcd(A_{k-2}) = 1$, and so $A_{k-2} = \{0, 1, 2, \cdots, k-2\}$. Hence

$$A = \{1, 2, \cdots, k-2, a_{k-1}, M\}.$$

This implies that

$$2^\wedge A_k = \{1, 2, \cdots, k-2+M\} \cup \{a_{k-1} + M\}.$$

If $a_{k-1} > k-1$, it is easily seen that

$$a_1 + a_{k-2} + a_k = 1 + k - 2 + M \in S(A),$$

but does not belong to the right-hand side of (4), a contradiction. Therefore $a_k = k-1$, and so $A = \{1, 2, \cdots, k-1, M\}$.

Conversely, It is easy to check that the equality in (7) holds for $A = \{1, 2, \cdots, k-1, M\}$.

Case 2. $M \geq 2k-2$. It follows from Lemma 1 and Theorem A that

$$|2^\wedge A_k| \geq 3(k+1) + o(k),$$

and

$$|2^\wedge A_{k-2} + a_{k-1} + a_k| = |2^\wedge A_{k-2}| \geq 2(k-1) - 3 = 2k - 5.$$

Following from Case 1, we have

$$|S(A)| \geq |2^\wedge A_k| + |2^\wedge A_{k-2} + a_{k-1} + a_k| + \sum_{i=2}^{k-3} |B_i|$$

$$\geq 3(k+1) + o(k) + 2k - 5 + \frac{(k-4)(k-3)}{2} = \frac{k^2+3k+8}{2} + o(k).$$

Combining Case 1 and Case 2, Theorem 1 is proved.

Proof of Corollary 1. Let $A = A_1 \cup A_2$ such that

$$A_1 = \{a_1, a_2, \cdots, a_k\}, \quad A_2 = \{-b_l, \cdots, -b_2, -b_1\},$$

where

$$0 < a_1 < a_2 < \cdots < a_k = M, \quad -m = -b_l < \cdots < -b_2 < -b_1 < 0.$$

Obviously, we have

$$S(A) \supseteq S(A_1) \cup S(A_2) \cup \{a_1 - b_1\},$$

and $-b_1 < a_1 - b_1 < a_1$. It follows from Theorem 1 that

$$|S(A)| \geq |S(A_1)| + |S(A_2)| + 1 \geq \frac{k(k-1)}{2} + M + \frac{l(l-1)}{2} + m + 1.$$

Now suppose that the equality in (3) holds. Then we have that

$$|S(A_1)| = \frac{k(k-1)}{2} + M, \quad |S(A_2)| = \frac{l(l-1)}{2} + m.$$

By Theorem 1 we have

$$A = \{1, 2, \cdots, k-1, M\}, \quad B = \{-m, -(l-1), -(l-2), \cdots, -1\}.$$

Conversely, it is easy to check that the equality in (3) holds for

$$A = \{1, 2, \cdots, k-1, M\}, \quad B = \{-m, -(l-1), -(l-2), \cdots, -1\}.$$

References

[1] G. Freiman, L. Low and J. Pitman, Sumsets with distinct summands and the conjecture of Erdös-Heilbronn on sums of residues, *Astérisque* 258 (1999), 163–172.

[2] L. Ilie, A. Salomaa, On the expressiveness of subset-sum representations, *Acta Informatica* 36 (2000), 665–672.

[3] V. F. Lev, Restricted set addition in group I: the classical setting, *J. London Math. Soc.* 62(2) (2000), 27–40.

[4] M. B. Nathanson, Inverse theorem for subset sums, *Trans. Amer. Math. Soc.* 347(4) (1995), 1409–1418.

[5] M. B. Nathanson, *Additive number theory: inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[6] T. Schoen, The cardinality of restricted sumsets, *J. Number Theory* 96 (2002), 48–54.

(Received 6 May 2003)