Quan-Hui Yang; Jian-Dong Wu

Sum and difference sets containing integer powers

Czechoslovak Mathematical Journal, Vol. 62 (2012), No. 3, 787–793

Persistent URL: `http://dml.cz/dmlcz/143025`

Czechoslovak Mathematical Journal, 62 (137) (2012), 787–793

SUM AND DIFFERENCE SETS CONTAINING INTEGER POWERS

Quan-Hui Yang, Jian-Dong Wu, Nanjing

(Received June 13, 2011)

Abstract. Let $n > m \geqslant 2$ be positive integers and $n = (m+1)l + r$, where $0 \leqslant r \leqslant m$. Let C be a subset of $\{0, 1, \ldots, n\}$. We prove that if

$$|C| > \begin{cases} \lfloor n/2 \rfloor + 1 & \text{if } m \text{ is odd,} \\ ml/2 + \delta & \text{if } m \text{ is even,} \end{cases}$$

where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x and δ denotes the cardinality of even numbers in the interval $[0, \min\{r, m-2\}]$, then $C - C$ contains a power of m. We also show that these lower bounds are best possible.

Keywords: sum and difference set, integer power

MSC 2010: 11B13

1. Introduction

For a set of integers A, let $A + A = \{a_1 + a_2\colon a_1, a_2 \in A\}$ and $A - A = \{a_1 - a_2\colon a_1, a_2 \in A\}$. For any integers d and q, we define the sets

$$d + A = \{d + a\colon a \in A\},$$
$$d - A = \{d - a\colon a \in A\},$$

and

$$q * A = \{qa\colon a \in A\}.$$

In [3], Erdős and Freiman proved a conjecture of Erdős and Freud (see [2]) which states that if $C \subseteq [1, n]$ with $|C| > n/3$, then some power of 2 is the sum of distinct

This work was supported by the National Natural Science Foundation of China, Grant No. 11071121 and the Project of Graduate Education Innovation of Jiangsu Province (CXZZ12-0381).

elements of C. Later Nathanson and Sárközy [7] showed that at most 30961 distinct summands from C are needed to obtain a power of 2 and 30961 can be replaced by 3504 if the summands are not required to be distinct. In 1996, Lev [6] gave a very nice proof to reduce 3504 to 4. This result is sharp since Alon (see [1]) gave an example to show that here four elements cannot be replaced by three elements. The key of Lev's proof is the following lemma:

Let $C \subseteq [0, n]$, and assume $|C| \geqslant \frac{1}{2}n + 1$. Then either C contains a power of 2, or there exist two distinct elements of C whose sum is a power of 2.

By Lev's lemma, it is easy to get the following result:

Let $C \subseteq [0, n]$ with $0 \in C$ and $|C| \geqslant n/2 + 1$. Then there exists a power of 2 which can be represented as a sum of two elements of C.

Recently, Pan [8] extended this result to the power of m ($m \geqslant 3$):

Let $C \subseteq [0, n]$ with $0 \in C$ and $|C| \geqslant (1 - 1/m)n + 1$. Then there exists a power of m which can be represented as a sum of two elements of C.

For related results one may refer to ([4], [5]). In this paper we prove the following results.

Theorem 1. *Let $n > m \geqslant 2$ be positive integers and $n = (m + 1)l + r$, where $0 \leqslant r \leqslant m$. Let*

$$\tau(m, n) = \begin{cases} \lfloor n/2 \rfloor + 1 & \text{if } m \text{ is odd,} \\ ml/2 + \delta & \text{if } m \text{ is even,} \end{cases}$$

where δ denotes the cardinality of even numbers in the interval $[0, \min\{r, m - 2\}]$. Then

(i) *if C is a subset of $[0, n]$ with $|C| > \tau(m, n)$, then $C - C$ contains either 1 or m;*
(ii) *there exists a subset C of $[0, n]$ with $|C| = \tau(m, n)$ such that $C - C$ contains no power of m.*

Based on the method by Lev and Pan, in the following theorem we remove the condition $0 \in C$ in Pan's result.

Theorem 2. *Let $C \subseteq [0, n]$ and $|C| \geqslant (1 - 1/m)n + 1$. Then there exists a power of m which can be represented as a sum of two elements of C.*

2. Proofs

In the proof of Theorem 1, let $A, B, C, \ldots$ denote some strictly increasing sequences of non-negative integers and $a_n, b_n, c_n, \ldots$ be their n-th elements.

P r o o f of Theorem 1(i). Suppose that m is odd. Since

$$|C| > \lfloor n/2 \rfloor + 1,$$

there exists an integer n_0 such that $n_0 \in C$ and $n_0 + 1 \in C$. Otherwise,

$$c_{\lfloor n/2 \rfloor + 2} \geqslant c_{\lfloor n/2 \rfloor + 1} + 2 \geqslant \ldots \geqslant c_1 + 2(\lfloor n/2 \rfloor + 1) > n,$$

which is impossible. Since $(n_0 + 1) - n_0 = 1 \in C - C$, Theorem 1(i) holds when m is odd.

Suppose that m is even. Let $n = (m+1)l + r$, where $0 \leqslant r \leqslant m$. We first construct a maximal cardinality set $A \subseteq [0, n]$ by the greedy algorithm such that $A - A$ contains neither 1 nor m. Let

$$A = \left(\bigcup_{k=0}^{\infty} A_k \right) \cap [0, n],$$

where

$$A_k = k(m+1) + 2 * [0, m/2 - 1].$$

Then

$$|A| = ml/2 + \delta,$$

where δ denotes the cardinality of even numbers in the interval $[0, \min\{r, m-2\}]$. If we denote $|A|$ by h, then we have that $a_h \leqslant n < a_{h+1}$.

Suppose that $C \subseteq [0, n]$ with $|C| > h$ and $C - C$ contains neither 1 nor m. If we can prove that $c_{h+1} \geqslant a_{h+1}$, then $c_{h+1} > n$, a contradiction. Thus, in order to prove Theorem 1(i), it is sufficient to prove $c_k \geqslant a_k$ for all integers $k \leqslant h + 1$.

The proof is by induction on k. If $k = 1$, then $a_1 = 0$, and so $c_1 \geqslant a_1$. Let $j \geqslant 2$, and assume that $c_k \geqslant a_k$ for all integers $k < j$. Since $1 \notin C - C$, we have $c_{i+1} - c_i \geqslant 2$ for all $i \leqslant h$.

From the construction of the set A, we have that

$$a_{i+1} - a_i = 2 \quad \text{or} \quad a_{i+1} - a_i = 3$$

for all $i \leqslant h$. In addition, $a_{i+1} - a_i = 3$ if and only if $a_i - a_{i-m/2+1} = m - 2$.

If $a_j - a_{j-1} = 2$, then $c_j \geqslant c_{j-1} + 2 \geqslant a_{j-1} + 2 = a_j$.

Now we assume that $a_j - a_{j-1} = 3$. It follows that $a_{j-1} - a_{j-m/2} = m - 2$.

If $c_{j-1} \geqslant a_{j-1} + 1$, then $c_j \geqslant c_{j-1} + 2 \geqslant a_{j-1} + 3 = a_j$.

If $c_{j-1} = a_{j-1}$, then $c_{j-1} - c_{j-m/2} \geqslant 2(m/2 - 1) = m - 2$. On the other hand, by the induction hypothesis, we get

$$c_{j-1} - c_{j-m/2} = a_{j-1} - c_{j-m/2} \leqslant a_{j-1} - a_{j-m/2} = m - 2.$$

Therefore,

$$c_{j-1} = c_{j-m/2} + m - 2,$$

and so

$$c_j \neq c_{j-1} + 2.$$

Otherwise,

$$c_j = c_{j-1} + 2 = c_{j-m/2} + m$$

and then

$$c_j - c_{j-m/2} = m \in C - C,$$

which is a contradiction. Therefore we have that

$$c_j \geqslant c_{j-1} + 3 \geqslant a_{j-1} + 3 = a_j.$$

Hence $c_k \geqslant a_k$ for all $k \leqslant h + 1$.

This completes the proof of Theorem 1(i). $\square$

P r o o f of Theorem 1(ii). Let $\mathbb{N}$ denote all of the non-negative integers. Suppose that m is odd. Let C be all the even numbers in the interval $[0, n]$. Then $|C| = \lfloor n/2 \rfloor + 1$, and no power of m is contained in $C - C$.

Suppose that m is even. Let $C = A$, where A is the same as that in the proof of Theorem 1(i). Then $|C| = ml/2 + \delta$, where δ denotes the cardinality of even numbers in the interval $[0, \min\{r, m-2\}]$. Now, we prove that $C - C$ contains no power of m. Since $(A_k - A_k) \cap \mathbb{N} \subseteq 2 * [0, m/2 - 1]$ for any integer $k \in [0, l+1]$, we have that $A_k - A_k$ contains no power of m. Now we consider the set $A_{k_1} - A_{k_2}$ for all $k_1 \neq k_2$. Suppose that $0 \leqslant k_2 < k_1 \leqslant l + 1$.

If $2 \nmid k_1 + k_2$, then $A_{k_1} - A_{k_2}$ is a set of odd numbers excluding 1, and so it contains no power of m.

If $2 \mid k_1 + k_2$, then

$$(A_{k_1} - A_{k_2}) \cap \mathbb{N} \subseteq [(k_1 - k_2)(m+1) - m + 2, (k_1 - k_2)(m+1) + m - 2].$$

Since $2m+2 \mid m^{2k} + m$ and $2m+2 \mid m^{2k+1} - m$, for any l, we have $m^l = (2m+2)t \pm m$. It follows that $A_{k_1} - A_{k_2}$ contains no power of m, and then $A - A$ contains no power of m. Hence we see that $C - C$ also contains no power of m.

This completes the proof of Theorem 1(ii). $\square$

Corollary 1. *Let n be a positive integer. If C is a subset of $[0,n]$ with $|C| > \lfloor n/3 \rfloor + 1$, then $C - C$ contains a power of 2.*

Before the proof of Theorem 2, we set up a notation. For an interval A, let $|A|$ denote the cardinality of integers in the interval A.

Proof of Theorem 2. The proof is by induction on n. It is easy to check that the result is true for $n \leqslant m$. Let $n > m$, and assume that the result holds for all positive integers $n' < n$. Choose $t \geqslant 1$ such that $m^t \leqslant n < m^{t+1}$.

Case 1. $m^t \leqslant n < (m^{t+1}+1)/2$. Since

$$|C \cap [0, m^t]| \geqslant \Big(1 - \frac{1}{m}\Big) n + 1 - (n - m^t) > \frac{m^t + 1}{2},$$

there exists an integer $i \in [0, m^t]$ such that $i \in C$ and $m^t - i \in C$. It follows that

$$m^t = i + (m^t - i) \in C + C,$$

and thus the result holds in this case.

Case 2. $(m^{t+1}+1)/2 \leqslant n < m^{t+1}$. Suppose that m is odd. Let

$$r = n - (m^{t+1}+1)/2.$$

Then $r \geqslant 0$. Let

$$A = [0, (m^{t+1}-1)/2 - r - 1]$$

and

$$B = [(m^{t+1}-1)/2 - r, (m^{t+1}+1)/2 + r].$$

Then C is the disjoint union of $C \cap A$ and $C \cap B$, and

$$|C| = |C \cap A| + |C \cap B|.$$

If $m^{t+1} \notin (C \cap B) + (C \cap B)$, then $C \cap B$ contains at most one of the two integers $(m^{t+1}-1)/2 - i, (m^{t+1}+1)/2 + i$ for each $i = 0, 1, \ldots, r$. Therefore

$$|C \cap B| \leqslant r + 1 = \frac{|B|}{2}.$$

It follows that

$$\begin{aligned} |C \cap A| &= |C| - |C \cap B| \\ &\geqslant \Big(1 - \frac{1}{m}\Big)(|A| + |B| - 1) + 1 - \frac{|B|}{2} \\ &> \Big(1 - \frac{1}{m}\Big)(|A| - 1) + 1. \end{aligned}$$

Suppose that m is even. Let

$$r = n - \tfrac{1}{2}m^{t+1}.$$

Then $r \geqslant 1$. Let

$$A = [0, \tfrac{1}{2}m^{t+1} - r - 1]$$

and

$$B = [\tfrac{1}{2}m^{t+1} - r, \tfrac{1}{2}m^{t+1} + r].$$

If $m^{t+1} \notin (C \cap B) + (C \cap B)$, then

$$\frac{m^{t+1}}{2} \notin C \cap B$$

and $C \cap B$ contains at most one of the two integers $m^{t+1}/2 - i$, $m^{t+1}/2 + i$ for each $i = 1, \ldots, r$. It follows that

$$|C \cap B| \leqslant r = \frac{|B| - 1}{2}.$$

Thus, we also have

$$\begin{aligned} |C \cap A| &= |C| - |C \cap B| \\ &\geqslant \left(1 - \frac{1}{m}\right)(|A| + |B| - 1) + 1 - \frac{|B| - 1}{2} \\ &> \left(1 - \frac{1}{m}\right)(|A| - 1) + 1. \end{aligned}$$

If $A = \{0\}$, then $|C \cap A| > 1$, which is impossible. By the induction hypothesis, we infer that $(C \cap A) + (C \cap A)$ contains a power of m. Hence $C + C$ contains a power of m.

This completes the proof of Theorem 2. $\square$

Corollary 2. *Let $m \geqslant 3$ and n' be positive integers. Suppose that C' is a subset of $[0, n']$ such that $|C'| \geqslant (1 - 1/m)n' + 1$. Then some power of m is the sum of exactly four elements of C'.*

P r o o f of Corollary 2. Since $|C'| \geqslant (1 - 1/m)n' + 1$, we have $|C' + C'| \geqslant 2|C'| - 1 \geqslant 2(1 - 1/m)n' + 1$. Since $C' + C' \subseteq [0, 2n']$, we can apply Theorem 2 with $C = C' + C'$ and $2n' = n$. It follows that some power of m can be written as the sum of exactly four elements of C', which completes the proof of Corollary 2. $\square$

Acknowledgment. We sincerely thank our supervisor Professor Yong-Gao Chen for his valuable suggestions and useful discussions. We also would like to thank the referee for carefully reading our manuscript.

References

[1] *N. Alon*: Subset sums. J. Number Theory *27* (1987), 196–205.
[2] *P. Erdős*: Some problems and results on combinatorial number theory. Graph theory and its applications: East and West (Jinan, 1986). New York Academy of Sciences, Ann. N. Y. Acad. Sci. *576* (1989), 132–145.
[3] *P. Erdős, G. Freiman*: On two additive problems. J. Number Theory *34* (1990), 1–12.
[4] *G. A. Freiman*: Sumsets and powers of 2. Sets, graphs and numbers. A birthday salute to Vera T. Sós and András Hajnal. Amsterdam: North-Holland Publishing Company. Colloq. Math. Soc. János Bolyai *60* (1992), 279–286.
[5] *V. Kapoor*: Sets whose sumset avoids a thin sequence. J. Number Theory *130* (2010), 534–538.
[6] *V. F. Lev*: Representing powers of 2 by a sum of four integers. Combinatorica *16* (1996), 413–416.
[7] *M. B. Nathanson, A. Sárközy*: Sumsets containing long arithmetic progressions and powers of 2. Acta Arith. *54* (1989), 147–154.
[8] *H. Pan*: Note on integer powers in sumsets. J. Number Theory *117* (2006), 216–221.

Authors' address: Quan-Hui Yang (corresponding author), Jian-Dong Wu, School of Mathematical Sciences, Nanjing Normal University, Nanjing 210046, P. R. China, e-mail: yangquanhui01@163.com, wjd.njnu@163.com.