ACTA ARITHMETICA
132.3 (2008)

Powers of 2 with five distinct summands

by

VSEVOLOD F. LEV (Haifa)

0. Summary. We show that every sufficiently large, finite set of positive integers of density larger than 1/3 contains five or fewer pairwise distinct elements whose sum is a power of 2.

This provides a sharp answer to a question of Erdős and Freud.

1. Introduction: powers of 2 and subset sums. Let A be a set of integers. Evidently, if all elements of A are divisible by 3, then no integer power of 2 can be represented as a sum of elements of A. On the other hand, Erdős and Freud conjectured in [E89] that if $A \subseteq [1, l]$ and $|A| > l/3$ with a sufficiently large positive integer l, so that A cannot consist only of multiples of 3, then there exist pairwise distinct elements of A whose sum is a power of 2. Notice that if the elements are not required to be pairwise distinct, the assertion becomes trivial; indeed, it is well known that for any set A of coprime positive integers, all sufficiently large integers are representable as a sum of elements of A. On the other hand, the assumption that l is large excludes several sporadic exceptional sets, like $A = \{10, 11, 12, 13, 14\}$ or $A = \{7, 10, 11, 13, 17, 18, 20\}$.

The above-stated conjecture was settled by Erdős and Freiman in [EF90], and independently by Nathanson and Sárközy in [NS89]. As proven in the former of the two papers, there are at most $O(\ln l)$ pairwise distinct elements of A the sum of which is a power of 2. In the latter paper it is shown that at most 30961 distinct summands are needed, and if the requirement that the summands are distinct is dropped, then at most 3504 summands suffice. These results were further sharpened by Freiman who reduced in [F92] the number of summands to at most sixteen if they are required to be pairwise distinct, and at most six in the unconstrained case.

In [L96a] the present author showed that four not necessarily distinct summands suffice. This is best possible since, as Alon has observed (this

2000 *Mathematics Subject Classification*: Primary 11B75; Secondary 11B13, 11P99.
Key words and phrases: sumsets, subset sums.

example was presented with his kind permission in [L96a]), if $s \geq 4$ is an even integer, $l = 2^s + 3$, and $A = \{3, 6, 9, \ldots, l-1\} \cup \{l\}$, then one cannot represent a power of 2 as a sum of at most three elements of A. For, if $0 \leq t \leq s$, then $2^t < l$; if $t = s+1$, then $2^t \not\equiv l \pmod 3$ and $2^t < 2l$; and finally, if $t \geq s+2$ then $2^t \geq 4l - 12 > 3l$. (The interested reader will easily fill in the details.)

Similarly, if s is an *odd* positive integer, $l = 2^s + 3$, and $A = \{3, 6, 9, \ldots, l-2\} \cup \{l\}$, then no power of 2 can be represented as a sum of at most four pairwise distinct elements of A: for, if $0 \leq t \leq s$, then $2^t < l$; if $t = s+1$, then $2^t \not\equiv l \pmod 3$; and if $t \geq s+2$, then $2^t \geq 4l-12 > l+(l-2)+(l-5)+(l-8)$.

In this paper we show that at most *five* distinct elements suffice; in view of the example above, this is best possible. In fact, we even relax slightly the density condition.

THEOREM 1. *There exists a positive integer L with the following property. Let $l > L$ be an integer and suppose that $A \subseteq [1, l]$ is a set of integers with $|A| \geq \frac{6}{19} l$ and such that not all elements of A are divisible by* 3. *Then there exists a subset $B \subseteq A$ with $|B| \leq 5$ such that the sum of the elements of B is a power of* 2.

Using our method, the multiplicative factor $6/19$ in the statement of Theorem 1 can be replaced with any value, larger than $17/54$. There is little doubt that further minor refinements are possible, but obtaining the sharp constant may be difficult. We mention in this connection that if $s \geq 3$ is an integer, $l = 2^s + 3$, $k = 2^{s-2} + 1$, and $A = \{3, 6, \ldots, 3k\} \cup \{l\}$, then $|A| > 0.25l$ and no power of 2 can be represented as a sum of five or fewer pairwise distinct elements of A.

In the next section we prepare the ground for the proof of Theorem 1; the proof itself is presented in Section 3.

2. Notation and auxiliary results. Let A be a set of integers. We denote the smallest and largest elements of A by $\min A$ and $\max A$, respectively; these quantities are undefined if A is empty, unbounded from below (for $\min A$) or from above (for $\max A$). The greatest common divisor of the elements of A is denoted $\gcd A$; notice that the assumption $\gcd A = 1$ implies that A contains at least one non-zero element. For an integer $h \geq 1$ the *h-fold sumset* of A is defined by

$$hA := \{a_1 + \cdots + a_h : a_1, \ldots, a_h \in A\};$$

this is the set of all integers representable as a sum of exactly h elements of A. We set $hA = \{0\}$ for $h = 0$.

Most of the results gathered in this section show that if the set A is sufficiently dense, then the sumsets hA are large and well-structured.

THEOREM 2 (Freiman [F66, Theorem 1.9]). *Let A be a finite set of integers such that* $\min A = 0$ *and* $\gcd A = 1$. *Write* $n := |A|$ *and* $l := \max A$. *Then*

$$|2A| \ge \min\{l, 2n-3\} + n.$$

A generalization of Theorem 2 is as follows.

THEOREM 3 (Lev [L96b, Corollary 1]). *Let A be a finite set of integers such that* $\min A = 0$ *and* $\gcd A = 1$. *Write* $n := |A|$ *and* $l := \max A$ *and suppose that κ is an integer satisfying* $\kappa(n-2)+1 \le l \le (\kappa+1)(n-2)+1$. *Then for any non-negative integer h we have*

$$|hA| \ge \begin{cases} \dfrac{h(h+1)}{2}(n-2)+h+1 & \text{if } h \le \kappa, \\ \dfrac{\kappa(\kappa+1)}{2}(n-2)+\kappa+1+(h-\kappa)l & \text{if } h \ge \kappa. \end{cases}$$

COROLLARY 4. *Let A be a finite set of integers such that* $\min A = 0$ *and* $\gcd A = 1$. *Write* $n := |A|$ *and* $l := \max A$ *and suppose that* $l \ge 3n-5$. *Then*

$$|3A| \ge 6n-8.$$

Proof. If $n = 2$, then $A = \{0, 1\}$ and the assertion is immediate. If $n \ge 3$, set $\kappa := \lfloor (l-1)/(n-2) \rfloor$ and apply Theorem 3 observing that $\kappa \ge 3$. ∎

The following result describes the structure of the sets hA and shows that if h is sufficiently large, these sets contain long blocks of consecutive integers.

THEOREM 5 (Lev, reformulation of [L97, Theorem 1]). *Let A be a finite set of integers such that* $\min A = 0$ *and* $\gcd A = 1$. *Write* $n := |A|$ *and* $l := \max A$ *and suppose that κ is an integer satisfying* $\kappa(n-2)+1 \le l \le (\kappa+1)(n-2)+1$. *Then for any non-negative integer* $h \ge 2\kappa$ *we have*

$$[(2l-(\kappa+1)(n-2)-2)\kappa, hl-(2l-(\kappa+1)(n-2)-2)\kappa] \subseteq hA.$$

REMARK. The complicated-looking expression $(2l-(\kappa+1)(n-2)-2)\kappa$ provides a sharp bound: the interval of Theorem 5 is widest possible and cannot be extended in either direction. One can replace it with the narrower interval $[\kappa l, (h-\kappa)l]$, but in some applications (such as the one considered in this paper) this results in a critical loss of accuracy.

Applying Theorem 5 with $\kappa = 1$ and $h = 4$ we obtain

COROLLARY 6. *Let A be a finite set of integers such that* $\min A = 0$. *Write* $n := |A|$ *and* $l := \max A$ *and suppose that* $l \le 2n-3$. *Then* $[2l-2n+2, 2l+2n-2] \subseteq 4A$.

By a *three-term arithmetic progression* we mean a three-element set of real numbers, one of which is the arithmetic mean of the other two; thus, the zero difference is forbidden, and progressions with the differences d and $-d$ are considered identical. To pass from the sumsets hA to sums of *pairwise distinct* elements of A we use a theorem by Varnavides.

THEOREM 7 (Varnavides [V59]). *For any real number $\alpha > 0$ there exists a real number $c > 0$ (depending on α) with the property that if l is a positive integer and $A \subseteq [1, l]$ is a set of integers satisfying $|A| > \alpha l$, then A contains at least cl^2 three-term arithmetic progressions.*

The *sumset* of two potentially distinct sets of integers B and C is defined by $B+C := \{b+c : b \in B,\ c \in C\}$. The following lemma is a straightforward generalization of [L96a, Lemma 1] and a particular case of [A04, Lemma 2.1].

LEMMA 8. *Let l be a positive integer and suppose that $B, C \subseteq [0, l]$ are integer sets satisfying $|B| + |C| \ge l + 2$. Then the sumset $B + C$ contains a power of 2.*

We sketch the proof mainly for the sake of completeness.

Proof of Lemma 8. Assuming that $B + C$ does not contain a power of 2, we show that $|B|+|C| \le l+1$. We use induction on l; the case $l = 1$ is obvious and we assume that $l \ge 2$. Fix an integer $r \ge 1$ so that $2^r \le l < 2^{r+1}$. If $b \in B$, then $2^{r+1} - b \notin C$, and it follows that

$$|B \cap [2^{r+1} - l, l]| + |C \cap [2^{r+1} - l, l]| \le 2l + 1 - 2^{r+1}. \tag{1}$$

On the other hand, by the induction hypothesis we have

$$|B \cap [0, 2^{r+1} - l - 1]| + |C \cap [0, 2^{r+1} - l - 1]| \le 2^{r+1} - l, \tag{2}$$

unless $l = 2^{r+1} - 1$. Actually, (2) remains valid also if $l = 2^{r+1} - 1$, provided that at least one of the sets B and C does not contain 0. Since the inequality $|B| + |C| \le l + 1$ is a direct corollary of (1) and (2), it remains to consider the case where $l = 2^{r+1} - 1$ and $0 \in B \cap C$. In this case we have $2^r \notin B$ and $2^r \notin C$; in other words, if $b = 2^r$ then $b \notin B$ and $2^{r+1} - b \notin C$. Consequently, (1) can be strengthened to $|B \cap [1, l]| + |C \cap [1, l]| \le l - 1$, and the result follows. ∎

3. Proof of Theorem 1. The key ingredient of our proof is

THEOREM 9. *Let A be a finite set of integers with $\min A = 0$. Write $l := \max A$ and $n := |A|$ and suppose that $n \ge \frac{17}{54} l + 2$. Then the sumset $5A$ contains a power of 2, unless all elements of A are divisible by 3.*

Proof. Since $n > l/4 + 1$, we have $\gcd A \le 3$, and in fact $\gcd A = 1$ can be assumed without loss of generality: for, if $\gcd A = 2$, then one can replace A with the set $A' := \{a/2 : a \in A\}$.

If $l \le 2n-2$, then the sumset $2A \subseteq 5A$ contains a power of 2 by Lemma 8, applied to the sets $B = C = A$. If $l \ge 2n-1$, then

$$|2A| \ge 3n-3 \tag{3}$$

by Theorem 2; if, in addition, we assume that $l \le 3n-4$, then $2|2A| \ge 6n-6 \ge 2l+2$ and by Lemma 8 applied to $B = C = 2A \subseteq [0, 2l]$, the sumset $4A \subseteq 5A$ contains a power of 2. For the rest of the proof we assume that $l \ge 3n-3$, and so by Corollary 4,

$$|3A| \ge 6n-8. \tag{4}$$

We assume, furthermore, that $5A$ does not contain a power of 2 (and so neither do any of $A, 2A, 3A, 4A \subseteq 5A$) and obtain a contradiction.

By Lemma 8 we have

$$|2A| + |(3A) \cap [0, 2l]| \le 2l+1,$$

whence

$$|(3A) \cap [0, 2l]| \le 2l - 3n + 4$$

by (3); using (4) we get

$$|(3A) \cap [2l, 3l]| = |3A| + 1 - |(3A) \cap [0, 2l]| \ge 9n - 2l - 11$$

so that

$$|[2l, 3l] \setminus (3A)| \le 3l - 9n + 12. \tag{5}$$

Fix now a positive integer r with $2l < 2^r < 4l$. (The equalities $2^r = 2l$ and $2^r = 4l$ are ruled out by the assumption that $5A$ does not contain a power of 2.) For any $a \in A$ we have $2^r - a \notin 4A$, and hence

$$|[2^r - l, 2^r] \setminus (4A)| \ge n. \tag{6}$$

If $2^r > 3l$ then $3l \in [2^r - l, 2^r]$ and in view of $(3A) \cup (3A + l) \subseteq 4A$ we derive from (6) and (5) that

$$\begin{aligned} n &\le |[2^r - l, 3l] \setminus (4A)| + |[3l, 2^r] \setminus (4A)| \\ &\le |[2^r - l, 3l] \setminus (3A)| + |[2l, 2^r - l] \setminus (3A)| \\ &\le |[2l, 3l] \setminus (3A)| + 1 \\ &\le 3l - 9n + 13, \end{aligned}$$

whence $3l \ge 10n - 13 > (85/27)l$, a contradiction. Thus, $2l < 2^r < 3l$.

Next, we notice that if $b \in 2A$, then $2^r - b \notin 3A$. Consequently,

$$\begin{aligned} |(2A) \cap [0, 2^{r-1}]| &\le |[2^{r-1}, 2^r] \setminus (3A)| \\ &\le |[2^{r-1}, 2l-1] \setminus (2A)| + |[2l, 2^r] \setminus (3A)| \\ &= 2l - 2^{r-1} - |(2A) \cap [2^{r-1}, 2l-1]| + |[2l, 2^r] \setminus (3A)|, \end{aligned}$$

and using (3) we conclude that

$$2^{r-1} \le 2l - 3n + 4 + |[2l, 2^r] \setminus (3A)|. \tag{7}$$

In conjunction with (5) this gives

$$2^{r-1} \le 5l - 12n + 16 \le \left(5 - 12 \cdot \frac{17}{54}\right) l = \frac{11}{9}\, l < \frac{5}{4}\, l.$$

With this in mind and observing that if $b \in 2A$, then $2^{r+1} - b \notin 3A$, we get

$$|(2A) \cap [2^{r+1} - 3l, 2l]| \le |[2^{r+1} - 2l, 3l] \setminus (3A)|.$$

Taking into account (3) and applying Lemma 8 with $B = C = (2A) \cap [0, 2^{r+1} - 3l - 1]$ we obtain

$$\begin{aligned} |[2^{r+1} - 2l, 3l] \setminus (3A)| &\ge |2A| - |(2A) \cap [0, 2^{r+1} - 3l - 1]| \\ &\ge 3n - 3 - 2^r + \frac{3}{2}\, l. \end{aligned} \tag{8}$$

Finally, (5), (7), and (8) give

$$\begin{aligned} 6l - 18n + 24 &\ge 2|[2l, 3l] \setminus (3A)| \\ &\ge 2|[2l, 2^r] \setminus (3A)| + |[2^{r+1} - 2l, 3l] \setminus (3A)| \\ &\ge (2^r - 4l + 6n - 8) + \left(3n - 3 - 2^r + \frac{3}{2}\, l\right) \\ &= 9n - \frac{5}{2}\, l - 11, \end{aligned}$$

and therefore

$$\begin{aligned} \frac{17}{2}\, l &\ge 27n - 35, \\ n &\le \frac{17}{54}\, l + \frac{35}{27}, \end{aligned}$$

the contradiction sought. ∎

Proof of Theorem 1. Denote by A_0 the set of all those elements of A which are the midterm of at least four three-term arithmetic progressions with elements in A. Write $n_0 := |A_0|$, $l_0 := \max A_0$, and $A_1 := A \setminus A_0$. Evidently, the number of three-term arithmetic progressions in A_1 is at most $3|A_1| \le 3l$. If we had $|A_1| > l/1026 - 1$, then for sufficiently large l this would contradict Theorem 7. Consequently, we can assume that $|A_1| \le l/1026 - 1$, and hence $n_0 \ge (6/19)l - l/1026 + 1 = (17/54)l + 1$. We have $\gcd A_0 \le l_0/n_0 < 54/17 < 4$, so that in fact $\gcd A_0 \in \{1, 2, 3\}$, and we first consider the case where $\gcd A_0 < 3$. By Theorem 9 as applied to the set $A_0 \cup \{0\}$, there is an integer $1 \le k \le 5$ and elements $a_1, \dots, a_k \in A_0$ such that $\sigma := a_1 + \dots + a_k$ is a power of 2. Suppose that $k \ge 2$ and some of the a_i are equal; say, $a_1 = a_2$. By the definition of A_0, we can then find four representations of $a_1 + a_2$ as a sum of two elements of A, so that the two summands in each representation are distinct from each other and from the summands in all other representations. For at most three of the representations in question one of the summands lies in $\{a_3, \dots, a_k\}$, and it follows that there is a representation $a_1 + a_2 = a'_1 + a'_2$ such that each of a'_1 and a'_2 is distinct from $a_3, \dots, a_k$. We now write $\sigma = a'_1 + a'_2 + a_3 + \dots + a_k$, and repeating the procedure if necessary, we represent σ (which is a power of 2) as a sum of pairwise distinct elements of A, as desired.

It remains to consider the case where $\gcd A_0 = 3$. Write $A' := \{a/3 : a \in A_0\}$, so that $\max A' = l_0/3$, $\gcd A' = 1$, and $|A'| = n_0$. We have

$$l_0 \le \frac{54}{17}(n_0 - 1) < 6(n_0 - 1),$$

whence

$$l_0/3 < 2(n_0 + 1) - 3.$$

Therefore, applying Corollary 6 to the set $A' \cup \{0\}$, we conclude that every integer from the interval $T := [2l_0/3 - 2n_0 + 2, 2l_0/3 + 2n_0 - 2]$ is a sum of at most four elements of A'. Let a be an element of A, not divisible by 3. Since

$$a + 3(2l_0/3 + 2n_0 - 2) \ge 4(a + 3(2l_0/3 - 2n_0 + 2))$$

(as follows from $a \le l \le -2l + 10n_0 - 10 \le -2l_0 + 10n_0 - 10$), the interval $[a+3(2l_0/3-2n_0+2), a+3(2l_0/3+2n_0-2)]$ contains two consecutive powers of 2. One of them is congruent to a modulo 3, hence can be represented as $a + 3t$ with an integer $t \in T$ and furthermore as $a + a_1 + \dots + a_k$, where $1 \le k \le 4$ and $a_1, \dots, a_k \in A_0$. The proof can now be completed as above, by eliminating possible repetitions of the summands. ∎

Acknowledgements. The two exceptional sets at the beginning of the paper were found at our request by Talmon Silver, using an exhaustive computer search. For $l \le 60$, the complete list of all sets $A \subseteq [1, l]$ with $|A| > l/3$ and such that no power of 2 can be represented as a sum of pairwise distinct elements of A is

$$\{5,6,7\},\ \{3,6,9,11\},\ \{3,7,10,11\},\ \{3,9,10,11\},\ \{3,9,10,11,14\},$$
$$\{5,7,10,12,14\},\ \{3,9,10,12,14\},\ \{5,9,10,12,14\},\ \{3,10,11,12,14\},$$
$$\{6,9,11,13,14\},\ \{10,11,12,13,14\},\ \{7,10,11,13,17,18,20\},$$

and it is quite possible that no other sets with the property in question exist. We are grateful to Talmon Silver for this contribution.

References

[A04] T. Abe, *Sumsets containing powers of an integer*, Combinatorica 24 (2004), 1–4.

[E89] P. Erdős, *Some problems and results on combinatorial number theory*, in: Graph Theory and its Applications: East and West (Jinan, 1986), Ann. New York Acad. Sci. 576, New York Acad. Sci., New York, 1989, 132–145.

[EF90] P. Erdős and G. A. Freiman, *On two additive problems*, J. Number Theory 34 (1990), 1–12.

[F66] G. A. Freiman, *Elements of a structural theory of set addition*, Kazan. Gosudarstv. Ped. Inst., Elabuzh. Gosudarstv. Ped. Inst., Kazan, 1966 (in Russian); English transl. in: Transl. Math. Monogr. 37, Amer. Math. Soc., Providence, RI, 1973.

[F92] —, *Sumsets and powers of 2*, in: Sets, Graphs and Numbers (Budapest, 1991), Colloq. Math. Soc. János Bolyai 60, North-Holland, Amsterdam, 1992, 279–286.

[L96a] V. F. Lev, *Representing powers of 2 by a sum of four integers*, Combinatorica 16 (1996), 413–416.

[L96b] —, *Structure theorem for multiple addition and the Frobenius problem*, J. Number Theory 58 (1996), 79–88.

[L97] —, *Optimal representations by sumsets and subset sums*, ibid. 62 (1997), 127–143.

[NS89] M. B. Nathanson and A. Sárközy, *Sumsets containing long arithmetic progressions and powers of 2*, Acta Arith. 54 (1989), 147–154.

[V59] P. Varnavides, *On certain sets of positive density*, J. London Math. Soc. 34 (1959), 358–360.

Department of Mathematics
The University of Haifa at Oranim
Tivon 36006, Israel
E-mail: seva@math.haifa.ac.il

Received on 10.8.2006 (5260)