Discrete Mathematics 114 (1993) 367–377
North-Holland

On subset sums of r-sets

E. Lipkin*

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel-Aviv University, Israel

Received 6 March 1989
Revised 14 August 1990

Abstract

Lipkin, E., On subset sums of r-sets, Discrete Mathematics 114 (1993) 367–377.

A finite set of distinct integers is called an r-set if it contains at least r elements not divisible by q for each $q \geqslant 2$. Let $f(n,r)$ denote the maximum cardinality of an r-set $A \subset \{1,2,\ldots,n\}$ having no subset sum $\sum \varepsilon_i a_i$ ($\varepsilon_i = 0$ or 1, $a_i \in A$) equal to a power of two.

In this paper estimates for $f(n,r)$ are obtained. We prove that $\lim_{r\to\infty} \alpha_r = 0$, where $\alpha_r = \overline{\lim}_{n\to\infty} f(n,r)/n$. This result verifies a conjecture of Erdős and Freiman (1990).

1. Introduction

Let $A \subset [1,n]$ and A^* denote the set of all sums of subsets of A, i.e. $A^* = \{\sum_{b\in B} b, B \subseteq A\}$. Given $n \in \mathbf{N}$, let $f(n)$ denote the number of elements of a largest set $A \subset [1,n]$ for which A^* contains no power of 2. Erdős and Freiman [4] proved that $f(n) = [n/3]$ for $n > n_0$, where n_0 is a sufficiently large positive number. Note that this formula does not hold for all natural numbers n. The example of the set $A = \{10, 11, 12, 13, 14\}$ shows that $f(14) \geqslant 5$; hence, $n_0 > 13$. The upper bound $f(n) \leqslant n/3$ was obtained in [4] using analytical methods of number theory. The lower bound $f(n) \geqslant [n/3]$ was provided by Erdős' example [3] of the set $A = \{3\cdot 1, 3\cdot 2, \ldots, 3\cdot[n/3]\}$.

We note that the extremal example of Erdős is the subset of all multiples of 3. So, in the present paper we modify the problem and consider only those subsets in which not all the elements are divisible by a common number (see [4], p. 12). As a first example, we construct a set $A \subset [2,n]$ which contains all multiples of 6 and an arbitrary integer congruent to 1 modulo 6. We observe in this example that $2^s \notin A^*$ for any $s \geqslant 0$ since $2^s \equiv 2$ or $4 \pmod 6$ for all natural numbers s.

Correspondence to: E. Lipkin, School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv, Israel.

* Research supported by the Fund of Basic Research administered by the Israel Academy of Sciences.

Let $f(n,1)$ denote the number of elements of a largest set $A\subset[1,n]$ such that not all its elements are multiples of some prime number and A^* does not contain a power of 2. The above example gives $f(n,1)\geqslant[n/6]+1$ for $n\geqslant 7$. In Theorem 1.1 it is shown that $f(n,1)=[n/6]+2$ for $n>n_0$.

In general, we call a finite set of integers A an r-set if, for each integer $q\geqslant 2$, the set A contains at least r elements which are not multiples of q. For example, $\{1,2,3\}$ is a 2-set. Let $f(n,r)$ denote the maximum cardinality of an r-set $A\subset\{1,2,\ldots,n\}$ having no power of 2 in A^*. The function $f(n)$ defined above is the special case of $f(n,r)$ for $r=0$, i.e. $f(n)=f(n,0)$. The following examples give lower bounds for $f(n,r)$.

(1) Let $A=\{6\cdot 1,6\cdot 2,\ldots,6\cdot[n/6]\}\cup\{7,5\}$. This gives the bound $f(n,2)\geqslant[n/6]+2$ for $n\geqslant 7$.

(2) Let $A=\{12\cdot 1,12\cdot 2,\ldots,12\cdot[n/12]\}\cup\{a_1,\ldots,a_6\}$, where a_i are distinct integers such that $a_i\in[2,n]$ and $a_i\equiv 1\ (\mathrm{mod}\ 12)$ for $i=1,2,3$, $a_i\equiv -1\ (\mathrm{mod}\ 12)$ for $i=4,5,6$. Since $2^s\equiv\pm 4\ (\mathrm{mod}\ 12)$ for $s\geqslant 2$, $2^s\notin A^*$ for each $s\geqslant 0$. Thus, for $3\leqslant r\leqslant 6$ we obtain that $f(n,r)\geqslant[n/12]+6$ provided $n\geqslant 37$.

(3) The condition

$$2^k-1\leqslant r\leqslant 2^{k+1}-2 \tag{1.1}$$

for any $r\in\mathbf{N}$ determines the natural number k. Set $q=3\cdot 2^k$ and let $A=\{q,2q,\ldots,q\cdot[n/q]\}\cup\{a_1,a_2,\ldots,a_{2^{k+1}-2}\}$, where a_i are distinct integers such that $2^k\leqslant a_i\leqslant n$, $a_i\equiv 1\ (\mathrm{mod}\ q)$ for $i=1,2,\ldots,2^k-1$ and $a_i\equiv -1\ (\mathrm{mod}\ q)$ for $i=2^k,\ldots,2^{k+1}-2$. Since $2^s\equiv\pm 2^k\ (\mathrm{mod}\ 3\cdot 2^k)$ for $s\geqslant k$, $2^s\notin A^*$ for all integers $s\geqslant 0$. We obtain the lower bound

$$f(n,r)\geqslant\left[\frac{n}{3\cdot 2^k}\right]+2^{k+1}-2 \quad \text{for } r=2^k-1,\ldots,2^{k+1}-2, \tag{1.2}$$

where k is determined by (1.1), and $n\geqslant(2^k-1)q+1$.
In Section 3 it is shown that, for small r, the estimate (1.2) is precise:

Theorem 1.1. *For* $r\leqslant 30$,

$$f(n,r)=\left[\frac{n}{3\cdot 2^k}\right]+2^{k+1}-2, \tag{1.3}$$

where k is determined by (1.1) *and* $n>n_0$, *where* n_0 *is a sufficiently large positive constant.*

For general $r>30$, (1.3) is not true. In fact, in Section 3 we prove the following theorem.

Theorem 1.2. *For* $31\leqslant r\leqslant 38$ *and* $n>n_0(r)$,

$$f(n,r)=\left[\frac{n}{85}\right]+38.$$

In order to formulate the general result, we introduce a function $q(r)$ as follows. Let $r \geqslant 1$. First, we call a multiset A_q of residues modulo q an r-multiset if, for each divisor q' of q, $q' \neq 1$, there are at least r elements in A_q which are not divisible by q'. Also, let A_q^* denote the set of all sums of subsets of A_q, $A_q^* = \{\sum_{b \in B} b \pmod{q},\ B \subseteq A\}$. Now, for every fixed $r \geqslant 1$, consider the numbers q such that

(1) q is not a power of two, and

(2) there exists an r-multiset A_q such that A_q^* does not contain $2^s \pmod{q}$ for $s \geqslant s_0$, where s_0 is derived from the condition that $2^{s_0} \mid q$, but $2^{s_0+1} \nmid q$.

The smallest q satisfying the above criteria is denoted by $q(r)$. For example, $q(2) = 6$. Indeed, consider the 2-multiset $A_6 = \{1, -1\} \pmod{6}$. The set $A_6^* = \{1, 0, -1\}$ does not contain $2^s \pmod{6}$ for $s \geqslant 1$ (the inequality $s \geqslant 1$ is coming from the condition that $2 \mid 6$, $2^2 \nmid 6$), because $2^s \equiv 2$ or $-2 \pmod{6}$. Thus, $q(2) \leqslant 6$. Also, $q = 6$ is the minimal modulus satisfying the definition of $q(2)$. Indeed, $q = 2$ and $q = 4$ are powers of 2; further, since 2 is a primitive root modulo $q = 3$ then, for any multiset A_3 of nonzero residues mod 3, A_3^* contains a power of 2. The same argument shows $q(2) > 5$.

Using the function $q(r)$, we can find $f(n, r)$.

Theorem 1.3. *Let $r \in \mathbf{N}$. For every $n > n_0$, where $n_0 = n_0(r)$, there exists $C = C(n, r)$, satisfying $r \leqslant C < q(r)$, such that*

$$f(n, r) = \left[\frac{n}{q(r)} \right] + C \tag{1.4}$$

holds.

The lower bound

$$q(r) > r + 1 \tag{1.5}$$

will follow from Proposition 2.2. Combining the bound (1.5) and Theorem 1.3, we obtain the following theorem.

Theorem 1.4. *For $n > n_0(r)$,*

$$f(n, r) < \frac{n}{r+1} \tag{1.6}$$

holds, where $n_0(r)$ is some large positive number.

Since $3 \cdot 2^k \leqslant 3(r+1)$, (1.2) implies that $f(n, r) \geqslant n/3(r+1)$. Let $\alpha(r) = \overline{\lim}_{n \to \infty} f(n, r)/n$ and $\beta(r) = \underline{\lim}_{n \to \infty} f(n, r)/n$. We obtain

$$\alpha(r) \leqslant \frac{1}{r+1}, \qquad \beta(r) \geqslant \frac{1}{3(r+1)}. \tag{1.7}$$

Finally, from (1.7) we have the following result.

Theorem 1.5. $\lim_{r\to\infty} \alpha(r)=0$.

This theorem verifies the conjecture of Erdős and Frieman [4].

Theorem 1.3 reduces the study of $f(n,r)$ to the study of $q(r)$. This theorem as well as the bound (1.5) are proved in Section 2. We compute $q(r)$ and C for small r in Section 3, where Theorems 1.1 and 1.2 are proved. In Section 3 we also obtain the following estimates of $q(r)$:

(1) $q(r)\leqslant(85/32)\cdot 2^k<2.7\cdot 2^k$ for $r\in[2^k-1,2^k-1+(2^k/4))$, where $k\geqslant 5$;

(2) $q(r)\leqslant(4681/2048)\cdot 2^k<2.3\cdot 2^k$ for $r\in[2^k-1,2^k-1+(2^k/12))$, where $k\geqslant 11$.

These bounds improve, for some r, the estimate following from (1.2):

$$q(r)\leqslant 3\cdot 2^k,\quad \text{where } r\in[2^k-1,2^{k+1}-2] \tag{1.8}$$

Improving the lower bounds for $q(r)$ is is a difficult problem.

In Section 4 we study the structure of locally optimal sets. We call a set of integers $A\subset[1,n]$ locally optimal if A^* does not contain a power of two, but, for any larger set $A'\supset A$, $A'\subset[1,n]$, A' has 2^s as a subset sum for some s. We show that a locally optimal set is a union of an arithmetic progression and a small set, possibly empty. We prove that, for sufficiently large n, the only subset of $\{1,\dots,n\}$ of maximum cardinality, having no subset sum equal to a power of 2, is Erdős' set $\{3,6,\dots,3\cdot[n/3]\}$.

2. The proof of Theorem 1.3

To prove Theorem 1.3, we need two preliminary results from [1], [2].

Lemma 2.1 (Alon and Freiman [1] Lemma 3.4). *Suppose $\varepsilon>0$, $n>n(\varepsilon)$ and let $A\subset\{1,\dots,n\}$ be a set of distinct integers of cardinality x, where $x>3n^{2/3+\varepsilon}\log n$. Then there exists a subset $B\subseteq A$ of cardinality t and an integer $q\geqslant 1$ sastisfying the following conditions*:

(i) $t\geqslant x-n^{(2+\varepsilon)/3}$,

(ii) $q\leqslant n/t$,

(iii) $b_j\equiv 0 \pmod q$ *for each* $b_j\in B$,

(iv) *if* $S=\sum_{j=1}^t b_j$, *then every integer N which is divisible by q and satisfies $N_1\leqslant N\leqslant N_2$, where*

$$N_1=\frac{n^{2/3+\varepsilon}}{t}\cdot S+n^{4/3}\log n,\qquad N_2=S-\frac{n^{2/3+\varepsilon}}{t}\cdot S-n^{4/3}\log n, \tag{2.1}$$

belongs to $B^*\subset A^*$.

The second assertion follows from Proposition 3 in [2], which is given below.

Proposition 2.2. *Let A_q be a multiset of nonzero residues modulo q. Suppose that $|A_q| \geqslant q-1$ and $|A_{q'}| \geqslant q'-1$ for each divisor q' of q, $q' \neq 1$. Then the set A_q^* includes elements from all residue classes modulo q, except possibly* 0.

Recall now that $f(n,r)$ is the maximum cardinality of an r-set $A \subset \{1,\dots,n\}$ with no power of 2 in A^*. We want to prove that $f(n,r)=[n/q(r)]+C$ for sufficiently large n, when $C=C(n,r)$ satisfies $r \leqslant C < q(r)$, by way of estimating $f(n,r)$ from above and below by the same bound.

(1) We will obtain the upper bound for $f(n,r)$. Suppose that the cardinality of an r-set $A \subset \{1,\dots,n\}$ satisfies

$$|A| \geqslant \left[\frac{n}{q(r)}\right] + q(r). \tag{2.2}$$

We will show that, for sufficiently large n, there exists $s \in \mathbf{N}$ such that $2^s \in A^*$. By Lemma 2.1, there exists $q \geqslant 1$ such that every integer N satisfying $N \equiv 0 \pmod q$ and $N_1 \leqslant N \leqslant N_2$ belongs to A^*. We start with the case $q=2^u$ for some integer $u \geqslant 0$. In view of (2.1), $N_2 > 4N_1$ provided n is sufficiently large. Thus, we can find a natural number s such that $N_1 < 2^s < N_2$. Let $N=2^s$. Since $N \equiv 0 \pmod q$, we conclude that $2^s \in A^*$, as needed.

Assume now that the number q of Lemma 2.1 is different from any power of 2 and $q \neq 1$. We note that the inequality $q > q(r)$ never holds. Indeed, Lemma 2.1(ii) implies that $t \leqslant n/q$ and (i) implies that $x=|A| \leqslant n/q + n^{(2+\varepsilon)/3}$. In view of (2.2), we have $n/q + n^{(2+\varepsilon)/3} \geqslant n/q(r)+q(r)$, which cannot be satisfied if $q > q(r)$ and n is sufficiently large. Thus, we may assume $q \leqslant q(r)$ and q is not a power of 2.

Consider a multiset A_q of nonzero residues modulo q of elements of the set A. Because A is an r-set, A_q is an r-multiset. Assume that A_q^* contains $2^{s_1} \pmod q$ for some $s_1 \geqslant s_0$, where s_0 is determined by $2^{s_0} \mid q$ and $2^{s_0+1} \nmid q$. Then A^* contains a power of 2. Indeed, let δ be the index of 2 modulo $q_1 = q/2^{s_0}$. Then $2^\delta \equiv 1 \pmod{q_1}$ and $2^{\delta t + s_0} \equiv 2^{s_0} \pmod q$ for every integer $t \geqslant 0$, and also $2^{\delta t + s_1} \equiv 2^{s_1} \pmod q$ since $s_1 \geqslant s_0$. In view of our assumption, there exist m elements of A such that $M = a_{i_1} + \cdots + a_{i_m} \equiv 2^{s_1} \pmod q$, and $a_{i_k} \not\equiv 0 \pmod q$, $k=1,\dots,m$. Add M to the elements of B^* from Lemma 2.1. We obtain that all numbers N satisfying $N \equiv 2^{s_1} \pmod q$ and $N_1 + M \leqslant N \leqslant N_2 + M$ belong to A^*. Moreover, one of these numbers is a power of 2. Indeed, $(N_2+M)/(N_1+M) > 2^\delta$ holds for sufficiently large n. Take $t=t_1$ be the smallest number such that $N_1 + M < 2^{\delta t_1 + s_1}$. Since $2^{\delta(t_1-1)+s_1} \leqslant N_1 + M$, $2^{\delta t_1 + s_1} \leqslant 2^\delta (N_1+M) < N_2 + M$. Clearly, $N = 2^{\delta t_1 + s_1}$ is a desired number.

To complete the proof of Part 1 we need only show that A_q^* contains $2^{s_1} \pmod q$ for some $s_1 \geqslant s_0$, assuming $q \leqslant q(r)$. It is true if $q < q(r)$, because of the definition of $q(r)$. Let $q = q(r)$. In this case we will try to apply Proposition 2.2 to the multiset A_q and obtain that A_q^* contains all nonzero residue classes modulo q, including a power of 2. The number of elements in A, which are divisible by $q(r)$, does not exceed $[n/q(r)]$. Therefore, $|A_q|\geqslant q$, in view of (2.2). Let us check that also $|A_{q'}|\geqslant q'-1$ holds for each divisor q' of q, $q'\neq 1$. This is correct for $q'\leqslant q/3$. Indeed, by definition of r-multiset and using (1.8), we have $|A_{q'}|\geqslant r\geqslant 2^k-1\geqslant q/3-1\geqslant q'-1$. Finally, assume that q is even and consider $q'=q/2$. If $q/2\notin A_q$, then $|A_{q/2}|=|A_q|\geqslant q>q/2-1$ and the conditions of Proposition 2.2 are satisfied. Otherwise, suppose there exists $a\in A$ such that $a\equiv(q/2)(\operatorname{mod} q)$. The set $B^*\cup(B^*+a)$ is contained in A^*; so, all numbers N satisfying $N\equiv 0(\operatorname{mod} q/2)$ and $N_1+a\leqslant N\leqslant N_2+a$ belong to A^*. Because $q(r)$ is the smallest q for which there exists an r-multiset A_q without a power of 2 in A_q^*, the multiset $A_{q/2}^*$ contains a power of 2 modulo $q/2$. Part 1 is now completely proved.

(2) Now we obtain the lower bound for $f(n,r)$. By the definition of $q(r)$, there exists an r-multiset $A_{q(r)}$ such that $2^s(\operatorname{mod} q(r))\notin A_{q(r)}^*$ for all $s\geqslant s_0$. Thus, $f(n,r)\geqslant[n/q(r)]+r$. The proof of Theorem 1.3 is complete.

Now we show that the lower bound (1.5) holds. Suppose that $q(r)>r+1$ is not true. By the definition of $q(r)$, there exists an r-multiset of residues $A_{q(r)}$ such that $A_{q(r)}^*$ does not contain $2^s(\operatorname{mod} q(r))$ for $s\geqslant s_0$. But our assumption $r\geqslant q(r)-1$ implies that the conditions of Proposition 2.2 for $A_{q(r)}$ are satisfied. Hence, $A_{q(r)}^*$ contains all nonzero residues modulo $q(r)$. This contradicts the definition of $q(r)$.

3. Computation of $q(r)$ for small r

For $1\leqslant r\leqslant 30$, we can obtain the precise value of $q(r)$.

Proposition 3.1. *If* $1\leqslant r\leqslant 30$ *then* $q(r)=3\cdot 2^k$, *where* k *is defined by the condition* $r\in[2^k-1,2^{k+1}-2]$.

To prove this, we use the following lemma.

Lemma 3.2. *Assume that for some natural number* r *and an odd prime* p, *every multiset* A_p *of* r *nonzero residues modulo* p *satisfies* $2^s(\operatorname{mod} p)\in A_p^*$ *for some* $s\geqslant 0$. *Then every multiset* A_{2^ap} *containing* 2^ar+2^a-1 *residues modulo* 2^ap *satisfies* $2^s(\operatorname{mod} 2^ap)\in A_{2^ap}^*$ *for some* $s\geqslant a$, *provided* $a_i\not\equiv 0(\operatorname{mod} p)$ *for all* $a_i\in A_{2^ap}$.

Proof. Suppose that the multiset A_{2^ap} contains r nonzero residues divisible by 2^a, call these residues $2^aa_1,\ldots,2^aa_r$. Then their subset sum gives a power of two modulo 2^ap. Indeed, by the assumption of the lemma, $\sum_{i=1}^r\varepsilon_ia_i\equiv 2^s(\operatorname{mod} p)$ holds for some s and some $\varepsilon_i=1$ or 0. Hence, $\sum_{i=1}^r\varepsilon_i\cdot 2^aa_i\equiv 2^{s+a}(\operatorname{mod} 2^ap)$.

Note that if a_i, a_j, a_k are three residues mod 2^ap, none of which is divisible by p, then we can always choose two of them such that their sum is not divisible by p. Indeed, if $a_i+a_j\equiv 0(\operatorname{mod} p)$, $a_i+a_k\equiv 0(\operatorname{mod} p)$, $a_j+a_k\equiv 0(\operatorname{mod} p)$, then add the first two congruences and subtract the third. We obtain $2a_i\equiv 0(\operatorname{mod} p)$ and $a_i\equiv 0(\operatorname{mod} p)$, which contradicts that $p\not| a_i$.

Assume that the multisset $A_{2^a p}$ contains $2^a r+2^a-1$ residues modulo $2^a p$, not divisible by p, and suppose x of them are odd residues and y of them are even. We can choose $[(x-1)/2]$ pairs such that the sum of each pair is an even residue not divisible by p. We obtain the number $[(x-1)/2]+y$ of even residues in $A^*_{2^a p}$, which is minimal if $y=0$. Thus, we have at least $[(2^a{\cdot}r+2^a-2)/2]=2^{a-1}r+2^{a-1}-1$ residues divisible by 2.

Suppose that x of them are not divisible by 4, and y of them are divisible by 4. In a similar way, we obtain $2^{a-2}r+2^{a-2}-1$ residues in $A^*_{2^a p}$ divisible by 4 and not divisible by p. On the sth step we obtain $2^{a-s}r+2^{a-s}-1$ residues divisible by 2^s and not divisible by p. On the ath step we obtain r residues divisible by 2^a and not divisible by p, thus proving the stated lemma. □

Proof of Proposition 3.1. The proposition claims that $q(r)=3{\cdot}2^k$ for $r\in[2^k-1, 2^{k+1}-2]$, i.e. $q(r)=6$ for $r\in[1,2]$, $q(r)=12$ for $r\in[3,6]$, $q(r)=24$ for $r\in[7,14]$, $q(r)=48$ for $r\in[15,30]$.

The estimate (1.8), $q(r)\leqslant 3{\cdot}2^k$, where k is derived from $2^k-1\leqslant r\leqslant 2^{k+1}-2$, was obtained in Section 1. Let k, r and q be integers such that $1\leqslant k\leqslant 4$, $r\in[2^k-1, 2^{k+1}-2]$, $3{\cdot}2^{k-1}<q<3{\cdot}2^k$ and q is not a power of 2. We will show that every r-multiset A_q of residues modulo q satisfies

$$2^s \pmod q \in A^*_q \tag{3.2}$$

for some s. It suffices to check the statement for the worst case $r=2^k-1$.

Case $k=1$. Since $q<6$ and $q\neq 2^k$, we are considering $q=3$ and $q=5$; so, $r=1$. For $q=3$, (3.2) holds since 2 is a primitive root modulo 3. The same argument applies when $q=5$.

Case $k=2$. In this case $6\leqslant q<12$ and $q\neq 2^k$; so, $r=3$. Then we need to verify for $q=6,7,9,10,11$ that, for an arbitrary r-multiset A_q, with $|A_q|\geqslant 3$, (3.2) holds.

In view of Lemma 3.2, the statement is true for $q=6$ and $q=10$.

Let $q=7$. Assume that, for a multiset $A_q=\{a_1,a_2,a_3\}$ of nonzero residues modulo 7, $2^s \pmod 7 \notin A^*_q$ holds for all $s\geqslant 0$. Denote by $k(a_i)$ a multiplicity of a_i in A_q. Since $2^s \pmod 7 \equiv 1$ or 2 or 4, we see that $k(1)=k(2)=k(4)=0$. Also, $k(3)\leqslant 2$, $k(5)\leqslant 2$, $k(6)\leqslant 2$. If $k(3)>0$ then $k(5)=0$, $k(6)=0$ and we have $|A_q|\leqslant 2$, which is contrary to the assumption. Thus, $k(3)=0$. If $k(5)>0$ then $k(6)=0$ and we have $|A_q|\leqslant 2$. Therefore, $k(3)=k(5)=0$ and we obtain $|A_q|\leqslant 2$ again, which contradicts the assumption that $|A_q|=3$. Thus, the statement for $q=7$ is proved.

Let $q=9$. Assume that, for a multiset $A_q=\{a_1,a_2,a_3\}$ of nonzero residues modulo 9, $2^s \pmod 9 \notin A^*_q$ holds for all natural s. Since $2^s \pmod 9$ is congruent to one of the numbers $1,2,4,5,7,8$, $a_i\equiv 3$ or $6 \pmod 9$, which contradicts that A_q is an r-multiset.

Let $q=11$. Since 2 is a primitive root modulo 11, (3.2) holds.

Cases $k=3$ and $k=4$ are verified similarly. □

For $r>30$, we have for $q(r)$ the upper bound (1.8): $q(r)\leqslant 3{\cdot}2^k$, where k is defined by the condition $r\in[2^k-1, 2^{k+1}-2]$. For r's in the first quarter of each interval

$[2^k-1, 2^{k+1}-2]$ starting with $k=5$, we obtain a more precise estimate, as given by the following proposition.

Proposition 3.3. *$q(r) \leqslant (85/32) \cdot 2^k = 2.65625 \cdot 2^k$ holds for $r \in (2^k-1, 2^k-1+2^k/4)$ and $k \geqslant 5$.*

Proof. Let $k=5$. In the same way as in Section 1, where we obtained the upper bound $q(r) \leqslant 6$ for $r \in [1,2]$, here the estimate $q(r) \leqslant 85$ for $r \in [31, 38]$ is given by the multiset $A_q = \{a_1, \ldots, a_{36}, b_1, b_2\}$ of residues $a_i \equiv 7 \pmod{85}$, $b_i \equiv -7 \pmod{85}$. Indeed, the smallest positive x which sastisfies the congruence $ax \equiv 2^s \pmod{85}$ for some $s \geqslant 0$ is $x_{\min} = 37$ when $a \equiv 7 \pmod{85}$ and $x_{\min} = 3$ when $a \equiv -7 \pmod{85}$. For $k > 5$, we use a similar example. Let $m \geqslant 1$. The minimal positive solution of the congruence $ax \equiv 2^s \pmod{85 \cdot 2^m}$, where $s \geqslant m$, is $x_{\min} = 37 \cdot 2^m$ when $a \equiv 7 \pmod{85 \cdot 2^m}$ and $x_{\min} = 3 \cdot 2^m$ when $a \equiv -7 \pmod{85 \cdot 2^m}$. Note that $2^s \pmod{85 \cdot 2^m} \notin [1, 2^m)$ for $s \geqslant m$. Thus, the set $A \subset [1, n]$ having $2^s \notin A^*$ for any s is the union of three sets: (1) the arithmetic progression of all multiples of $85 \cdot 2^m$; (2) the set of $37 \cdot 2^m - 1$ distinct numbers $a_i \in [2^m, n]$, $a_i \equiv 7 \pmod{85 \cdot 2^m}$; (3) the set of $3 \cdot 2^m - 1$ distinct numbers $b_i \in [2^m, n]$, $b_i \equiv -7 \pmod{85 \cdot 2^m}$. So, $|A_q| = 40 \cdot 2^m - 2 = (5/4) \cdot 2^k - 2 = 2^k - 2 + 2^k/4$. The conditions $a_i \geqslant 2^m$, $b_i \geqslant 2\mathrm{m}$ ensure that $2^s \notin A^*$ for $s = 0, 1, \ldots, m-1$. □

Proposition 3.4. *$q(r) = 85$ for $r = 31, \ldots, 38$.*

Proof. We checked for $r=31$ that every r-multiset A_q of nonzero residues modulo q, $48 \leqslant q < 85$, $q \neq 2^m$, satisfies $2^s \pmod{q} \in A_q^*$ for some $s \geqslant 0$. With the estimate $q(r) \leqslant 85$ for $r \in [31, 38]$ from Proposition 3.3, it implies the stated equality. □

For $r=39$ and $q=85$, every r-multiset A_q sastisfies $2^s \pmod{q} \in A_q^*$ for some $s \geqslant 0$; therefore, $q(39) > 85$.

The next improvement of the upper bound for $q(r)$ is given by the following example [7]. The estimate $q(r) \leqslant 4681$ for $r \in [2047, 2222]$ is provided by the multiset A_q of residues modulo $q = 4681$, $a_i \equiv 15 \pmod{q}$ for $1 \leqslant i \leqslant 2184$, $b_i \equiv -15 \pmod{q}$ for $1 \leqslant i \leqslant 38$. For this, set$|A_q| = 2222$ and $2^s \pmod{q} \notin A_q^*$ for $s \geqslant 0$ holds. Continuing as in Proposition 3.3, we have the following result.

Proposition 3.5. *$q(r) \leqslant (4681/2048) \cdot 2^k$ for $r \in [2^k-1, (2224/2048) \cdot 2^k - 2]$, $k \geqslant 11$.*

This implies that $q(r) \leqslant 2.3 \cdot 2^k$ for $r \in [2^k-1, 2^k-2+2^k/12]$, $k \geqslant 11$.

Two more series of upper bounds for $q(r)$ are provided by the following sets A_q [7]:
(1) $q = 1285$, $|A_q| = 598$, $a_i \equiv 127 \pmod{q}$, $b_i \equiv -127 \pmod{q}$;
(2) $q = 1365$, $|A_q| = 670$, $a_i \equiv 31 \pmod{q}$, $b_i \equiv -31 \pmod{q}$.

Table 1 lists the exact values of $q(r)$ for $1 \leqslant r \leqslant 38$, and Table 2 lists our upper bounds of $q(r)$ for $38 < r \leqslant 2^{12} - 2$. Different columns of the tables correspond to different sequences $3 \cdot 2^k, 85 \cdot 2^j$ and so on, where $k, j = 1, 2, \ldots$.

Table 1
Values of $q(r)$

k	$r\in[2^k-1,2^{k+1}-1)$	$q(r)$	
1	[1,2]	6	
2	[3,6]	12	
3	[7,14]	24	
4	[15,30]	48	
5	[31,38]		85

Table 2
Upper bounds of $q(r)$

k	$r\in[2^k-1,2^{k+1}-1)$	$q(r)$				
5	[39,62]	96				
6	[63,78]		170			
	[79,126]	192				
7	[127,158]		340			
	[159,254]	384				
8	[255,318]		680			
	[319,510]	768				
9	[511,598]			1285		
	[599,638]		1360			
	[639,670]				1365	
	[671,1022]	1536				
10	[1023,1198]			2570		
	[1199,1278]		2720			
	[1279,1342]				2730	
	[1343,2046]	3072				
11	[2047,2222]					4681
	[2223,2398]			5140		
	[2399,2558]		5440			
	[2559,2686]				5460	
	[2687,4094]	6144				

Now we can prove Theorem 1.1, which states that, for sufficiently large n, $f(n,r)=[n/3{\cdot}2^k]+2^{k+1}-2$ if $1\leqslant r\leqslant 30$ and k is defined by $r\in[2^k-1,2^{k+1}-2]$. The lower bound for $f(n,r)$ is given by (1.2). The same bound estimates $f(n,r)$ from above. Indeed, by Proposition 3.1, $q(r)=3\cdot 2^k$ if r as above. Then, by Theorem 1.3, $f(n,r)=[n/3{\cdot}2^k]+C$, where $r\leqslant C<q(r)$. In Proposition 3.1 we checked that, for r satisfying $1\leqslant r\leqslant 30$, $r\in[2^k-1,2^{k+1}-2]$, and $q=3\cdot 2^k$, each r-multiset A_q has a power of 2 in A_q^*. This implies that $C=2^{k+1}-2$, which proves Theorem 1.1. In a similar way, we obtain Theorem 1.2.

4. Structure of locally optimal Sets

As in Section 1, consider again the set $A=\{3,6,\ldots,3\cdot[n/3]\}$, where n is sufficiently large. Its cardinality is maximum among the sets with no power of 2 as a subset sum. By adding a single element, A becomes a set having 2^s as a subset sum. We can characterize the optimality of a set A not by maximality of its size but by maximality of A with respect to a certain property. Let us call a set $A\subset\{1,\dots,n\}$ a locally optimal set if $2^s\notin A^*$ for $s\geqslant 0$, but if we enlarge A even by a single integer from the range $[1,n]$ then there will be a subset sum of the form 2^s. By inspection, the following are locally optimal sets for sufficiently large n: $B=\{5t\,|\,5t\leqslant n\}$, $C=\{11t\,|\,11t\leqslant n\}$, $D=\{6t\,|\,6t\leqslant n\}\cup\{a_1,a_2\}$, where $a_1\equiv 1 \pmod 6$, $a_2\equiv -1 \pmod 6$, etc.

Similarly, we call a multiset A_q of nonzero residues modulo q locally optimal if $2^s \pmod q \notin A_q^*$ for $s\geqslant 0$, but if we enlarge A_q by any residue $x\not\equiv 0 \pmod q$ then we obtain $2^s \pmod q$ as a subset sum for some $s\geqslant 0$. If q is a prime such that 2 is a primitive root modulo q, then locally optimal multisets of residues modulo q are necessarily empty. For an arbitrary q, the number of elements in a locally optimal multiset is bounded by $(q-1)^2$, as shown by the following proposition.

Proposition 4.1. *Let A_q be a locally optimal multiset of residues modulo q. Then $|A_q|\leqslant(q-1)^2$.*

Proof. Denote by $k(x)$ the multiplicity of a residue x in A_q. We will show that $k(x)\leqslant q-1$, which implies the assertion. Suppose that $k(x)=v$, that is, $x_i\equiv x \pmod q$ for $i=1,\dots,v$. Enlarge A_q by one more element $x_0\equiv x \pmod q$; then there will be a subset sum of the form $2^s \pmod q$. So, there exist $s\geqslant 0$ and $a_1,\dots,a_l\not\equiv x \pmod q$ such that $a_1+\cdots+a_l+x_1+\cdots+x_u+x_0\equiv 2^s \pmod q$. Clearly, $u=v$; otherwise, we replace x_0 by x_{u+1} in the last congruence and obtain a contadiction to the definition of A_q. Thus, $a_1+\cdots+a_l+x_1+\cdots+x_v+x_0\equiv 2^s \pmod q$. Suppose $v\geqslant q$. Note that $x_1+\cdots+x_q\equiv xq\equiv 0 \pmod q$; therefore, $a_1+\cdots+a_l+x_{q+1}+\cdots+x_v+x_1\equiv 2^s \pmod q$, which contradicts that A_q is locally optimal. Thus, $v<q$. The proof is complete. □

Now we will show that a locally optimal subset of $\{1,\dots,n\}$ has the following structure: it is the union of the arithmetic progression of multiples of q for some $q\neq 2^s$, and a small number, at most $(q-1)^2$, of other integers.

Proposition 4.2. *Suppose $\varepsilon>0$, $n>n(\varepsilon)$, and let $A\subset\{1,\dots,n\}$ be a set of distinct integers, with $|A|>n^{2/3+\varepsilon}$. A is a locally optimal set iff there exists an integer $q\neq 2^s$ such that $A=B(q)\cup C$, where $B(q)=\{q,2q,\dots,q\cdot[n/q]\}$, $|C|\leqslant(q-1)^2$ and, corresponding to C, the multiset C_q of nonzsero residues modulo q is locally optimal.*

Proof. (1) Let A be a locally optimal set. Clearly, $a_i\neq 2^s$ for all $a_i\in A$, $s\geqslant 0$. By Lemma 2.1, there exists an integer $q\geqslant 1$ and $B\subseteq A$ such that all the elements of B are divisible by q and B^* contains all multiplies of q in the range defined by (2.1). We use the notation $C=A\backslash B$. The subset B consists of all multiples of q in the range $[1,n]$. Indeed, suppose that $qk\notin B$ for some $1\leqslant k\leqslant[n/q]$. By the definition of locally optimal set, $2^s \notin A^*$ for $s \geqslant 0$. Let us enlarge A by the element qk. Since $qk \equiv 0 \pmod q$, we still do not have a power of 2 as a subset sum, which contradicts the definition of A. Thus,

$$B = B(q) = \left\{q, 2q, \ldots, q \cdot \left[\frac{n}{q}\right]\right\} \tag{4.1}$$

Clearly, $q \neq 2^s$, $s \geqslant 0$. For a subset C of nonmultiples of q in A, the corresponding multiset C_q is locally optimal since A is locally optimal. By Proposition 4.1, $|C| \leqslant (q-1)^2$.

(2) Suppose that $A = B(q) \cup C$, where $B(q)$ is defined by (4.1) and, corresponding to C, the multiset C_q of residues modulo q is locally optimal. $2^s \notin A^*$ for $s \geqslant 0$; otherwise, $2^s \pmod q \in C_q^*$. If we enlarge A by any integer $x \in [1, n]$, $x \not\equiv 0 \pmod q$, then $(A \cup x)^*$ will contain a power of 2 because multiset $C_q \cup x \pmod q$ has a power of 2 modulo q as a subset sum. Thus, A is locally optimal. The proof is complete. □

The assertion above implies, in particular, that, for sufficiently large n, the only subset of $[1, n]$ having no power of 2 as a subset sum and the cardinality $[n/3]$ is Erdős' set $\{3, 6, \ldots, 3 \cdot [n/3]\}$. Indeed, as we mentioned in the beginning of Section 1, the maximum cardinality of A having no power of 2 in A^* is $[n/3]$. A set A of maximum cardinality is locally optimal; therefore, A is a union of an arithmetic progression of multiples of q and a small set C. Clearly, $q = 3$ and C is empty, as needed.

In this section we studied the structure of sets of integers A by a certain given property of a set of subset sums A^*. This is a kind of Inverse Additive Problem which was introduced by Freiman [5, 6].

References

[1] N. Alon and G. Frieman, On sums of subsets of a set of integers, Combinatorica 8 (1988) 297–306.

[2] M. Chaimovich, An efficient algorithm for subset sum problem, Math. Programming, submitted.

[3] P. Erdős, Some problems and results on combinatorial number theory, First China Conference in Combinatorics, 1986.

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

[5] G. Freiman, Foundations of a Structural Theory of Set Addition (Amer. Math. Soc, Providence, RI, 1973).

[6] G. Freiman, What is the structure of K if $K+K$ is small?, Lecture Notes in Math., Vol. 1240 (Springer, Berlin, 1984) 109–134.

[7] O. Margalit, Computer program "Sets without 2^s as subset sum".