ISRAEL JOURNAL OF MATHEMATICS **90** (1995), 221–233

ON SUM SETS OF SIDON SETS, II

BY

P. ERDŐS, A. SÁRKÖZY* AND V.T. SÓS*

Mathematical Institute of the Hungarian Academy of Sciences
Budapest, P.O.B. 127, H-1364, Hungary

ABSTRACT

It is proved that there is no Sidon set selected from $\{1, 2, \dots, N\}$ whose sum set contains $c_1 N^{1/2}$ consecutive integers, but it may contain $c_2 N^{1/3}$ consecutive integers. Moreover, it is shown that a finite Sidon set cannot be well-covered by generalized arithmetic progressions.

1. The set of the real numbers, integers, resp. positive integers will be denoted by $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{N}$. $\mathcal{A}, \mathcal{B}, \dots$ will denote (finite or infinite) subsets of $\mathbb{N}$, and their counting functions will be denoted by $A(N), B(N), \dots$ so that, e.g.,

$$A(n) = |\{a\colon a \le n,\ a \in \mathcal{A}\}|.$$

For $g \in \mathbb{N}$, $B_2[g]$ denotes the class of all (finite or infinite) sets $\mathcal{A} \subset \mathbb{N}$ such that for every integer n, the equation

$$a + a' = n, \quad a \le a', \quad a, a' \in \mathcal{A} \tag{1.1}$$

has at most g solutions. The sets $\mathcal{A} \subset \mathbb{N}$ with $\mathcal{A} \in B_2[1]$ are called Sidon sets, i.e., $\mathcal{A}$ is a Sidon set if the sums $a + a'$ with $a \le a'$, $a, a' \in \mathcal{A}$ are distinct. An excellent account of the theory of Sidon sets and $B_2[g]$ sets is given in [4] (see [1] for a more recent result). For $\mathcal{A} \subset \mathbb{N}$ we write $\mathcal{S}_{\mathcal{A}} = \{s_1, s_2, \dots\} = \mathcal{A} + \mathcal{A}$ (where $\mathcal{A} + \mathcal{A}$ is the set of the integers that can be represented in the form $a + a'$ with $a, a' \in \mathcal{A}$). The counting function of $\mathcal{S}_{\mathcal{A}}$ will be denoted by $\mathcal{S}_{\mathcal{A}}(N)$.

* Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. 1901.
Received August 3, 1993

For $m, \ell_1, \ell_2, \dots, \ell_m \in \mathbb{N}$, $e, f_1, f_2, \dots, f_m \in \mathbb{Z}$ the set

$$\begin{aligned}\mathcal{P} &= \mathcal{P}(e, f_1, f_2, \dots, f_m; \ell_1, \ell_2, \dots, \ell_m) \\ &= \{n: n = e + x_1 f_1 + \dots + x_m f_m, x_i \in \{1, \dots, \ell_i\} \text{ for } i = 1, \dots, m\}\end{aligned}$$

is called a generalized arithmetic progression of dimension m, and the quantity

$$Q(\mathcal{P}) = \ell_1 \ell_2 \cdots \ell_m$$

is called the size of $\mathcal{P}$.

$c_1, c_2, \dots$ will denote positive absolute constants. If $f(n) = O(g(n))$, then we write $f(n) \ll g(n)$.

2. Clearly, for a finite set $\mathcal{A} \subset \mathbb{N}$ we have

$$2|\mathcal{A}| - 1 \leq |\mathcal{S}_{\mathcal{A}}| \leq \binom{|\mathcal{A}|}{2} + |\mathcal{A}| \tag{2.1}$$

where $|\mathcal{S}_{\mathcal{A}}|$ is equal to the upper bound if and only if $\mathcal{A}$ is a Sidon set. Freiman [3] studied the structure of the sum set $\mathcal{S}_{\mathcal{A}}$ under the assumption that

$$|\mathcal{S}_{\mathcal{A}}| < \alpha |\mathcal{A}| \tag{2.2}$$

where α is fixed and $|\mathcal{A}| \to +\infty$. He showed that it follows from this assumption that $\mathcal{A}$ and thus also $\mathcal{S}_{\mathcal{A}}$ must have a nice structure: $\mathcal{A}$ can be well-covered by a generalized arithmetic progression. Indeed, there exist numbers $c_1 = c_1(\alpha)$, $c_2 = c_2(\alpha)$ such that (2.2) implies the existence of a generalized arithmetic progression $\mathcal{P}$ of dimension $m \leq c_1$ with $\mathcal{A} \subset \mathcal{P}$ and $Q(\mathcal{P}) \leq c_2 |\mathcal{A}|$.

In Part I [2] of this paper we studied the other extreme case when $|\mathcal{S}_{\mathcal{A}}|$ is close to the upper bound in (2.1), i.e., $\mathcal{A}$ is a Sidon set or "nearly" Sidon set. In particular, we estimated the number of integers n with $n - 1 \notin \mathcal{S}_{\mathcal{A}}$, $n \in \mathcal{S}_{\mathcal{A}}$; moreover, we studied the size of the gaps between the consecutive elements of $\mathcal{S}_{\mathcal{A}}$ (both for Sidon sets $\mathcal{A}$).

In this paper, first we will continue the study of the structure of sum sets of Sidon sets by estimating the length of blocks of consecutive integers in $\mathcal{S}_{\mathcal{A}}$. In the second half of the paper we will show that a Sidon set has an "antistructure" in the Freiman sense (our results in Part I point to the same direction), namely, it cannot be well-covered by generalized arithmetic progressions.

3. If $\mathcal{A}$ is a (finite or infinite) Sidon set and $N \in \mathbb{N}$, then let $h(\mathcal{A}, N)$ denote the greatest integer h such that there is an integer m with $m \leq N$ and $m+1 \in \mathcal{S}_{\mathcal{A}}$, $m+2 \in \mathcal{S}_{\mathcal{A}}, \dots, m+h \in \mathcal{S}_{\mathcal{A}}$. Moreover, for $n \in \mathbb{N}$ write

$$H(N) = \max h(\mathcal{A}, N)$$

where the maximum is taken over all Sidon sets $\mathcal{A}$ with $\mathcal{A} \subset \{1, 2, \dots, N\}$. We will show that

$$N^{1/3} \ll H(N) \ll N^{1/2}. \tag{3.1}$$

(We remark that the upper bound seems to be closer to the truth; unfortunately, we have not been able to improve on the lower bound.)

First we will prove the upper bound in (3.1) in the following much sharper form:

THEOREM 1: *Assume that $N \in \mathbb{N}$, $L \in \mathbb{N}$, and $\mathcal{A} \subset \{1, 2, \dots, N\}$ is a Sidon set. Then for all $K \in \mathbb{Z}$ we have*

$$\mathcal{S}_{\mathcal{A}}(K+L) - \mathcal{S}_{\mathcal{A}}(K) < \frac{1}{2}L + 7L^{1/2}N^{1/4}. \tag{3.2}$$

Applying Theorem 1 with $L = [200N^{1/2}]$, we obtain

COROLLARY 1: *For $N > N_0$ we have*

$$H(N) < 200N^{1/2}.$$

Proof of Theorem 1: We need the following fact: if $\mathcal{A}$ is a Sidon set, then we have

$$A(X+Y) - A(X) \leq 2Y^{1/2} \quad \text{for all } X \in \mathbb{R},\ \mathbb{Y} \in \mathbb{N}. \tag{3.3}$$

Indeed, if $\mathcal{A} \cap (X, X+Y] = \{a_1, a_2, \dots, a_t\}$, then the $\binom{t}{2} + t$ sums $a_i + a_j$ with $1 \leq i \leq j \leq t$ are distinct, and all these sums belong to the interval $(2X, 2X+2Y]$ of length $2Y$ which implies (3.3).

(3.2) is trivial for $L \leq N^{1/2}$, thus we may assume that

$$L > N^{1/2}. \tag{3.4}$$

Let $U = [L^{1/2}N^{1/4}] + 1$, and write $I_m = [m-U+1, m]$ and

$$|\mathcal{A} \cap I_m| = |\{a\colon a \in \mathcal{A}, m-U < a \leq m\}| = x_m$$

for $m = 1, 2, \dots, N+U-1$. Here we count every $a \in \mathcal{A}$ for exactly U values of m, thus in view of (3.3) we have

$$\sum_{m=1}^{N+U-1} x_m = U|\mathcal{A}| \le 2UN^{1/2}. \tag{3.5}$$

We will count the number T of the triples (a, a', m) with

$$a, a' \in \mathcal{A} \cap I_m, \quad a < a'. \tag{3.6}$$

If we fix m, then a pair a, a' satisfying (3.6) can be selected in $\binom{x_m}{2}$ ways. Thus by (3.5) we have

$$T = \sum_{m=1}^{N+U-1} \binom{x_m}{2} \ge \frac{1}{2} \sum_{m=1}^{N+U} x_m^2 - UN^{1/2}. \tag{3.7}$$

On the other hand, if we fix a pair (a, a') with $0 < a' - a < U$ in (3.6), then clearly, m in (3.6) may assume the $U - (a' - a)$ values $m = a', a'+1, \dots, a' + (U - (a' - a) - 1)$. Thus we have

$$T = \sum_{\substack{a, a' \in \mathcal{A} \\ 0 < a' - a < U}} (U - (a' - a)).$$

Since $\mathcal{A}$ is a Sidon set, thus

$$a' - a = i, \quad a, a' \in \mathcal{A}$$

has at most one solution for all i. Thus we have

$$T \le \sum_{i=1}^{U-1} (U - i) = \frac{(U-1)U}{2} \le \frac{U^2}{2}. \tag{3.8}$$

By (3.7) and (3.8) we have

$$\sum_{m=1}^{N+U-1} x_m^2 \le U^2 + 2UN^{1/2}. \tag{3.9}$$

It follows that there is an integer t with $-U < t \le 0$ and

$$\sum_{\substack{m \equiv t \pmod{U} \\ 1 \le m < N+U}} x_m^2 \le U + 2N^{1/2}. \tag{3.10}$$

For $i = 1, 2, \dots, [(N - t + U - 1)/U]$, write

$$\mathcal{A}_i = \mathcal{A} \cap I_{t+iU}$$

and

$$y_i = |\mathcal{A}_i| = x_{t+iU}$$

so that by (3.10) we have

$$\sum_{i=1}^{[(N-t+U-1)/U]} y_i^2 \le U + 2N^{1/2}. \tag{3.11}$$

Let M denote the set of the pairs (a, a') with

$$a, a' \in \mathcal{A}, \quad K < a + a' \le K + L. \tag{3.12}$$

Clearly, for each of these pairs a, a' there is a unique pair i, j with

$$a \in \mathcal{A}_i, \quad a' \in \mathcal{A}_j \tag{3.13}$$

and

$$(\mathcal{A}_i + \mathcal{A}_j) \cap \{K + 1, K + 2, \dots, K + L\} \ne \emptyset. \tag{3.14}$$

For fixed i, j, the number of pairs a, a' satisfying (3.13) is $y_i y_j$, thus the total number of the pairs $(a, a') \in M$ is

$$|M| \le \sum_i \sum_j y_i y_j \le \frac{1}{2} \sum_i \sum_j (y_i^2 + y_j^2) \tag{3.15}$$

where i, j run over all pairs satisfying (3.14). Clearly, for fixed i, (3.14) may hold for at most $[L/U] + 2$ (consecutive) values of j, and similarly, for fixed j, i may assume as most $[L/U] + 2$ distinct values. Thus in view of (3.4) and (3.11), we obtain from (3.15) that

$$|M| \le \frac{1}{2} \cdot 2([L/U] + 2) \sum_{i=1}^{[(N-t+U-1)/U]} y_i^2 \le \Big(\frac{L}{U} + 2\Big)(U + 2N^{1/2})$$

$$= L + (2U + 4N^{1/2}) + 2\frac{LN^{1/2}}{U} < L + 10L^{1/2}N^{1/4}. \tag{3.16}$$

If $s \in \mathcal{S}_{\mathcal{A}} \cap (K, K+L]$, then either s has two representations in the form $s = a + a'$ with integers a, a' satisfying (3.12) and $a \neq a'$, or s is of the form $s = 2a$ with $a \in \mathcal{A} \cap (K/2, (K+L)/2]$ and then (3.12) holds with $a' = a$. Thus in view of (3.3) and (3.16), we have

$$\mathcal{S}_{\mathcal{A}}(K+L) - \mathcal{S}_{\mathcal{A}}(K) \leq \frac{1}{2}(|M| + (A((K+L)/2) - A(K/2)))$$
$$\leq \frac{1}{2}\left(L + 10L^{1/2}N^{1/4} + 2([L/2]+1)^{1/2}\right) < \frac{1}{2}L + 7L^{1/2}N^{1/4}$$

which completes the proof of Theorem 1. ∎

4. In this section, we will show that

$$H(N) \gg N^{1/3}.$$

Indeed, we will prove this in the following sharper form:

THEOREM 2: *There is an infinite Sidon set $\mathcal{A}$ such that for $n > n_0$ we have*

$$h(\mathcal{A}, n) > \frac{1}{50} n^{1/3}. \tag{4.1}$$

Of course, this implies

$$H(N) > \frac{1}{50} N^{1/3} \quad \textit{for } N > N_0.$$

Proof of Theorem 2: We will define an infinite sequence of sets $\mathcal{B}_0, \mathcal{B}_1, \dots$ with the following properties: writing $\mathcal{A}_k = \bigcup_{j=0}^{k-1} \mathcal{B}_j$ for $k = 1, 2, \dots$, we have

$$\mathcal{A}_k \subset \{1, 2, \dots, 8^k\},$$
$$|\mathcal{A}_k| \leq 2^{k-1},$$
$$\mathcal{A}_k \quad \text{is a Sidon set,}$$

and, for $k \geq 5$,

$$6 \cdot 8^{k-1} + i \in \mathcal{S}_{\mathcal{A}_k} = \mathcal{A}_k + \mathcal{A}_k \quad \text{for} \quad 1 \leq i \leq \frac{1}{3} \cdot 2^{k-3}. \tag{4.2}$$

Indeed, let $\mathcal{B}_k = \{8^k + 1\}$ for $k = 0, 1, 2, 3$. If $\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_{k-1}$ (and thus also $\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_k$) have been defined, then we define the set $\mathcal{B}_k = \{b_1, b_2, \dots, b_u\}$ so that

$$\mathcal{B}_k \subset \{8^k + 1, 8^k + 2, \dots, 8^{k+1}\},$$
$$|\mathcal{B}_k| = 2u \leq \frac{1}{3} \cdot 2^{k-1},$$
$$\mathcal{A}_k \cup \mathcal{B}_k \quad \text{is a Sidon set}$$

and

$$6 \cdot 8^k + i \in (\mathcal{A}_k \cup \mathcal{B}_k) + (\mathcal{A}_k \cup \mathcal{B}_k) \quad \text{for} \quad 1 \le i \le \frac{1}{3} \cdot 2^{k-2}.$$

The elements $b_1, b_2, \ldots, b_u$ of $\mathcal{B}_k$ are defined recursively by using the greedy algorithm. In each step we define two further b's. Assume that

$$0 \le j \le \frac{1}{3} \cdot 2^{k-2} - 1 \tag{4.3}$$

(the case $j = 0$, i.e., the construction of b_1, b_2 is included), and $b_1, \ldots, b_{2j}$ have been defined so that

$$\begin{gathered} \{b_1, \ldots, b_{2j}\} \subset \{8^k + 1, \ldots, 8^{k+1}\}, \\ \mathcal{A}_k \cup \{b_1, \ldots, b_{2j}\} \quad \text{is a Sidon set} \end{gathered} \tag{4.4}$$

and

$$6 \cdot 8^k + i \in (\mathcal{A}_k \cup \{b_1, \ldots, b_{2j}\}) \cup (\mathcal{A}_k \cup \{b_1, \ldots, b_{2j}\}) \quad \text{for } i = 1, \ldots, j. \tag{4.5}$$

If (4.5) holds for all $1 \le i \le \frac{1}{3} \cdot 2^{k-2}$, then the construction terminates, i.e., we take $\mathcal{B}_k = \{b_1, \ldots, b_{2j}\}$. If there is an i such that $1 \le i \le \frac{1}{3} \cdot 2^{k-2}$ and (4.5) does not hold, then we consider the smallest i, say i_0, with these properties. Then it suffices to show that there is an

$$x \in \{1, 2, \ldots, 8^k\} \tag{4.6}$$

such that writing

$$b_{2j+1} = 3 \cdot 8^k - x, \quad b_{2j+2} = 3 \cdot 8^k + i_0 + x, \tag{4.7}$$

these numbers can be added to the set $\{b_1, \ldots, b_{2j}\}$, i.e.,

$$(\mathcal{A}_k \cup \{b_1, \ldots, b_{2j}\}) \cup \{b_{2j+1}, b_{2j+2}\} \quad \text{is a Sidon set.} \tag{4.8}$$

((4.4) and (4.5), both with $j + 1$ in place of j, follow trivially from (4.7) and (4.8).) Write $\mathcal{D}_j = \mathcal{A}_k \cup \{b_1, \ldots, b_{2j}\}$ so that, by (4.3), we have

$$|\mathcal{D}_j| \le |\mathcal{A}_k| + 2j \le 2^{k-1} + \frac{1}{3} \cdot 2^{k-1} - 2 < \frac{1}{3} \cdot 2^{k+1}. \tag{4.9}$$

If an x satisfying (4.6) is "bad", i.e., (4.8) does not hold for this x, then there are $d_1, d_2, d_3 \in \mathcal{D}_j$ such that

$$d_1 + d_2 = d_3 + b_{2j+1}, \quad d_1 + d_2 = d_3 + b_{2j+2} \quad \text{or} \quad d_1 + b_{2j+1} = d_2 + b_{2j+2}$$

holds ($d_1 + d_2 = b_{2j+1} + b_{2j+2}$ is impossible by the definition of i_0). Each of these equations eliminates at most $|\mathcal{D}_j|^3$ "bad" x values, thus by (4.9), the total number of the "bad" x values is

$$\leq 3 \cdot \left(\frac{1}{3} \cdot 2^{k+1}\right)^3 < 8^k.$$

Thus there is at least one "good" x satisfying (4.6) which completes the definition of $\mathcal{B}_k$.

Finally, clearly $\mathcal{A} = \bigcup_{k=1}^{+\infty} \mathcal{A}_k$ is a set of the desired properties ((4.1) follows from (4.2)) and this completes the proof of Theorem 2. ∎

5. In order to study coverings of sum sets of ("nearly") Sidon sets by generalized arithmetic progressions, first we have to introduce a measure of well-covering of this type. Such a measure was introduced by Erdős about 30 years ago in the one-dimensional special case. For a finite set $\mathcal{A} \subset \mathbb{N}$ and for $m \in \mathbb{N}$, consider the coverings

$$\mathcal{A} \subset \bigcup_{i=1}^{T} \mathcal{P}_i, \quad \dim \mathcal{P}_i = m \quad (\text{for } i = 1, 2, \dots, m) \tag{5.1}$$

of $\mathcal{A}$ by generalized arithmetic progressions of dimension m, and write

$$D_m(\mathcal{A}) = \min T \sum_{i=1}^{T} Q(P_i)$$

where the minimum is taken over all coverings of the form (5.1) of $\mathcal{A}$. Clearly, for every finite $\mathcal{A} \subset \mathbb{N}$ and all $m \in \mathbb{N}$ we have

$$|\mathcal{A}| \ll D_m(\mathcal{A}) \ll |\mathcal{A}|^2.$$

For $n \in \mathbb{N}$, denote the set of the squares x^2 with $x^2 \leq n$ by $\mathcal{M}_n$. Erdős conjectured that for $\varepsilon > 0$, $n > n_0(\varepsilon)$ we have

$$D_1(\mathcal{M}_n) > n^{1-\varepsilon}. \tag{5.2}$$

Sárközy [7] proved this by showing that

$$D_1(\mathcal{M}_n) \gg \frac{n}{(\log n)^2}. \tag{5.3}$$

(Note that probably we have $D_1(\mathcal{M}_n) \gg n$, however, (5.3) has not been improved yet.)

Using the measure $D_m(\mathcal{A})$ of well-covering, a consequence of Freiman's result cited in Section 2 can be formulated in the following way: for $\alpha > 0$ there exist $c_3 = c_3(\alpha)$, $c_4 = c_4(\alpha)$ such that assuming (2.2), for some $m < c_3$ we have

$$D_m(\mathcal{A}) < c_4|\mathcal{A}|.$$

Here our goal is to show that in the other extreme case when $\mathcal{A}$ is a Sidon set or, more generally, $B_2[g]$ set, then $\mathcal{A}$ cannot be well-covered by generalized arithmetic progressions:

THEOREM 3: *If $\mathcal{A} \subset \mathbb{N}$, $\mathcal{A}$ is finite, $g \in \mathbb{N}$, $m \in \mathbb{N}$ and*

$$\mathcal{A} \subset B_2[g], \tag{5.4}$$

then we have

$$D_m(\mathcal{A}) > \frac{1}{2^{m+1}g}|\mathcal{A}|^2. \tag{5.5}$$

Putting $g = 1$ here, we obtain

COROLLARY 1: *If $\mathcal{A}$ is a finite Sidon set, then*

$$D_m(\mathcal{A}) > \frac{1}{2^{m+1}}|\mathcal{A}|^2.$$

Moreover, for $\varepsilon > 0$, $n > n_0(\varepsilon)$, $1 \le u \le n$ the number of solutions of

$$x^2 + y^2 = u, \quad x, y \in \mathbb{N}$$

is

$$\le d(u) \le \exp\Big((1+\varepsilon)\log 2 \frac{\log n}{\log\log n}\Big).$$

Thus it follows from Theorem 3 that for $n > n_0(\varepsilon)$ we have

$$D_m(\mathcal{M}_n) > 2^{-m} n \exp\Big(-(1+\varepsilon)\log 2 \frac{\log n}{\log\log n}\Big)$$

which, for $m = 1$, proves (5.2) but it is weaker than (5.3).

Proof of Theorem 3: Assume that

$$\mathcal{A} \subset \bigcup_{i=1}^{T} \mathcal{P}_i \tag{5.6}$$

where $\mathcal{P}_i = \mathcal{P}(e^{(i)}, f_1^{(i)}, \dots, f_m^{(i)}; \ell_1^{(i)}, \dots, \ell_m^{(i)})$ and write

$$\mathcal{A}_i = \mathcal{A} \cap \mathcal{P}_i \quad (\text{for } i = 1, 2, \dots, T).$$

Consider all the pairs (a, a') with $a, a' \in \mathcal{A}_i$, $a \le a'$. The number of these pairs is

$$\binom{|\mathcal{A}_i|}{2} + |\mathcal{A}_i| > \frac{|\mathcal{A}_i|^2}{2},$$

and for each of these pairs (a, a') we have

$$a + a' \in \mathcal{P}_i + \mathcal{P}_i =$$
$$\mathcal{P}\left(2e^{(i)} + f_1^{(i)} + \dots + f_m^{(i)}, f_1^{(i)}, \dots, f_m^{(i)}; 2\ell_1^{(i)} - 1, \dots, 2\ell_m^{(i)} - 1\right).$$

Thus denoting the number of solutions of (1.1) by $r(n)$, we have

$$\sum_{n \in \mathcal{P}_i + \mathcal{P}_i} r(n) \ge |\{(a, a') \colon a, a' \in \mathcal{A}_i, a \le a'\}| > \frac{|\mathcal{A}_i|^2}{2}. \tag{5.7}$$

On the other hand, it follows from (5.4) that

$$\sum_{n \in \mathcal{P}_i + \mathcal{P}_i} r(n) \le \sum_{n \in \mathcal{P}_i + \mathcal{P}_i} g \le gQ(\mathcal{P}_i + \mathcal{P}_i)$$
$$= g \prod_{j=1}^{m} (2\ell_j^{(i)} - 1) < g \prod_{j=1}^{m} 2\ell_j^{(i)} = 2^m g Q(\mathcal{P}_i). \tag{5.8}$$

By (5.7) and (5.8) we have

$$\sum_{i=1}^{T} |\mathcal{A}_i|^2 < 2^{m+1} g \sum_{i=1}^{T} Q(\mathcal{P}_i). \tag{5.9}$$

By Cauchy's inequality and (5.6), we have

$$\sum_{i=1}^{T} |\mathcal{A}_i|^2 \ge \frac{1}{T} \Big(\sum_{i=1}^{T} |\mathcal{A}_i| \Big)^2 \ge \frac{|\mathcal{A}|^2}{T}. \tag{5.10}$$

It follows from (5.9) and (5.10) that

$$T\sum_{i=1}^{T} Q(\mathcal{P}_i) > 2^{-m-1}g^{-1}|\mathcal{A}|^2$$

which proves (5.5). ∎

6. In this section we will show that Theorem 3 is nearly sharp:

THEOREM 4: *For all $g, m, q \in \mathbb{N}$ there exist finite sets $\mathcal{A} \subset \mathbb{N}$ such that*

$$|\mathcal{A}| = 2gq, \tag{6.1}$$

$$\mathcal{A} \subset B_2[g] \tag{6.2}$$

and

$$D_m(\mathcal{A}) \le \frac{1}{2g}|\mathcal{A}|^2. \tag{6.3}$$

Proof: Let $\mathcal{E} = \{e_1, e_2, \dots, e_q\}$ be a Sidon set with $|\mathcal{E}| = q$ and

$$|e_i + e_j - e_u - e_v| > (4g)^{q+2} \quad \text{for all } i < u \le v < j. \tag{6.4}$$

(Such a Sidon set $\mathcal{E}$ can be obtained by taking a Sidon set of cardinality q, and then multiplying each element of it by $2 \cdot (4g)^{q+2}$.) Then for $i = 1, 2, \dots, q$, let $\mathcal{P}_i$ denote the m-dimensional generalized arithmetic progression

$$\mathcal{P}_i = \mathcal{P}(e_i - (4g)^i - (m-1), (4g)^i, 1, \dots, 1; 2g, 1, \dots, 1)$$

so that

$$\mathcal{P}_i = \{e_i, e_i + (4g)^i, e_i + 2(4g)^i, \dots, e_i + (2g-1)(4g)^i\},$$

and let

$$\mathcal{A} = \bigcup_{i=1}^{q} \mathcal{P}_i. \tag{6.5}$$

Then (6.1) holds trivially. Moreover, the union on the right hand side of (6.5) is a covering of $\mathcal{A}$ of the form (5.1) by m-dimensional arithmetic progressions, thus by (6.1) we have

$$D_m(\mathcal{A}) \le q\sum_{i=1}^{q} Q(\mathcal{P}_i) = q|\mathcal{A}| = \frac{1}{2g}|\mathcal{A}|^2$$

which proves (6.3).

It remains to show that (6.2) also holds. Assume that

$$a_1 + a_2 = a_3 + a_4 \tag{6.6}$$

and $a_1, a_2, a_3, a_4 \in \mathcal{A}$ so that

$$a_1 \in \mathcal{P}_w, \quad a_2 \in \mathcal{P}_x, \quad a_3 \in \mathcal{P}_y, \quad a_4 \in \mathcal{P}_z, \quad w \le x, \quad y \le z \tag{6.7}$$

can be assumed. Then it follows from (6.6) and the construction of $\mathcal{A}$ that

$$|e_w + e_x - e_y - e_z| \le 4(2g-1)(4g)^q < (4g)^{q+2}.$$

By (6.4) and (6.7), this implies that

$$w = y, \quad x = z. \tag{6.8}$$

Since the representation of a positive integer in the number system of base $4g$ is unique, thus by (6.6), (6.7) and (6.8), it follows from the construction that if $a_1 \ne a_3$, $a_1 \ne a_4$ in (6.6), then we have $w = y = z = x$. Thus denoting the number of solutions of (1.1) again by $r(n)$, $r(n) > 1$ implies that n is of the form

$$(e_x + u \cdot (4g)^x) + (e_x + v \cdot (4g)^x) = n, \quad 0 \le u \le v \le 2g-1, \tag{6.9}$$

and $r(n)$ is equal to the number of pairs (u, v) satisfying (6.9). Clearly, the number of these pairs is $\le g$ which proves (6.2). ∎

7. There is a gap between the lower and upper bounds given in Theorems 3 and 4 which becomes greater as the dimension m increases. In order to tighten this gap, one would need a possibly sharp estimate for the cardinality of a maximal $B_2[g]$ set selected from a given generalized arithmetic progression of dimension m. The first difficulty is here that much less is known on $B_2[g]$ sets, than on Sidon sets. There is an even more serious difficulty: even in the special case $g = 1$, i.e., in case of Sidon sets, only very weak estimates are known for $m \to +\infty$ (cf. [5,6]). Correspondingly, the following question cannot be answered at present: Is it true that for all $\varepsilon > 0$ there is a $Q_0 = Q_0(\varepsilon)$ such that if $\mathcal{P}$ is a generalized arithmetic progression with $Q(\mathcal{P}) > Q_0$, and $\mathcal{A}$ is a Sidon set with $\mathcal{A} \subset \mathcal{P}$, then $|\mathcal{A}| < (Q(\mathcal{P}))^{(1/2)+\varepsilon}$?

Moreover, we remark that although in the most important special case $g = m = 1$ our estimates are quite satisfactory, even in this special case there are problems that we have not been able to settle. In particular, we could not answer the following question: Is it true that if $\mathcal{A} \subset \{1, 2, \dots, N\}$ is a Sidon set with $|\mathcal{A}| \gg N^{1/2}$, then $\mathcal{A}$ cannot be covered by $\ll N^{1/4}$ (one dimensional) arithmetic progressions of length $[N^{1/2}]$?

We would like to thank the referee of this paper for the remark that this is not true for $B_2[2]$ sets instead of Sidon sets. Indeed, let $\mathcal{B} = \{b_1, b_2, \dots, b_t\}$ be a maximal Sidon set selected from $\{1, 2, \dots [\frac{1}{2}N^{1/2}] - 1\}$ so that $t \gg N^{1/4}$ and let $\mathcal{A}$ denote the set of the integers of the form $b_i + b_j[N^{1/2}]$, $1 \le i, j \le t$. Then clearly, $\mathcal{A} \subset \{1, 2, \dots, N\}$, $\mathcal{A} \gg N^{1/2}$, $\mathcal{A}$ is a $B_2[2]$ set and $\mathcal{A}$ can be covered by the $t = O(N^{1/4})$ arithmetic progressions $\{b_i + [N^{1/2}], b_i + 2[N^{1/2}], \dots, b_i + [N^{1/2}]^2\}$, $i = 1, 2, \dots, t$ of length $[N^{1/2}]$.

References

[1] P. Erdős and R. Freud, *On sums of a Sidon-sequence*, Journal of Number Theory **38** (1991), 196–205.

[2] P. Erdős, A. Sárközy and V. T. Sós, *On sum sets of Sidon sets, I*, Journal of Number Theory **47** (1994), 329–347.

[3] G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Translations of Mathematical Monographs, Vol. 37, American Mathematical Society, Providence, R.I., 1973.

[4] H. Halberstam and K. F. Roth, *Sequences*, Springer-Verlag, Berlin–Heidelberg–New York, 1983.

[5] B. Lindström, *Determination of two vectors from the sum*, Journal of Combinatorial Theory **6** (1969), 402–407.

[6] B. Lindström, *On B_2-sequences of vectors*, Journal of Number Theory **4** (1972), 261–265.

[7] A. Sárközy, *On squares in arithmetic progressions*, Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae **25** (1982), 267–272.