JOURNAL OF NUMBER THEORY 47, 329–347 (1994)

On Sum Sets of Sidon Sets, I

P. ERDŐS, A. SÁRKÖZY,* AND T. SÓS*

Mathematical Institute of the Hungarian Academy of Sciences, H-1053 Budapest, Reáltanoda u. 13-15, Hungary

Communicated by Alan C. Woods

Received March 15, 1993

DEDICATED TO THE MEMORY OF PROFESSOR HANS ZASSENHAUS

A (finite or infinite) set $\mathscr{A}$ of positive integers is said to be a Sidon set if the sums $a+a'$ with $a\in\mathscr{A}$, $a'\in\mathscr{A}$, $a\leqslant a'$ are distinct. Denote the sum set $\mathscr{A}+\mathscr{A}$ of a Sidon set $\mathscr{A}$ by $\mathscr{S}_{\mathscr{A}}=\{s_1, s_2, \ldots\}$. The size of the gaps $s_{i+1}-s_i$, the length of the blocks of consecutive integers in $\mathscr{S}_{\mathscr{A}}$, and the number of solutions of $s\leqslant n$, $s-d\notin\mathscr{A}$, $s\in\mathscr{A}$ are studied. © 1994 Academic Press, Inc.

1

The set of the positive integers will be denoted by $\mathbb{N}$. $\mathscr{A}$, $\mathscr{B}$, ... will denote (finite or infinite) subsets of $\mathbb{N}$, and their counting functions will be denoted by $A(n)$, $B(n)$, ... so that, e.g.,

$$A(n)=|\{a: a\leqslant n, a\in\mathscr{A}\}|.$$

We denote the sum set $\mathscr{A}+\mathscr{A}$ (i.e., the set of the numbers that can be represented in the form $a+a'$ with $a, a'\in\mathscr{A}$) by $\mathscr{S}_{\mathscr{A}}=\{s_1, s_2, \ldots\}$. For $\mathscr{A}\subset\mathbb{N}$, $d\in\mathbb{N}$ we write

$$\mathscr{B}(\mathscr{A}, d)=\{a: a-d\notin\mathscr{A}, a\in\mathscr{A}\}$$

and we denote the counting function of this set by $B(\mathscr{A}, d, n)$. $c_1, c_2, \ldots$ 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 $\mathscr{A}\subset\mathbb{N}$ we have

$$2|\mathscr{A}|-1\leqslant|\mathscr{S}_{\mathscr{A}}|\leqslant\binom{|\mathscr{A}|}{2}+|\mathscr{A}|. \tag{2.1}$$

* Research partially supported by Hungarian National Foundation for Scientific Research, Grant 1901.

0022-314X/94 $6.00

If in (2.1) the upper bound is assumed, i.e., the sums $a+a'$ with $a, a' \in \mathcal{A}$, $a \leqslant a'$ are distinct, then $\mathcal{A}$ is said to be a Sidon set. An excellent account of the theory of Sidon sets is given in [5] (see [2] for a more recent result).

Freiman [4] 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 this assumption implies that $\mathcal{A}$ can be "well-covered" by a generalized arithmetic progression. It follows from his results that assuming (2.2), there is a number $\eta = \eta(\alpha)$ and an integer $d = d(\mathcal{A}) \in \mathbb{N}$ such that for $|\mathcal{A}| \geqslant 2$ we have

$$|\mathcal{B}(\mathcal{S}_{\mathcal{A}}, d)| \leqslant (1-\eta)\,|\mathcal{S}_{\mathcal{A}}|.$$

While Freiman studied the case when $|\mathcal{S}_{\mathcal{A}}|$ is close to the lower bound in (2.1), here our goal is to study the other extreme case when $|\mathcal{S}_{\mathcal{A}}|$ is close to the upper bound, i.e., $\mathcal{A}$ is a Sidon set or "nearly" Sidon set. Indeed, we will show that for Sidon sets $\mathcal{A}$ the structure of $\mathcal{S}_{\mathcal{A}}$ is just the opposite of the one in Freiman's case, i.e., nontrivial lower bound can be given for $|\mathcal{B}(\mathcal{S}_{\mathcal{A}}, d)|$ for all $d \in \mathbb{N}$. Next, we will estimate the size of the gaps between the consecutive elements of the sum set $\mathcal{S}_{\mathcal{A}}$ of a Sidon set $\mathcal{A}$. Finally, in the last section we will discuss several unsolved problems concerning Sidon sets.

In Part II of this series we will estimate the number of elements of sum sets of Sidon sets in short intervals. Moreover, we will show that the sum set of a Sidon set cannot be well-covered by generalized arithmetic progressions.

It follows from (2.1) that for every finite $A \subset \mathbb{N}$ and all $d \in \mathbb{N}$ we have

$$|\mathcal{B}(\mathcal{S}_{\mathcal{A}}, d)| \leqslant |\mathcal{S}_{\mathcal{A}}| \leqslant |\mathcal{A}|^2. \tag{3.1}$$

On the other hand, we can show that for every finite Sidon set $\mathcal{A}$ and all $d \in \mathbb{N}$ we have $|\mathcal{B}(\mathcal{S}_{\mathcal{A}}, d)| \gg |\mathcal{A}|^2$:

THEOREM 1. *There is a positive constant c_1 such that for every finite Sidon set $\mathcal{A}$ and all $d \in \mathbb{N}$ we have*

$$|\mathcal{B}(\mathcal{S}_{\mathcal{A}}, d)| > c_1\,|\mathcal{A}|^2.$$

In particular, choosing $d = 1$ we obtain that if we represent $\mathcal{S}_{\mathcal{A}}$ as the union of $t = |\mathcal{B}(\mathcal{S}_{\mathcal{A}}, d)|$ blocks of consecutive integers:

$$\mathcal{S}_{\mathcal{A}} = \bigcup_{i=1}^{t} \{k_i, k_i+1, \ldots, k_i+l_i\}, \qquad k_i - 1 \notin \mathcal{S}_{\mathcal{A}},$$

then the number t of these blocks is $\gg |\mathcal{A}|^2$.

We can prove an analogous result for infinite Sidon sets:

THEOREM 2. *There is a positive absolute constant c_2 such that for every infinite Sidon set $\mathscr{A}$ and all $d \in \mathbb{N}$ we have*

$$\lim_{N \to +\infty} \sup B(\mathscr{S}_{\mathscr{A}}, d, N)(A(N))^{-2} > c_2. \tag{3.2}$$

Indeed, it will be shown that here $c_2 = 10^{-7}$ can be taken.

Note that if $\mathscr{A} = \{a_1, a_2, ..., a_n, ...\}$ is an infinite set of positive integers, then for all N we have

$$B(\mathscr{S}_{\mathscr{A}}, d, N)(A(N))^{-2} < c_3.$$

Moreover, a simple construction show that the lim sup in (3.2) cannot be replaced by lim inf. Indeed, define $N_1, N_2, ...$ by the following recursion: let $N_1 = 1000$ and $N_{k+1} = N_k^{N_k}$ for $k = 1, 2, ...$ Furthermore, let $\mathscr{A}_1 = \{1\}$ and if $\mathscr{A}_k \subset \{1, 2, ..., N_k\}$ has been defined, then, by using the greedy algorithm, it can be shown that there is a set $\mathscr{B}_k \subset \mathbb{N}$ such that $\mathscr{B}_k \subset [N_{k+1} - [N_{k+1}^{1/2}], N_{k+1}]$, $|\mathscr{B}_k| \gg N_{k+1}^{1/10}$ and $\mathscr{A}_k \cup \mathscr{B}_k$ is a Sidon set. Let $\mathscr{A}_{k+1} = \mathscr{A}_k \cup \mathscr{B}_k$. Then it is easy to see that $\mathscr{A} = \bigcup_{k=1}^{+\infty} \mathscr{A}_k$ is a Sidon set and we have

$$\begin{aligned} B(\mathscr{S}_{\mathscr{A}}, d, N_k) &\leqslant |\mathscr{S}_{\mathscr{A}} \cap [1, N_k]| \leqslant |\mathscr{A}_{k-1}|^2 + |\mathscr{A}_{k-1}|\,|\mathscr{B}_k| \\ &\ll A(N_{k-1}) \log A(N_{k-1}). \end{aligned}$$

Thus Theorem 2 is best possible apart from the value of the constant c_2.

Since Theorems 1 and 2 can be proved similarly but the proof of Theorem 1 is simpler, thus here we will give only the proof of the more difficult Theorem 2.

4

Proof of Theorem 2. We start out from the indirect assumption that for al $\delta > 0$ there is an infinite Sidon set $\mathscr{A}$ such that

$$\lim_{N \to +\infty} \sup B(\mathscr{S}_{\mathscr{A}}, d, N)(A(N))^{-2} < \delta. \tag{4.1}$$

We will show that for sufficiently small δ, (4.1) leads to a contradiction.

First we will show that for an infinite set $\mathscr{A} \in \mathbb{N}$, there exist infinitely many integers N such that

$$\frac{A(N+j)}{A(N)} < \left(\frac{N+j}{N}\right)^2 \qquad \text{for all} \quad j \in \mathbb{N}. \tag{4.2}$$

We will prove this by contradiction. Assume that contrary to this assertion, (4.2) holds only for finitely many integers N. Then there exists an integer N_0 such that

$$A(N_0) \geqslant 1$$

and for all $N \geqslant N_0$ there exists an integer $N' = N'(N)$ satisfying $N' > N$ and

$$\frac{A(N')}{A(N)} \geqslant \left(\frac{N'}{N}\right)^2.$$

Then we get by induction that there exist integers $N_0 < N_1 < N_2 < \cdots < N_j < \cdots$ such that

$$\frac{A(N_{j+1})}{A(N_j)} \geqslant \left(\frac{N_{j+1}}{N_j}\right)^2$$

(in fact, N_{j+1} can be defined by $N_{j+1} = N'(N_j)$). It follows that for all $k \in \mathbb{N}$ we have

$$\frac{A(N_{k+1})}{A(N_0)} = \prod_{j=0}^{k} \frac{A(N_{j+1})}{A(N_j)} \geqslant \prod_{j=0}^{k} \left(\frac{N_{j+1}}{N_j}\right)^2 = \left(\frac{N_{k+1}}{N_0}\right)^2.$$

Thus for large enough k we have

$$A(N_{k+1}) \geqslant A(N_0)\left(\frac{N_{k+1}}{N_0}\right)^2 \geqslant N_0^{-2} N_{k+1}^2 > N_{k+1}^{3/2}$$

which contradicts the trivial inequality

$$A(N_{k+1}) = |\{a: a \leqslant N_{k+1}, a \in \mathscr{A}\}| \leqslant |\{a: a \leqslant N_{k+1}, a \in \mathbb{N}\}| = N_{k+1},$$

and this contradiction proves the existence of infinitely many integers N satisfying (4.2).

5

Throughout the rest of the Proof of Theorem 2, we use the following notations:

δ is a small but fixed positive number, $\mathscr{A}$ is an infinite Sidon set satisfying (4.1), and N is a large integer satisfying (4.2). We write $e^{2\pi i\alpha} = e(\alpha)$, and we put $r = e^{-1/N}$, $z = re(\alpha)$ where α is a real variable (so that a function of form $p(z)$ is a function of the real variable α: $p(z) = p(re(\alpha)) = P(\alpha)$). We write

$$f(z) = \sum_{a \in \mathscr{A}} z^a.$$

(By $r<1$, this infinite series and all the other infinite series in the rest of the proof are absolutely convergent.)

We start out from the integral

$$\mathscr{J}=\int_0^1 |(1-z^d)\,f^2(z)|^2\,d\alpha.$$

We will give lower and upper bounds for $\mathscr{J}$. Comparing these bounds, we will get an inequality contradicting (4.1) for small enough δ, and this will complete the Proof of Theorem 2.

6

In this section, we give a lower bound for $\mathscr{J}$. By $|z|=|re(\alpha)|=r<1$ we have

$$\frac{|1-z^d|}{2}\leqslant 1 \qquad \text{for all} \quad 0\leqslant\alpha\leqslant 1.$$

Thus by the Cauchy–Schwarz inequality we have

$$\begin{aligned}\mathscr{J}&=\int_0^1 |(1-z^d)\,f^2(z)|^2\,d\alpha\geqslant\int_0^1 |(1-z^d)\,f^2(z)|^2\,\frac{|1-z^d|^2}{4}\,d\alpha\\&=\frac{1}{4}\int_0^1 |(1-z^d)\,f(z)|^4\,d\alpha\geqslant\frac{1}{4}\left(\int_0^1 |(1-z^d)\,f(z)|^2\,d\alpha\right)^2. \qquad (6.1)\end{aligned}$$

Write

$$(1-z^d)\,f(z)=\sum_{n=0}^{+\infty} t(n)\,z^n$$

so that $t(n)=1$ for all $n\in\mathscr{B}(\mathscr{A},d)$. By Parseval's formula, it follows that

$$\begin{aligned}\int_0^1 |(1-z^d)\,f(z)|^2\,d\alpha&=\int_0^1\left|\sum_{n=0}^{+\infty} t(n)\,z^n\right|^2 d\alpha=\sum_{n=0}^{+\infty} t^2(n)\,r^{2n}\\&\geqslant\sum_{n=0}^{N} t^2(n)\,r^{2N}\geqslant r^{2N}\sum_{n\leqslant N,\,n\in\mathscr{B}(\mathscr{A},d)} t^2(n)\\&=e^{-2}B(\mathscr{A},d,N). \qquad (6.2)\end{aligned}$$

By our assumption $\mathscr{A}$ is a Sidon set, thus

$$a-a'=d, \qquad a,a'\in\mathscr{A}$$

has at most one solution. This implies that for all large N we have

$$B(\mathscr{A}, d, N) \geqslant A(N) - 1 > \frac{A(N)}{2}. \tag{6.3}$$

It follows from (6.1), (6.2), and (6.3) that for all large N we have

$$\mathscr{J} \geqslant \frac{1}{4}\left(e^{-2}\frac{A(N)}{2}\right)^2 > 10^{-4}A^2(N). \tag{6.4}$$

7

In this section, we will give an upper bound for $\mathscr{J}$. Write

$$f^2(z) = \sum_{n=0}^{+\infty} u(n)\, z^n$$

so that

$$u(n) = \begin{cases} 0 & \text{if and only if } n \notin \mathscr{S}_{\mathscr{A}}, \\ 1 & \text{if and only if } n = 2\alpha \text{ for some } a \in \mathscr{A}, \\ 2 & \text{if and only if } n = a + a' \text{ for some } a \in \mathscr{A},\ a' \in \mathscr{A},\ a < a'. \end{cases} \tag{7.1}$$

Moreover, write

$$(1 - z^d) f^2(z) = \sum_{n=1}^{+\infty} (u(n) - u(n-d))\, z^n = \sum_{n=1}^{+\infty} v(n)\, z^n.$$

Then by Parseval's formula we have

$$\mathscr{J} = \int_0^1 |(1 - z^d) f^2(z)|^2\, d\alpha = \int_0^1 \left| \sum_{n=1}^{+\infty} v(n)\, z^n \right|^2 d\alpha = \sum_{n=1}^{+\infty} v^2(n)\, r^{2n}. \tag{7.2}$$

It follows from (7.1) that

$$|v(n)| = 0,\ 1,\ \text{or } 2 \qquad \text{for all } n; \tag{7.3}$$

if $|v(n)| > 0$, then one of the followings holds:

$$n \in \mathscr{S}_{\mathscr{A}},\ n - d \notin \mathscr{S}_{\mathscr{A}}, \text{ i.e., } n \in \mathscr{B}(\mathscr{S}_{\mathscr{A}}, d); \tag{7.4}$$

$$n \notin \mathscr{S}_{\mathscr{A}}, \qquad n - d \in \mathscr{S}_{\mathscr{A}}; \tag{7.5}$$

$$n - d = 2a \text{ or } n = 2a \qquad \text{for some} \quad a \in \mathscr{A}. \tag{7.6}$$

Let $\mathscr{D}$ and $\mathscr{E}$ denote the set of the positive integers n satisfying (7.5) and (7.6), respectively. Clearly, for all $m \in \mathbb{N}$ we have

$$B(\mathscr{S}_{\mathscr{A}}, d, m) \geqslant D(m) \tag{7.7}$$

and

$$E(m) \leqslant 2A(m). \tag{7.8}$$

Thus writing

$$V(m) = \sum_{n=1}^{m} v^2(n),$$

by formulas (7.3)–(7.8) we have

$$\begin{aligned} V(m) &\leqslant \sum_{n \leqslant m,\, |v(n)|>0} 4 \leqslant 4(B(\mathscr{S}_{\mathscr{A}}, d, m) + D(m) + E(m)) \\ &\leqslant 4(B(\mathscr{S}_{\mathscr{A}}, d, m) + B(\mathscr{S}_{\mathscr{A}}, d, m) + 2A(m)) \\ &= 8(B(\mathscr{S}_{\mathscr{A}}, d, m) + A(m)) \qquad \text{for all} \quad m \in \mathbb{N}. \end{aligned} \tag{7.9}$$

By (4.1), (7.2) and (7.9), if N satisfies (4.2) and $N \to +\infty$, then we have

$$\begin{aligned} \mathscr{J} &= \sum_{n=1}^{+\infty} (V(n) - V(n-1))\, r^{2n} \\ &= \sum_{n=1}^{+\infty} V(n)(r^{2n} - r^{2n+2}) = (1-r^2) \sum_{n=1}^{+\infty} V(n)\, r^{2n} \\ &\leqslant (1+r)(1-r) \sum_{n=1}^{+\infty} 8(B(\mathscr{S}_{\mathscr{A}}, d, n) + A(n))\, r^{2n} \\ &< 2(1-e^{-1/N}) \left(O(1) + 8 \sum_{n=1}^{+\infty} (\delta A^2(n) + A(n))\, r^{2n} \right) \\ &< 2 \cdot \frac{1}{N} \left(O(1) + 9\delta \sum_{n=1}^{+\infty} A^2(n)\, r^{2n} \right) \\ &= O(1) + 18\delta N^{-1} \sum_{n=1}^{+\infty} A^2(n)\, r^{2n} \end{aligned} \tag{7.10}$$

since we have

$$1 - e^{-x} < x \qquad \text{for} \quad 0 < x < 1.$$

(Here the $O(1)$ term may be depend on δ and $\mathscr{A}$, but it is bounded for fixed δ and $\mathscr{A}$ as $N \to +\infty$.)

By (4.2) we have

$$\sum_{n=1}^{+\infty} A^2(n)\, r^{2n} = \sum_{n=1}^{N} A^2(n)\, r^{2n} + \sum_{n=N+1}^{+\infty} A^2(n)\, r^{2n}$$

$$< NA^2(N) + \sum_{n=N+1}^{+\infty} \left(A(N) \left(\frac{n}{N} \right)^2 \right)^2 r^{2n}$$

$$< NA^2(N) + A^2(N)\, N^{-4} \sum_{n=1}^{+\infty} n^4 r^{2n}. \tag{7.11}$$

For $0 < x < 1$ we have

$$(1-x)^{-5} = 1 + \sum_{n=1}^{+\infty} \binom{n+4}{4} x^n > \frac{1}{24} \sum_{n=1}^{+\infty} n^4 x^n.$$

Thus it follows from (7.11) that

$$\sum_{n=1}^{+\infty} A^2(n)\, r^{2n} < NA^2(N) + A^2(N)\, N^{-4} \cdot 24(1-r^2)^{-5}$$

$$= A^2(N)(N + 24N^{-4}(1 - e^{-2/N})^{-5})$$

$$< A^2(N)(N + 24N^{-4} \cdot N^5) = 25NA^2(N) \tag{7.12}$$

since we have

$$1 - e^{-x} > \frac{x}{2} \qquad \text{for} \quad 0 < x < 1.$$

If N is large enough, then it follows from (7.10) and (7.12) that

$$\mathscr{J} < O(1) + 18\delta N^{-1} \cdot 25NA^2(N) < 500\delta A^2(N) \tag{7.13}$$

for every large N satisfying (4.2).

8

In this section, we will complete the proof of Theorem 2. By (6.4) and (7.13) we have

$$10^{-4} A^2(N) < \mathscr{J} < 500\delta A^2(N)$$

(for every large N satisfying (4.2)). It follows that

$$10^{-4} < 500\delta$$

which cannot hold for sufficiently small δ (say, for $\delta = 10^{-7}$). Thus, indeed, the indirect assumption (4.1) leads to a contradiction which completes the proof of the theorem.

9

In Sections 9–11 we will study the following question: how small can one make the difference between the consecutive elements of $\mathscr{S}_{\mathscr{A}}$ for a (finite or infinite) Sidon set? First we will study finite Sidon sets. For $n \in \mathbb{N}$ define $H(n)$ as the smallest positive integer H such that there is a Sidon set $\mathscr{A} \subset \{1, 2, ..., n\}$ with

$$\{i+1, i+2, ..., i+H\} \cap \mathscr{S}_{\mathscr{A}} \neq \varnothing \qquad \text{for} \quad i = 0, 1, ..., n.$$

We will prove

THEOREM 3. *For $n \in \mathbb{N}$, $n > n_0$ we have*

$$H(n) \leqslant 3n^{1/2}.$$

We remark that almost certainly we have

$$H(n) = o(n^{1/2})$$

but unfortunately we have not been able to prove this, and, perhaps, even

$$H(n) = o(n^{\varepsilon})$$

holds (for all $\varepsilon > 0$).

Proof of Theorem 3. We have to show that for $n > n_0$ there is a Sidon set $\mathscr{A} \subset \{1, 2, ..., n\}$ such that

$$\{i+1, i+2, ..., i+[3n^{1/2}]\} \cap \mathscr{S}_{\mathscr{A}} \neq 0 \qquad \text{for} \quad i = 0, 1, ..., n. \tag{9.1}$$

Since the construction will be similar to the one given by Erdős (see [6] and also [5, p. 90]) we shall leave some details to the reader.

Let p denote the smallest prime number with

$$2(p-2)\, p > n$$

so that by the prime number theorem we have

$$p = (1 + o(1))(n/2)^{1/2}. \tag{9.2}$$

Let

$$a_k = 2(k-1)\,p + r(k^2, p) \qquad \text{for} \quad k = 1, 2, ..., p-1$$

where $r(k^2, p)$ denotes the least non-negative residue of k^2 modulo p so that

$$r(k^2, p) \equiv k^2 (\text{mod } p) \qquad \text{and} \qquad 0 \leqslant r(k^2, p) < p,$$

and let

$$\mathscr{A} = \{a_1, a_2, ..., a_{p-1}\} \cap \{1, 2, ..., n\}.$$

Then we have $\mathscr{A} \subset \{1, 2, ..., n\}$, and it is easy to see that $\mathscr{A}$ is a Sidon set. Clearly, $a_1 = 1$ and by the definition of p we have

$$a_{p-1} > 2(p-2)p > n. \tag{9.3}$$

Moreover, we have

$$s_1 = a_1 + a_1 = 2 \in \mathscr{S}_{\mathscr{A}} \tag{9.4}$$

and

$$a_i + a_1 \in \mathscr{S}_{\mathscr{A}} \qquad \text{for all} \quad a_i \leqslant n. \tag{9.5}$$

Finally, in view of (9.2), for $i = 1, 2, ..., p-2$ and large n we have

$$0 < (a_{i+1} + a_1) - (a_i + a_1) = a_{i+1} - a_i < (2ip + p) - 2(i-1)p = 3p < 3n^{1/2}.$$

(9.1) follows from (9.3), (9.4), 9.5), and (9.6), and this completes the Proof of Theorem 3.

10

For infinite Sidon sets, we can prove the following slightly weaker result:

THEOREM 4. *For all $\varepsilon > 0$ there is a Sidon set $\mathscr{A}$ and a positive integer i_0 such that the sum set $\mathscr{S}_{\mathscr{A}} = \mathscr{A} + \mathscr{A} = \{s_1, s_2, ...\}$ satisfies*

$$s_{i+1} - s_i < s_i^{1/2} (\log s_i)^{(3/2)+\varepsilon} \tag{10.1}$$

for $i > i_0$.

We remark that probably the right-hand-side of (10.1) can be replaced by s_i^{ε} but it seems to be hopeless to prove this.

Proof of Theorem 4. We shall adapt the probabilistic method of Erdős and Rényi [1, 3]. The Halberstam–Roth book [5] contains an excellent exposition of this method thus we use the terminology and notation of this book.

Let Ω denote the family of the subsets of $\mathbb{N}$, and for $n = 1, 2, \ldots$ write

$$\alpha_n = n^{-3/4}(\log(n+3))^{-(1+\varepsilon)/4}. \tag{10.2}$$

Then we have

$$0 < \alpha_n < 1 \qquad \text{for} \quad n = 1, 2, \ldots.$$

Consider the probability space (Ω, s, μ) with the following two properties (cf. Theorem 13 in [5, p. 142]):

(i) For every $n \in \mathbb{N}$, the event $B^{(n)} = \{\mathcal{A}: \mathcal{A} \in \Omega, n \in \mathcal{A}\}$ is measurable, and $\mu(B^{(n)}) = \alpha_n$.

(ii) The events $B^{(1)}, B^{(2)}, \ldots$ are independent. Moreover, denote the number of solutions of

$$a + a' = n, \qquad a, a' \in \mathcal{A}, \qquad a \leqslant a'$$

by $r_n(\mathcal{A})$. First we will prove two lemmas.

LEMMA 1. *Let E_n denote the event*

$$E_n = \{\mathcal{B}: \mathcal{B} \in \Omega, r_n(\mathcal{B}) > 1\},$$

and write

$$F = \Omega \setminus \bigcap_{j=1}^{+\infty} \left(\bigcup_{n=j}^{+\infty} E_n \right) \tag{10.3}$$

so that $\mathcal{B} \in F$ if and only if there is a number $n_0 = n_0(\mathcal{B})$ such that we have

$$r_n(\mathcal{B}) \leqslant 1 \qquad \text{for} \quad n \geqslant n_0. \tag{10.4}$$

Then we have

$$\mu(F) = 1. \tag{10.5}$$

Proof of Lemma 1. For $1 \leqslant i < j \leqslant n/2$, let $G_n(i, j)$ denote the event

$$G_n(i, j) = \{\mathcal{B}: \mathcal{B} \in \Omega, i \in \mathcal{B}, n - i \in \mathcal{B}, j \in \mathcal{B}, n - j \in \mathcal{B}\}.$$

Then clearly,

$$E_n \subset \bigcup_{1 \leqslant i < j \leqslant n/2} G_n(i, j)$$

whence

$$\mu(E_n) \leqslant \sum_{1 \leqslant i < j \leqslant n/2} \mu(G_n(i, j)). \tag{10.6}$$

By (i) and (ii) we have

$$\mu(G_n(i, j)) = \begin{cases} \alpha_i \alpha_{n-i} \alpha_j \alpha_{n-j} & \text{for } 1 \leqslant i < j < n/2 \\ \alpha_i \alpha_{n-i} \alpha_{n/2} & \text{for } 1 \leqslant i < j = n/2. \end{cases}$$

Thus by (10.2), we obtain by a simple calculation that

$$\begin{aligned} \sum_{1 \leqslant i < j \leqslant n} \mu(G_n(i, j)) &= \sum_{1 \leqslant i < j < n/2} \alpha_i \alpha_{n-i} \alpha_j \alpha_{n-j} + \delta_n \alpha_{n/2} \sum_{1 \leqslant i < n/2} \alpha_i \alpha_{n-i} \\ &\leqslant \left(\sum_{1 \leqslant i < n/2} \alpha_i \alpha_{n-i} + \delta_n \alpha_{n/2} \right)^2 \\ &\ll n^{-1} (\log n)^{-(1+\varepsilon)} \end{aligned} \tag{10.7}$$

where $\delta_n = 1$ if n is even and $\delta_n = 0$ if n is odd, and the implicit constant depends on ε. By (10.6) and (10.7) we have

$$\sum_{n=1}^{+\infty} \mu(E_n) < +\infty.$$

Thus by the Borel–Cantelli lemma (cf. [5, p. 135]), with probability 1 at most a finite number of the events E_n can occur which, by (10.3), proves (10.5) and this completes the proof of Lemma 1.

Now for a fixed $\varepsilon > 0$, define the integers $u_1 < u_2 < \cdots$ by the following recursion: Let

$$u_1 = 1000.$$

If u_n have been defined, then let

$$v_n = [\tfrac{1}{6} u_n^{1/2} (\log u_n)^{(3/2)+\varepsilon}]$$

and

$$u_{n+1} = u_n + 2v_n.$$

LEMMA 2. *Let K_n denote the event $K_n = \{\mathscr{B}: \mathscr{B} \in \Omega$, there are no $b, b' \in \mathscr{B}$ with $[u_n/10] \leqslant b < b'$, $u_n \leqslant b + b' < u_{n+1}\}$, and write*

$$L = \Omega \setminus \bigcap_{j=1}^{+\infty} \left(\bigcup_{n=j}^{+\infty} K_n \right) \tag{10.8}$$

so that $\mathscr{B} \in L$ *if and only if there is a number* $n_1 = n_1(\mathscr{B})$ *such that for* $n \geqslant n_1$ *there are integers* b, b' *with*

$$b, b' \in \mathscr{B},\ [u_n/10] \leqslant b < b', \qquad u_n \leqslant b + b' < u_{n+1}. \tag{10.9}$$

Then we have

$$\mu(L) = 1. \tag{10.10}$$

Proof of Lemma 2. First we will estimate $\mu(K_n)$. Define the positive integer j_0 by

$$[u_n/10] + j_0 v_n < u_n/2 \leqslant [u_n/10] + (j_0 + 1)\, v_n$$

so that for $n \to +\infty$ we have

$$j_0 = (1 + o(1))\frac{2u_n}{5v_n}. \tag{10.11}$$

For $1 \leqslant j \leqslant j_0$, let $M_n(j)$ denote the event that there are no b, b' with

$$b \in [[u_n/10] + (j-1)\, v_n,\ [u_n/10] + jv_n) \stackrel{\text{def}}{=} I_j,$$

$$b' \in [u_n - [u_n/10] - (j-1)\, v_n,\ u_n - [u_n/10] - (j-2)\, v_n) \stackrel{\text{def}}{=} I'_j.$$

Then clearly,

$$K_n \subset \bigcap_{j=1}^{j_0} M_n(j),$$

moreover, the events $M_n(1), \ldots, M_n(j_0)$ are independent so that

$$\mu(K_n) \leqslant \prod_{j=1}^{j_0} \mu(M_n(j)). \tag{10.12}$$

It remains to estimate $\mu(M_n(j))$. For $n \to +\infty$ clearly we have

$$\mu(M_n(j)) = 1 - \left(1 - \prod_{i \in I_j} (1 - \alpha_i)\right)\left(1 - \prod_{i \in I'_j} (1 - \alpha_i)\right) < 1 - (1 - (1 - \alpha_{u_n})^{v_n})^2$$

$$= 1 - (1 + o(1))(v_n \alpha_{u_n})^2 \qquad \text{(uniformly for } 1 \leqslant j \leqslant j_0\text{)}. \tag{10.13}$$

It follows from (10.11), (10.12) and (10.13) that for sufficiently large n we have

$$\mu(K_n) \leqslant (1 - (1 + o(1))(v_n \alpha_{u_n})^2)^{j_0} = \exp(-(1 + o(1))\, j_0 (v_n \alpha_{u_n})^2)$$

$$= \exp(-(\tfrac{2}{5} + o(1))\, u_n v_n \alpha_{u_n}^2) = \exp(-(\tfrac{1}{15} + o(1)) \log u_n)^{1 + (\varepsilon/2)}) < u_n^{-2}.$$

It follows that

$$\sum_{n=1}^{+\infty} \mu(K_n) < +\infty.$$

Thus again by the Borel–Cantelli lemma, with probability 1 at most a finite number of the events K_n can occur which, by (10.8), proves (10.10) and this completes the proof of Lemma 2.

Completion of the Proof of Theorem 4. By Lemmas 1 and 2, we have

$$\mu(F \cap L) = 1$$

so that $F \cap L$ is non-empty. Consider a set

$$\mathscr{B} \in F \cap L.$$

By $\mathscr{B} \in F$, there is a number $n_0 = n_0(\mathscr{B})$ such that (10.4) holds. Let

$$\mathscr{A} = \mathscr{B} \cap [n_0, +\infty). \tag{10.13}$$

It follows from (10.4) that $\mathscr{A}$ is a Sidon set. To complete the proof of the theorem, it suffices to show that if i is large enough, then there are a, a' with $a, a' \in \mathscr{A}$ and

$$s_i < a + a' < s_i + s_i^{1/2}(\log s_i)^{(3/2)+\varepsilon}. \tag{10.14}$$

Define n by

$$u_{n-1} \leqslant s_i < u_n. \tag{10.15}$$

By $\mathscr{B} \in L$, if i is large enough in terms of the number $n_1 = n_1(\mathscr{B})$ defined in Lemma 2, then there exist b, b' with

$$b, b' \in \mathscr{B}, \qquad u_n/10 \leqslant b < b' \tag{10.16}$$

and

$$u_n \leqslant b + b' < u_{n+1}. \tag{10.17}$$

If i and thus also n is large enough, then it follows from (10.13) and (10.16) that $b, b' \in \mathscr{A}$. Moreover, by the definition of the numbers $u_1, u_2, \ldots$, it follows from (10.15) and (10.17) that (10.14) holds with b and b' in place of a and a', respectively, and this completes the proof of Theorem 4.

11

So far we have given upper bounds for the large gaps between the consecutive elements of $\mathscr{S}_{\mathscr{A}}$ for Sidon sets. In case of infinite Sidon sets, a result of Erdős gives a lower bound for these gaps. In fact, Erdős [6] or [5, p. 89] proved the following result: if $\mathscr{A}$ is an infinite Sidon set, then we have

$$\lim_{n \to +\infty} \inf A(n)\, n^{-1/2} (\log n)^{1/2} < +\infty. \tag{11.1}$$

It is easy to see that this implies

$$\lim_{i \to +\infty} \sup (s_{i+1} - s_i)(\log s_i)^{-1} > 0. \tag{11.2}$$

We conjecture that the limit on the left hand side is $+\infty$, but this seems to be very difficult.

Moreover, the method of the proof of (11.1) can be adapted easily to the finite case. In this way, we get

THEOREM 5. *There is a positive absolute constant c_4 such that if $\mathscr{A}$ is a finite Sidon set with $|\mathscr{A}| \geqslant 2$ and we write $\mathscr{S}_{\mathscr{A}} = \{s_1, s_2, ..., s_u\}$, then we have*

$$\max_{1 \leqslant i \leqslant u-1} (s_{i+1} - s_i) > c_4 \log |\mathscr{A}|.$$

Proof. Write $\mathscr{A} = \{a_1, a_2, ..., a_v\}$ where $a_1 < a_2 < \cdots < a_v$. If $a_1 > 1$, then we may replace $\mathscr{A}$ by $\mathscr{A}' = \{a_1', a_2', ..., a_v'\}$ where $a_i' = a_i - (a_1 - 1)$. Then we have $a_1' = 1$, and the differences between the consecutive elements of $\mathscr{S}_{\mathscr{A}}$, resp. $\mathscr{S}_{\mathscr{A}'}$ are the same; thus we may assume that

$$a_1 = 1. \tag{11.3}$$

Moreover, clearly we may assume that $|\mathscr{A}| = v$ is large enough:

$$v > v_0. \tag{11.4}$$

Write $N = [a_v^{1/2}]$ so that

$$N^2 \leqslant a_v. \tag{11.5}$$

Let

$$\tau_{\mathscr{A}}(N) = \min_{l = 1, 2, ..., N} A(lN) \left(\frac{\log lN}{lN} \right)^{1/2}.$$

Then the argument in [5, pp. 89–90] gives that

$$\tau_{\mathscr{A}}(N) \ll 1$$

so that there is an l such that

$$1 \leqslant l \leqslant N \tag{11.6}$$

and

$$A(lN)\left(\frac{\log lN}{lN}\right)^{1/2} = \tau_{\mathscr{A}}(N) < c_5$$

whence

$$A(lN) < c_5\left(\frac{lN}{\log lN}\right)^{1/2} < c_5\left(\frac{lN}{\log N}\right)^{1/2}. \tag{11.7}$$

Write

$$\mathscr{S}^* = \mathscr{S}_{\mathscr{A}} \cap \{1, 2, ..., lN\} = \{s_1, s_2, ..., s_t\}.$$

Then by (11.3) we have

$$s_1 = a_1 + a_1 = 2. \tag{11.8}$$

Moreover, it follows from (11.5) and (11.6) that

$$lN \leqslant N^2 \leqslant a_v < a_v + a_v \in \mathscr{S}_{\mathscr{A}}.$$

Thus $\mathscr{S}_{\mathscr{A}}$ has at least one element s_{t+1} greater than lN:

$$s_{t+1} > lN. \tag{11.9}$$

By (11.7) we have

$$t = |\mathscr{S}^*| = |\{(a, a'): a \in \mathscr{A}', a' \in \mathscr{A}, a + a' \leqslant lN\}|$$

$$\leqslant |\{a: a \in \mathscr{A}, a \leqslant lN\}|^2 = A^2(lN) < c_6 \frac{lN}{\log N}. \tag{11.10}$$

It follows from (11.4), (11.8), and (11.9) that

$$\sum_{i=1}^{t} (s_{i+1} - s_i) = s_{t+1} - s_1 > lN - 2 > \tfrac{1}{2} lN$$

whence, by (11.4) and (11.10),

$$\max_{1 \leqslant i \leqslant t} (s_{i+1} - s_i) > \frac{lN}{2t} > c_7 \log N > c_8 \log a_v \geqslant c_8 \log v = c_8 \log |\mathscr{A}|$$

and this completes the proof of Theorem 5.

12

Finally, we will discuss several unsolved problems concerning Sidon sets.

Problem 1. We conjecture that for finite Sidon sets $\mathscr{A}$ we have

$$\lim_{|\mathscr{A}| \to +\infty} |\{s: s-1 \notin \mathscr{S}_{\mathscr{A}}, s \in \mathscr{S}_{\mathscr{A}}, s+1 \notin \mathscr{S}_{\mathscr{A}}\}| = +\infty.$$

Is it true that we have

$$|\{s: s-1 \notin \mathscr{S}_{\mathscr{A}}, s \in \mathscr{S}_{\mathscr{A}}, s+1 \notin \mathscr{S}_{\mathscr{A}}\}| \gg |\mathscr{A}|^2?$$

For infinite Sidon sets $\mathscr{A}$, the problem is to estimate the function

$$F(\mathscr{A}, n) = |\{s: s \leqslant n, s-1 \notin \mathscr{S}_{\mathscr{A}}, s \in \mathscr{S}_{\mathscr{A}}, s+1 \notin \mathscr{S}_{\mathscr{A}}\}|.$$

Problem 2. Is it true that if for finite Sidon sets $\mathscr{A}$ we write $\mathscr{S}_{\mathscr{A}} = \{s_1, s_2, ..., s_t\}$ (so that $t = |\mathscr{S}_{\mathscr{A}}| = \binom{|\mathscr{A}|}{2} + |\mathscr{A}|$), then for $|\mathscr{A}| \to +\infty$ we have

$$\frac{1}{t} \sum_{i=1}^{t-1} (s_{i+1} - s_i)^2 \to +\infty?$$

(Again, the problem can be extended to infinite Sidon sets.)

Problem 3. Is it true that if $\mathscr{A} \subset \{1, 2, ..., n\}$ is a finite Sidon set with

$$|\mathscr{A}| = (1 + o(1)) n^{1/2}, \tag{12.1}$$

then $\mathscr{S}_{\mathscr{A}}$ must be well-distributed in the residue classes of small moduli? In particular, is it true that (12.1) implies that about half of the elements of $\mathscr{S}_{\mathscr{A}}$ are even and half of them are odd?

Problem 4. Let $F(N)$ denote the cardinality of a maximal Sidon set selected from $\{1, 2, ..., N\}$. Is it true that for every $k \in \mathbb{N}$ there is a number $N_0 = N_0(k)$ such that

$$F(N+k) - F(N) \leqslant 1 \qquad \text{for} \quad N > N_0?$$

Perhaps, this holds even with $\varepsilon N^{1/2}$ in place of k.

Problem 5. One might like to extend the problems studied above to "nearly" Sidon sets. In particular, is it true that if $\mathscr{A}$ is a finite set with

$$|\mathscr{S}_{\mathscr{A}}| = (\tfrac{1}{2} + o(1))\,|\mathscr{A}|^2,$$

then $|\mathscr{B}(\mathscr{S}_{\mathscr{A}}, d)|$ must be large (perhaps, $\geqslant |\mathscr{A}|^2$) for all $d \in \mathbb{N}$? The method used in the Proof of Theorem 2 cannot be adapted to study this problem.

Problem 6. Let $\mathscr{D}_{\mathscr{A}}$ denote the difference set of the finite set $\mathscr{A}$, i.e., the set of the positive integers $\mathscr{A}$ that can be represented in the form $a - a' = d$ with $a, a' \in \mathscr{A}$. One might like to study the difference analogues of the problems discussed in Sections 3–11, i.e., to replace the set $\mathscr{S}_{\mathscr{A}}$ in each of these problems by $\mathscr{D}_{\mathscr{A}}$. Indeed, the proofs given above can be modified easily to prove the difference analogues of Theorems 1 and 3 so that, e.g., we can prove (by the method used in the Proof of Theorem 2) that for a finite Sidon set $\mathscr{A}$ we have

$$|\{n: n - d \notin \mathscr{D}_{\mathscr{A}}, n \in \mathscr{D}_{\mathscr{A}}\}| > c_9\,|\mathscr{A}|^2.$$

On the other hand, it can be shown easily that there is an infinite Sidon set $\mathscr{A}$ such that $\mathscr{D}_{\mathscr{A}} = \mathbb{N}$, so that the difference analogues of Theorem 2 and (11.2) fail, while the difference analogue of the problem studied in Theorem 4 is trivial. The difference analogue of Theorem 5 gives the only interesting new question and, indeed, we cannot answer the following question: is it true that if for finite Sidon sets $\mathscr{A}$ we write $\mathscr{D}_{\mathscr{A}} = \{d_1, d_2, \ldots, d_v\}$, then for $|\mathscr{A}| \to +\infty$ we have

$$\max_{1 \leqslant i \leqslant v-1} (d_{i+1} - d_i) \to +\infty?$$

Problem 7. Does there exist a Sidon set $\mathscr{A} \subset \{1, 2, \ldots, n\}$ such that $|\mathscr{A}| \ll n^{1/3}$ and it is a "maximal" Sidon set in the sense that there is no b such that $b \in \{1, 2, \ldots, n\}$, $b \notin \mathscr{A}$ and $\mathscr{A} \cup \{b\}$ is a Sidon set? (The answer to this question would throw more light on the role of the "greedy algorithm" in this field.)

Problem 8. Does there exist an infinite Sidon set $\mathscr{A}$ which is an asymptotic basis of order 3?

Problem 9. A set $\mathscr{A}$ is said to be a $B_2[g]$ set if for all $n \in \mathbb{N}$, the equation

$$a + a' = n,\ a \leqslant a', \qquad a \in \mathscr{A},\ a' \in \mathscr{A}$$

has at most g solutions (so that a Sidon set is a $B_2[1]$ or briefly B_2 set). One might like to extend the problems and results above to $B_2[g]$ sets.

This seems to be very difficult and, indeed, the difficulties concerning $B_2[g]$ sets can be illustrated by the following fact: while we have a quite good asymptotics for the cardinality of a maximal Sidon set $\mathscr{A}$ with $\mathscr{A} \subset \{1, 2, ..., n\}$ (it is known that $|\max |\mathscr{A}| - n^{1/2}| \ll n^{5/16}$), we do not have any asymptotic formula for the cardinality of a maximal $B_2[g]$ set $\mathscr{A}$ with $\mathscr{A} \subset \{1, 2, ..., n\}$. Moreover, it is not known whether (11.1) can be extended to $B_2[2]$, or more generally, $B_2[g]$ sets. In other words, is it true that an infinite $B_2[2]$ set $\mathscr{A}$ must satisfy

$$\lim_{n \to +\infty} \inf A(n)\, n^{-1/2} = 0?$$

REFERENCES

1. P. ERDŐS, Problems and results in additive number theory, "Colloque sur la Théorie des Nombres (CBRM) (Bruxelles, 1955), Georges Thone, Liège; Masson et Cie, Paris, 1956," pp. 127–137.
2. P. ERDŐS AND R. FREUD, On sums of a Sidon-sequence, *J. Number Theory* **38** (1991), 196–205.
3. P. ERDŐS AND A. RÉNYI, Additive properties of random sequences of positive integers, *Acta Arith.* **6** (1960), 83–110.
4. G. A. FREIMAN, Foundations of a Structural Theory of Set Addition, "Translations of Mathematical Monographs," Vol. 37, Amer. Math. Soc., Providence, RI, 1973.
5. H. HALBERSTAM AND K. F. ROTH, "Sequences," Springer-Verlag, Berlin/Heildelberg/New York, 1983.
6. A. STÖHR, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe, II, *J. Reine Angew. Math.* **194** (1955), 111–140.