ELSEVIER

Discrete Mathematics 136 (1994) 75–99

DISCRETE MATHEMATICS

On additive properties of general sequences

P. Erdős, A. Sárközy [1], V.T. Sós *, [1]

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

Received 1 September 1993; revised 20 October 1993

Abstract

The authors give a survey of their papers on additive properties of general sequences and they prove several further results on the range of additive representation functions and on difference sets. Many related unsolved problems are discussed.

1.

The set of the integers, nonnegative integers, resp. positive integers is denoted by $\mathbb{Z}, \mathbb{N}_0$ and $\mathbb{N}$. $\mathscr{A}, \mathscr{B}, \ldots$ denote (finite or infinite) subsets of $\mathbb{N}_0$, and their counting functions are denoted by $A(n), B(n), \ldots$ so that, e.g.,

$$A(n) = |\{a\colon 0 < a \leqslant n, a \in \mathscr{A}\}|.$$

The asymptotic density $d(\mathscr{A})$ of the set $\mathscr{A} \subset \mathbb{N}_0$ is defined by

$$d(\mathscr{A}) = \lim_{n \to +\infty} \frac{\mathscr{A}(n)}{n}$$

if this limit exists. $\mathscr{A}_1 + \mathscr{A}_2 + \cdots + \mathscr{A}_k$ denotes the set of the integers that can be represented in the form $a_1 + a_2 + \cdots + a_k$ with $a_1 \in \mathscr{A}_1, a_2 \in \mathscr{A}_2, \ldots, a_k \in \mathscr{A}_k$; in particular, we write $\mathscr{A} + \mathscr{A} = 2\mathscr{A} = \mathscr{S}(\mathscr{A})$. For $\mathscr{A} \in N, \mathscr{D}(\mathscr{A})$ denotes the difference set of the set $\mathscr{A}$, i.e., the set of the positive integers that can be represented in the form $a - a'$ with $a \in \mathscr{A}$, $a' \in \mathscr{A}$.

For $\mathscr{A} \subset \mathbb{N}_0$, $k \in \mathbb{N}$ the number of solutions of the equations

* Corresponding author.

[1] Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. 1901.

Elsevier Science B.V.
SSDI 0012-365X(94)00108-U

$$a_1 + a_2 + \cdots + a_k = n, \quad a_1, a_2, \ldots, a_k \in \mathscr{A},$$

$$a_1 + a_2 + \cdots + a_k = n, \quad a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k, \quad a_1, a_2, \ldots, a_k \in \mathscr{A},$$

$$a_1 + a_2 + \cdots + a_k = n, \quad a_1 < a_2 < \cdots < a_k, \quad a_1, a_2, \ldots, a_k \in \mathscr{A},$$

is denoted by $r_1(\mathscr{A},n,k)$, $r_2(\mathscr{A},n,k)$, resp. $r_3(\mathscr{A},n,k)$, and in the special case $k=2$ we write $r_i(n) = r_i(\mathscr{A},n) = r_i(\mathscr{A},n,2)$ for $i = 1, 2, 3$. The number of solutions of the equation

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

is denoted by $f(\mathscr{A}, d)$.

For k, $g \in \mathbb{N}, B_k[g]$ denotes the class of all (finite or infinite) sets $\mathscr{A} \subset \mathbb{N}_0$ such that for all $n \in \mathbb{N}$ we have $r_2(\mathscr{A}, n, k) \leqslant g$, i.e., the equation

$$a_1 + a_2 + \cdots + a_k = n, \quad a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k, \; a_1, a_2, \ldots, a_k, \in \mathscr{A}$$

has at most g solutions. The sets $\mathscr{A} \in B_k$ [1] are called B_k sets. In particular, the B_2 sets are called Sidon sets. An excellent account of the theory of additive representation functions, Sidon sets and $B_k[g]$ sets is given in [17].

If $F(n) = \mathrm{O}(G(n))$, then we write $F(n) \ll G(n).c_1, c_2, \ldots$ denote positive absolute constants.

In the last 10 years, we have written 7 papers [7–13] on the representation functions $r_1(n), r_2(n), r_3(n)$ and on Sidon sets. In this paper first (in Section 2) we will survey the main results and the most interesting unsolved problems discussed in these papers, and we will add several further unsolved problems. We remark that in this field the combinatorial tools dominate. In many cases, the crucial tool in the proof is a combinatorial theorem, e.g., the main result in Erdős' paper [4] (see also [6]) is proved by using Ramsey's theorem. Even in the papers where analytical or probabilistic tools are used, the main difficulty is usually to force out the applicability of the analytical-probabilistic machinery by using an elementary-combinatorial argument.

In the second part of this paper (Sections 3 and 4) we will continue the study of additive representation functions by investigating the range of these functions. Finally, we will study difference sets (Sections 5–8).

2.

In an old paper Erdős [3] proved the following result: there is an infinite set $\mathscr{A} \subset \mathbb{N}$ such that

$$c_1 \log n < r_1(\mathscr{A},n) < c_2 \log n \quad \text{for } n > n_0 \,. \tag{2.1}$$

The first two authors [7, 8] extended the problem by estimating $|r_1(\mathscr{A},n) - F(n)|$ for 'nice' functions $F(n)$. First we proved (see [7]) the following theorem.

Theorem 1. *If $F(n)$ is an arithmetic function satisfying*

$$F(n) \to +\infty,$$

$$F(n+1) \geqslant F(n) \quad \textit{for } n \geqslant n_0$$

and

$$F(n) = \mathrm{o}\left(\frac{n}{(\log n)^2}\right),$$

then

$$\max_{n \leqslant N} |r_1(\mathscr{A}, n) - F(n)| = \mathrm{o}((F(N))^{1/2}) \tag{2.2}$$

cannot hold.

Indeed, we proved this in the sharper form that (2.2) cannot hold in mean square sense.

On the other hand, the first two authors proved [8] that if $F(n)$ is a 'nice' function, then there is an $\mathscr{A}$ with

$$|r_1(\mathscr{A}, n) - F(n)| \ll (F(n) \log n)^{1/2} :$$

Theorem 2. *If $F(n)$ is an arithmetic function satisfying*

$$F(n) > 36 \log n \quad \textit{for } n > n_0,$$

and there exist a real function $g(x)$, defined for $0 < x < +\infty$, and real numbers x_0, n_1 such that

(i) *$g'(x)$ exists and it is continuous for $0 < x < +\infty$,*
(ii) *$g'(x) \leqslant 0$ for $x \geqslant x_0$,*
(iii) *$0 < g(x) < 1$ for $x \geqslant x_0$,*
(iv) *$|F(n) - 2\int_0^{n/2} g(x) g(n-x) dx| < (F(n) \log(n)^{1/2}$ for $n > n_1$,*

then there exists a sequence $\mathscr{A}$ such that

$$|r_1(\mathscr{A}, n) - F(n)| < 8(F(n) \log n)^{1/2} \quad \textit{for } n > n_2. \tag{2.3}$$

In particular, it follows from this theorem that

(i) there is an $\mathscr{A}$ satisfying (2.1);
(ii) there is an $\mathscr{A}$ with

$$r_1(\mathscr{A}, n) \sim \log n \log \log n$$

(where $\log \log n$ can be replaced by any $\omega(n) \to +\infty$ which increases regularly enough);

(iii) for all $0 < \alpha < 1$, there is an $\mathscr{A}$ with

$$|r_1(\mathscr{A}, n) - n^\alpha| \ll n^{\alpha/2} (\log n)^{1/2}.$$

Problem 1. (2.3) is worse than (2.2) by a factor $(\log n)^{1/2}$; the problem is to tighten this gap. In particular, the following old question of Erdős is undecided yet: does there exist an infinite set $\mathscr{A}$ with

$$r_1(\mathscr{A},n) \sim c \log n \quad (\text{with } c > 0)\,?$$

In [11] we studied the following problem: what condition is needed to ensure

$$\lim_{n\to+\infty} \sup |r_1(\mathscr{A},n+1) - r_1(\mathscr{A},n)| = +\infty\,? \tag{2.4}$$

It turned out that one needs an assumption in terms of the function

$$B(\mathscr{A},N) = |\{n\colon n \leqslant N,\ n \in \mathscr{A}, n-1 \notin \mathscr{A}\}|\,:$$

Theorem 3. *If*

$$\lim_{N\to+\infty} B(\mathscr{A},N)N^{-1/2} = +\infty\,,$$

then (2.4) *holds.*

We showed that this theorem is nearly sharp.

Theorem 4. *For all $\varepsilon > 0$, there exists an infinite sequence $\mathscr{A}$ such that*

$$B(\mathscr{A},N) \gg N^{-1/2-\varepsilon}$$

and $r_1(\mathscr{A},N)$ is bounded (so that $|r_1(\mathscr{A},N+1) - r_1(\mathscr{A},N)|$ is also bounded).

Two related questions that we could not settle are given below.

Problem 2. Is it true that

$$\lim_{N\to+\infty} \sup B(\mathscr{A},N)N^{-1/2} = \infty$$

implies (2.4)?

Problem 3. Is it true that

$$\lim_{N\to+\infty} \inf B(\mathscr{A},N)N^{-1/2} > 0$$

implies (2.4)?

In [9, 10] we studied the monotonicity properties of the three representation functions $r_1(n), r_2(n), r_3(n)$. This is the only case where the behaviour of the three functions is different.

Theorem 5. (i) *$r_1(\mathscr{A},n)$ is monotone increasing from a certain point on, i.e.,*

$$r_1(\mathscr{A},n+1) \geqslant r_1(\mathscr{A},n) \quad \text{for } n \geqslant n_0$$

if and only if A contains all the positive integers from a certain point on.

(ii) *If*

$$\lim_{N\to+\infty} \frac{N-A(N)}{\log N} = +\infty\,,$$

then $r_2(\mathscr{A},n)$ cannot be monotone increasing from a certain point on.

(iii) *If*

$$A(N) = \mathrm{o}\left(\frac{N}{\log N}\right),$$

then $r_3(\mathscr{A},n)$ cannot be monotone increasing from a certain point on. On the other hand, there is an infinite set $\mathscr{A}$ such that

$$N - A(N) \gg N^{1/3} \tag{2.5}$$

and $r_3(\mathscr{A},n)$ is monotone increasing from a certain point on.

The result in (ii) was proved independently by Balasubramanian [2].

Problem 4. Does there exist an infinite set $\mathscr{A} \subset \mathbb{N}$ such that $\mathbb{N}\setminus\mathscr{A}$ is infinite and $r_2(\mathscr{A},n)$ is increasing from a certain point on?

Problem 5. There is a large gap between the lower and upper bounds in (iii); the problem is to tighten this gap. The upper bound in (2.5) seems to be closer to the truth. Correspondingly, one might like to show that if $r_3(\mathscr{A},n)$ is monotone increasing from a certain point on, then $d(\mathscr{A}) = 1$.

Problem 6. What condition is needed to ensure that

$$r_i(\mathscr{A},n) > \max(r_i(\mathscr{A},n-1), r_i(\mathscr{A},n+1))\,,$$

resp.

$$r_i(\mathscr{A},n) < \min(r_i(\mathscr{A},n-1), r_i(\mathscr{A},n+1))$$

holds infinitely often (for $i = 1,2,3$)?

Problem 7. What condition is needed to ensure that

$$\lim_{n\to+\infty} \sup(r_i(\mathscr{A},n) - \max(r_i(\mathscr{A},n-1), r_i(\mathscr{A},n+1))) = +\infty\,,$$

resp.

$$\lim_{n\to+\infty} \sup(\min(r_i(\mathscr{A},n-1), r_i(\mathscr{A},n+1)) - r_i(\mathscr{A},n)) = +\infty\,,$$

(for $i = 1,2,3$)?

Problem 8. So far we have studied the case of two summands, i.e., the functions $r_i(\mathscr{A}, n, 2)$. The problem is to extend these results to the case of k summands, i.e., to the functions $r_i(\mathscr{A}, n, k)$. In the case of Theorems 1–4, we expect results of similar nature for $k > 2$, while in the case of the monotonicity properties we get a problem of completely different nature for $k > 2$.

In [12, 13] we studied Sidon sets, mostly the structure of the sum set $\mathscr{S}(\mathscr{A}) = \{s_1, s_2, \dots,\}$ of a Sidon set $\mathscr{A}$. In [12] first we studied the number of blocks of consecutive integers in $\mathscr{S}(\mathscr{A})$.

Theorem 6. *There is a positive constant c_3 such that for every finite Sidon set $\mathscr{A}$ and all $d \in \mathbb{N}$ we have*

$$|\{s\colon\ s \in \mathscr{S}(\mathscr{A}),\ s - d \notin \mathscr{S}(\mathscr{A})\}| > c_3|\mathscr{A}|^2 . \tag{2.6}$$

Note that clearly the left-hand side of (2.6) is $\leqslant |\mathscr{A}|^2$ (for all $\mathscr{A}$ and d) so that (2.6) is the best possible apart from the value of the constant c_3. In particular, choosing $d = 1$ we obtain that if we represent $\mathscr{S}(\mathscr{A})$ as the union of t blocks (of length $v_1, v_2, \dots, v_t$) of consecutive integers:

$$\mathscr{S}(\mathscr{A}) = \bigcup_{i=1}^{t} \left(\bigcup_{j=1}^{v_i} \{u_i + j\} \right), \quad u_i \notin \mathscr{S}(\mathscr{A}), \tag{2.7}$$

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

We also proved a theorem similar to Theorem 6 for infinite Sidon sets.

Problem 9. Do there exist finite Sidon sets $\mathscr{A}$ such that $|\mathscr{A}| \to +\infty$, and representing $\mathscr{S}(\mathscr{A})$ in the form (2.7), we have

$$\left(\sum_{i=1}^{t} v_i^2 \right) |\mathscr{A}|^{-2} \to +\infty\,?$$

Problem 10. Is it true that for finite Sidon sets $\mathscr{A}$ we have

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

Next, we studied the size of the gaps between the consecutive elements of the sum set $\mathscr{S}(\mathscr{A})$ of a Sidon set $\mathscr{A}$.

Theorem 7. *For all $\varepsilon > 0$ there is an infinite Sidon set $\mathscr{A}$ and a positive integer i_0 such that the sum set $\mathscr{S}(\mathscr{A}) = \mathscr{A} + \mathscr{A} = \{s_1, s_2, \dots\}$ satisfies*

$$s_{i+1} - s_i < s_i^{1/2} (\log s_i)^{(3/2)+\varepsilon} \quad \textit{for } i > i_0 . \tag{2.8}$$

Probably this is true with s_i^ε on the right hand side of (2.8) but it seems to be hopeless to prove this. Again, we proved a similar result for finite Sidon sets.

On the other hand we proved the following theorem.

Theorem 8. *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 $\mathscr{S}(\mathscr{A}) = \{s_1, s_2, \ldots, s_u\}$ (where $s_1 < s_2 < \cdots < s_u$), then we have*

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

(The analogous result for infinite Sidon sets follows from an old result of Erdős.)

The proof of Theorem 8 gives the existence of a gap $s_{i+1} - s_i > c_4 \log |\mathscr{A}|$ with an i 'much smaller' than u (typically, $i < u^{1/2+\varepsilon}$).

Problem 11. Is it true that if $\varepsilon > 0$ and $|\mathscr{A}| > n_0(\varepsilon)$, then every interval of length εu contains a large gap, i.e., for all $x \in Z$ there is a $y \in \mathbb{Z}$ such that $x < y < x + \varepsilon u$ and $y + j \notin \mathscr{S}(\mathscr{A})$ for $1 \leqslant j \leqslant c(\varepsilon) \log |\mathscr{A}|$? Perhaps, this holds already for intervals much shorter than εu.

Problem 12. Is it true that if $\mathscr{A}$ is a finite Sidon set whose sum set is $\mathscr{S}(\mathscr{A}) = \{s_1, s_2, \ldots, s_u\}$ (so that $u = |\mathscr{S}(\mathscr{A})| = \binom{|\mathscr{A}|}{2} + |\mathscr{A}|$), then for $|\mathscr{A}| \to +\infty$ we have

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

In [13] first we estimated the length of blocks of consecutive integers in sum sets of Sidon sets. We proved that the maximal length of a block of consecutive integers in the sum set of a Sidon set selected from $\{1, 2, \ldots, N\}$ is between $c_5 N^{1/3}$ and $c_6 N^{1/2}$:

Theorem 9. *If $N \in \mathbb{N}, L \in \mathbb{N}$ and $\mathscr{A} \subset \{1, 2, \ldots, N\}$ is a Sidon set, then for all $K \in Z$ we have*

$$|\{s : s \in \mathscr{S}(\mathscr{A}), K < s \leqslant K + L\}| < 1/2L + 6L^{1/2} N^{1/4} .$$

Applying this theorem with $L = [200 N^{1/2}]$, we obtain that for large $N, \mathscr{S}(\mathscr{A})$ cannot contain more than $200 N^{1/2}$ consecutive integers.

On the other hand, we have the following theorem.

Theorem 10. *There is an infinite Sidon set $\mathscr{A}$ such that for all $n > n_0, \mathscr{S}(\mathscr{A}) \cap \{1, 2, \ldots, n\}$ contains a block consisting of more than $\frac{1}{50} n^{1/3}$ consecutive integers.*

Finally (inspired by Freiman's results [15]) in [13] we showed that $B_2[g]$ sets, in particular, Sidon sets cannot be well-covered by generalized arithmetic progressions; these results are too complicated to give the details here.

Problem 13. Is it true that if $\mathscr{A} \subset \{1, 2, \ldots, N\}$ is a finite Sidon set with

$$|\mathscr{A}| = (1 + o(1))N^{1/2}, \tag{2.9}$$

then $\mathscr{S}(\mathscr{A})$ must be well-distributed in the residue classes of small moduli? In particular, is it true that (2.9) implies that about half of the elements of $\mathscr{S}(\mathscr{A})$ are even and half of them are odd?

Problem 14. Does there exist an infinite Sidon set $\mathscr{A}$ which is an asymptotic basis of order 3?

Problem 15. 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.)

Some of the problems studied above could be extended to 'nearly' Sidon sets and $B_2[g]$ sets. Moreover, some of them could be extended to other structures along the lines described in [19].

3.

Nathanson [18] studied the following problem: when is A uniquely determined by the sequence $r_1(\mathscr{A}, n_0), r_1(\mathscr{A}, n_0 + 1), r_1(\mathscr{A}, n_0 + 2), \ldots$? The following related questions can be asked.

For what sets $\mathscr{A}$ does the set $\mathscr{S}(\mathscr{A})$ uniquely determine $\mathscr{A}$?

Moreover, for $i = 1, 2, 3$, let $\mathscr{R}_i(\mathscr{A})$ denote the range of the function $r_i(\mathscr{A}, n)$, i.e., $\mathscr{R}_i(\mathscr{A})$ denotes the set of the integers m such that there is a number $n \in \mathbb{N}$ with

$$r_i(\mathscr{A}, n) = m .$$

For what sets $\mathscr{B} \subset \mathbb{N}_0$ can one find a set $\mathscr{A}$ with

$$\mathscr{R}(\mathscr{A}) = \mathscr{B}, \quad \mathscr{A} \subset \mathbb{N}\,? \tag{3.1}$$

This last question can be answered relatively easily. Here we restrict ourselves to the case $i = 1$ since the cases $i = 2, 3$ can be handled similarly:

Theorem 11. *For a set $\mathscr{B} \subset N_0$, (3.1) can be solved if and only if either $\mathscr{B} = \{0, 1\}$ or*

$$\{0, 1, 2\} \subset \mathscr{B} . \tag{3.2}$$

Proof. If (3.1) can be solved and $\mathscr{A} = \{a_1, a_2, \ldots\}$ (where $0 < a_1 < a_2 < \cdots$) is a solution, then clearly

$$r_1(\mathscr{A},1)=0, \qquad r_1(\mathscr{A},2a_1)=1$$

so that $\{0,1\}\subset\mathscr{R}_1(\mathscr{A})$. Moreover, for $|\mathscr{A}|=1$ we have $\mathscr{R}_1(\mathscr{A})=\{0,1\}$, while for $|\mathscr{A}|>1$ we have

$$r_1(\mathscr{A},a_1+a_2)=2$$

so that (3.2) holds in this case.

Conversely, assume that (3.2) holds and let $\mathscr{B}=\{b_0,b_1,b_2,\ldots\}$ where $b_0=0$, $b_1=1$, $b_2=2$ and $b_2<b_3<\cdots$ (The case $\mathscr{B}=\{0,1\}$ is trivial: we may take $\mathscr{A}=\{1\}$.) Then we will define a sequence of sets $\mathscr{A}_1,\mathscr{A}_2,\ldots$ by recursion so that

$$\mathscr{A}_1\subset\mathscr{A}_2\subset\cdots \tag{3.3}$$

and

$$\mathscr{R}_1(\mathscr{A}_k)=\{b_0,b_1,\ldots,b_k\} \quad (=\{0,1,2,\ldots\}). \tag{3.4}$$

Indeed, let

$$\mathscr{A}_1=\{1\};$$

then clearly

$$\mathscr{R}_1(\mathscr{A}_1)=\{0,1\}$$

so that (3.4) holds with 1 in place of k. Assume that $k\in\mathbb{N}$ and $\mathscr{A}_1,\mathscr{A}_2,\ldots,\mathscr{A}_k$ have been defined so that

$$\mathscr{A}_i\subset\mathscr{A}_{i+1} \quad (\text{for } k\geqslant 2,\ i=1,2,\ldots,k-1) \tag{3.5}$$

and

$$\mathscr{R}_1(\mathscr{A}_i)=\{b_0,b_1,\ldots,b_i\} \quad (\text{for } i=1,2,\ldots,k). \tag{3.6}$$

Then define $\mathscr{A}_{k+1}$ in the following way: write

$$t_k=[b_{k+1}/2].$$

Let $\mathscr{E}=\{e_1,e_2,\ldots,e_{t_k}\}$ (where $e_1<e_2<\cdots<e_{t_k}$) be a Sidon set such that

$$e_1>2\max_{a\in\mathscr{A}_k} a$$

and

$$e_{i+1}-e_i>\max_{a\in\mathscr{A}_k} a \quad \text{for } i=1,2,\ldots,t_k-1;$$

the existence of such a Sidon set can be shown easily by using the greedy algorithm. Write

$$x_k = 2e_{t_k} + 1$$

and

$$\mathscr{F}_k = \{e_1, e_2, \ldots, e_{t_k}, 2x_k - e_{t_k}, -2x_k - e_{t_k} - 1, \ldots, 2x_k - e_1\}.$$

Let

$$\mathscr{A}_{k+1} = \begin{cases} \mathscr{A}_k \cup \mathscr{F}_k & \text{if } b_{k+1} \text{ is even,} \\ \mathscr{A}_k \cup \mathscr{F}_k \cup \{x_k\} & \text{if } b_{k+1} \text{ is odd.} \end{cases}$$

Then clearly, (3.5) also holds with $k+1$ in place of k. Moreover, an easy consideration shows that

$$r_1(\mathscr{A}_{k+1}, n) = r_1(\mathscr{A}_k, n) \quad \text{for } n \in \mathscr{S}(\mathscr{A}_k),$$
$$r_1(\mathscr{A}_{k+1}, n) \in \{0,1,2\} \quad \text{for } n \notin \mathscr{S}(\mathscr{A}_k), n \neq 2x_k$$

and

$$r_1(\mathscr{A}_{k+1}, 2x_k) = b_{k+1},$$

so that (3.6) also holds with $k+1$ in place of i which completes the proof of the existence of sets $\mathscr{A}_1, \mathscr{A}_2, \ldots$ with the desired properties.

It follows trivially from the construction that the set

$$\mathscr{A} = \bigcup_i \mathscr{A}_i$$

satisfies (3.1) and this completes the proof of Theorem 11. □

4.

As Theorem 11 and its proof shows, (3.2) is necessary for the solvability of (3.1) (assuming $|\mathscr{A}| > 1$), and the necessity of this condition is a consequence of the behaviour of the function $r_1(\mathscr{A}, n)$ for 'small' values of n. Thus if we want to get rid of this condition, then we have to modify the definition of $\mathscr{R}_1(\mathscr{A})$ so that it should not depend on the values assumed by $r_1(\mathscr{A}, n)$ for small n's. Indeed, for $i = 1,2,3$, define $R_i^\infty(\mathscr{A})$ as the set of the integers m such that there are infinitely many integers $n \in \mathbb{N}$ satisfying

$$r_i(\mathscr{A}, n) = m.$$

Theorem 12. *For each $i = 1,2,3$ and for all $\mathscr{B} \subset \mathbb{N}_0$, the equation*

$$R_i^\infty(\mathscr{A}) = \mathscr{B} \tag{4.1}$$

can be solved.

Proof. We restrict ourselves to the case $i=1$ since the cases $i=2,3$ are similar. Moreover, the case $\mathscr{B}=\emptyset$ is trivial, thus we may assume that $\mathscr{B}\neq\emptyset$. The proof of the existence of an $\mathscr{A}$ satisfying (4.1) will be based on the following lemma. □

Lemma 1. *There exist absolute constants c_7, c_8, c_9 and n_0, and a set $\mathscr{E}\subset\mathbb{N}$ such that*

$$c_7 \log n < r_1(\mathscr{E},n) < c_8 \log n \quad \text{for } n > n_0 \tag{4.2}$$

and, denoting the solution set of

$$e+e'=n, e, e' \in \mathscr{E},$$

i.e., the set of the integers e with $e\in\mathscr{E}, n-e\in\mathscr{E}$ by $\mathscr{T}(\mathscr{E},n)$, we have

$$|\mathscr{T}(\mathscr{E},m)\cap\mathscr{T}(\mathscr{E},n)| < c_9 \quad \text{for all } m,n\in\mathbb{N},\ m\neq n. \tag{4.3}$$

Proof of Lemma 1. This is a combination of results of Erdős, Nathanson and Tetali [3, 5, 14]. □

To construct a set $\mathscr{A}$ of the desired properties, consider first an infinite sequence $f_1, f_2, \ldots$ of nonnegative integers such that $f_n\in\mathscr{B}$ for all $n\in\mathbb{N}$, and if $b\in\mathscr{B}$, then there are infinitely many $n\in\mathbb{N}$ with $f_n=b$. By recursion we will construct an infinite sequence $\mathscr{G}=\{g_1,g_2,\ldots\}\subset\mathbb{N}$ and an infinite sequence $\mathscr{H}_0,\mathscr{H}_1,\ldots$ of subsets of $\mathbb{N}$ with the following properties:

$$g_k > 2g_{k-1} \quad \text{for } k=2,3,\ldots, \tag{4.4}$$

$$\mathscr{H}_0=\mathscr{E}, \tag{4.5}$$

$$\mathscr{H}_k\subset\mathscr{H}_{k-1} \quad \text{for } k=1,2,\ldots, \tag{4.6}$$

$$\mathscr{H}_k\cap(0,g_k/2)=\mathscr{H}_{k-1}\cap(0,g_k/2) \quad \text{for } k=1,2,\ldots, \tag{4.7}$$

$$r_1(\mathscr{H}_k,g_k)=f_k \quad \text{for } k=1,2,\ldots, \tag{4.8}$$

$$r_1(\mathscr{H}_k,n) > \frac{c_7}{2}\log n \quad \text{for } n>n_0, n\notin\{g_1,g_2,\ldots,g_k\} \tag{4.9}$$

(where c_7 and n_0 are defined in Lemma 1). Then clearly, the set

$$\mathscr{A}=\bigcap_{k=0}^{+\infty}\mathscr{H}_k$$

satisfies

$$r_1(\mathscr{A},g_k)=f_k \quad \text{for } k=1,2,\ldots$$

and

$$r_1(\mathscr{A},n) > \frac{c_7}{2}\log n \quad \text{for } n>n_0, n\notin\mathscr{G},$$

whence, by the definition of $f_1, f_2, \ldots$, it follows that this set $\mathscr{A}$ satisfies (4.1).

To construct this $\mathscr{G}$ and $\mathscr{H}_0, \mathscr{H}_1, \ldots$, first define $\mathscr{H}_0$ by (4.5). Assume now that $k \in \mathbb{N}$ and $\mathscr{H}_0, \mathscr{H}_1, \ldots, \mathscr{H}_{k-1}$ and (if $k > 1$) $g_1, g_2, \ldots, g_{k-1}$ have been defined so that also

$$r_1(\mathscr{H}_i, n) \geqslant r_1(\mathscr{H}_{i-1}, n) - c_9 \geqslant r_1(\mathscr{E}, n) - c_9 i$$
$$\text{for } k > 1,\ i = 1, 2, \ldots, k-1,\ n \geqslant g_i/2,\ n \neq g_i\,. \tag{4.10}$$

Then let g_k be the smallest integer with the following properties (n_0, c_7 and c_9 are defined in Lemma 1):

$$g_k > \begin{cases} 2n_0 & \text{if } k = 1, \\ 2g_{k-1} & \text{if } k > 1, \end{cases} \tag{4.11}$$

$$\frac{c_7}{2} \log(g_k/2) > f_k + c_9 k \tag{4.12}$$

and

$$g_i is \begin{cases} \text{odd if } f_k \text{ is even}, \\ \text{even and } g_k/2 \in \mathscr{H}_{k-1} \text{ if } f_k \text{is odd}\,. \end{cases} \tag{4.13}$$

It follows from (4.2), (4.10), (4.11) and (4.12) that

$$r_1(\mathscr{H}_{k-1}, g_k) \geqslant r_1(\mathscr{E}, g_k) - c_9(k-1) > c_7 \log g_k - c_9(k-1) > 2f_k\,.$$

Thus denoting the integers h with $h \in \mathscr{H}_{k-1}$, $g_k/2 < h < g_k$, $h \in \mathscr{T}(\mathscr{H}_{k-1}, g_k)$ by $h_1 < h_2 < \cdots < h_x$, we have $x \geqslant [f_k/2]$. Let $\mathscr{L}_k = \{h_{[f_k/2]+1}, h_{[f_k/2]+2}, \ldots, h_x\}$, and define $\mathscr{H}_k$ by

$$\mathscr{H}_k = \mathscr{H}_{k-1} \backslash \mathscr{L}_k\,.$$

Then (4.4), (4.5), (4.6), (4.7) and (4.8) hold trivially. Moreover, it follows from $\mathscr{L}_k \subset \mathscr{T}(\mathscr{H}_{k-1}, g_k) \subset \mathscr{T}(\mathscr{E}, g_k)$ and (4.3) (with $m = g_k$) that (4.10) holds also with k in place of i. Finally, we have

$$r_1(\mathscr{H}_k, n) = r_1(\mathscr{H}_{k-1}, n) \quad \text{for } n < g_k/2$$

and it follows from (4.2), (4.10), (4.11) and (4.12) that

$$r_1(\mathscr{H}_k, n) \geqslant r_1(\mathscr{H}_{k-1}, n) - c_9 \geqslant r_1(\mathscr{E}, n) - c_9 k$$
$$> c_7 \log n - c_9 k > \frac{c_7}{2} \log n \quad \text{for } g_k/2 \leqslant n, n \neq g_k$$

which proves also (4.9) and this completes the proof of Theorem 12. □

Note that in the proof of Theorem 12, we constructed a solution $\mathscr{A}$ of (4.1) (with $i = 1$) such that for almost all n we have $r_1(\mathscr{A}, n) \notin \mathscr{B}$ (indeed, we have $r_1(\mathscr{A}, n) \to +\infty$ on a set of density 1). The problem becomes much more difficult if we are looking for solutions $\mathscr{A}$ such that $r_1(\mathscr{A},n) \in \mathscr{B}$ apart from a 'thin' set of integers n.

Problem 16. For what sets $\mathscr{B} \subset N_0$ has Eq. (4.1) a solution $\mathscr{A}$ such that for almost all n we have $r_i(\mathscr{A},n) \in \mathscr{B}$?

Problem 17. For what sets $\mathscr{B} \subset \mathbb{N}_0$ has Eq. (4.1) a solution such that for $n > n_0$ we have $r_i(\mathscr{A},n) \in \mathscr{B}$?

Problem 17 seems to be very difficult. Indeed, Erdős and Turán conjectured long ago that if $r_1(\mathscr{A},n) \geqslant 1$ for $n > n_0$, then

$$\lim_{n\to+\infty} r_1(\mathscr{A},n) = +\infty .$$

This conjecture has not been settled yet, and at present it seems to be hopelessly difficult. Correspondingly, it cannot be decided whether there is a finite set $\mathscr{B} \subset \mathbb{N}$ such that $r_1(\mathscr{A},n) \in \mathscr{B}$ for $n > n_0$.

5.

So far we have studied sums $a + a'$. In the second half of this paper we will study differences $a - a'$. In particular, we will study the following questions:

(1) For what sequences $\lambda_1, \lambda_2, \ldots$ of nonnegative integers can one find a set $\mathscr{A} \subset \mathbb{N}_0$ such that

$$f(\mathscr{A},d) = \lambda_d \tag{5.1}$$

for all $d \in \mathbb{N}$?

(2) For what sets $\mathscr{B} \subset \mathbb{N}$ can one find a set $\mathscr{A} \subset \mathbb{N}_0$ such that

$$\mathscr{D}(\mathscr{A}) = \mathscr{B}? \tag{5.2}$$

(3) Do there exist sets $\mathscr{B} \subset \mathbb{N}$ such that there is a set $\mathscr{A} \subset \mathbb{N}_0$ satisfying (5.2) and, apart from translation (replacing $\mathscr{A}$ by $\mathscr{A} + \{m\}$), this $\mathscr{A}$ is unique? If such sets $\mathscr{B}$ exist, then what conditions are needed to ensure the uniqueness of $\mathscr{A}$?

In each of these cases, it seems to be hopeless to give a complete answer. Instead, we will be looking for possibly general sufficient conditions.

As a partial answer to question 1, Grošek and Jajcay [16] proved the following theorem.

Theorem 13 (Grošek and Jajcay). *If λ_1, $\lambda_2, \ldots$ are integers such that*

$$\lambda_d \geqslant 2 \quad (\textit{for } d = 1,2,\ldots),$$

then there is a set $\mathscr{A}$ satisfying (5.1) *for all $d \in \mathbb{N}$.*

First we will sharpen this theorem:

Theorem 14. *If $\lambda_1, \lambda_2, \ldots$ are nonnegative integers such that for all $k \in \mathbb{N}$ there is an integer $n = n(k)$ with*

$$\lambda_d \geqslant 2 \quad \text{for } d = n-k, n-k+1, \ldots, n,$$

then there is a set $\mathscr{A}$ satisfying (5.1) *for all $d \in \mathbb{N}$.*

Note that the theorem could be extended easily to the case when also $\lambda_d = +\infty$ is allowed (i.e., for some d's (5.1) must have infinitely many solutions); however, to simplify the discussion here we restrict ourselves to the case when all the λ's are finite.

It follows from Theorem 14 that if $\mathscr{B} \subset \mathbb{N}$ and $\mathscr{B}$ contains arbitrary long sequences of consecutive integers, then there is an $\mathscr{A} \subset \mathbb{N}_0$ with $\mathscr{D}(\mathscr{A}) = \mathscr{B}$:

Corollary 1. *If $\mathscr{B} \subset \mathbb{N}$ and for all $k \in \mathbb{N}$ there is an integer $n = n(k) \in \mathbb{N}$ with*

$$n - i \in \mathscr{B} \quad \text{for } i = 0, 1, \ldots, k,$$

then there is a set $\mathscr{A}$ satisfying (5.2).

Proof of Theorem 14. We will construct the elements $a_1 < a_2 < \cdots$ of $\mathscr{A}$ recursively.

Let d_0 denote the least integer d with $\lambda_d > 0$, and let $a_1 = 1, a_2 = a_1 + d_0 = 1 + d_0$.

Assume now that for some $i \in \mathbb{N}$, the numbers $a_1 < a_2 < \cdots < a_{2i}$ have been defined so that, writing $\mathscr{A}_i = \{a_1, a_2, \ldots, a_{2i}\}$,

(i) we have

$$f(\mathscr{A}_i, d) \leqslant \lambda_d \quad \text{for all } d \in \mathbb{N},$$

(ii) if j_i is defined by

$$\sum_{d=1}^{j_i} \lambda_d \leqslant i < \sum_{d=1}^{j_1+1} \lambda_d,$$

then we have

$$f(\mathscr{A}_i, d) = \lambda_d \quad \text{for } d = 1, 2, \ldots, j_i \tag{5.3}$$

and

$$\sum_{d=1}^{j_i+1} f(\mathscr{A}_i, d) = \sum_{d=1}^{j_i} \lambda_d + f(\mathscr{A}_i, j_i + 1) \geqslant i$$

(Note that by the definition of a_1 and a_2, both (i) and (ii) hold with $i = 1$.)

Then we define a_{2i+1} and a_{2i+2} in the following way:

Let r denote the smallest integer with

$$\lambda_r > f(\mathscr{A}_i, r)$$

By the assumption in the theorem, there is an integer n such that

$$n > 2a_{2i} + r \tag{5.4}$$

and

$$\lambda_d \geqslant 2 \quad \text{for } d = n - (a_{2i} + r), n - (a_{2i} + r) + 1, \ldots, n\,. \tag{5.5}$$

Then let $a_{2i+1} = n - r, a_{2i+2} = n$,

$$\mathscr{A}_{i+1} = \mathscr{A}_i \cup \{a_{2i+1}, a_{2i+2}\} = \{a_1, a_2, \ldots, a_{2i+2}\}\,.$$

It is easy to see that the differences $a - a'$ with $a, a' \in \mathscr{A}_{i+1}$, $a > a'$, $a \notin \mathscr{A}_i$ (so that $a = a_{2i+1}$ or $a = a_{2i+2}$) assume the following values:

(a) $a - a' = r$ for $a = a_{2i+2}, a' = a_{2i+1}$;

(b) $a - a'$ assumes one of the values

$$(a_{2i+1} - a_{2i} =) n - (a_{2i} + r),\ n - (a_{2i} + r) + 1, \ldots, a_{2i+2} - a_1\,,$$

and each of these values is assumed only by at most two differences $a - a'$ of this type. Note that in this case, by (5.4) we have

$$a - a' \geqslant n - (a_{2i} + r) > a_{2i}$$

and thus $a - a' \notin \mathscr{D}(\mathscr{A}_i)$.

(a) and (b) imply that

$$f(\mathscr{A}_{i+1}, r) = f(\mathscr{A}_i, r) + 1\,, \tag{5.6}$$

$$0 \leqslant f(\mathscr{A}_{i+1}, d) \leqslant 2 \quad \text{for } n - (a_{2i} + r) \leqslant d \leqslant n \tag{5.7}$$

and

$$f(\mathscr{A}_{i+1}, d) = f(\mathscr{A}_i, d) \quad \text{if } d \in \mathbb{N},\ d \neq r,$$
$$d \notin \{n - (a_{2i} + r), n - (a_{2i} + r) + 1, \ldots, n\}\,. \tag{5.8}$$

By the definition of n, it follows from (5.6), (5.7) and (5.8) that (i) and (ii) hold also with $i + 1$ in place of i, and this completes the construction.

Finally, it follows from (5.3) that the set $\mathscr{A}$ defined in this way satisfies (5.1) and this completes the proof of Theorem 14. □

Proof of Corollary 1. This follows from Theorem 14 by choosing

$$\lambda_d = \begin{cases} 2 & \text{for } d \in \mathscr{B}, \\ 0 & \text{for } d \notin \mathscr{B}\,. \quad \square \end{cases} \tag{5.9}$$

6.

The method of the proof of Theorem 14 is similar to the one used by Grošek and Jajcay in [16], and in both cases, there are differences $d \in \mathscr{D}(\mathscr{A})$ such that representing them in the form $a - a' = d$, the numbers a and a' are large in terms of d. One might like to know whether this must be so or this is only a weakness of the method and, perhaps, having the additional assumption that $\mathscr{B}$ is 'dense', for a given $\mathscr{B}$ one can also find an $\mathscr{A}$ such that $\mathscr{D}(\mathscr{A}) = \mathscr{B}$, and for all $b \in \mathscr{B}$, the equation $a - a' = b$ has at least one solution a, a' 'not very large' in terms of b. We will show

Theorem 15. *Assume that the function $F(x)$ is nonnegative in $0 < x < +\infty$ and $\lim_{x\to+\infty} F(x) = +\infty$. Then there is an infinite set $\mathscr{B} \subset \mathbb{N}$ such that*

(i) *the asymptotic density $d(\mathscr{B})$ of $\mathscr{B}$ exists and*

$$d(\mathscr{B}) = 1; \tag{6.1}$$

(ii) *there is an $\mathscr{A} \subset \mathbb{N}$ such that*

$$\mathscr{D}(\mathscr{A}) = \mathscr{B}; \tag{6.2}$$

(iii) *if $\mathscr{A}$ satisfies* (6.2), *then for infinitely many $b \in \mathscr{B}$,*

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

implies $a > F(b)$.

Proof. (6.1) implies that $\mathscr{B}$ contains arbitrarily long blocks of consecutive integers, so that by Corollary 1, it follows from (6.1) that there is an $\mathscr{A}$ satisfying (6.2). Thus it suffices to show that there is a set $\mathscr{B}$ satisfying properties (i) and (iii).

First define the integers $n_1 < n_2 < \cdots, d_1 < d_2 < \cdots$ by the following recursion: Let $n_1 = 2$, $d_1 = 3$. If $k \in \mathbb{N}$ and $n_1, n_2, \ldots, n_k, d_1, d_2, \ldots, d_k$ have been defined, then let

$$n_{k+1} = \max\left(\max_{d_k^2 < d \leqslant 2d_k^2} [F(d)] + 1, 2d_k^2\right)$$

and $d_{k+1} = n_{k+1} + 1$. Let $\mathscr{B}_1 = \{1, 2\}$, and for $k \in \mathbb{N}$ let

$$\mathscr{B}_{k+1} = \{b : b \in \mathbb{N}, n_k < b \leqslant n_{k+1}, d_k \nmid b\}.$$

Finally, let

$$\mathscr{B} = \bigcup_{k=1}^{+\infty} \mathscr{B}_k .$$

We will show that this set $\mathscr{B}$ satisfies both (i) and (iii) in the theorem.

Clearly, for $k, n \in \mathbb{N}$, $n_k < n \leqslant n_{k+1}$ we have

$$B(n) - B(n_k) = B_{k+1}(n) \geqslant (n - n_k)\left(1 - \frac{1}{d_k}\right) - 1 .$$

Thus by

$$\lim_{k \to +\infty} n_{k+1}/n_k = +\infty ,$$

for $n \to +\infty$ and defining k by $n_k < n \leqslant n_{k+1}$ we have

$$\begin{aligned} B(n) &\geqslant (B(n) - B(n_k)) + (B(n_k) - B(n_{k-1})) \\ &\geqslant (n - n_k)\left(1 - \frac{1}{d_k}\right) - 1 + (n_k - n_{k-1})\left(1 - \frac{1}{d_{k-1}}\right) - 1 \\ &\geqslant (n - n_{k-1})\left(1 - \frac{1}{d_{k-1}}\right) - 2 = (n - \mathrm{o}(n))\left(1 - \frac{1}{d_{k-1}}\right) - 2 \\ &= n - \frac{n}{d_{k-1}} - \mathrm{o}(n) = n - \mathrm{o}(n) \end{aligned}$$

which proves (i).

In order to prove (iii), assume that $\mathscr{A} = \{a_1, a_2, \ldots\}$ (where $a_1 < a_2 < \cdots$) satisfies (6.2). First we will show that this implies

$$A(n_{k+1}) \leqslant d_k \quad (\text{for } k \in \mathbb{N}) . \tag{6.3}$$

Indeed, assume that contrary to this assertion we have

$$a_{d_k+1} \leqslant n_{k+1} .$$

Then by the pigeon hole principle, there exist i, j such that

$$(a_1 \leqslant) a_i < a_j \leqslant n_{k+1}$$

and

$$a_i \equiv a_j \pmod{d_k} .$$

Then in view of (6.2) we have

$$a_j - a_i \in \mathscr{D}(\mathscr{A}) = \mathscr{B} , \tag{6.4}$$

$$a_j - a_i < n_{k+1} \tag{6.5}$$

and

$$d_k \mid (a_j - a_i) . \tag{6.6}$$

On the other hand, by the construction of $\mathscr{B}$, there is no b with $b \in \mathscr{B}, b \leqslant n_{k+1}, d_k | b$. This contradicts (6.4), (6.5) and (6.6), and this contradiction proves (6.3).

It follows from (6.3) that

$$|\mathscr{D}(\mathscr{A}\cap\{1,2,\ldots,n_{k+1}\})| \leqslant \binom{A(n_{k+1})}{2} \leqslant \binom{d_k}{2} < \frac{d_k^2}{2}. \tag{6.7}$$

By (6.1), for $k \to +\infty$ we have

$$B(2d_k^2) - B(d_k^2) = (1+o(1))d_k^2. \tag{6.8}$$

It follows from (6.7) and (6.8) that for k large enough there is a b such that

$$b \in \mathscr{B}, \tag{6.9}$$

$$d_k^2 < b \leqslant 2d_k^2 \tag{6.10}$$

and

$$b \notin \mathscr{D}(\mathscr{A}\cap\{1,2,\ldots,n_{k+1}\}). \tag{6.11}$$

By (6.11),

$$a - a' = b, \quad a, a' \in \mathscr{A} \tag{6.12}$$

implies that

$$a > n_{k+1}. \tag{6.13}$$

By the definition of n_{k+1}, it follows from (6.10) and (6.13) that

$$a > [F(b)] + 1 > F(b). \tag{6.14}$$

Thus for every large k there is a b such that (6.9) and (6.10) hold, and (6.12) implies (6.14) which proves (iii) and this completes the proof of the theorem. □

7.

Note that in the construction of the set $\mathscr{B}$ in the proof of Theorem 15, the order of magnitude of $n - B(n)$ depends on the function $F(x)$. This dependence cannot be eliminated, i.e., (i) in Theorem 15 cannot be sharpened as the following theorem shows:

Theorem 16. *If the function $F(x)$ is nonnegative in $0 < x < +\infty$ and $\lim_{x\to+\infty} F(x) = +\infty, \lim_{x\to+\infty}(F(x)/x) = 0$, then there is a function $G(x)$, defined in $0 < x < +\infty$, with the following properties:*
If $\mathscr{B} \subset \mathbb{N}$ and

$$x - B(x) \leqslant F(x) \quad \textit{for all } x > 0, \tag{7.1}$$

then there is a set $\mathscr{A} \subset \mathbb{N}$ such $\mathscr{D}(\mathscr{A}) = \mathscr{B}$ and for all $b \in \mathscr{B}$,

$$a - a' = b, \quad a, a' \in \mathscr{A}$$

can be solved with

$$a < G(b).$$

Proof. The proofs of Theorem 14 and Corollary 1 give this result. Indeed, all one has to observe is the following: defining the λ's by (5.9), for the smallest n satisfying (5.4) and (5.5) one can give an upper bound depending only on i and the function $F(x)$ in (7.1). □

8.

If ε is a set of positive integers and there is a set $\mathscr{A}$ of nonnegative integers such that

$$\mathscr{D}(\mathscr{A}) = \mathscr{E}, \tag{8.1}$$

then we say that $\mathscr{E}$ can be difference represented, and (8.1) is said to be a difference representation of $\mathscr{E}$. If $\mathscr{A} = \{a_1, a_2, \ldots\}, \mathscr{B} = \{b_1, b_2, \ldots\}$ are sets of nonnegative integers such that one of them can be obtained from the other one by a translation, i.e., there is an integer m with $a_n + m = b_n$ for $n = 1, 2, \ldots$, then the sets $\mathscr{A}$, $\mathscr{B}$ are said to be equivalent. If the set $\mathscr{E}$ of positive integers can be difference represented, and

$$\mathscr{D}(\mathscr{A}) = \mathscr{D}(\mathscr{B}) = \mathscr{E}$$

implies that $\mathscr{A}$ and $\mathscr{B}$ are equivalent, then we say that the difference representation of $\mathscr{E}$ is unique.

One might like to study difference sets whose difference representation is unique. The first question to answer is whether there is a difference set $\mathscr{E}$ whose difference representation is unique. If such a set $\mathscr{E}$ exists, then when is the difference representation of a difference set unique? Is it true that if a difference set is 'thin' in a well-defined sense, then its difference representation is unique? How 'dense' can be a difference set with a unique difference representation? The following theorem provides a partial answer to some of these questions:

Theorem 17. *If $\mathscr{A}$ is an infinite B_3 set of nonnegative integers with*

$$0 \in \mathscr{A}, \tag{8.2}$$

and $\mathscr{B}$ is a set of nonnegative integers with

$$\mathscr{D}(\mathscr{B}) = \mathscr{D}(\mathscr{A}) \tag{8.3}$$

and

$$0 \in \mathscr{B}, \tag{8.4}$$

then we have $\mathscr{B} = \mathscr{A}$.

Note that by the greedy algorithm, there is an infinite B_3 set $\mathscr{A}$ with

$$A(n) \gg n^{1/5}.$$

Then writing $\mathscr{D}(\mathscr{A}) = \mathscr{E}$, we have

$$E(n) \gg n^{2/5}$$

so that there is an infinite difference set $\mathscr{E}$ with unique difference representation whose counting function grows like $n^{2/5}$.

Proof of Theorem 17. Assume that $\mathscr{B}$ satisfies (8.3) and (8.4), and write $\mathscr{A} = \{a_0, a_1, \ldots\}, \mathscr{B} = \{b_0, b_1, \ldots\}$ where $a_0 = 0 < a_1 < a_2 < \cdots, b_0 = 0 < b_1 < b_2 < \cdots$

Clearly, the assumption that $\mathscr{A}$ is a B_3 set implies that

$$\mathscr{A} \text{ is a } B_2 \text{ set} \tag{8.5}$$

as well. It follows from (8.5) that

$$0 < a_x - a_y = a_u - a_v \quad \text{implies } x = u, y = v. \tag{8.6}$$

Now we will show that

$$\mathscr{B} \subseteq \mathscr{A}. \tag{8.7}$$

Assume that $b_i \in \mathscr{B}$. Then by (8.3) and (8.4), we have

$$b_i = b_i - b_0 \in \mathscr{D}(\mathscr{B}) = \mathscr{D}(\mathscr{A})$$

so that by the definition of $\mathscr{D}(\mathscr{A})$, there are $u = u(i), v = v(i)$ such that $b_i = a_u - a_v$:

$$\text{for all } b_i \in \mathscr{B}, \text{there are } a_u, a_v \in \mathscr{A} \text{ with } b_i = a_u - a_v. \tag{8.8}$$

Note that by (8.6), b_i determines a_u and a_v in (8.8) uniquely.

We will prove (8.7) by contradiction. Assume that for some $b_i \in \mathscr{B}$, we have

$$b_i \notin \mathscr{A}. \tag{8.9}$$

Then by (8.2), (8.4), (8.8) and (8.9), b_i can be represented in the form

$$b_i = a_u - a_v, \quad a_u \in \mathscr{A},\ a_v \in \mathscr{A},\ u > v > 0. \tag{8.10}$$

Let us consider all the pairs (u,v) which satisfy (8.10) for some $b_i \in \mathscr{B}$, and let (u_0, v_0) denote the pair (u,v) for that $a_u - a_v$ is minimal. (Note that the pair (u_0, v_0) is unique by (8.6).) Write

$$a_{u_0} - a_{v_0} = b_{i_0}, \tag{8.11}$$

so that

$$0 < v_0 < u_0. \tag{8.12}$$

Now we will show that every

$$b_i \in \mathscr{B}, \qquad b_i > 0 \tag{8.13}$$

is of the form either

$$b_i = a_x - a_{v_0}, \quad x \geqslant u_0 \tag{8.14}$$

or

$$b_i = a_{u_0} - a_y, \quad y > v_0 . \tag{8.15}$$

In fact, by (8.8), (8.13) implies that there are u, v with

$$b_i = a_u - a_v, \quad u > v . \tag{8.16}$$

By (8.11), b_{i_0} is of the form (8.14), thus we may assume that

$$i \neq i_0$$

Then we have either

$$0 < b_i - b_{i_0} \in \mathscr{D}(\mathscr{B}) = \mathscr{D}(\mathscr{A})$$

or

$$0 < b_{i_0} - b_i \in \mathscr{D}(\mathscr{B}) = \mathscr{D}(\mathscr{A})$$

so that, by the definition of $\mathscr{D}(\mathscr{A})$, there exist $a_z \in \mathscr{A}$, $a_t \in \mathscr{A}$ such that

$$b_i - b_{i_0} = a_z - a_t \tag{8.17}$$

and

$$z \neq t . \tag{8.18}$$

It follows from (8.11), (8.16) and (8.17) that

$$b_i - b_{i_0} = (a_u - a_v) - (a_{u_0} - a_{v_0}) = a_z - a_t$$

whence

$$a_u + a_{v_0} + a_t = a_z + a_v + a_{u_0} . \tag{8.19}$$

Since $\mathscr{A}$ is a B_3 set, it follows from (8.12), (8.16), (8.18) and (8.19) that either

$$a_u = a_z, \qquad a_{v_0} = a_v, \qquad a_t = a_{u_0} \tag{8.20}$$

or

$$a_u = a_{u_0}, \qquad a_{v_0} = a_z, \qquad a_t = a_v . \tag{8.21}$$

In case (8.20), (8.14) holds with $x = z$, while in case (8.21), (8.15) holds with $y = t$ so that, indeed, (8.13) implies either (8.14) or (8.15).

Now we will show that (8.15) cannot occur, i.e., (8.13) implies that b_i is of the form (8.14). We will prove this by contradiction: assume that there are p, q with

$$0 < p, \tag{8.22}$$

$$v_0 < q < u_0, \tag{8.23}$$

$$b_p = a_{u_0} - a_q \tag{8.24}$$

(note that $q < u_0$ follows from (8.22) and (8.24)). (8.13) and (8.15) imply that $v_0 < y < u_0$, thus there are only finitely many b_i's of the form (8.15).
On the other hand, since $\mathscr{A}$ is infinite, thus $\mathscr{D}(\mathscr{A}) = \mathscr{D}(\mathscr{B})$ is infinite, so that $\mathscr{B}$ must be infinite as well. It follows that there are infinitely many b_i's of the form (8.14); thus there are r, s with

$$b_r = a_s - a_{v_0}, \tag{8.25}$$

$$s > u_0, \tag{8.26}$$

$$r > p. \tag{8.27}$$

Then by (8.24) and (8.25) we have

$$b_r - b_p = (a_s - a_{v_0}) - (a_{u_0} - a_q). \tag{8.28}$$

On the other hand, by (8.27) and $b_r - b_p \in \mathscr{D}(\mathscr{B}) = \mathscr{D}(\mathscr{A})$ there exist f, g with

$$b_r - b_p = a_f - a_g, \tag{8.29}$$

$$f > g. \tag{8.30}$$

It follows from (8.28) and (8.29) that

$$a_s + a_q + a_g = a_f + a_{v_0} + a_{u_0}. \tag{8.31}$$

Since $\mathscr{A}$ is a B_3 set, (8.12), (8.26) and (8.31) imply that

$$a_s = a_f \tag{8.32}$$

so that

$$a_q + a_g = a_{v_0} + a_{u_0}.$$

By (8.23), here we have $q \neq v_0$, $q \neq u_0$ which contradicts (8.5), and this proves that every b_i with (8.13) is of the form (8.14).

Now consider an arbitrary $a_w \in \mathscr{A}$ with

$$w > 0. \tag{8.33}$$

By

$$a_w = a_w - a_0 \in \mathscr{D}(\mathscr{A}) = \mathscr{D}(\mathscr{B}),$$

a_w can be represented in the form

$$a_w = b_u - b_v \quad \text{with } b_u, b_v \in \mathscr{B}. \tag{8.34}$$

Assume first that $b_v = b_0 = 0$. Then by (8.33),

$$a_w = b_u > 0$$

and thus a_w can be represented in form (8.14):

$$a_w = b_u = a_k - a_{v_0}$$

for some $k > v_0$ whence

$$a_w + a_{v_0} = a_k = a_k + a_0 .$$

By (8.5) and (8.33), it follows that $w = k, v_0 = 0$ which contradicts (8.12).

Assume now that in (8.34) we have

$$u > v > 0 .$$

Then both b_u and b_v can be represented in form (8.14):

$$b_u = a_k - a_{v_0}, \qquad b_v = a_l - a_{v_0} \tag{8.35}$$

for some

$$k > l > v_0 \quad (> 0). \tag{8.36}$$

Then by (8.34) and (8.35) we have

$$a_w = b_u - b_v = (a_k - a_{v_0}) - (a_l - a_{v_0}) = a_k - a_l$$

whence

$$a_w + a_l = a_k = a_k + a_0 .$$

Then by (8.5) and (8.33), it follows that $w = k$, $l = 0$ which contradicts (8.36). Thus indeed, (8.9) leads to a contradiction which completes the proof of (8.7).

It remains to show that there is no $a_i \in \mathscr{A}$ with

$$a_i \notin \mathscr{B} . \tag{8.37}$$

Assume that contrary to this assertion, there is an i satisfying (8.37). It follows from (8.4) and (8.37) that

$$i > 0 . \tag{8.38}$$

Clearly we have

$$a_i = a_i - a_0 \in \mathscr{D}(\mathscr{A}) = \mathscr{D}(\mathscr{B}),$$

thus a_i can be represented in the form

$$a_i = b - b' \quad \text{with } b, b' \in \mathscr{B}. \tag{8.39}$$

By (8.7), there exist m, n such that $b = a_m$, $b' = a_n$ so that

$$a_i = b - b' = a_m - a_n$$

whence

$$a_i + a_n = a_m = a_m + a_0 .$$

By (8.5) and (8.38), it follows that $n = 0$ so that $b' = a_n = a_0 = 0$ and thus by (8.39),

$$a_i = b - b' = b \in \mathscr{B}$$

which contradicts (8.37) and this completes the proof of the theorem. □

References

[1] N. Alon and P. Erdős, An application of graph theory to additive number theory, European J. Combin. 6 (1985) 201–203.
[2] R. Balasubramanian, A note on a result of Erdős, Sárközy and Sós, Acta Arithmetica 49 (1987) 45–53.
[3] P. Erdős, Problems and results in additive number theory, Colloque sur la Théorie des Nombres (CBRM) (Bruxelles, 1956) 127–137.
[4] P. Erdős, Some applications of Ramsey's theorem to additive number theory, European J. Combin. 1 (1980) 43–46.
[5] P. Erdős, M.B. Nathanson and P. Tetali, Independence of solution sets and minimal asymptotic bases, preprint.
[6] P. Erdős, J. Nešetřil and V. Rödl, On Pisier type problems and results (Combinatorial applications to number theory), in: J. Nešetřil and V. Rödl, eds., Mathematics of Ramsey Theory, Algorithms and Combinatorics Vol. 5 (Springer, Berlin, 1990) 214–231.
[7] P. Erdős and A. Sárközy, Problems and results on additive properties of general sequences, I, Pacific J. 118 (1985) 347–357.
[8] P. Erdős and A. Sárközy, Problems and results on additive properties of general sequences, II, Acta Math. Hungar. 48 (1986) 201–211.
[9] P. Erdős, A. Sárközy and V.T. Sós, Problems and results on additive properties of general sequences, IV, in: Number Theory, Proceedings, Ootacamund, India, 1984, Lecture Notes in Mathematics Vol. 1122 (Springer, Berlin, 1985) 85–104.
[10] P. Erdős, A. Sárközy and V.T. Sós, Problems and results on additive properties of general sequences, V, Monatshefte Math. 102 (1986) 183–197.
[11] P. Erdős, A. Sárközy and V.T. Sós, Problems and results on additive properties of general sequences, III, Studia Sci. Math. Hungar. 22 (1987) 53–63.
[12] P. Erdős, A. Sárközy and V.T. Sós, On sum sets of Sidon sets, I, J. Number Theory, to appear.
[13] P. Erdős, A. Sárközy and V.T. Sós, On sum sets of Sidon sets, II, Israel J. Math., to appear.
[14] P. Erdős P. Tetali, Representations of integers as the sum of k terms, Random Structures and Algorithms 1 (1990) 245–261.

[15] G.A. Freiman, Foundations of a Structural Theory of Set Additions, Translations of Mathematical Monographs 37 (Amer. Math. Soc., Providence, RI, 1973).
[16] O. Grošek and R. Jajcay, Generalized difference sets on infinite cyclic semigroup, preprint.
[17] H. Halberstam and K.F. Roth, Sequences (Springer, New York, 1983).
[18] M.B. Nathanson, Representation functions of sequences in additive number theory, Proc. Amer. Math. Soc. 72 (1978) 16–20.
[19] V.T. Sós, An additive problem in different structures, in: ed:, Y. Alavi et al., Graph Theory, Combinatorics, Algorithms, and Applications (SIAM, Philadelphia, 1991).