Martin Máčaj; Milan Paštéka; Tibor Šalát; Marek Žabka

On difference sets of sets of positive integers

Mathematica Slovaca, Vol. 53 (2003), No. 2, 129--144

Persistent URL: http://dml.cz/dmlcz/136880

Math. Slovaca, **53** (2003), No. 2, 129–144

Mathematica
Slovaca

ON DIFFERENCE SETS OF SETS OF POSITIVE INTEGERS

Martin Máčaj* — Milan Paštéka** — Tibor Šalát* — Marek Žabka*

(*Communicated by Stanislav Jakubec*)

ABSTRACT. The relation between densities of sets $A \subset \mathbb{N} = \{1, 2, \dots n, \dots\}$ and their difference sets is studied in this paper. Further, using dyadic values of sets $A \subset \mathbb{N}$, some properties of difference bases of various types are investigated here.

Introduction and notation

The concept of a difference set (distance set) of a set was introduced and studied originally for sets of real numbers (cf. [15]). If $A, B \subset \mathbb{R}$ (or $A, B \subset \mathbb{N}$), then we put

$$D(A, B) = \{x - y : \ x \in A, \ \ y \in B\}.$$

If $A = B$, then we write $D(A)$ instead of $D(A, A)$.

In [15] a fundamental result for difference sets of sets of real numbers is proved.

If $A \subset \mathbb{R}$ is a set of positive Lebesgue measure, then the set $D(A)$ contains an interval of the form $(-\eta, \eta)$, $\eta > 0$.

This result was extended in various directions (see e.g. [5], [6], [8], [9], [11], [14]).

Difference sets $D(A)$ for $A \subset \mathbb{N}$ are investigated in [13]. It was proved here that if the upper asymptotic density of a set $A \subset \mathbb{N}$ is greater than $\frac{1}{2}$, then each integer z can be expressed in infinitely many ways in the form $z = x - y$, where $x, y \in A$.

The study of difference sets $A \subset \mathbb{N}$ suggested the introduction of several types of difference bases (cf. [3], [16]). These bases will be studied in the second section of the paper.

2000 Mathematics Subject Classification: Primary 11B05, 11B13.
Keywords: asymptotic density, uniform density, difference set.

As usual we put for $A \subset \mathbb{N}$:

$$A(n) = \operatorname{card}\big(\{1,2,\dots,n\} \cap A\big)\,,$$
$$\underline{d}(A) = \liminf_{n\to\infty} \frac{A(n)}{n}\,, \qquad \overline{d}(A) = \limsup_{n\to\infty} \frac{A(n)}{n}$$

(the *lower* and *upper asymptotic density* of A). If $\underline{d}(A) = \overline{d}(A)$, then we set

$$d(A) = \underline{d}(A) = \overline{d}(A)\,, \qquad d(A) = \lim_{n\to\infty} \frac{A(n)}{n}$$

(cf. [10; p. 70–71]). Observe that all these numbers belong to the interval $[0,1]$.

We recall the concept of uniform density of a set $A \subset \mathbb{N}$. For integers t, s, $t \geq 0$, $s \geq 1$, we put

$$A(t+1, t+s) = \operatorname{card}\big([t+1, t+s] \cap A\big)\,.$$

Further

$$\alpha_s = \liminf_{t\to\infty} A(t+1, t+s)\,, \qquad \alpha^s = \limsup_{t\to\infty} A(t+1, t+s)\,.$$

Then there exist

$$\underline{u}(A) = \lim_{s\to\infty} \frac{\alpha_s}{s}\,, \qquad \overline{u}(A) = \lim_{s\to\infty} \frac{\alpha^s}{s}\,.$$

If $\underline{u}(A) = \overline{u}(A)$, then we put

$$u(A) = \underline{u}(A) = \overline{u}(A)\,,$$

and $u(A)$ is called the *uniform density* of A (cf. [2]).

For every $A \subset \mathbb{N}$ we have

$$\underline{u}(A) \leq \underline{d}(A) \leq \overline{d}(A) \leq \overline{u}(A)\,, \tag{1}$$

and these numbers belong to $[0,1]$ (cf. [2]).

If $n \in \mathbb{N}$, then interval $(0,1]$ can be expressed as a union of intervals

$$i_n^{(k)} = \left(\frac{k}{2^n}, \frac{k+1}{2^n}\right]\,, \qquad 0 \leq k \leq 2^n - 1$$

(so called the intervals of the nth order).

To every $i_n^{(k)}$, a finite sequence

$$\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \tag{2}$$

of 0's and 1's corresponds in such a way that if $x \in i_n^{(k)}$, $x = \sum\limits_{j=1}^{\infty} c_j 2^{-j}$ (non-terminating dyadic expansion of x), then $c_j = \varepsilon_j$ $(j = 1,2,\dots,n)$. We say briefly that $i_n^{(k)}$ is *associated* with the sequence (2).

If $A \subset \mathbb{N}$ is an infinite set and

$$A = \{a_1 < a_2 < \cdots < a_n < \dots\},$$

then we put

$$\varrho(A) = \sum_{n=1}^{\infty} 2^{-a_n} \in [0,1].$$

The number $\varrho(A)$ is called the *dyadic value* of the set A. (Dualwert der Menge A, cf. [17]). This number can be written also in the form

$$\varrho(A) = \sum_{n=1}^{\infty} \varepsilon_n 2^{-n},$$

where ε_n is the characteristic function of the set A. (i.e. $\varepsilon_n = 1$ if $n \in A$ and $\varepsilon_n = 0$ otherwise.)

Denote by $\mathcal{U}$ the class of all infinite subsets of $\mathbb{N}$. Then $\varrho\colon \mathcal{U} \to (0,1]$, ($\varrho(A)$ is defined before) is a one-to-one mapping of $\mathcal{U}$ onto $(0,1]$.

For $\mathcal{S} \subset \mathcal{U}$ we set $\varrho(\mathcal{S}) = \{\varrho(A) : A \in \mathcal{S}\}$. The set $\varrho(\mathcal{S}) \subset (0,1]$ can be regarded as a means for "measuring" the magnitude of the class $\mathcal{S}$.

In what follows $\lambda(M)$ (for $M \subset \mathbb{R}$) stands for the Lebesgue measure of M, and $\dim M$ for the Hausdorff dimension of M.

This paper consists of two sections. In the first one we will deal with the relation between the densities of sets of positive integers and properties of related difference sets. Among other things, we improve the result of W. Sierpiński (cf. [13]). In the second section we will investigate the properties of some types of difference bases of the set $\mathbb{N}$ and $\mathbb{Z}$ (the set of all integers) and related sets $\varrho(\mathcal{S})$. $\mathcal{S}$ being the class of all difference bases of a given type.

1. Densities of sets of positive integers and properties of related difference sets

In [1] the following result is proved:

THEOREM B. *Let $A, B \subset \mathbb{N}$. Suppose that one of the following conditions is satisfied:*

(a) $d(A) > \frac{1}{2}$, $\overline{d}(B) > \frac{1}{2}$,
(b) $\overline{d}(A) > \frac{1}{2}$, $d(B) > \frac{1}{2}$.

Then, for every $z \in \mathbb{Z}$, there exist infinitely many pairs $(x,y) \in A \times B$ such that $z = x - y$.

We improve the previous theorem and prove that it is the best in some sense (see Remark after Theorem 1.1).

THEOREM 1.1. *Let* $A, B \subset \mathbb{N}$ *satisfy one of the following conditions:*

(i) $\overline{d}(A) + \underline{d}(B) > 1$,

(ii) $\underline{d}(A) + \overline{d}(B) > 1$.

Then for every $z \in \mathbb{Z}$ *there exist infinitely many pairs* $(x, y) \in A \times B$ *such that* $z = x - y$.

Proof. Suppose that (i) holds. Then

$$1 - \underline{d}(B) < \overline{d}(A),$$

and so we can choose numbers t_1, t_2 such that

$$1 - \underline{d}(B) < t_1 < t_2 < \overline{d}(A). \tag{3}$$

We proceed indirectly. Assume that there is a $z \in \mathbb{Z}$ such that only for a finite number of pairs $(a, b) \in A \times B$ we have $z = a - b$. Then there exists a $b_0 \in B$ such that

$$(\forall b \in B)(b > b_0 \implies b + z \notin A). \tag{4}$$

Let $n > b_0$, $b_0 < b \leq n$, $b \in B$. Then $b + z \notin A$ by (4). The number of such b's is $B(n) - B(b_0)$. A simple estimation yields

$$A(n + |z|) \leq n + |z| - \big(B(n) - B(b_0)\big). \tag{5}$$

Further by (3) we get $\underline{d}(B) > 1 - t_1$. From this it follows that there exists an $n_1 \in \mathbb{N}$ such that

$$(\forall n)\left(n > n_1 \implies \frac{B(n)}{n} > 1 - t_1\right). \tag{6}$$

On the other hand (see (3)), $\overline{d}(A) > t_2$. This yields that an n_2 can be chosen in such a way that

$$n_2 > \max\left\{n_1, \frac{|z| + b_0}{t_2 - t_1}\right\} \tag{7}$$

and simultaneously

$$\frac{A(n_2)}{n_2} > t_2. \tag{7'}$$

Since $n_2 > n_1$, we get from (6)

$$\frac{B(n_2)}{n_2} > 1 - t_1. \tag{7''}$$

Summing (7′), (7″) we obtain

$$A(n_2) + B(n_2) > n_2(1 + t_2 - t_1). \tag{8}$$

By a simple estimation we can obtain from (5)

$$A(n_2) \leq A\big(n_2 + |z|\big) \leq n_2 + |z| - B(n_2) + b_0\,,$$

thus

$$A(n_2) + B(n_2) \leq n_2 + |z| + b_0\,. \tag{9}$$

From (8), (9) we have

$$n_2 < \frac{|z| + b_0}{t_2 - t_1}$$

contrary to (7).

The case (ii) can be proved similarly. □

Remark. Theorem 1.1 is the best possible in the sense that the equality

$$\overline{d}(A) + \underline{d}(B) = 1$$

is in general not sufficient for every $z \in \mathbb{Z}$ to be expressed in the form $z = x - y$ for infinitely many pairs $(x, y) \in A \times B$. To see it, we can choose

$$A = B = \{2, 4, \dots, 2k, \dots\}\,.$$

Then $d(A) + d(B) = 1$ and no odd number can be expressed in the mentioned form.

In [13], the following result is proved:

THEOREM S. *If $A \subset \mathbb{N}$ and $\overline{d}(A) > \frac{1}{2}$, then, for every $z \in \mathbb{Z}$, there exist infinitely many pairs $(x, y) \in A \times A$ such that $z = x - y$.*

We will improve this result by replacing $\overline{d}$ by $\overline{u}$ (see (1)).

THEOREM 1.2. *If $A \subset \mathbb{N}$ and $\overline{u}(A) > \frac{1}{2}$, then for every $z \in \mathbb{Z}$ there exist infinitely many pairs $(x, y) \in A \times A$ such that $z = x - y$.*

Proof. We prove the equivalent statement: If A does not have the property mentioned in Theorem 1.2, then $\overline{u}(A) \leq \frac{1}{2}$. Hence, suppose that there is an $l \in \mathbb{N}$ and only a finite number of pairs $(x, y) \in A \times A$ such that $l = x - y$. Then there exists an $n_0 \in \mathbb{N}$ such that, for $m > n_0$, at most one of the numbers m, $m + l$ belongs to A.

Consider the number $A(m+1, m+s)$ ($s \in \mathbb{N}$) of elements of A belonging to interval $[m+1, m+s]$. Put $s = 2kl + r$, $k \in \mathbb{N}$, $0 \leq r < 2l$. We can decompose the sequence $m+1, m+2, \dots, m+s$ into the pairs of sequences each having the length l and a rest sequence as follows:

$$\begin{array}{ll} m+1,\dots,m+l; m+l+1,\dots,m+2l & \text{the first pair}\,, \\ m+2l+1,\dots,m+3l; m+3l+1,\dots,m+4l & \text{the second pair}\,, \\ \vdots & \\ m+(2k-2)l+1,\dots,m+(2k-1)l; & \\ & \text{the } k\text{th pair}\,, \\ m+(2k-1)l+1,\dots,m+2kl & \\ m+2kl+1,\dots,m+2kl+r & \text{the rest sequence}\,. \end{array} \tag{10}$$

If a number $m+i$ $(1 \le i \le l)$ belonging to the first sequence of the length l belongs to A, then $m+l+i$ (belonging to the second sequence of the length l) does not belong to A, and conversely. Thus the number of elements of A belonging to the first pair of sequences (10) does not exceed the number l, i.e.

$$A(m+1, m+2l) \le l\,.$$

Similarly

$$A(m+2l+1, m+4l) \le l\,,$$
$$\vdots$$
$$A\big(m+(2k-2)l+1, m+2kl\big) \le l\,,$$

and trivially

$$A(m+2kl+1, m+2kl+r) \le 2l\,.$$

Summing these inequalities we get $A(m+1, m+s) \le kl + 2l$. Thus

$$\alpha^s = \limsup_{m\to\infty} A(m+1, m+s) \le (k+2)l\,,$$

and so

$$\frac{\alpha^s}{s} \le \frac{(k+2)l}{s} = \frac{(k+2)l}{2kl+r}\,, \tag{11}$$

where $0 \le r < 2l$. If $s \to \infty$, then $k \to \infty$, and from (11) we obtain

$$\overline{u}(A) = \lim_{s\to\infty} \frac{\alpha^s}{s} \le \frac{1}{2}\,.$$

□

The following example shows that the previous Theorem 1.2 is really an improvement of S z i e r p i n s k i's theorem from [13].

EXAMPLE. Put $A = \bigcup_{k=1}^{\infty} \{2^k + 1, \dots, 2^k + k\}$. Then it is easy to check that $d(A) = 0$. Hence Theorem of Sierpiński cannot be applied to A. But $\overline{u}(A) = 1$ and so by Theorem 1.2 each $z \in \mathbb{Z}$ can be expressed in the form $z = x - y$ for $x, y \in A$ in infinitely many manners.

In Theorem 1.2 we have applied the concept of uniform density of sets $A \subset \mathbb{N}$. This fact evokes the question whether an analogous application of this concept would be possible also in Theorem 1.1. In what follows we will give an affirmative answer to this question.

THEOREM 1.3. *Let $A, B \subset \mathbb{N}$ satisfy one of the following conditions:*

(i) $\overline{u}(A) + \underline{u}(B) > 1$,
(ii) $\underline{u}(A) + \overline{u}(B) > 1$.

Then, for every $z \in \mathbb{Z}$, there exist infinitely many pairs $(x, y) \in A \times B$ such that $z = x - y$.

Proof. Suppose that (i) holds. Then $1 - \underline{u}(B) < \overline{u}(A)$. Choose two numbers t_1, t_2 such that

$$1 - \underline{u}(B) < t_1 < t_2 < \overline{u}(A). \tag{12}$$

We proceed indirectly. Suppose that there is a $z \in \mathbb{Z}$ such that exists only a finite number of pairs $(a, b) \in A \times B$ with $z = a - b$. Then there is a $b_0 \in B$ such that

$$(\forall b > b_0)(b \in B \implies b + z \notin A). \tag{13}$$

From this we obtain for every $n > b_0 + z$

$$A(n+1, n+s) + B(n-z+1, n-z+s) \le s. \tag{14}$$

Further in virtue of (12) we have $\underline{u}(B) > 1 - t_1$. Hence

$$(\exists s_B)(\forall s > s_B)(\exists n(s))(\forall n > n(s))(B(n+1, n+s) > s(1-t_1)). \tag{15}$$

Further by (12) we have $\overline{u}(A) > t_2$. This yields

$$(\exists s_A)(\forall s > s_A)(\forall m)(\exists n > m)(A(n+1, n+s) > st_2). \tag{16}$$

Choose $s > \max\{s_A, s_B\}$ and $m > \max\{b_0 + z, n(s) + z\}$. Then by (16) we get for a suitable $n' > m$

$$A(n'+1, n'+s) > st_2, \qquad B(n'-z+1, n'-z+s) > s(1-t_1).$$

Summing these inequalities we get

$$A(n'+1, n'+s) + B(n'-z+1, n'-z+s) > s.$$

This contradicts (14).

Let (ii) holds. Let $z \in \mathbb{Z}$, then by the previous part we conclude that for $-z$ there are infinitely many pairs $(b, a) \in B \times A$ such that $-z = b - a$, i.e. $z = a - b$. The proof is finished. □

We finish this section with discussion about the assumptions of Theorem 1.1 and 1.3 and by showing that these theorems are in fact incomparable.

Choose $A = B = \{2, 4, \dots, 2n, \dots\}$. This shows that the strict inequalities in assumptions of Theorems 1.1, 1.3 cannot be replaced by the symbol $\geq$.

It is easy to show that the lower densities in these theorems cannot be replaced by upper densities. We show this by the following example.

EXAMPLE 1.1. Put

$$A = \bigcup_{k=1}^{\infty} \{2^{2^{2k}} + 1, \dots, 2^{2^{2k+1}} - 1\}$$

and

$$B = \bigcup_{k=1}^{\infty} \{2^{2^{2k+1}} + 1, \dots, 2^{2^{2k+2}} - 1\}.$$

Then

$$\frac{A(2^{2^{2k+1}})}{2^{2^{2k+1}}} \geq \frac{2^{2^{2k+1}} - 2^{2^{2k}} - 2}{2^{2^{2k+1}}} \longrightarrow 1$$

as $k \to \infty$. And so $\overline{d}(A) = 1$. Similarly $\overline{d}(B) = 1$, hence $\overline{u}(A) = \overline{u}(B) = 1$ (see (1)). So we get

$$\overline{u}(A) + \overline{u}(B) = \overline{d}(A) + \overline{d}(B) = 2 > 1,$$

but $D(A, B)$ does not contain 1, -1.

The question arises whether the assumptions formulated in Theorems 1.1 and 1.3 can be mixed. For instance suppose that

$$\overline{u}(A) + \underline{d}(B) > 1 \tag{a}$$

or

$$\underline{u}(A) + \overline{d}(B) > 1 \tag{b}$$

holds. We ask whether under (a) or (b) every $z \in \mathbb{Z}$ can be expressed in the form $z = a - b$, $a \in A$, $b \in B$ infinitely many ways.

In the case (b) we have (see (1)) $\underline{d}(A) + \overline{d}(B) > 1$, and so by Theorem 1.1 the answer to our question is yes.

In the case (a) the answer is no. Choose for instance the set A in such a way that its characteristic function $\chi_A = (\varepsilon_n)$ can expressed in the form $\chi_A = (0, 0^k, 0, 1^k)_{k=1}^{\infty}$, where a^k is the block $a, a, \dots, a$ (k-times).

Further put $\chi_B = (0, 1^k, 0, 0^k)_{k=1}^{\infty}$. Then it is easy to check that $\overline{u}(A) = 1$, $d(B) = \frac{1}{2}$, but 1, -1 do not belong to $D(A, B)$. Hence in this case the answer is negative.

The relation (1) does not enable to compare the condition

$$\underline{u}(A) + \overline{u}(B) > 1 \tag{a}$$

from Theorem 1.3 with the condition

$$\underline{d}(A) + \overline{d}(B) > 1 \tag{b}$$

from Theorem 1.1. We will construct a pair of sets A, B such that they satisfy (a) but not (b), and a pair of sets A, B such that they satisfy (b) but not (a).

EXAMPLE 1.2.

a) Choose A, B in such a way that $\chi_A = \left((01)^{2^k}(11)^k\right)_{k=1}^{\infty}$ and B is the set of all even numbers. Then $d(A) + d(B) = 1$, hence (b) is not satisfied, but $\overline{u}(A) + \underline{u}(B) = 1 + \frac{1}{2}$, hence (a) is satisfied.

b) Put now $\chi_A = \left((011)^{2^k}0^k\right)_{k=1}^{\infty}$ and $\chi_B = \left((01)^{2^k}0^k\right)_{k=1}^{\infty}$. Then $\underline{u}(A) + \overline{u}(B) = 0 + \frac{1}{2} < 1$, hence (a) is not satisfied, but the condition (b) is satisfied since $\underline{d}(A) + \overline{d}(B) = \frac{2}{3} + \frac{1}{2} > 1$.

2. Metric and topological properties of dyadic values

DEFINITION 2.1.

a) A set $A \subset \mathbb{N}$ is called a *difference basis* for $\mathbb{N}$ if $\mathbb{N} \subset D(A)$.

b) A set $A \subset \mathbb{N}$ is called a *strong difference basis* for $\mathbb{N}$ if for every $n \in \mathbb{N}$ there exist infinitely many pairs $(x, y) \in A \times A$ such that $n = x - y$.

c) A set $A \subset \mathbb{N}$ is called a *restricted difference basis* for $\mathbb{N}$ if for every $n \in \mathbb{N}$ there exists a pair $(x, y) \in A \times A$ such that $n = x - y$ and $y \leq \frac{x}{2}$.

(cf. [3])

The concept of a difference basis enables us to formulate Theorem 1.2 as follows:

PROPOSITION 2.1. *If $A \subset \mathbb{N}$ and $\overline{u}(A) > \frac{1}{2}$, then A is a strong difference basis for $\mathbb{N}$.*

Remark. Proposition 2.1 gives only a sufficient condition for a set $A \subset \mathbb{N}$ to be a strong difference basis for $\mathbb{N}$. There exist difference bases for $\mathbb{N}$ with zero densities. Take e.g. an arbitrarily slowly increasing sequence

$$a_1 < a_2 < \dots < a_n < \dots$$

of positive integers, $a_{n+1} - a_n > 1$, $n = 1, 2, \dots$, and put

$$A = \{a_1, a_1+1, a_2, a_2+2, \dots, a_k, a_k+k, \dots\}$$

(cf. [16]). A little modification of the construction of A gives an example of a strong difference basis for $\mathbb{N}$ with the asymptotic density 0.

In what follows, we denote by $\mathcal{D}$, $\mathcal{D}^*$, $\mathcal{D}_0$ the class of all difference bases, strong difference bases and restricted difference bases for $\mathbb{N}$, respectively. In this section, we will deal with the investigation of "the magnitude" of sets $\varrho(\mathcal{D})$, $\varrho(\mathcal{D}^*)$, $\varrho(\mathcal{D}_0)$. According the magnitude of these sets, we can judge about the magnitude of related classes $\mathcal{D}$, $\mathcal{D}^*$, $\mathcal{D}_0$, respectively.

Since $\mathcal{D}^* \subset \mathcal{D}$ and $\mathcal{D}_0 \subset \mathcal{D}$, we have

$$\varrho(\mathcal{D}^*) \subset \varrho(\mathcal{D}), \qquad \varrho(\mathcal{D}_0) \subset \varrho(\mathcal{D}). \tag{18}$$

In the first place, we will deal with the magnitude of the previous sets from the metric point of view. For this purpose we shall use the Lebesgue measure λ, Hausdorff dimension and the concept of the Baire's categories of sets. For this notions we refer to the classical monographs on the structure of real axis. Remark that the Hausdorff dimension is usually used as a means for classification of sets of Lebesgue measure 0 (cf. e.g. [19]). In the following the interval $(0, 1]$ will be recognized as a metric space with Euclidean metric.

THEOREM 2.1. *We have* $\lambda(\varrho(\mathcal{D}^*)) = 1$.

Then (18) yields:

COROLLARY. *We have* $\lambda(\varrho(\mathcal{D})) = 1$.

Proof of Theorem 2.1. Denote by $N^{(2)}$ the set of all dyadicaly normal numbers of the interval $(0, 1]$. Let $b_1, \dots, b_k$, $(k \geq 1)$ be a sequence of 0's and 1's. Such a sequence will be called a block. Let $x \in N^{(2)}$, $x = \sum\limits_{j=1}^{\infty} \varepsilon(x) 2^{-j}$ be the non-terminating dyadic expansion of x. Put $X_n = \varepsilon_1(x), \dots, \varepsilon_n(x)$. For an arbitrary block B_k with k terms, denote by $N(B_k, X_n)$ the number of occurrence of the block B_k in X_n. Then

$$\lim_{n \to \infty} \frac{N(B_k, X_n)}{n} = \frac{1}{2^k}$$

(cf. [10; p. 193]). From this we see that each block B_k occurs in the infinite sequence $\varepsilon_1(x),\dots,\varepsilon_n(x),\dots$ infinitely many times. Put

$$\mathcal{D}^2 = \{A \in \mathcal{U}:\ \varrho(A) \in N^{(2)}\}.$$

We show that

$$\mathcal{D}^2 \subset \mathcal{D}^*. \tag{19}$$

Let $A \in \mathcal{D}^2$, $m \geq 1$. Consider the block $B = 11\dots1$ consisting of $m+1$ ones. If $x = \varrho(A) = \sum_{j=1}^{\infty} c_j 2^{-j}$ is the dyadic expansion of $\varrho(A)$ (i.e. $c_k = 1$ if $k \in A$ and $c_k = 0$ if $k \in \mathbb{N} \setminus A$), then the block B occurs in the sequence $c_1, c_2, \dots, c_j, \dots$ infinitely many times. Hence there exists a sequence of positive integers $i_1 < i_2 < \dots < i_j < \dots$ such that $c_{i_j+r} = 1$ for $r = 1,\dots,m+1$, and $j = 1,2,\dots$. But then the numbers $i_j + r$ for $r = 1,\dots,m+1$, and $j = 1,2,\dots$ belong to A, and according to equality

$$m = i_j + m + 1 - (i_j + 1),$$

we see that the number m can be expressed as a difference of two numbers from A in infinite number of ways. From this $A \in \mathcal{D}^*$ follows. So the inclusion (19) is established. The theorem follows from it immediately with regard to the fact that $\lambda(N^{(2)}) = 1$ (cf. [10; p. 193]). $\square$

The previous theorem shows that "almost" all infinite subsets of $\mathbb{N}$ are strong difference bases for $\mathbb{N}$. In what follows we shall see that also from the topological point of view the class $\mathcal{D}^*$ can be considered a very rich class of subsets of $\mathbb{N}$.

For $\mathcal{S} \subset \mathcal{U}$ we put $\mathrm{C}\,\mathcal{S} = \mathcal{U} \setminus \mathcal{S}$. Since the mapping $\varrho = \mathcal{U} \to (0,1]$ is injective, we have $\varrho(\mathrm{C}\,\mathcal{S}) = (0,1] \setminus \varrho(\mathcal{S})$. Hence the sets $\varrho(\mathrm{C}\,\mathcal{D}^*) = (0,1] \setminus \varrho(\mathcal{D}^*)$, $\varrho(\mathrm{C}\,\mathcal{D}) = (0,1] \setminus \varrho(\mathcal{D})$ are null-sets by Theorem 2.1, i.e. $\lambda(\varrho(\mathrm{C}\,\mathcal{D}^*)) = 0 = \lambda(\varrho(\mathrm{C}\,\mathcal{D}))$. This fact evokes the question about the Hausdorff dimensions of these sets. We will give only some partial results in this direction.

Denote by $\mathcal{D}_k$ the class of all sets $A \subset \mathbb{N}$ with $k \in D(A)$. Then $\mathcal{D} = \bigcap_{k=1}^{\infty} \mathcal{D}_k$. By de Morgan's rule, we obtain

$$\mathrm{C}\,\mathcal{D} = \bigcup_{k=1}^{\infty} \mathrm{C}\,\mathcal{D}_k. \tag{20}$$

B o d o V o l k m a n in [20] studied the Hausdorff dimension of the sets given by the g-adic expansion of its elements. Remark that $x \in \varrho(\mathcal{D}_1)$ if and only if the block 11 does not occur in the dyadic expansion of x, thus directly from [20; p. 259, Satz 1]) Theorem 2.2 follows.

THEOREM 2.2. $\dim \varrho(\mathrm{C}\mathcal{D}_1) = \log_2(1+\sqrt{5}) - 1$.

Remark. Observe that $\log_2(1+\sqrt{5}) - 1 < 1$.

Using Theorem 2.2 we can determine $\dim \varrho(\mathrm{C}\mathcal{D})$. Let $\mathcal{D}_k$, $\mathrm{C}\mathcal{D}_k$ have the previous meaning. Hence

$$\mathrm{C}\mathcal{D}_k = \{A \in \mathcal{U} : k \notin D(A)\}, \qquad k = 1,2,\dots .$$

Thus if $x = \sum\limits_{i=1}^{\infty} c_i 2^{-i}$ belongs to $\varrho(\mathrm{C}\mathcal{D}_k)$, then $c_i = 1 \implies c_{i+k} = 0$, $i = 1,2,\dots$. If $i_n^{(j)}$ is an interval of the nth order, associated to a sequence

$$\varepsilon_1, \dots, \varepsilon_n ,$$

then $i_n^{(j)}$ contains an element from $\varrho(\mathrm{C}\mathcal{D}_k)$ if and only if

$$\varepsilon_i = 1 \implies \varepsilon_{i+k} = 0, \qquad i = 1,\dots,n-k. \tag{21}$$

Denote by J_n^k the set of all intervals with the property (21), and denote by $P_n^{(k)}$ the number of these intervals. Remark that J_n^k is a 2^{-n} covering of the set $\varrho(\mathrm{C}\mathcal{D}_k)$. The number $P_{nk}^{(k)}$ denote the number of the sequences

$$\varepsilon_1, \dots, \varepsilon_{kn}$$

satisfying (21) (where $n := nk$). Every this sequence consists from the blocks

$$\begin{gathered}
\varepsilon_1, \varepsilon_{1+k}, \dots, \varepsilon_{1+(n-1)k} , \\
\varepsilon_2, \varepsilon_{2+k}, \dots, \varepsilon_{2+(n-1)k} , \\
\vdots \\
\varepsilon_k, \varepsilon_{k+k}, \dots, \varepsilon_{k+(n-1)k} ,
\end{gathered}$$

where each line is a sequence satisfying (21) for $k = 1$ and we have k lines. Put $P_n = P_n^{(1)}$, thus each line can be selected by P_n ways, thus we have the following result.

LEMMA 2.1. *For $k \geq 1$ there holds $P_{nk}^{(k)} = P_n^{(k)}$.*

We now deduce a recurrent relation for P_n. Observe that P_{n+1} can be expressed as a sum of two numbers. The first of them is the number of the sequences

$$\varepsilon_1, \dots, \varepsilon_n, 0 ,$$

where $\varepsilon_1, \dots, \varepsilon_n$ runs over all the sequences (21) for $k = 1$. This number is P_n. The second number is the number of such sequences

$$\varepsilon_1, \dots, \varepsilon_n, \varepsilon_{n+1}$$

in which $\varepsilon_{n+1} = 1$, thus $\varepsilon_n = 0$, and so the number of these sequences is P_{n-1}. Hence

$$P_{n+1} = P_n + P_{n-1}, \qquad n \geq 2. \tag{22}$$

Thus P_n is the well-known Fibonacci sequence, and we have (see [4] or [18])

$$P_n = \frac{2+\sqrt{5}}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} + \frac{2-\sqrt{5}}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}. \tag{23}$$

Since the second summand on the right-hand side converges to 0 as $n \to \infty$, we see that

$$P_n = O\left(\left(\frac{1+\sqrt{5}}{2}\right)^n\right).$$

Lemma 2.1 now yields

$$P_{kn}^{(k)} = O\left(\left(\frac{1+\sqrt{5}}{2}\right)^{kn}\right) \tag{24}$$

and so we can prove the following theorem.

THEOREM 2.3. *We have*

a) $\dim \varrho(\mathrm{C}\mathcal{D}_k) \leq \log_2(1+\sqrt{5}) - 1$, $k = 1, 2, \dots$.
b) $\dim \varrho(\mathrm{C}\mathcal{D}) = \log_2(1+\sqrt{5}) - 1$.

Proof. Remark that the part b) we obtain from well-known inequality $\dim \varrho(\mathrm{C}\mathcal{D}) \leq \sup\limits_{k=1,2,\dots} \dim \varrho(\mathrm{C}\mathcal{D}_k)$.

Thus it suffices to prove the part a). Clearly $\varrho(\mathrm{C}\mathcal{D}_k) \subset J_{kn}^k$. Let $\eta > 0$. Choose n such that $2^{-nk} < \eta$. Then J_{nk}^k is an η-cover of the set $\varrho(\mathrm{C}\mathcal{D}_k)$. Hence, by definition of the α-dimensional Hausdorff measure, $\mu^{(\alpha)}$ (see [19]) we have

$$\mu_\eta^{(\alpha)}\big(\varrho(\mathrm{C}\mathcal{D}_k)\big) \leq K \left(\frac{1+\sqrt{5}}{2}\right)^{nk} \cdot \frac{1}{2^{nk\alpha}} = K \cdot 2^{nk(\log_2(1+\sqrt{5})-1-\alpha)}, \tag{25}$$

where K is a positive constant from (24).

The inequality (25) holds for each $n \in \mathbb{N}$ with $2^{-nk} < \eta$. Thus by $n \to \infty$ we get

$$\mu_\eta^{(\alpha)}\big(\varrho(\mathrm{C}\mathcal{D}_k)\big) = 0 \tag{26}$$

provided that

$$\log_2(1+\sqrt{5}) - 1 < \alpha. \tag{26'}$$

So from the equality (26) we have

$$\mu^{(\alpha)}\big(\varrho(\mathrm{C}\,\mathcal{D}_k)\big) = \lim_{\eta\to 0+} \mu_\eta^{(\alpha)}\big(\varrho(\mathrm{C}\,\mathcal{D}_k)\big) = 0$$

for α satisfying $(26')$. Then, by the definition of the Hausdorff dimension, we get

$$\dim \varrho(\mathrm{C}\,\mathcal{D}_k) \le \log_2\big(1+\sqrt{5}\big) - 1 .$$

$\square$

We will now study the magnitude of the sets $\varrho(\mathcal{D})$, $\varrho(\mathcal{D}^*)$ and $\varrho(\mathcal{D}_0)$ from the topological point of view.

The first result in this direction is the following theorem showing that the class $\mathcal{D}^*$ is very rich also from the topological point of view.

THEOREM 2.4. *The set $\varrho(\mathcal{D}^*)$ is residual in* $(0,1]$.

COROLLARY. *The set $\varrho(\mathcal{D})$ is residual in* $(0,1]$. (*See* (18).)

Proof of Theorem 2.4. We shall prove that the set $(0,1]\setminus\varrho(\mathcal{D}^*)$ is a set of the first Baire category in $(0,1]$.

Denote by $\mathcal{S}_k$, $k\in\mathbb{N}$, the class of all infinite sets $A\subset\mathbb{N}$ such that there is only a finite number of pairs $(x,y)\in A\times A$ with $k=x-y$. Then we have

$$(0,1]\setminus\varrho(\mathcal{D}^*) = \bigcup_{k=1}^{\infty} \varrho(\mathcal{S}_k) .$$

Therefore it suffices to prove that each of the sets $\varrho(\mathcal{S}_k)$, $k=1,2,\dots$, is a set of the first Baire category in $(0,1]$. Denote by $\mathcal{S}_k^n$ $(n\ge 0)$ the class of all infinite sets $A\subset\mathbb{N}$ with the following property: For the number k there exist at most n pair $(x,y)\in A\times A$ such that $k=x-y$. Then

$$\mathcal{S}_k = \bigcup_{n=1}^{\infty} \mathcal{S}_k^n , \qquad \varrho(\mathcal{S}_k) = \bigcup_{n=1}^{\infty} \varrho(\mathcal{S}_k^n) .$$

Thus, it suffices to show that each of the sets $\varrho(\mathcal{S}_k^n)$, $n=1,2,\dots$, is a nowhere dense set in $(0,1]$.

This fact will be proved in what follows using the following test of nowhere-density: A set $M\subset(0,1]$ is nowhere-dense in $(0,1]$ if every non-empty interval $I\subset(0,1]$ contains an interval $J\subset I$ such that $J\cap M=\emptyset$ (cf. [7; p. 37]).

Let $I\subset(0,1]$ be an interval. Choose the numbers j, l, $j\in\mathbb{N}$, $0\le l\le 2^j-1$ in such a way that $i_j^{(l)}\subset I$. Suppose that $i_j^{(l)}$ is associated with the sequence

$$\varepsilon_1^0,\dots,\varepsilon_j^0 .$$

Construct the sequence

$$\varepsilon_1^0, \dots, \varepsilon_j^0, 1, 0, 0, \dots, 0, 1, 0, 0, \dots, 0, 1, \dots, 0, 0, \dots, 0, 1\,. \tag{27}$$

This sequence contains $n+1$ blocks $0, 0, \dots, 0, 1$ each having $k-1$ zeros and in the last place 1. The number of all terms of the sequence (27) is $h = j + 1 + (n+1)k$. Let $i_h^{(r)}$ $(0 \le r \le 2^h - 1)$ be the interval of hth order which is associated with the sequence (27). If $x \in i_h^{(r)}$, $x = \varrho(A)$, then the numbers $j+1, j+1+k, \dots, j+1+(n+1)k$ belong to A. Thus the number k can be expressed in the form $k = x - y$, $x, y \in A$, at least in $n+1$ ways. From this we see that $i_h^{(r)} \cap \varrho(\mathcal{S}_k^n) = \emptyset$, and so $\varrho(\mathcal{S}_k^n)$ is a nowhere dense set in $(0,1]$. $\square$

The following result shows that the topological structure of the set $\varrho(\mathcal{D}_0)$ is wholly distinct from that of $\varrho(\mathcal{D}^*)$.

THEOREM 2.5. *The set $\varrho(\mathcal{D}_0)$ is a nowhere dense set in $(0,1]$.*

P r o o f. We shall use the same test as in the previous proof. Let $I \subset (0,1]$ be an interval. Choose m, s $(0 \le s \le 2^m - 1)$ such that $i_m^{(s)} \subset I$. Let $i_m^{(s)}$ be associated with the sequence

$$\varepsilon_1^0, \dots, \varepsilon_m^0\,.$$

Construct the sequence

$$\varepsilon_1^0, \dots, \varepsilon_m^0, 0, 0, \dots 0$$

having $2m$ terms. Let $i_{2m}^{(l)}$ be the interval of $2m$th order associated with this sequence.

Let $A \in \mathcal{U}$, $\varrho(A) \in i_{2m}^{(l)}$. Then

$$m + i \notin A\,, \qquad i = 1, \dots, m\,. \tag{28}$$

We will show that the number m cannot be expressed in the form $m = a - b$, $b \le \frac{a}{2}$, $a, b \in A$.

Suppose in contrary that $m = a - b$, $b \le \frac{a}{2}$, $a, b \in A$. Then a simple estimation yields $m \ge \frac{a}{2}$, thus $a \le 2m$. Since $a > m$, we have $a = m + i$, $1 \le i \le m$. But this is a contradiction to (28). Thus $\varrho(\mathcal{D}_0) \cap i_{2m}^{(l)} = \emptyset$ and the assertion is proved. $\square$

REFERENCES

[1] BEREKOVÁ, H.: *On difference sets of sets of non-negative integers*, Acta Fac. Rerum Natur. Univ. Comenian. **27** (1972), 107–115.

[2] BROWN, T. C.—FREEDMAN, A. R.: *The uniform density of sets of integers and Fermat's last theorem*, C. R. Math. Rep. Acad. Sci. Canada **12** (1990), 1–6.

[3] HARTER, E.: *Differenzen von Mengen nicht negative Zahlen*, J. Reine Angew. Math. **232** (1968), 112–116.

[4] HOGGATT JR., V. E.—ALLADI, K.: *Limiting ratios of convalued recursive sequences*, Fibbonacci Quart. **15** (1977), 211–214.

[5] KOMINEK, Z.: *On the sum and difference of two sets in topological vector spaces*, Fund. Math. **71** (1971), 165–169.

[6] KUCZMA, M. E.—KUCZMA, M.: *An elementary proof and an extension of a theorem of Steinhaus*, Glas. Mat. Ser. III **6(26)** (1971), 11–18.

[7] KURATOWSKI, C.: *Topologie I*, PWN, Warszawa, 1958.

[8] NEUBRUNN, T.—ŠALÁT, T.: *On sets of distances of sets of a metric space*, Mat.-Fyz. Časopis SAV **9** (1959), 222–235. (Slovak)

[9] NEUBRUNN, T.—ŠALÁT, T.: *Distance sets, ratio sets and certain transformations of sets of real numbers*, Časopis Pěst. Mat. **94** (1969), 381–393.

[10] OSTMANN, H. H.: *Additive Zahlen - Theorie I*, Springer-Verlag, Berlin-Gottingen-Heidelberg, 1956.

[11] ŠALÁT, T.: *On sets of distances of linear discontinuous*, Časopis Pěst. Mat. **87** (1962), 4–16. (Russian)

[12] ŠALÁT, T.: *Über die Cantorsche Reihen*, Czechoslovak Math. J. **18** (1968), 25–56.

[13] SIERPIŃSKI, W.: *Sur une propriete des nombres naturels*, Elem. Math. **19** (1964), 27–29.

[14] SILVERMAN, S.: *Intervals contained in arithmetic combinations of sets*, Amer. Math. Monthly **102** (1995), 351–353.

[15] STEINHAUS, H.: *Sur les distances des points des ensembles de measure positive*, Fund. Math. **1** (1920), 99–104.

[16] STOHR, W.: *Geloste und ungeloste Fragen uber Basen naturlichen Zahle - Reihe I; II*, J. Reine Angew. Math. **194** (1955), 40–65; 111–140.

[17] VOLKMANN, B.: *Zwei Bemerkungen über pseudorationale Mengen*, J. Reine Angew. Math. **193** (1954), 126–128.

[18] VOROBJOV, N. N.: *Fibonacci Numbers*, Gos. Izd. Tech.-Teoret. Lit., Moscow-Leningrad, 1951. (Russian)

[19] WHEEDEN, R. L.—ZYMUND, A.: *Measure and Integrals*, Marcel Dekker, New York, 1977.

[20] VOLKMANN, B.: *Über Hausdorfsche Dimensionen von Mengen, die durch Ziffereigenschaften charakterisiert sind*, Math. Z. **59** (1953), 259–270.

Received June 27, 2002
Revised August 25, 2002

* *Department of Algebra and Number Theory*
Faculty of Mathematics Physiscs and Informatic
Comenius University
Mlynská Dolina 5
SK-842 15 Bratislava
SLOVAKIA

** *Mathematical Institute*
Slovak Academy of Sciences
Štefánikova 49
SK-814 73 Bratislava
SLOVAKIA