COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **16** (1) (1996) 87–106

DIFFERENCE SETS AND INVERTING THE DIFFERENCE OPERATOR

ZOLTÁN FÜREDI, CARL G. JOCKUSCH, JR., and LEE A. RUBEL†

Received April 12, 1994

For a set A of non-negative numbers, let $D(A)$ (the difference set of A) be the set of non-negative differences of elements of A, and let D^k be the k-fold iteration of D. We show that for every k, almost every set of non-negative integers containing 0 arises as $D^k(A)$ for some A. We also give sufficient conditions for a set A to be the unique set X such that $0 \in X$ and $D^k(X) = D^k(A)$. We show that for each m there is a set A such that $D(X) = D(A)$ has exactly 2^{m} solutions X with $0 \in X$.

1. Introduction and Notation

For a set A of non-negative numbers, let $D(A) = \{|a-b| : a, b \in A\}$. We call $D(A)$ the *difference set* of A. Difference sets of sets of positive density have been studied, for example, in [7] and [8]. For a general reference on sequences, see, for example, [5]. In 1974 I. Z. Ruzsa [6, p. 156] asked: Under what conditions will a set be the difference set of another?

Our goal in this paper is to show that many sets (in various senses of "many") occur as difference sets and also to analyze the possibilities for $D^{-1}(B) = \{A : D(A) = B\}$ as B varies. In a sequel [1], we will use the concepts and methods of recursion theory to compare the "complexity" of $D(A)$ to that of A. One goal behind the results in both this paper and [1] is to characterize the family of all difference sets or else to show that this family is not Borel. (The latter result would indicate that no reasonable characterization is possible.) We have not yet reached this goal, but we hope that the results in these papers may provide some helpful steps in this direction.

Mathematics Subject Classification (1991): 11 B 05, 05 C 65

This work was supported by grants DMS 92-02833 and DMS 91-23478 from the National Science Foundation. The first author acknowledges the support of the Hungarian National Science Foundation under grants, OTKA 4269, and OTKA 016389, and the National Security Agency (grant No. MDA904-95-H-1045).

† Lee A. Rubel died March 25, 1995. He is very much missed by his coauthors.

The following is a simple example of a result (due to A. Sárközy, given here as Theorem 2.1) showing that many sets occur as difference sets: Let B be a set with $0 \in B$ which contains arbitrarily long blocks of consecutive integers. Then there are uncountably many sets A such that $D(A)=B$. It follows that the family of difference sets is of measure 1 and comeager on $\{B \subseteq \mathbb{N}_0 : 0 \in B\}$, in terms of the usual (product) topology and measure on the latter set. Extending this result, we show that, among sets B with $0 \in B$, almost every set B (in the sense of both measure and category) is a k^{th} difference set for all positive integers k, i.e. for some A the set B is of the form $D^k(A)$, where $D^0(A)=A$ and $D^{k+1}(A)=D(D^k(A))$.

It is obvious that if B is a nonempty difference set it is the difference set of infinitely many sets (since $D(A)=D(A+m)$ for all m.) To eliminate this triviality, we often identify sets which differ only by a translation. We say that B is a *unique difference set* if there is a set A such that $D(A)=B$ and any set $\hat{A}$ with $D(\hat{A})=B$ is of the form $A+k$ for some k. Ruzsa [6, page 156] also asked for conditions implying the uniqueness of $D(A)$. He mentions an example where the members of A grow exponentially. Here we will give many more examples, even ones having positive density.

Call A a *B_ℓ-set* if distinct multisets of ℓ elements of A always have distinct sums. We show that if A is a B_3 set, then $D(A)$ is a unique difference set. (This result was independently discovered by Erdős, A. Sárközy, and V. T. Sós [3].) We also give examples to show that for each t there is a set B which is the difference set of exactly 2^t sets (modulo translation).

All infinite and finite sets here consist of nonnegative integers, unless otherwise stated. The set of positive integers is denoted by $\mathbb{N}$, and the set of non-negative integers is denoted by $\mathbb{N}_0$, as usual. The notations $A+B$, AB, as usual, denote the sets $\{a+b : a \in A, b \in B\}$, $\{ab : a \in A, b \in B\}$ respectively. $\{p\}+A$ and $\{p\}A$ are abbreviated as $p+A$ and pA respectively.

The $n+1$'st element of the sequence A (B, C...) is denoted by a_n or $a(n)$ (b_n or $b(n)$, ...), whichever is more convenient.

2. Almost every set is a difference set

If $A \subseteq \mathbb{N}_0$ contains arbitrarily long strings of consecutive integers, then $D(A)=\mathbb{N}_0$. Thus almost all sets have $\mathbb{N}_0$ as their difference set. Nonetheless, the following result of Sárközy shows that almost all sets containing 0 occur as difference sets. For completeness we repeat the (10-line) proof in a language which will be useful later. The result will be extended, with a much more complicated proof utilizing new ideas, to k^{th} difference sets in Theorem 8.2.

Theorem 2.1. (Sárközy, see [6, p. 156], and Erdős, A. Sárközy, and V. T. Sós [3, Corollary 1 to Theorem 14]). *Let B be any set such that $0 \in B$ and B contains arbitrarily long strings of consecutive integers. Then there are uncountably many sets A such that $D(A)=B$.*

Proof. We construct a single set A such that $D(A)=B$. It will then be clear how to vary the construction to produce uncountably many such A. The set A will be constructed as the union of a chain $F_0 \subseteq F_1 \subseteq \ldots$ of finite sets. Call a finite set F *acceptable* if $D(F) \subseteq B$. We will arrange that each F_n is acceptable and that, if $k \in B$, then $k \in D(F_k)$. From this it follows that $D(A)=B$, where $A=\cup_k F_k$. To obtain the sets F_k recursively, it suffices to prove the following lemma:

Lemma 2.2. *Let F be any acceptable set, and assume that $k \in B$. Then there is an acceptable set $G \supseteq F$ such that $k \in D(G)$.*

Proof. Let $G=F \cup \{a, a+k\}$ where a is chosen so that G is acceptable. Specifically, choose $a > max(F)$ so that $a - F \subseteq B$ and $a+k-F \subseteq B$, where this is possible because B contains arbitrarily long blocks of consecutive integers. ∎

3. B_3 sequences have unique difference sets

Definition 3.1. A set of numbers A is called a *B_ℓ-set* (ℓ a positive integer) if $a_1, \ldots, a_{2\ell} \in A$, $\sum_{1 \le i \le \ell} a_i = \sum_{\ell+1 \le i \le 2\ell} a_i$ implies that the sequences $\{a_1, \ldots, a_\ell\}$ and $\{a_{\ell+1}, \ldots, a_{2\ell}\}$ are identical up to a permutation, (i.e., identical as multisets). A B_2 sequence is called a *Sidon* sequence (cf. [5]). The following result was obtained independently and at about the same time by P. Erdős, A. Sárközy, and V. T. Sós [3, Theorem 17]. It will be extended to k^{th} difference sets, too, in Theorem 9.1.

Theorem 3.2. *Suppose that the sequences of reals $A=\{a(0)=0<a(1)<\ldots<a(n)<\ldots\}$ and $B=\{b(0)=0<b(1)<\ldots<b(n)<\ldots\}$ have the same difference set, i.e. $D(A)=D(B)$. If A is a B_3 sequence, then $A=B$.*

Proof. The proof presented below is considerably shorter than that in [3], though it uses the same ideas. The proof of the generalization (Theorem 9.1) requires different ideas borrowed from linear algebra and the theory of hypergraphs.

As $D(A)=D(B)$, one can define functions f and g for all positive integers i such that $b(i)-b(i-1)=a(f(i))-a(g(i))$. Here $f(i) > g(i) \ge 0$. Consider $b(i+1)-b(i-1) \in D(B)=D(A)$, and write it in the form $a(u)-a(v)$, $(u>v \ge 0)$. The identity $(b(i+1)-b(i))+(b(i)-b(i-1))=b(i+1)-b(i-1)$ implies that $a(f(i+1))+a(f(i))+a(v)=a(g(i+1))+a(g(i))+a(u)$. So the multisets of indices coincide, i.e. $\{f(i+1), f(i), v\}=\{g(i+1), g(i), u\}$. Hence $\{f(i+1), f(i)\} \cap \{g(i+1), g(i)\} \neq \emptyset$. However, $f(i+1)>g(i+1)$ and $f(i)>g(i)$, so either $f(i+1)=g(i)$ or $f(i)=g(i+1)$ (but not both) holds. In the first case we say $i \in R$, in the second $i \in S$. The crucial point of the proof is the following claim:

$$i \in R \text{ implies } (i+1) \in R. \tag{3.3}$$

Indeed, suppose, on the contrary, that i belongs to R and $(i+1) \in S$, i.e., $g(i)=f(i+1)=g(i+2)$. This and the conditions $f(j)>g(j)$ imply that

$$f(i+2),\ f(i) > g(i+2) = g(i) = f(i+1) > g(i+1). \tag{3.4}$$

Write $b(i+2)-b(i-1)$ in the form $a(x)-a(y)$. On the other hand

$$b(i+2)-b(i-1) = a(f(i+2))-a(g(i+2))+a(f(i+1))-a(g(i+1))+a(f(i))-a(g(i))$$
$$= a(f(i+2)) + a(f(i)) - a(g(i+1)) - a(g(i)),$$

so the B_3-property implies that $\{x, g(i+1), g(i)\} = \{y, f(i+2), f(i)\}$. However, $\{g(i+1), g(i)\} \cap \{f(i+2), f(i)\} = \emptyset$ by (3.4), a contradiction. This proves (3.3).

If $R \neq \emptyset$, say $i \in R$, then (3.3) implies that all integers $j > i$ belong to R. We have $g(i) = f(i+1) > g(i+1) = f(i+2) > g(i+2) = f(i+3) > \ldots > \ldots$ an infinite descending sequence of nonnegative integers, a contradiction.

It follows that $R = \emptyset$, so $f(i) = g(i+1)$ holds for every $i \geq 1$, i.e. $b(i+1) - b(i) = a(f(i+1)) - a(f(i))$. Define $f(0) := g(1)$. Then we have that $b(i) - b(i-1) = a(f(i)) - a(f(i-1))$ for all $i \geq 1$. This implies that for all $j > i \geq 0$ one has $b(j) - b(i) = a(f(j)) - a(f(i))$, which gives $b(i) = b(i) - b(0) = a(f(i)) - a(f(0))$ for all i, and $f(0) < f(1) < \ldots < f(i) < \ldots$. We obtain that $f(j) \geq j$.

We claim that $f(j) = j$ for all j. Suppose, on the contrary, that j is the smallest number with $f(j) > j$. Then $j \notin f(\mathbb{N}_0)$, because f is strictly monotone, $0 = f(0), \ldots, j-1 = f(j-1)$, $j < f(j) < f(j+1) < \ldots$. The B_3-property implies that $a(f(j)) - a(j)$ cannot be written in the form $a(f(x)) - a(f(y))$, because $a(f(j)) - a(j) = a(f(x)) - a(f(y))$ implies $\{f(j), f(y)\} = \{f(x), j\}$, but $j \notin f(\mathbb{N}_0)$. So $a(f(j)) - a(j)$ does not belong to $D(B)$, contradicting that $D(B) = D(A)$. Since $f(j) = j$ for all j, $b(i) = a(f(i)) - a(f(0)) = a(i) - a(0) = a(i)$ for all i. Hence $A = B$. ∎

4. Dense sequences with unique difference sets

A B_3-sequence, A, can have at most $O(n^{1/3})$ members from $\{0, 1, 2, \ldots, n\}$. (This is so, because for $|A \cap \{0, 1, 2, \ldots, n\}| = c$ all the distinct $\binom{c+2}{3}$ triple sums, where now we have counted the triples with repetitions, lie in the interval $\{0, \ldots, 3n\}$, so this binomial coefficient is at most $3n+1$.) In this section we present further examples with unique difference sets which can have far more elements, even arbitrary positive density up to $1/3$. If $0 \in A \subseteq \mathbb{N}_0$ has a unique difference set, then $D(A) \neq \mathbb{N}_0$, say $d \notin D(A)$, which implies that $|\{x, x+d\} \cap A| \leq 1$ for all x, so the density of A is at most $1/2$. Whether it can exceed $1/3$ remains undecided.

We say that the sequence C with $0 \in C = \{c_0 = 0 < c_1 < \ldots < c_i < \ldots\} \subseteq \mathbb{N}_0$ is *decomposable* if it can be written in the form $C = C' + S$, where $C', S \subseteq \mathbb{N}_0$ and $|S| > 1$ but S is finite. Note that $0 \in S$, C' because $0 \in C$ and no element of $C' \cup S$ is negative. Otherwise, C is *indecomposable*, i.e., $C' \subseteq \mathbb{N}_0$, $S \subseteq \mathbb{N}_0$, S is finite, and $C = C' + S$ imply $S = \{0\}$. Most sequences are indecomposable. For example, C is indecomposable if it has arbitrarily large double gaps:

$$\limsup_i \min\{c_i - c_{i-1}, c_{i+1} - c_i\} = \infty. \tag{4.1}$$

Such a C can have density 1. To see that decomposable sequences cannot satisfy (4.1), consider a decomposition $C = C' + S$ with $0 \in S$ and $\max S > 0$. Let $c \in C$ be

given, and let $c = c' + s$ for some $c' \in C'$, $s \in S$. Choose $s' \in S$ with $s' \neq s$. Then $c'+s' \in C$ and $0 < |c-(c'+s')| \leq \max S$. It follows that $\min\{c_i - c_{i-1}, c_{i+1} - c_i\} \leq \max S$ for all i, so (4.1) fails.

Theorem 4.2. *If C is indecomposable and $0 \in C$, then the sequence $A = \{1\} \cup 3C$ has a unique difference set.*

The proof of this Theorem is immediate from the following Lemma.

Lemma 4.3. *Suppose that $0 \in C \subseteq \mathbb{N}_0$, $p \geq 3$ integer, $A = \{1\} \cup pC$, and $0 \in X \subseteq \mathbb{N}_0$ with $D(X) = D(A)$. Then either $X = A$, or there exists a decomposition of $C = C' + S$ such that X can be obtained as follows. S is a finite subset of C, with $0 \in S$, $c_k = \max\{x : x \in S\} > 0$, and C' is a subsequence $C' \subseteq C$, such that $X = (pc_k - pS) \cup (pC' + (pc_k - 1))$.*

Proof. Suppose that $0 \in X \subseteq \mathbb{N}_0$, $D(X) = D(A)$. As $X \subseteq D(X) = D(A)$, every element $x \in X$ can be written either in the form $x = p(c_j - c_i)$ (where $j \geq i \geq 0$), or in the form $x = pc_i - 1$ ($i \geq 1$), or $x = 1$. Let $X^{(r)} = \{x \in X : x \equiv r \pmod p\}$. Then $X = X^{(0)} \cup X^{(-1)} \cup X^{(1)}$ and $X^{(1)} \subseteq \{1\}$.

Suppose, first, that $1 \in X$, i.e., $X^{(1)} = \{1\}$. There is no member $x \in X^{(-1)}$ with $x > 2$, because then $x - 1 \equiv -2 \pmod p$, $x - 1 > 1$, $(x-1) \in D(X) = D(A)$, a contradiction. If $2 \in X^{(-1)}$, i.e. $p = 3$, then there is no $y \in X^{(0)}$ ($y \equiv 0 \pmod 3$) with $y > 3$, otherwise we get another difference (namely $y - 2$) belonging to $X^{(1)}$. Hence in this case $X \subseteq \{0,1,2,3\}$, contradicting the fact that X is infinite. So $X \subseteq \{1\} \cup \{0, p, 2p, \ldots, ip, \ldots\}$. $D(X)$ contains all the differences of the form $pc_i - 1$, so we obtain that $pC \subseteq X$. For the same reason X cannot have more elements of the form ip, so $X = A$.

From now on, we suppose that $1 \notin X$, i.e. $X = X^{(0)} \cup X^{(-1)}$. As $1 \in D(X)$, there is an element $py \in X^{(0)}$ such that $(py-1) \in X^{(-1)}$. But $X^{(-1)} \subseteq \{pc_i - 1 : i \geq 1\}$, so we have that for some $k \geq 1$, $y = c_k$. We claim that pc_k is the largest element of $X^{(0)}$, and $pc_k - 1$ is the smallest element of $X^{(-1)}$. Indeed, for $py \in X^{(0)}$ with $y > c_k$, we get $(py - (pc_k - 1)) \in D(X)$, however 1 is the only element of $D(X)$ congruent to 1 (mod p). Similarly, for $(py-1) \in X^{(-1)}$ with $y < c_k$, we get $(pc_k - (py-1)) \in D(X)$, the same contradiction.

Define $S = \{s : p(c_k - s) \in X^{(0)}\}$ and $C' = \{t : (pt + pc_k - 1) \in X^{(-1)}\}$. We claim that $C' \subseteq C$, $S \subseteq C$, $|S| > 1$ and $C = C' + S$, so they form a decomposition of C. To see that $C' \subseteq C$ suppose that $(pt + pc_k - 1) \in X^{(-1)}$, $t > 0$ and consider the difference between $(pt + pc_k - 1)$ and $pc_k \in X^{(0)}$. It must be of the form $pc_i - 1$. Similarly, for $s \in S$, $s > 0$, we obtain $s \in C$ considering the difference of $(pc_k - 1) \in X^{(-1)}$ and $p(c_k - s) \in X^{(0)}$. It must be of the form $pc_i - 1$, too, so $s \in C$. Moreover, $0 \in C$, so we conclude that $S \subseteq C$. Since $\{0, pc_k\} \subseteq X$ we have $\{0, c_k\} \subseteq S$, implying $|S| > 1$.

For $s \in S$, $t \in C'$ with $st \neq 0$ we have that the difference of the members $(pt+pc_k-1) \in X^{(-1)}$ and $p(c_k-s) \in X^{(0)}$ is $p(t+s)-1$. This belongs to $D(X)=D(A)$, so it is of the form pc_i-1, implying $(t+s) \in C$. Hence $C'+S \subseteq C$. Finally, the differences $\{x^{(-1)}-x^{(0)} : x^{(i)} \in X^{(i)}\}$ yield all the numbers of the form pc_i-1. To see this, note that every $x^{(-1)} \in X^{(-1)}$ can be written in the form $pt+pc_k-1$ with $t \in C'$, and every $x^{(0)} \in X^{(0)}$ can be written in the form $p(c_k-s)$ with $s \in S$. Thus, pc_i-1 can be written in the form $pt+pc_k-1-p(c_k-s)$, where $s \in S$ and $t \in C'$. Hence $c_i=t+s$, and so $C \subseteq C'+S$. We are done. ∎

5. Any nontrivial set of powers of 2 has a unique difference set

Although the set of powers of 2 does not form a B_3-set (e.g., $2^n+2^m+2^m = 2^{n-1}+2^{n-1}+2^{m+1}$), the following holds.

Proposition 5.1. *Any infinite set of powers of 2, $P=P(A)=\{2^a : a \in A \subseteq \mathbb{N}_0\}$, has a unique difference set, except when A is a final segment of $\mathbb{N}_0$.*

Fix $k \in \mathbb{N}_0$, and let $P^{[k]}=\{2^a : a \geq k\}$. We have $D(P^{[k]})=D(P^{[k]} \cup \{0\})$. Our proof will show that (up to translation, of course) this is the only other sequence with the same difference set. So we have an example B such that $D(X)=B$ has exactly two solutions modulo translations. We return to this phenomenon in Section 6.

Note that the above remark corrects a small error from [6, page 156], where it was mistakenly claimed that the set of powers of 2 has a unique difference set.

Proof of 5.1. The proof is similar to the proof of Lemma 4.3. Let $X \subseteq \mathbb{N}_0$ such that $D(X)=D(P)$ and $\min X = \min P$. If $\min P$ is denoted by 2^c, then all members of P (and therefore X) are divisible by 2^c. So without loss of generality we may suppose that $\min P = 1$, i.e., $0 \in A$. Define $X^{(r)}=\{x \in X : x \equiv r \pmod 2\}$. Now $1=\min X$ implies that $(X-1) \subseteq D(X)=D(P)=\{2^b-2^a : b \geq a \geq 0, b, a \in A\}$. So we have that $X^{(0)} \subseteq P \setminus \{1\}$ and $X^{(1)} \subseteq \{2^b-2^a+1 : b \geq a \geq 1,\ b, a \in A\}$.

Suppose, first, that $|X^{(1)}| \geq 2$, i.e., $(2^b-2^a+1) \in X^{(1)}$ for some $b>a \geq 1$, $b, a \in A$. We claim that for every member $2^c \in X^{(0)}$ one has $c \leq b$, i.e., $X^{(0)}$ is finite. Indeed,

$$2^x + 2^y = 2^u + 2^v \text{ , } x, y, u, v \in \mathbb{N}_0 \text{ imply } \{x, y\} = \{u, v\}. \tag{5.2}$$

For $c \geq b$ the difference $2^c-(2^b-2^a+1)$ is odd and belongs to $D(P)$; therefore it must be of the form 2^d-1. Then $\{c, a\}=\{b, d\}$, so $c=b$ (because $c>d$). As $X^{(0)}$ is finite, $X^{(1)}$ should be infinite.

The set $X^{(0)}$ cannot be empty, so let $2^c \in X^{(0)}$ be an arbitrary element ($c \geq 1$), and suppose that $y \in X^{(1)}$, $y > 2^{c+1}$. Write y in the form $2^u - 2^v + 1$. Consider the difference $(2^u - 2^v + 1) - 2^c$; it must be in the form $2^d - 1$, so

$$2^u + 2 = 2^v + 2^d + 2^c. \tag{5.3}$$

Here $d \in A$ and $d > c$ because, by definition, $2^u - 2^v + 1$ is larger than 2×2^c, so $2^d - 1$ is larger than 2^c. Moreover, $u \geq c+2$, so subtracting $(1/4)2^u$ from both sides of (5.3) yields that $(3/4)2^u < 2^v + 2^d$. But $u > v$, $u > d$, so we obtain $u - 1 = v = d$. Then (5.3) gives $c = 1$, so $X^{(0)} = \{2\}$, the only even member of X. To get the odd differences for $D(X)$ the only possibility is to take an element of $X^{(1)}$ and the element $2 \in X^{(0)}$. So all the elements of $X^{(1)}$ exceeding 4 have the form $2^a + 1$ ($a \in A$, $a \geq 2$), i.e., $X^{(1)} \setminus \{1,3\} \subseteq \{2^a + 1 : a \in A,\ a \geq 2\}$.

We are going to show that $A = \mathbb{N}_0$ and $X = \{1,2\} \cup \{2^a + 1 : a \in \mathbb{N}_0 \setminus \{0\}\}$. As $\{1,2\} \subseteq X$, we have that $1 \in D(X) = D(P)$, so $2^1 \in P$. Choose $2^b \in P$ such that $b > 2$ and consider the difference $(2^b - 2^1) \in D(P)$; it is in $D(X^{(1)})$. As all elements of $X^{(1)} \setminus \{1\}$ have the form $2^x + 1$, this difference cannot be obtained using the element 1, so (5.2) implies that $(2^b + 1) \in X$ and $(2^1 + 1) \in X$. Hence $2 \in D(P)$ which implies that $2^2, 2^1 \in P$. Now let a be any member of A with $a \geq 2$. As $2^a \in P$, we have $(2^a - 1) \in D(X)$, so $(2^a + 1) \in X^{(1)}$. This implies that $2^a \in D(X^{(1)}) \subseteq D(P)$, so $(a+1) \in A$. We have shown that indeed, $A = \mathbb{N}_0$, and $X = 1 \cup (1 + P)$ as claimed.

From now on we may suppose that $|X^{(1)}| = 1$, i.e., $X^{(1)} = \{1\}$. Considering the odd differences of P we obtain that $X = P$. ∎

6. Finitely many sequences with the same difference set

In this section we show that for each positive integer t there is a sequence B such that $D(X) = B$ has exactly 2^t solutions X with $0 \in X \subseteq \mathbb{N}_0$. Let $C = \{c_0 = 0 < c_1 < \ldots\} \subseteq \mathbb{N}_0$ be an infinite sequence, and suppose that A is obtained from C by multiplying by a large number p and by taking a little perturbation. This means that p, r are positive integers, $p > 4r$, $0 \in R_i \subseteq \{0,1,\ldots,r\} = [0,r]$, and $A = \cup_i (pc_i + R_i)$. Suppose that $D(X) = D(A)$. Then $X \subseteq D(A) = \cup_{j>i} (p(c_j - c_i) + (R_j - R_i)) \cup \cup_i D(R_i)$. Write X in the form $\cup_\ell (py_\ell + Q_\ell)$, where $Q_\ell \subseteq [-r,r]$, $0 \in Q_0 \subseteq [0,r]$. Then for the sequence $Y = \{y_0 < y_1 < \ldots\}$ we claim that

$$D(X) = D(A) \text{ implies } D(Y) = D(C). \tag{6.1}$$

Indeed, $(y_i - y_j) \in D(Y)$ means that for some $i \geq j \geq 0$, $q_i \in Q_i$, $q_j \in Q_j$ we have that $(py_i + q_i) \in X$ and $(py_j + q_j) \in X$. Hence $p(y_i - y_j) + (q_i - q_j)$ belongs to $D(X)$. But

then it also belongs to $D(A)$, so it can be written in the form $p(c_u-c_v)+(r_u-r_v)$, where $c_u, c_v \in C$, $u \geq v \geq 0$ and $r_u \in R_u$, $r_v \in R_v$. Here $|q_i|+|q_j|+r_u+r_v \leq 4r < p$, so the above equality yields $y_i - y_j = c_u - c_v$, implying $D(Y) \subseteq D(C)$. The proof of the reverse inclusion, $D(C) \subseteq D(Y)$, is similar: Take $c_u, c_v \in C$, $u \geq v \geq 0$. Then there exist $r_u \in R_u$, $r_v \in R_v$ such that $(pc_u + r_u) \in A$, $(pc_v + r_v) \in A$ and therefore $p(c_u - c_v) + (r_u - r_v) \in D(A) = D(X)$. Write it in the form $p(y_i - y_j) + (q_i - q_j)$ and apply again that $|q_i| + |q_j| + r_u + r_v \leq 4r < p$.

From now on, we suppose that C itself is a B_3-set, so Theorem 3.2 and (6.1) give that $Y = C$. So $X = \cup_i (pc_i + Q_i)$, where

$$Q_j - Q_i = R_j - R_i \text{ for all } j > i \geq 0, \tag{6.2}$$

$$0 \in Q_0 \subseteq [0, r], \quad \cup_i D(Q_i) = \cup_i D(R_i). \tag{6.3}$$

Suppose now, that $r \in R_i$ for all $i \in \mathbb{N}_0$. We will show that this implies that

$$\{0, r\} \subseteq Q_i \subseteq [0, r] \text{ for all } i. \tag{6.4}$$

Indeed, (6.2)-(6.3) give (which we already know) that $Q_j = Q_j - 0 \subseteq Q_j - Q_0 = R_j - R_0 \subseteq [-r, r]$, i.e., $\max Q_j \leq r$ ($j \geq 1$, but this holds for Q_0, too). On the other hand, $r = (r-0) \in R_j - R_0 = Q_j - Q_0$. As Q_0 consists of only non-negative numbers, this implies that $\max Q_j \geq r$, implying $\max Q_j = r$ for all $j \geq 1$. Let ℓ_i be the length of the shortest interval containing Q_i, $\ell_i = \max Q_i - \min Q_i$. We have that $\ell_j + \ell_i = \max Q_j - \min Q_j + \max Q_i - \min Q_i = (\max Q_j - \min Q_i) - (\min Q_j - \max Q_i) = \max(Q_j - Q_i) - \min(Q_j - Q_i) = \max(R_j - R_i) - \min(R_j - R_i) = r - (-r) = 2r$. This implies that $\ell_i = r$ for all i, so we get (6.4).

Recall that our aim is to define a sequence B such that $D(X) = B$ has exactly 2^t solutions X with $0 \in X \subset \mathbb{N}_0$. Let $S(i) = \{0, i, 4\}$, where $i = 1$ or 3. Fix an integer $m \geq 100$, let $\mathbf{i} = (i_0, i_1, \ldots, i_{t-1}) \in \{1,3\}^t$ be a vector of dimension t, and define $S(\mathbf{i}) = S(i_0) + mS(i_1) + \ldots + m^{t-1} S(i_{t-1})$. Then $S(\mathbf{i}) - S(\mathbf{i}) = D + mD + \ldots + m^{t-1} D$, where $D = \{-4, -3, -1, 0, 1, 3, 4\}$. Let $D(t) = D + mD + \ldots + m^{t-1} D$, and let $D(t)^+$ be the set of non-negative elements of $D(t)$.

Theorem 6.5. *Let $0 \in C \subset \mathbb{N}_0$, C a B_3-set, and let $B = \cup_{j>i} \{p(c_j - c_i) + D(t)\} \cup D(t)^+$, where $p > 4m^{t-1}$. Then there are exactly 2^t sequences X with $0 \in X \subseteq \mathbb{N}_0$ satisfying $D(X) = B$, namely $X = pC + S(\mathbf{i})$, where $\mathbf{i} \in \{1,3\}^t$ and $S(\mathbf{i})$, D are as above.*

Proof. First, note that $D(pC + S(\mathbf{i})) = B$ for all $\mathbf{i} \in \{1,3\}^t$. Now, suppose that $D(X) = B$, $0 \in X \subseteq \mathbb{N}_0$ and apply (6.1). We get that $X = \cup_i (pc_i + Q_i)$, satisfying (6.2)-(6.4) with $r = \sum_{0 \leq i < t} 4m^i$, i.e.,

$$Q_j - Q_i = D(t) \text{ for all } j > i \geq 0,$$

$$0 \in Q_0 \subseteq [0, r], \quad \cup_i D(Q_i) = \cup_i D(t)^+$$

$$\{0, r\} \subseteq Q_i \subseteq [0, r] \text{ for all } i.$$

Then, our theorem follows from the following:

Proposition 6.6. $\{0,r\} \subseteq U, V \subseteq [0,r]$, $U - V = D(t)$, $U - U \subseteq D(t) - D(t)$, $V - V \subseteq D(t) - D(t)$ *imply that* $U = V = S(\mathbf{i})$ *for some* $\mathbf{i} \in \{1,3\}^t$.

Proof. As $0 \in U$ and $U - U \subseteq D(t)$, we have that $U \subseteq D(t)$. Write any member of $u \in U$ (and $v \in V$) in the form $u = \sum_{j<t} u_j m^j$ (and $v = \sum_{j<t} v_j m^j$). Such a form is uniquely determined if we suppose that $u_i \in D$ (and $v_j \in D$). Let $U_j = \{u_j : u \in U\}$, $V_j = \{v_j : v \in V\}$. To complete the proof, it suffices to show that $U_j = V_j \in \{S(1), S(3)\}$. We have that $\{0,4\} \subseteq U_j, V_j$ (because $0, r \in U, V$), and that

$$U_j - V_j = D, \quad U_j - U_j \subseteq D, \quad V_j - V_j \subseteq D.$$

It follows that $U_j, V_j \subseteq [0,4]$. As $2, -2 \notin D$ we get that $2 \notin U_j$, V_j. Similarly 1 and 3 cannot be in U_j simultaneously, because $U_j - U_j \subseteq D$. The roles of U_j and V_j are symmetric (also the role of 1 and 3), so suppose that $1 \in U_j$, so $U_j = \{0,1,4\}$. Then $3 \notin V_j$, but $1 \in V_j$ (to get the difference $3 \in U_j - V_j = D$). Hence $U_j = V_j = S(1)$ (or $S(3)$ in the symmetric case.) In the only remaining case, $U_j = V_j = \{0,4\}$, we get $U_j - V_j \neq D$, a contradiction. ∎

7. Sequences with unique difference sets do not form an ideal

We have seen in the third section that every infinite B_3-set A has a unique difference set. All subsets of A are B_3-sets, so all of its infinite subsets have unique difference sets. Let $\mathcal{A}$ denote the set of sequences with a unique difference set ($0 \in A \subseteq \mathbb{N}_0$ for all $A \in \mathcal{A}$). There are sequences $A \in \mathcal{A}$ such that some of their subsets are not in $\mathcal{A}$. (Of course, for all infinite sequences $0 \in B \subseteq \mathbb{N}_0$ there exist continuum many $A \in \mathcal{A}$ with $A \subseteq B$.)

The easiest example is to take a sequence $0 \in C \subseteq \mathbb{N}_0$ with arbitrarily large double gaps, ($\limsup_i \min(c_i - c_{i-1}, c_{i+1} - c_i) = \infty$) and with arbitrarily long segments in it. Then $D(3C) = 3\mathbb{N}_0$, so $3C$ is one of the $2^{\aleph_0}$ solutions. However, $3C$ is indecomposable, so $1 \cup 3C$ has a unique difference set as was shown in Theorem 4.2.

Another example can be obtained from the results of Section 6. Let $0 \in C \subseteq \mathbb{N}_0$ be a B_3-set, and consider $A = pC \cup (pC+1) \cup (pC+4) \cup \{3\}$, with $p > 16$. $A \setminus \{1\}$ is one of the two solutions of the equation $D(X) = D(A \setminus \{1\})$ (by Theorem 6.5). However, A has a unique difference set. Indeed, assuming that $D(X) = D(A)$ and using (6.1)-(6.4) we get that $X = \cup(pc_i + Q_i)$ where $\{0,4\} \subseteq Q_i \subseteq [0,4]$. We obtain from Theorem 6.5 that $X \setminus \{0,1,3,4\}$ should be either $p(C \setminus \{0\}) + \{0,1,4\}$ or $p(C \setminus \{0\}) + \{0,3,4\}$. In the latter case 1, $2 \notin Q_0$, i.e., $Q_0 \subseteq \{0,1,4\}$, hence $-2 \notin Q_i - Q_0$ contradicting $(pc_i - 2) \in D(X)$. We obtain that $Q_1 = \ldots = Q_i = \ldots = \{0,1,4\}$. As $pc_i + 2 \notin D(X)$, we have that $2 \notin Q_0$, so $Q_0 \subseteq \{0,1,3,4\}$. On the other hand $2 \in D(X)$, so $2 \in Q_0 - Q_0$ implying $\{1,3\} \subseteq Q_0$, hence $Q_0 = \{0,1,3,4\}$. ∎

Ruzsa [6, p. 156] gave an example, namely $A_1 = \{2^k : k \in \mathbb{N}_0\}$ and $A_2 = \{2k : k \in \mathbb{N}_0\}$, where $D(A_1) \cup D(A_2)$ is not a difference set at all.

8. Almost all sets are k^{th} difference sets

It was shown in Theorem 2.1 that every set B with $0 \in B$ which contains arbitrarily long strings of consecutive integers is a difference set. Below, we extend this result to k^{th} difference sets by strengthening the hypothesis that B contains arbitrarily long strings of consecutive integers as follows.

Definition 8.1. Let t be a positive integer. A set $B \subseteq \mathbb{N}_0$ is *t-big* if for any finite set $\{u_1x+v_1, u_2x+v_2, \ldots, u_jx+v_j\}$ of linear polynomials with integer coefficients, where $1 \le u_i \le t$, there are infinitely many $x \in \mathbb{N}_0$ with $(u_ix+v_i) \in B$ for all i, $1 \le i \le j$.

For example, the 1-big sets are precisely the sets B which contain arbitrarily long blocks of consecutive integers. Hence, by Theorem 2.1, every 1-big set is a difference set. More generally, a set B is k-big if and only if for each positive integer n there exists $x \ge n$ such that each of the k intervals $[x-n, x+n], [2x-n, 2x+n], \ldots, [kx-n, kx+n]$ is contained in B. Also almost every set is t-big for every t (in the sense that the family of sets which are t-big for every t is comeager and of measure 1). (For measure, this follows because for any sequence $\{F_j\}_{j \in \mathbb{N}_0}$ of pairwise disjoint finite subsets of $\mathbb{N}_0$ of *fixed* cardinality, almost every set B will have the property that $F_j \subseteq B$ for some j.) Note also that the linear case of Schinzel's hypothesis almost says that the primes are t-big for every t, except that it is required that no integer $n > 1$ can divide all values of the product of the polynomials. The following result subsumes Theorem 2.1.

Theorem 8.2. *Every 2^{k-1}-big set B with $0 \in B$ is a k^{th} difference set.*

Proof. Let B be 2^{k-1}-big. We first need some definitions.

For any sequence $A \subseteq \mathbb{N}_0$ and any positive even integer ℓ, let $\mathcal{L}(\ell, A)$ be the set of nonnegative numbers which can be obtained as a linear combination of the form $\sum_i \alpha_i a_i$, where all α_i's are nonzero integers, $\sum_i \alpha_i = 0$, and $\sum_i |\alpha_i| \le \ell$. An element $x \in \mathcal{L}(\ell, A)$ can be written in the form $\sum_{1 \le i \le \ell} \varepsilon^{(i)} a^{(i)}$ where $\varepsilon^{(i)} \in \{1, -1\}$, $\sum \varepsilon^{(i)} = 0$, and $(a^{(1)}, \ldots, a^{(i)}, \ldots, a^{(\ell)})$ is a *sequence* (or *multiset*) of some members of A. Then $D^k(A) \subseteq \mathcal{L}(2^k, A)$ for any sequence $A \subseteq \mathbb{N}_0$. Here equality does not necessarily hold.

Call a finite set F *acceptable* (more precisely, *k-acceptable for B*) if $\mathcal{L}(2^k, F) \subseteq B$. Just as in the proof of Theorem 2.1, it suffices to prove the following lemma. In fact, it follows from the lemma there is a set A such that $D^k(A) = \mathcal{L}(2^k, A) = B$.

Lemma 8.3. *Let F be acceptable and suppose that $b \in B$. Then there is an acceptable set $G \supseteq F$ with $b \in D^k(G)$.*

Proof. Let $x_1, x_2, \ldots, x_{2^k}$ be indeterminates, and define the following homogeneous linear polynomials $p_j(x_1, \ldots, x_{2^j})$ for $1 \leq j \leq k$ by recursion on j:

$$p_1(x_1, x_2) = x_2 - x_1,$$
$$p_{j+1}(x_1, \ldots, x_{2^{j+1}}) = p_j(x_{2^j+1}, \ldots, x_{2^{j+1}}) - p_j(x_1, \ldots, x_{2^j}).$$

It is clear by induction on j that $p_j(x_1, \ldots, x_{2^j})$ has the form $c_1^j x_1 + \ldots + c_{2^j}^j x_{2^j}$ where $|c_i^j| = 1$ for $1 \leq i \leq 2^j$. It is also clear by induction on j that if values are assigned to $x_1, \ldots, x_j$ in a way which $p_j(x_1, \ldots, x_{2^j})$ and the polynomials which arise in its recursive definition above are all positive, then $p_j(x_1, \ldots, x_{2^j}) \in D^j(\{x_1, \ldots, x_{2^j}\})$. (For example, if $j=2$, we have $p_2(x_1, \ldots, x_4) = (x_4 - x_3) - (x_2 - x_1)$ and require that $x_2 > x_1, x_4 > x_3$, and $(x_4 - x_3) > (x_2 - x_1)$. It then follows that $p_2(x_1, \ldots, x_4) \in D^2(\{x_1, \ldots, x_4\})$.)

We will let $G = F \cup \{x_1, \ldots x_{2^k}\}$ for values of $x_1, \ldots, x_{2^k}$ chosen so that $p_k(x_1, \ldots, x_{2^k})$ and the polynomials used in its inductive definition are all positive as required above. Thus, to ensure that $b \in D^k(G)$, we also require that $p_k(x_1, \ldots, x_{2^k}) = b$ for these values of $x_1, \ldots, x_{2^k}$. This condition determines x_{2^k} in terms of $x_1, \ldots, x_{2^k - 1}$, and in fact solving it for x_{2^k} yields $x_{2^k} = q(x_1, \ldots, x_{2^k - 1}) + b$ where q is a homogeneous linear polynomial in $x_1, \ldots, x_{2^k - 1}$ with coefficients of absolute value 1. The main part of the argument is then to use the 2^{k-1}-bigness of B to show that we can choose x_i for $1 \leq i < 2^k$ to make G acceptable. To do this we use the following lemma which implies that B has an apparently stronger property involving several linear polynomials in several variables.

Lemma 8.4. *Suppose that A is t-big and that P is a finite set of linear nonconstant polynomials with integer coefficients in the indeterminates $x_1, \ldots, x_s$. Suppose further that for each polynomial $\sum_{i \leq s} a_i x_i + d$ in P, we have $1 \leq a_i \leq t$ for the leading coefficient a_i, i.e. the greatest i such that $a_i \neq 0$. Then it is possible to choose positive integer values of $x_1, \ldots, x_s$ in such a way that all of the polynomials in P take values in A.*

Proof. The proof of this is easy. First choose a value for x_1 so that all polynomials in P having no variable other than x_1 take values in A. From now on, treat x_1 as a constant. Then choose a value for x_2 so that all polynomials in P having x_2 as their only (remaining) indeterminate take values in A. Continue in this fashion until all of $x_1, \ldots, x_s$ have been assigned values so that all polynomials in P take values in A. Note that in the above process it is possible to first choose x_1 arbitrarily large, and then x_2 arbitrarily large, etc. ∎

By Lemma 8.4, to make G acceptable it suffices to construct a finite set P of polynomials satisfying the hypotheses of Lemma 8.4 with $A = B$, $t = 2^{k-1}$ and $s = 2^k - 1$ so that every element of $\mathscr{L}(2^k, G) \setminus (\mathscr{L}(2^k, F) \cup \{b\})$ can be expressed as the

value of a polynomial in P. First note that each x_i, $i < 2^k$, is obtained simply as the value of the polynomial x_i, while x_{2^k} is obtained as $q(x_1,\dots,x_{2^k-1})+b$, where all the coefficients in the linear homogeneous polynomial q have absolute value 1. It follows that any element u of $\mathscr{L}(2^k,G)$ can be written as $\sum_{j<2^k} b_j x_j + e$, where $|b_j| \le 2^k$ and $|e| \le m$, where $m = 2^{k-1}\max(F\cup\{b\})$. (The coefficients used to express elements of $\mathscr{L}(2^k,G)$ as linear combinations of elements of G cannot exceed 2^{k-1} in absolute value because these coefficients must sum to 0 and the sum of their absolute values is at most 2^k. Also, each x_j for $j < 2^k$ occurs exactly twice in the polynomials giving $x_1,\dots,x_{2^k}$.)

Let Q be the (finite) set of linear polynomials over the integers which are of the form $\sum_{j<2^k} b_j x_j + e$ where $|b_j| \le 2^k$ for all $j < 2^k$ and $|e| \le m$. The preceding argument shows that each $u \in \mathscr{L}(2^k,G)$ is the value of a polynomial in Q. Now let P be the set of all (necessarily nonconstant) polynomials in Q whose leading coefficient b_i satisfies $1 \le b_i \le 2^{k-1}$. Assume $u \in \mathscr{L}(2^k,G)$ and $u = b(x_1,\dots,x_{2^k-1}) = \sum_{j\le 2^k} b_j x_j + f$, where $b(x_1,\dots,x_{2^k-1}) \in Q$, and in fact $b(x_1,\dots,x_{2^k-1})$ is obtained by the procedure outlined above. Let b_i be the leading coefficient of $b(x_1,\dots,x_{2^k-1})$, where we assume temporarily that this polynomial is nonconstant. It must be shown that $1 \le b_i \le 2^{k-1}$. Finally we justify the assumption that the polynomial is nonconstant, provided that, in addition, $u \notin \mathscr{L}(2^k,F)\cup\{b\}$.

We first use a sign argument to show that $|b_i| \le 2^{k-1}$. (Of course, this can be omitted if we assume that A is 2^k-big rather than 2^{k-1}-big.) Since $u \in \mathscr{L}(2^k,G)$, we have $u = \sum_{j\le 2^k} d_j x_j + r$, where the sum of the positive (and also of the negative) d_j's is at most 2^{k-1} in absolute value and $|r| \le 2^{k-1}\cdot\max F$. Replacing x_{2^k} by $q(x_1,\dots,x_{2^k-1})+b$, where $q(x_1,\dots,x_{2^k-1}) = \sum_{j<2^k} q_j x^j$, we obtain $u = \sum_{j<2^k}(d_{2^k}q_j+d_j)x_j + r + d_{2^k}b$, so we may define $b_j = d_{2^k}q_j + d_j$ for $j < 2^k$. Consider first the case where $i = 2^k-1$ for the leading coefficient b_i. Then $b_i = d_{2^k} + d_{2^k-1}$, since $q_{2^k-1} = 1$. If $d_{2^k}\cdot d_{2^{k-1}} \ge 0$, then $|b_i| = |d_{2^k}+d_{2^k-1}| \le 2^{k-1}$. If $d_{2^k}\cdot d_{2^k-1} < 0$, then $|b_i| \le \max\{|d_{2^k}|,|d_{2^k-1}|\} \le 2^{k-1}$. This completes consideration of the case where $i = 2^k-1$. Suppose now that $i < 2^k-1$. If $q_i = 1$, then $b_i = d_{2^k} + d_i$, and we conclude that $|b_i| \le 2^{k-1}$ since the argument for the case $i = 2^k-1$ actually shows that $|d_v + d_u| \le 2^{k-1}$ whenever $1 \le u < v \le 2^k$. Suppose now that $q_i = -1$. Note that $0 = b_{2^k-1} = d_{2^k} + d_{2^k-1}$ (since b_{2^k-1} is not the leading coefficient). Hence $b_i = -d_{2^k} + d_i = d_{2^k-1} + d_i$, and again $|b_i| \le 2^{k-1}$ by the same principle, with $u = i, v = 2^k-1$. This completes the proof that $|b_i| \le 2^{k-1}$.

Next we show that $b_i > 0$. For this it suffices to ensure that the value of any polynomial in Q will have the same sign as the leading coefficient of the polynomial.

Specifically, we require that $x_1 > m$ and, for $1 < i < 2^k$, $x_i > 2^{k-1} \cdot \max\{x_j : j < i\} + m$. This is possible by the final remark in the proof of Lemma 8.4 and completes the proof that we may take $b_i > 0$. We also use the fact that polynomials in Q have the same sign as their leading coefficient to show that the polynomials $p_i(x_a, \ldots, x_c)$ (where $1 \leq i \leq k$, $1 \leq a$, and $c = a + 2^i - 1 \leq 2^k$) take positive values and thus that $b \in D^k(\{x_1, \ldots, x_{2^k}\})$ as mentioned at the beginning of the proof. This is immediate when $c < 2^k$, since each p_i has a positive leading coefficient and x_{2^k} does not appear, so $p_i(x_a, \ldots, x_c) \in Q$. However, if $c = 2^k$, then x_{2^k} must be replaced by $q(x_1, \ldots, x_{2^k-1}) + b$ before the leading coefficient is computed, so an additional argument is needed. We show by reverse induction on j that $p_j(x_a, \ldots, x_{2^k}) := n_j > 0$ for $1 \leq j \leq k, a = 2^k - 2^j + 1$. The base step when $j = k$ is immediate since $n_k = b > 0$ by choice of x_{2^k}. Also, $n_{j+1} = n_j - p_j(x_a, \ldots, x_c)$ where $c = 2^k - 2^j$ and $a = c - 2^j + 1$, by the definition of p_{j+1}. We have already remarked that $p_j(x_a, \ldots, x_c) > 0$ for $c < 2^k$, so if $n_{j+1} > 0$, it follows that $n_j > 0$, completing the reverse induction.

The above arguments show that every element u of $\mathcal{L}(2^k, G)$ can be expressed as the value of a polynomial in Q which is constant or is in P. We complete the proof by showing that the polynomial is non-constant, under the additional hypothesis that $u \notin \mathcal{L}(2^k, F)$. Thus there are no polynomials needed to express elements of $\mathcal{L}(2^k, G)$ in which all the x_i's for $i < 2^k$ are used but "unexpectedly" cancel out, which would ruin the argument. To prove this, let $v_j = x_j$ for $1 \leq j < 2^k$, and let $v_{2^k} = q(x_1, \ldots, x_{2^k-1})$. (Recall that $q(x_1, \ldots, x_{2^k-1}) + b = x_{2^k} \in G$.) We view $v_1, \ldots, v_{2^k}$ as elements in the vector space of homogeneous linear forms in $x_1, \ldots, x_{2^k-1}$ over the real field. Obviously, $v_1, \ldots, v_{2^k-1}$ are linearly independent since they form the standard basis of this $(2^k - 1)$-dimensional space. Now, let N be the set of 2^k-tuples $(c_1, \ldots, c_{2^k})$ in $\mathbb{R}^{2^k}$ such that $\sum_{j=1}^{2^k} c_j v_j = 0$. Then N is a 1-dimensional subspace of $\mathbb{R}^{2^k}$, by basic linear algebra. Since q has $2^k - 1$ coefficients and all have absolute value 1, there is a vector $\mathbf{p} = (p_1, p_2, \ldots, p_{2^k}) \in N$ such that $p_{2^k} = 1$, $\sum_{j \leq 2^k} |p_j| = 2^k$, and each p_j is an integer. Since N is 1-dimensional, it follows that any vector in N with integer components is an integer multiple of $\mathbf{p}$. Thus $\pm\mathbf{p}$ are the only nonzero vectors in N whose components are integers whose absolute values sum to at most 2^k.

Suppose now that $d \in \mathcal{L}(2^k, G) \setminus \mathcal{L}(2^k, F)$. We must show that either d is the value of a polynomial in P or $d = b$. Write d as $\sum_j d_j g^{(j)}$, where $g^{(j)} \in G, \sum d_j = 0$, and $\sum |d_j| \leq 2^k$. We cannot have $g^{(j)} \in F$ for all j since $d \notin \mathcal{L}(2^k, F)$. Now let c_i be the coefficient of x_i for $1 \leq i \leq 2^k$ in this linear combination, and let $\mathbf{n} = (c_1, \ldots, c_{2^k}) \neq \mathbf{0}$. If $\mathbf{n} \notin N$, then d is the value of a polynomial in P, since $x_1, \ldots, x_{2^k-1}$ do not all cancel out. If $\mathbf{n} \in N$, then $\mathbf{n} = \pm\mathbf{p}$. Thus $\sum |c_i| = 2^k \geq \sum |d_j| \geq \sum |c_i|$, so no terms

from $G\backslash F$ appear. Hence $d=\sum_{i\le 2^k} c_i x_i = c_1 v_1 + \ldots + c_{2^k-1} v_{2^k-1} + c_{2^k}(v_{2^k}+b)$. Since $(c_1,\ldots,c_{2^k}) \in N$ and $|c_{2^k}|=1$, it follows that $d=\pm b$. Since d,b are nonnegative, it follows that $d=b$, so the proof is complete. ∎

Remark 8.5. The following is a slightly different approach to the proof of Lemma 8.3. It is based on the same choice of G as $F\cup\{x_1,\ldots x_{2^k}\}$, where $b=p_k(x_1,\ldots,x_{2^k})$, but the x_i's are now expressed in terms of new variables $y_1,\ldots,y_{2^k}$. Considering the dual of the inequality system required for the x_i's in Lemma 8.3 one can write them as linear polynomials of the non-negative variables $y_1,\ldots,y_{2^k}$ as follows. Let $h(n)$ be the maximum h such that 2^h divides n. Define $x_n = y_n + y_{n-1} + y_{n-2} + y_{n-4} + y_{n-8} + \ldots + y_{n-2^{h(n)}-1}$ (exactly $h(n)+1$ terms), for example $x_n = y_n$ for all odd n, and $x_8 = y_8+y_7+y_6+y_4$. In general define $x_n^{(i)} = \sum\{y_j : j = 2^i n, 2^i n - 2^i, \ldots, 2^i n - 2^{i+h-1}\}$. Then for even n we have $x_n^{(i)} - x_{n-1}^{(i)} = x_{n/2}^{(i+1)}$, finally $x_1^{(k)} = y_{2^k}$. Fix $y_{2^k} = b$, and choose $y_1,\ldots,y_{2^k-1}$ to be any rapidly growing sequence. Then positivity of the differences used to obtain $b \in D^k(G)$ and the inequalities $0 < b_i \le 2^{k-1}$ for the coefficients of the leading terms of polynomials in the variables $y_1,\ldots,y_{2^k-1}$ needed to express elements of $\mathcal{L}(2^k,G)\setminus(\mathcal{L}(2^k,F)\cup\{b\})$ follow immediately. Of course, Lemma 8.4 is now applied to these polynomials rather than to polynomials in $x_1,\ldots,x_{2^k-1}$. The rest of the proof (linear independence, b is the only constant added to $\mathcal{L}(2^k,G)$) becomes somewhat more involved.

9. Sequences with a unique k^{th} difference set

The following result is an extension of Theorem 3.2. The reader may wish to assume that $k=1$ in a first reading of the proof. This simplifies some aspects of the argument and gives a proof of Theorem 3.2 which is different from, but related to, the proof in Section 3.

Theorem 9.1. *Suppose that $0 \in A \subseteq \mathbb{N}_0$ is a B_ℓ-set with $\ell = 2^{2k-1}+2^{k-1}$ ($k \in \mathbb{N}_0$, $k \ge 1$). If $0 \in X \subseteq \mathbb{N}_0$ has the same k'th difference set, $D^k(X) = D^k(A)$, then $X = A$.*

Proof. As in the proof of Theorem 8.2, let $\mathcal{L}(t,A)$ be defined as the set of positive numbers which can be obtained as a linear combination of the form $x=\sum_{i\in S}\alpha_i a_i$, where all α_i's are nonzero integers, $\sum_{i\in S}\alpha_i = 0$, and $\sum_{i\in S}|\alpha_i| \le t$. (For $S=\emptyset$ the sum is 0.) The set $S = S(x) = \{i : \alpha_i \ne 0\} \subseteq \mathbb{N}_0$ is called the *support* of the sum, and also the support of x. Note that the number $x \in \mathcal{L}(t,A)$ can have more than one support, (then $S(x)$ is defined as one of the supports), and distinct numbers (like $2a_i - 2a_j$ and $a_i - a_j$) can have the same support. Moreover, an x can have a unique support in $\mathcal{L}(t,A)$ and several supports in $\mathcal{L}(t',A)$ for some $t' > t$. (Hence the precise notation would be $S(t,x)$ for a support of $x \in \mathcal{L}(t,A)$, but the omission of t will not cause any misunderstanding.) We frequently write an element

$x \in \mathscr{L}(t,A)$ in the form $\sum_{i\in I}\varepsilon^{(i)}a^{(i)}$ where $\varepsilon^{(i)} \in \{1,-1\}$, $|I| \le t$, $\sum\varepsilon^{(i)} = 0$, and $(a^{(1)},\dots,a^{(i)},\dots,a^{(|I|)})$ is a *sequence* (or *multiset*) of some members of A.

We have that $D^k(C) \subseteq \mathscr{L}(2^k,C)$ holds for any sequence with $0 \in C \subseteq \mathbb{N}_0$. Here equality does not necessarily hold, but one can prove by induction on k that for any sequence $c^{(1)},\dots,c^{(i)},\dots,c^{(2^k)}$ ($c^{(i)} \in C$, $c^{(i)} = c^{(j)}$ is allowed) of length 2^k one can find a sequence $\varepsilon^{(i)} \in \{1,-1\}$ such that $\sum_{1\le i\le 2^k}\varepsilon^{(i)} = 0$ and

$$\sum_{1\le i\le 2^k} \varepsilon^{(i)}c^{(i)} = y \in D^k(C). \tag{9.2}$$

Note that $S(y)$ contains each element i of the multiset $\{i : c_i \in (c^{(1)},\dots,c^{(i)},\dots)\}$ which occurs only once (and those appearing with odd multiplicities).

As A is a B_ℓ-set, every element of $X \subseteq \mathscr{L}(2^k,A)$ has a unique support. Even more, $x_1 \in \mathscr{L}(4^k,A)$, $x_2 \in \mathscr{L}(2^k,A)$, $x_1 = x_2$ imply that $S(x_1) = S(x_2)$. To see this, note that $x_1 = u_1 - v_1$, where u_1, v_1 are each sums of n_1 elements of C (with repetitions allowed) and $2n_1 \le 4^k$. Similarly, $x_2 = u_2 - v_2$, where u_2, v_2 are each sums of n_2 elements of C (with repetitions allowed) and $2n_2 \le 4^k$. We then apply the B_ℓ-property of C to the equation $u_1 + v_2 = u_2 + v_1$ to conclude that the terms from C used in the combined sum $u_1 + v_2$ coincide as a multiset with the terms in $u_2 + v_1$. Since there is no overlap between the terms in u_1 and v_1 or between the terms in u_2 and v_2, it follows that the terms for u_1 coincide with those for u_2, and the terms for v_2 coincide with those for v_1, and thus the corresponding supports are the same. We now apply this fact to show that elements x of $D^k(X)$ can be represented as a linear combination of elements of X whose supports have a special property. Let $x \in D^k(X)$, and write it in the form $x = \sum_{i\in I}\alpha_i x_i$ (where α_i are non-zero integers with $\sum\alpha_i = 0$, $\sum|\alpha_i| \le 2^k$, because $D^k(X) \subseteq \mathscr{L}(2^k,X)$), and let $S_i' = S(x_i) \setminus \left(\cup_{j\ne i, j\in I} S(x_j)\right)$, (i.e., S_i' consists of the indices of the a_j's used only in the linear combination providing $x_i \in \mathscr{L}(2^k,A)$). Then

$$\sum_{i\in I} |S_i'| \le 2^k. \tag{9.3}$$

Indeed, as $x_i = \sum_{m\in I_i}\alpha_{i,m}a_m \in \mathscr{L}(2^k,A)$, x can be written as a member of $\mathscr{L}(4^k,A)$. However, $x \in D^k(X) = D^k(A) \subseteq \mathscr{L}(2^k,A)$, so we can write it as a $\pm$ sum of at most 2^k members of A.

$$\sum_{i\in I}\alpha_i\Big(\sum_{m\in I_i}\alpha_{i,m}a_m\Big) = x = \sum_{j\in J}\varepsilon^{(j)}a_j.$$

The B_ℓ property, (where $2\ell = 4^k + 2^k$), implies that these two sums coincide. So all but at most 2^k terms in the left hand side cancel each other. Obviously, the terms corresponding to the elements in (9.3) do not cancel, finishing its proof.

The very same proof gives the following sharpening of (9.3). Not only is the total size of the disjoint sets S_i' at most 2^k, but the total size of the coefficients appearing in them cannot exceed the same bound. Using the notations of the previous paragraph we have

$$\sum_{i\in I}\left(\sum_{m\in S_i'}|\alpha_{i,m}|\right)\le 2^k. \tag{9.4}$$

Let $\mathcal{S}$ be the family of supports of the elements of X in $\mathcal{L}(2^k,A)$, i.e., fix $t=2^k$. Then $S(x)$ is uniquely determined and has at most 2^k elements for each $x\in X$. Using (9.3), (9.4), and some hypergraph theory we are going to prove that $\mathcal{S}=\{\emptyset\}\cup\{\{0,i\}:i\in\mathbb{N}_0\setminus\{0\}\}$, which will easily imply $X=A$. In the course of the proof we will verify more and more properties of the family $\mathcal{S}$ until our final conclusion. Note that the support of $a_0=0$ is $\emptyset$, and, for $i\neq 0$, the support of $a_i\in A$ in $\mathcal{L}(4^k,A)$ is $S(a_i)=\{0,i\}$; (we have $(A\cup X)\subseteq D^k(A)=D^k(X)\subseteq\mathcal{L}(2^k,X)\subseteq\mathcal{L}(4^k,A)$).

For any $S\in\mathcal{S}$ there are only finitely many $x\in X$ with the same support $S=S(x)$. As $|X|=\infty$ this implies that $\mathcal{S}$ contains infinitely many distinct supports. Divide $\mathcal{S}$ into subfamilies according to the cardinalities of its members, let $\mathcal{S}_i=\{S\in\mathcal{S}:|S|=i\}$ $(0\le i\le 2^k)$. Suppose that $\mathcal{S}_0\cup\ldots\cup\mathcal{S}_{a-1}$ is finite, but $|\mathcal{S}_a|=\infty$. We will use the following result of Erdős and Rado [2]: For all positive integers a, b if $\mathcal{F}$ is a family of sets each having at most a elements such that $|\mathcal{F}|>a!(b-1)^a$, then $\mathcal{F}$ contains a *delta system* of size b, i.e., there exist $S_1,\ldots,S_b\in\mathcal{F}$ and a set K (called a *kernel*) such that $K\subseteq S_j$ for all $1\le j\le b$, and the sets $S_j\setminus K$ are pairwise disjoint. Actually, for our application we may assume that $\mathcal{F}$ is infinite, and in this case the result is very easy. (Let K be a set of maximal cardinality such that $K\subseteq S$ for infinitely many $S\in\mathcal{F}$. If T is any finite set such that $T\supseteq K$, then all but finitely many $S\in\mathcal{F}$ satisfy $S\cap T=K$. Then one may recursively define sets $S_1,S_2,\ldots\in\mathcal{F}$ so that $S_i\supseteq K$ and $S_i\cap\cup_{j<i}S_j=K$. Thus K is a kernel for the *infinite* sequence $S_1,S_2,\ldots$.) Applying the result of Erdős and Rado [2] with $b=2^{k+1}$ and $\mathcal{F}=\mathcal{S}_a$, we obtain that there exists a 2^{k+1}-element set $J\subseteq\mathbb{N}_0$, a set K such that $K\subseteq S(x_j)$ for all $j\in J$, and the sets $S(x_j)\setminus K$ are pairwise disjoint, distinct, nonempty sets.

We claim that for *all* $x\in X$,

$$|S(x)\setminus K|\le 1. \tag{9.5}$$

Indeed, let $x\in X$ be arbitrarily chosen. As $|S(x)|\le 2^k$ the pairwise disjointness of the members of $\{S(x_j)\setminus K:j\in J\}$ imply that there exists a (2^k-1)-element set $I\subseteq J$ such that $(S(x_i)\setminus K)\cap S(x)=\emptyset$ for all $i\in I$. The 2^k sets of the form $S(x)\setminus K$ and $S(x_i)\setminus K$ $(i\in I)$ are pairwise disjoint. By (9.2) there is a linear combination of x_i's and x with suitable $\varepsilon,\varepsilon_i=\pm 1$ coefficients such that $y=\varepsilon x+\sum_{i\in I}\varepsilon_i x_i$ belongs to $D^k(X)$. Then (9.3) implies that $|S(x)\setminus K|+\sum_{i\in I}|S(x_i)\setminus K|\le 2^k$. Here all the 2^k-1 sets $S(x_i)\setminus K$ are non-empty, hence $|S(x)\setminus K|\le 1$.

Let $N=\{x\in X:|S(x)\setminus K|=1\}$. (9.5) implies that $\mathcal{S}_a$ forms an (infinite) delta system (with kernel K). All but finitely many members of X belong to N. For any member $y=\sum_i \alpha_i a_i \in \mathcal{L}(2^k,A)$ the *restriction* $y|K$ is defined as $\sum_{i\in K}\alpha_i a_i$. One can find $x_1,\dots,x_{2^k}\in N$ such that $x_j|K=d$ is a constant, and the 1-element sets $S(x_j)\setminus K$ are pairwise disjoint. (Here we are dropping the convention that x_i is the $(i+1)^{st}$ element of X.) Write the elements x_j $(1\le j\le 2^k)$ in the form $x_j=\sum_{i\in K}\alpha_i a_i+\alpha(x_j)a_{f(x_j)}=d+\alpha(x_j)a_{f(x_j)}$. As the sum of the coefficients of any member of $\mathcal{L}(2^k,A)$ is 0, we get that $\alpha(x_j)=-\sum_{i\in K}\alpha_i =:\alpha$ is a constant, too. Fix the numbers x_j, $1\le j\le 2^k$ and the corresponding coefficients $\alpha_j(x)$ and α_i $(i\in K)$, as well as the numbers d and α.

Write all $x\in N$ in the form $\sum_{i\in K}\alpha_i(x)a_i+\alpha(x)a_{f(x)}$. We claim that for all $x\in N$ their restrictions coincide and in fact:

$$\alpha_i(x)=\alpha_i \text{ for all } i\in K \text{ and } \alpha(x)=\alpha. \tag{9.6}$$

Indeed, there is a set $J\subseteq\{1,\dots,2^k\}$ of size 2^k-1 such that for every $j\in J$ the sets $S(x_j)\setminus K$ avoid $S(x)\setminus K$. Consider a suitable linear combination, $y\in D^k(X)$, provided by (9.2) of these 2^k-1 numbers $\{x_j:j\in J\}$ and x. We get the coefficients $\varepsilon_j\in\{1,-1\}$ $(j\in J)$ and $\varepsilon(x)\in\{1,-1\}$ such that $\varepsilon(x)+\sum_{j\in J}\varepsilon_j=0$ and

$$y=\varepsilon(x)x+\sum_{j\in J}\varepsilon_j x_j=$$

$$\alpha(x)\varepsilon(x)a_{f(x)}+\sum_{j\in J}\alpha\varepsilon_j a_{f(x_j)}+\sum_{i\in K}\left(\alpha_i(x)\varepsilon(x)+\alpha_i\sum_{j\in J}\varepsilon_j\right)a_i. \tag{9.7}$$

The support of this linear combination (in $D^k(X)\subseteq\mathcal{L}(2^k,A)$) contains the 2^k elements $a_{f(x)},a_{f(x_j)},j\in J$ outside K, so its restriction to K should give 0 (by the uniqueness of the support in $D^k(X)$). We have that $y|K=0$, so the coefficient of a_i in (9.7) is 0 for every $i\in K$, giving $\alpha_i(x)\varepsilon(x)=-\alpha_i\sum_{j\in J}\varepsilon_j$. However the last sum equals $-\varepsilon(x)$, so it gives the first statement in (9.6). The second statement follows from the fact that the sum of coefficients of x is 0, $\alpha(x)+\sum_{i\in K}\alpha_i=0$, and this is the same for all x_j.

From (9.6) and the fact that all $x\in N$ have the restriction d fixed two paragraphs above, we see that each $x\in N$ can be written in the form $x=d+\alpha a_{f(x)}$. Inequality (9.4) (applied to y in (9.7)) implies that $2^k|\alpha|\le 2^k$, so $|\alpha|=1$. Only finitely many numbers of the form $d-a_j$ can be nonnegative, but N is infinite, so necessarily $\alpha=1$. Hence, for all $x\in N$

$$x=d+a_{f(x)}, \tag{9.8}$$

where the $a_{f(x)}$'s are distinct members of A.

Our next claim is that $|K| = 1$. If $x \in X$, then its support $S(x)$ cannot be a singleton, because the sum of the coefficients (in $\mathcal{L}(2^k, A)$) is 0. Since N is nonempty, there exists $x \in X$ with $|S(x) - K| = 1$, so $K \neq \emptyset$. Let $x_0 = 0$ so x_0 has empty support, i.e. $S(x_0) = \emptyset$. Take an appropriate 2^k-element linear combination $\varepsilon_0 x_0 + \sum_{j \in J} \varepsilon_j x_j = z \in D^k(A)$ provided by (9.2), (here $|J| = 2^k - 1$, $x_j \in N$, $x_j = d + a_{f(x_j)}$). The support of z is $\cup_{j \in J} S(x_j)$, which has cardinality $|J| + |K| = 2^k - 1 + |K|$. Since any element of $D^k(A)$ has support of cardinality at most 2^k, it follows that $|K| \leq 1$, so $|K| = 1$.

Let $K = \{v\}$, so by the definition of d, $d = \alpha_v a_v$. Thus, by (9.8), each $x \in N$ can be written in the form $x = \alpha_v a_v + 1 \cdot a_{f(x)}$. Since the coefficients in this linear combination must sum to 0, we get that $\alpha_v = -1$, implying

$$x = a_{f(x)} - a_v \tag{9.9}$$

for all $x \in N$.

We claim that *each* element $x \in X$, other than $x_0 = 0$, can be written in the form (9.9). To prove this it suffices to show that $X \setminus \{0\} \subseteq N$. But this is clear, since if $x \in X$ and $x \neq 0$, the support of X cannot be a singleton (as already remarked) and so must have at least two elements, so $S(X) \subseteq K$ cannot hold.

Next, we show that $a_v = 0$, and hence, by (9.9) that $X \subseteq A$. We now return to our usual convention that x_i is the $(i+1)^{st}$ element of X (instead of being fixed as before). Since $a_v = a_v - a_0 \in D^k(A) = D^k(X)$, we have that $a_v \in \mathcal{L}(2^k, X)$. Let $a_v = \sum_{i \in I} \beta_i x_i$, where $\sum_{i \in I} \beta_i = 0$ and $\sum_{i \in I} |\beta_i| \leq 2^k$. Then, by (9.9)

$$a_v = \sum_{i \in I} \beta_i a_{f(x_i)} - \sum_{i \in I} \beta_i a_v = \sum_{i \in I} \beta_i a_{f(x_i)}. \tag{9.10}$$

We now assume for a contradiction that $a_v > 0$ and show that (9.10) violates the hypothesis that A is a B_ℓ set. To do this, we first rewrite (9.10) as an equality of sums of elements of A. Let $I_+ = \{i \in I : \beta_i > 0\}$ and $I_- = \{i \in I : \beta_i < 0\}$. Then, by (9.10),

$$a_v + \sum_{i \in I_-} |\beta_i| a_{f(x_i)} = \sum_{i \in I_+} \beta_i a_{f(x_i)}. \tag{9.11}$$

By "padding out" each side of (9.11) with sufficiently many terms equal to $a_0 = 0$, each side of (9.11) may be viewed as a sum of ℓ elements of A. Thus, since A is a B_ℓ-set, the two sides of (9.11) are identical up to a rearrangement, after this padding. Since, by (9.9), $f(x_i) > v$ for all $i > 0$ (and we may take $f(x_0) = v$ to make (9.9) hold for $x = x_0$), it follows from the assumption that $a_v > 0$ that $0 \notin I = I_- \cup I_+$. Thus the two sides of (9.11) are padded with the same number of terms a_0, and thus the two

sides of (9.11) differ by at most a rearrangement even before the padding. Hence $I_- \subseteq I_+$, since every term which occurs on the left-hand side of (9.11) must occur on the right-hand side also. Since $I_- \cap I_+ = \emptyset$, it follows that $I_- = \emptyset$, so $I = I_+$. Summing the coefficients from the two sides of (9.10), we get that $1 = \sum_{i \in I} \beta_i = 0$, our desired contradiction. Hence $a_v = 0$. (We thank I. Ruzsa for pointing out a gap in our original proof that $a_v = 0$.)

To complete the proof that $X = A$, we show that $A \subseteq X$. We have $a_0 = 0 \in X$ by hypothesis. Assume for a contradiction that $a_j \in A \setminus X$, where $j > 0$. Then $a_j \in D^k(X) \subseteq D^k(A \setminus \{a_j\})$, since $X \subseteq A \setminus \{a_j\}$. Thus $j \notin S(a_j)$, contradicting the fact that $a_j = a_j - a_0$ and the uniqueness of supports. ∎

Remark 9.11. With a little more effort we can prove the following result about finite B_ℓ sequences. If $a_0 = 0 < a_1 < \ldots < a_n$ is a B_ℓ sequence with $\ell = 2^{2k-1} + 2^{k-1}$, $x_0 = 0 < x_1 < \ldots < x_m$, $D^k(A) = D^k(X)$ and $n > 2^{4k2^k}$, then either $X = A$ or $X = a_n - A$. One can get a smaller bound for n if instead of the Erdős-Rado theorem one uses the following result of Füredi and Tuza [4]: If $\mathcal{F}$ is a family of at most a element sets with $|\mathcal{F}| > \binom{a+b-1}{a}$, then it contains b disjointly representable members, i.e., $S_1, \ldots, S_b \in \mathcal{F}$ such that $S_i \setminus \left(\cup_{j \neq i} S_j\right) \neq \emptyset$ for all $1 \leq i \leq b$.

10. Some questions

1. Is $\{D(X) : X \subseteq \mathbb{N}_0\}$ a Borel subset of $2^{\mathbb{N}_0}$ with its usual (product) topology?

2. Is there a sequence B such that $D(X) = B$ has exactly $\aleph_0$ solutions X with $0 \in X \subseteq \mathbb{N}_0$?

3. For which positive integers m is there a sequence B^m such that $D(X) = B^m$ has exactly m solutions X with $0 \in X \subseteq \mathbb{N}_0$? (We showed that every power of 2 is such an m.)

4. Which real numbers occur as densities of sets which have unique difference sets?

5. Given k, what is the least $t = t(k)$ such that every t-big set is a k^{th} difference set? It seems reasonable to conjecture that $t(k) = k$ although from Theorem 8.2 we know only that $t(k) \leq 2^{k-1}$. It seems likely that the proof of Theorem 8.2 can be modified to show that $t(3) \leq 3$. We have no lower bounds for $t(k)$.

6. Does the set of primes have a unique difference set? What about other sets of integers commonly studied in number theory?

Acknowledgements. The authors are indebted to the referees for their helpful comments and to I. Z. Ruzsa for pointing out a small gap in our original proof of Theorem 9.1.

References

[1] R. DOWNEY, Z. FÜREDI, C. JOCKUSCH and L. A. RUBEL: Difference sets and recursion theory, in preparation

[2] P. ERDŐS and R. RADO: Intersection theorems for systems of sets, *J. London Math. Soc.* **35** (1960), 85–90.

[3] P. ERDŐS, A. SÁRKÖZY, and V. T. SÓS: On additive properties of general sequences, *Discrete Math*, **136** (1994), 75–99.

[4] Z. FÜREDI and ZS. TUZA: Hypergraphs without a large star, *Discrete Mathematics* **55** (1985), 317–321.

[5] H. HALBERSTAM and K. F. ROTH: *Sequences*, Springer-Verlag, New York, 1983.

[6] I. Z. RUZSA: On difference-sequences, *Acta Arithmetica*, **25** (1974), 151–157.

[7] I. Z. RUZSA: On difference sets, *Studia Scientiarum Mathematicarum Hungarica*, **13** (1978), 319–326.

[8] I. Z. RUZSA: Difference sets and the Bohr topology, I, preprint.

Department of Mathematics,
University of Illinois, 1409 West Green St.,
Urbana, IL 61801-2917, USA
z-furedi@math.uiuc.edu,
jockusch@math.uiuc.edu