Difference sets and the Bohr topology

by I. Z. Ruzsa*

Mathematical Institute of the
Hungarian Academy of Sciences
Budapest, Pf. 127.
H-1364 Hungary.

Abstract. The structure of difference sets of sets of natural numbers having a positive upper density is investigated, with a particular attention to their behaviour in the Bohr topology.

* Partially supported by Hungarian National Foundation for Scientific Research Grant No. 1811.

0. Outline

This work investigates difference sets of sets of integers having a positive upper density. Our primary point of view is number theoretical, but the problem has also a topological aspect - these are explained in sections 1 and 2, respectively.

Theorems denoted by letters are quotations, numbered ones are new.

1. Arithmetical introduction

We shall be interested in the structure of the difference set

$$D(A) = A-A = \{a-a' : a, a' \in A\}$$

of large sets A of integers, "large" meaning for most of the time a positive (upper) asymptotical density. If we use the same letter A to denote the counting function

$$A(x) = |\{a: a \in A, 1 \leq a < x\}|$$

(observe that only the positive elements have been taken into account), then this assumption is

$$\overline{d}(A) = \limsup A(x)/x > 0 .$$

Problems concerning the structure of these sets arose in two different contexts, one number-theoretical and another topological - group-theoretical, to be detailed in the next section.

It was conjectured by L. Lovász (and perhaps earlier by P. Erdős), and proved by A. Sárközy [1978 abc], that the difference set $A-A$ of an arbitrary set A of positive upper density always contains a square, a prime-minus-one and a prime-plus-one

(generally not with the same prime).

1.1 Definition. We call a set H of positive integers intersective, if

$$(A-A) \cap H \neq \emptyset ,$$

whenever $\bar{d}(A)>0$.

Thus the sets $H_1=(n^2)$, $H_2=(p-1:\ p \text{ prime})$ and $H_3=(p+1:\ p \text{ prime})$ are examples of intersective sets. Other examples include: every set H that contains arbitrarily long intervals; every set H with the property that for arbitrary k one can find a set B of k integers such that all the positive elements of $B-B$ belong to H .

We want to decide which sets are intersective and which are not; in other terms, we are interested in the filter $\underset{\sim}{D}$ generated by the difference sets of sets of positive upper density:

(1.2) $$\underset{\sim}{D} = (D:\ D\subset\mathbb{Z},\ D\supset D(A) \text{ for some } A \text{ with } \bar{d}(A)>0) .$$

That this is indeed a filter was proved by Stewart and Tijdeman [1979]. This means that for any two sets A_1 , A_2 with $\bar{d}(A_1)>0$ and $\bar{d}(A_2)>0$, there is a third set A such that $\bar{d}(A)>0$ and

(1.3) $$(A-A) \subset (A_1-A_1) \cap (A_2-A_2) .$$

The sharp inequality $\bar{d}(A)\geq\bar{d}(A_1)\bar{d}(A_2)$ was proved by Ruzsa [1978].

Every result concerning intersective sets has a dual formulation in terms of this filter. For example (1.3) means that the union of two non-intersective sets is not intersective either. The result that an H containing arbitrarily long intervals is

intersective asserts that $D(A)$ has bounded gaps if A has a positive upper density.

Among non-intersective sets we introduce a hierarchy by defining a measure of intersectivity.

1.4 Definition. By the measure of intersectivity of a set H of integers we mean the quantity

(1.5) $$\delta(H) = \sup \{\bar{d}(A): H \cap (A-A)=\emptyset\} .$$

So intersective sets have $\delta(H) = 0$.

It is known (Stewart-Tijdeman [15] and Ruzsa [13]), that the concept of intersectivity remains unchanged, even the value of $\delta(H)$ is not affected, if we replace upper density by lower density or asymptotical density, or if we loosen the requirement to $d(A\cap(A+h))=0$ for all $h\in H$.

The most effective method known to prove that a set is intersective makes use of another class of sets which we shall call correlative.

1.6 Definition. We say that a set H of integers is correlative, if every sequence (y_n) of complex numbers, bounded in square mean, that is satisfying

$$\sum_{n\le N} |y_n|^2 = O(N)$$

and having "H-correlation" 0 , that is

$$\sum_{n\le N} y_{n+h}\bar{y}_n = o(N)$$

for all $h\in H$, must have a zero "mean":

$$\sum_{n\le N} y_n = o(N) .$$

THEOREM A (Kamae - Mendes France [8]). Correlative sets are intersective.

It is easy to understand why: given a set A, put $y_n=1$ if $n\in A$, 0 otherwise. The applicability of this criterion lies in the less obvious equivalent formulations.

THEOREM B (Kamae - Mendes France [8], Ruzsa [13]). Correlativity is equivalent to each of the following properties:

a) Van der Corput's property: if (u_n) is a sequence of real numbers such that $(u_{n+h}-u_n)$ is uniformly distributed modulo one for every $h\in H$, then (u_n) itself must also be uniformly distributed.

b) Positive polynomial property: for every $\varepsilon>0$ there exists a trigonometrical polynomial

$$f(x) = c_0 + \sum_{h\in H} c_h \cos hx \tag{1.7}$$

such that $f(0)=1$, $f(x)\geq 0$ for all x and $c_0\leq\varepsilon$.

c) Every measure Λ on $[0, 2\pi)$ with the property

$$\int \cos hx \, d\Lambda(x) = 0$$

for all $h\in H$ must be continuous at 0, that is $\Lambda(\{0\})=0$.

For applications, the form b) with trigonometric polynomials seems to be best suited.

Kamae and Mendes France also gave the following criterion.

THEOREM C. If the set H is such that for every natural number d there is a sequence $(h_j^{(d)})$ of elements of H, all divisible by d and such that $(h_j^{(d)}u)$ is uniformly distributed

modulo 1 for every irrational u, then H is correlative and a fortiori intersective.

While this condition is easily seen not to be necessary, it has the advantage that it is expressed in terms of a property that has been investigated for most "natural" sets (primes, values of polynomials &c).

Until recently, every set known to be intersective was also correlative.

THEOREM D (Bourgain [5]). There exists an intersective set that is not correlative.

The hardest part in constructing such an example is to find a method to prove intersectivity, which is not even in a hidden connection with correlativity; Bourgain solves this by an ingenious combinatorial argument.

On the other hand, to check the intersectivity of a set we may try it on certain subclasses of the class of sets of positive density.

1.8 Definition. A set H is combinatorially intersective, if it has the following property: no matter how we split the set of natural numbers into finitely many classes

$$\mathbb{N} = A_1 \cup \ldots \cup A_k , \tag{1.9}$$

some of them must have a difference in H, that is

$$H \cap \bigcup (A_i - A_i) \neq \emptyset .$$

Since in a partition (1.9) at least one of the sets A_i must have a positive upper density, intersective sets are also

combinatorially intersective.

1.10 Definition. Call a set H weakly intersective, if it intersects the difference set of every set A with bounded gaps, that is, if $A=(a_1, a_2, \ldots)$ where always $a_j<a_{j+1}<a_j+K$ with some fixed K, then $H\cap(A-A)\neq\emptyset$.

If A has bounded (by K) gaps and its minimal element is a, put $A_i=A-a+i$ for $i=1, \ldots K$. Then clearly

$$\bigcup A_i = \underset{\sim}{N}$$

and $D(A_i)=D(A)$ for all i. This consideration shows that combinatorially intersective sets are weakly intersective. The converse is also true.

THEOREM 1. The concepts of weak and combinatorial intersectivity are equivalent. In other words, if the sets $A_1, \ldots, A_k$ form a partition of the set of natural numbers, then there is a set B with bounded gaps and a j, $1\leq j\leq k$ such that

(1.11) $$D(A_j) \supset D(B) .$$

One can even find a B that is infinite in both directions:

$$B = (b_j)_{j=-\infty}^{\infty}, \qquad b_j<b_{j+1}<b_j+K ,$$

while (1.11) can be strengthened as follows: for every finite $C\subset B$ there is an integer m such that $C+m\subset A_j$.

Observe that (1.11) is the case $|C|=2$ of this last assertion.

On the other hand, combinatorial intersectivity does not imply intersectivity.

THEOREM E (Kríz [9]). <u>There exists a combinatorially intersective set H that is not intersective; we can even have $\delta(H)>1/2-\varepsilon$. In terms of difference sets, there is a set A of density $d(A)>1/2-\varepsilon$ such that A-A does not contain any set of the form B-B, where B has bounded gaps.</u>

The 1/2 in Theorem E is optimal. If $\bar{d}(A)>1/2$, then (exercise) $A-A=\mathbb{Z}$. If $\bar{d}(A)=1/2$ and A-A does not contain every integer, say $m\notin A-A$, then it is easily shown that all multiples of 2m are in A-A.

We devote sections 6-9 to a new proof of this important result. The relation of my proof to Kríz's is discussed in §10

Let us try now even more special sets. Arithmetical progressions are too special; the next idea is generalized arithmetical progressions

$$U(u,\ \varepsilon) = \{n:\ \|un\|<\varepsilon\} \tag{1.12}$$

with some $\varepsilon>0$, where the "norm" of x now is

$$\|x\| = \min\ (\{x\},\ 1-\{x\}),$$

the distance of x from the nearest integer. For $u=1/q$ and $\varepsilon<1/q$ we obtain the set of multiples of q.

While the intersection of ordinary arithmetical progressions is also an arithmetical progression, this does not hold for these generalized sequences, thus it is worth considering a multidimensional version. For

$$\underline{u} = (u_1,\ \ldots\ u_k) \qquad (u_i \text{ real})$$

let

$$U(\underline{u},\ \varepsilon) = \{n:\ \|u_j n\|<\varepsilon \text{ for } j=1,\ \ldots\ k\}, \tag{1.13}$$

These sets are well known (and easily seen) to have a positive density, even bounded gaps, and the filters generated by them and their difference sets are the same, since

$$U(\underline{u}, \varepsilon) \subset D(U(\underline{u}, \varepsilon)) \subset U(\underline{u}, 2\varepsilon) .$$

Hence if a set is weakly intersective, it must intersect the difference set of every $U(\underline{u}, \varepsilon)$, which is equivalent to saying that it intersects every $U(\underline{u}, \varepsilon)$.

1.14 Definition. Call a set H of integers approximative, if it intersects every $U(\underline{u}, \varepsilon)$, or in other words, if for every real $u_1, \ldots u_k$ and $\varepsilon>0$ there is a $h\in H$ such that

$$\|hu_j\| < \varepsilon , \quad j=1, \ldots k .$$

We can summarize the know implications as follows:

correlative $\not\Rightarrow$ intersective $\not\Rightarrow$ combinatorially intersective $\rightarrow$ approximative .

1.15 Main problem. Are combinatorial intersectivity and approximativity equivalent?

2. Topological introduction

The problem about intersective and correlative sets has also arisen in a different context. For a non-compact topological group G (the simplest of which, the group of integers, will be in the focus of our interest), there exists a certain finest topology that is coarser than the original and that makes the group bounded (it may not be a Hausdorff topology). This is the so called Bohr topology, which is of primary importance to the study of almost periodic functions and gives rise to the Bohr compactification.

"Coarser" means that our new open sets must be open in the old sense; "bounded" means that if U is a new open set, G can be covered by a finite number of translates of U :

$$G = \bigcup_{j=1}^{k} (U+a_j) \tag{2.1}$$

with some $a_1, \ldots a_k \in G$. In general, call a set U big, if (2.1) holds with suitable $a_1, \ldots a_k$.

Observe that for integers, this is the condition of bounded gaps. From this aspect, the natural set to consider is the set of all integers, positive and negative; this fact, however, does not affect seriously the majority of our considerations.

Now, in a topological group, if U is a neighbourhood of 0 , then we can always find neighbourhoods U_k of 0 , such that $U_1=U$, $U_{k+1}-U_{k+1} \subset U_k$. In particular, if U is a Bohr neighbourhood, then there is a chain (U_k) of big open sets (big in the

sense (2.1)) such that $U_1=U$ and $U_{k+1}-U_{k+1}\subset U_k$ for every k. This can serve as a definition of the Bohr topology.

Now the question arises whether one could reduce the number of steps in this process, that is whether instead of an infinite sequence, a sequence of a fixed length is sufficient. For a large class of groups this is indeed the case, see Alfsen-Holm [1] and Landstad [10].

For commutative groups, the Bohr topology can also be characterized as the coarsest topology making all the (continuous) characters continuous. This means that we can select the sets

$$U(\gamma_1, \ldots \gamma_k, \varepsilon) = \{g: |\gamma_j(g)-1|<\varepsilon, \ j=1, \ldots, k\}$$

as a basis of neighbourhoods, where $\gamma_1, \ldots \gamma_k$ are characters and $\varepsilon>0$. Observe that for the group of integers, the characters are the functions

$$n \to e^{iun}, \quad u\in\underset{\sim}{R},$$

and hence the basic neighbourhoods are just the sets $U(\underline{u}, \varepsilon)$ defined in (1.13).

It was proved by Bogolyubov [3] in 1939 for the case of integers, and generalized by Følner [6] for general commutative groups, that the second difference set of a "big" set is always a Bohr neighbourhood. Recall that for integers, "big" means bounded gaps. In fact, Bogolyubov used the weaker concept of positive upper density, and Følner [7] generalized this for groups using Banach means.

Let us state Bogolyubov's theorem exactly.

THEOREM F. If A is a set of natural numbers and $\bar{d}(A)>0$, then the set

$$D(D(A)) = A+A-A-A$$

is a Bohr neighbourhood of 0, that is, it contains an $U(u, \varepsilon)$ of the form (1.13) with some u and $\varepsilon>0$.

Kríz's Theorem E implies that we cannot replace the second difference set by the first; whether this can be done if A has bounded gaps remains open.

An analogous question is answered by the following classical theorem of Steinhaus: if A is a set of reals of positive Lebesgue measure, then A-A is a neighbourhood of 0.

Results of this type are often formulated with open symmetric big sets. If G is not discrete, then Bogolyubov-Følner's method yields only that A+A-A-A+V is a Bohr neighbourhood for any neighbourhood V of 0; thus if A is open, big, symmetric and contains 0, then A+A+A+A+A is a Bohr neighbourhood of 0. For integers, or in general for discrete groups, we can take $V=\{0\}$, thus 4 copies of A suffice. If now we consider sets of positive density, then three do not.

THEOREM 2. There is a symmetric set A of integers such that $0\in A$, the positive elements of A form a set of positive density and A+A+A is not a Bohr neighbourhood of 0.

On the other hand, it must have a nonempty interior.

THEOREM 3. If $\bar{d}(A)>0$, then there is an $a\in A$ such that A+A-A is a Bohr neighbourhood of a.

The curious possibility remains that this may also hold for

A-A (though I think it is very unlikely).

2.2 Problem. If $\bar{d}(A)>0$, may A-A have an empty interior in the Bohr topology?

Følner also proved that A-A "almost" contains a Bohr neighbourhood.

THEOREM G (Følner [6, 7]). If $\bar{d}(A)>0$, then there exists a u and an $\varepsilon>0$ such that the set

$$U(u, \varepsilon)\setminus(A-A)$$

has density 0.

In terms of intersective sets, this means that if H intersects every $U(u, \varepsilon)$ in a set of positive density, then it is intersective. From the arithmetical point of view this is of limited interest, since most "interesting" sets have density 0.

These problems, which are partially answered by the above theorems, have already been asked by P. Flor, including my 'main problem' 1.15 (written communication).

3. Proof of Theorem 1

Assume

$$A_1 \cup \ldots \cup A_k = \underset{\sim}{N}.$$

3.1 LEMMA. There is a subscript j, $1\le j\le k$, and an integer K with the following property: for arbitrary large m, the set A_j contains a subset

$$B_m = \{b_1^{(m)}, \ldots, b_m^{(m)}\}, \qquad b_1^{(m)}< \ldots <b_m^{(m)}$$

of m elements with gaps at most K (that is, $b_{i+1}^{(m)}-b_i^{(m)}\le K$).

Proof. Assume the contrary. Then for every j and K there is a $v_j(K)$ such that A_j has at most $v_j(K)$ consecutive elements with gaps not larger than K. Hence every interval of length $w_j(K)=K(1+v_j(K))$ contains a subinterval of length K that is free of elements of A_j.

Consider now any interval of length

$$w_1(w_2(\ldots\ (w_k(1))\ldots\ ))\ .$$

It contains a subinterval of length $w_2(\ldots)$ free of elements of A_1; this again contains a subinterval of length $w_3(\ldots)$ free of elements of A_2 and so on. Repeating this process k times, at the end we obtain an interval of length 1 and free of elements of $A_1, \ldots A_k$, that is, a number not contained in any of the A_j, a contradiction. ∎

Concentrate our attention on this set A_j and this number K. For every m, take a set C_m of $2m+1$ elements

$$C_m = \{c_{-m}, c_{-m+1}, \cdots c_{-1}, c_0, c_1, \cdots c_m\} \subset A_j$$

of gaps $\leq K$.

Let $B_{\sim m}$ be the class of all sets B of integers with the properties that

(i) $B \subset A_j+k$ with some integer k,

(ii) B has $2m+1$ elements, m of which are positive, m are negative and one is 0;

(iii) the difference between consecutive elements of B is

always at most K .

$\underset{\sim}{B}_m$ is clearly finite, and, $C_m - c_0$ being a set with these properties, it is not empty.

Now we form a graph by connecting a $B \in \underset{\sim}{B}_m$ to a $B' \in \underset{\sim}{B}_{m+1}$ if $B \subset B'$. Since every level $\underset{\sim}{B}_m$ is finite and every 'vertex' at level m is connected to some vertex in $\underset{\sim}{B}_{m-1}$, by a well known theorem of G. König there is an infinite path upwards, that is, a sequence (B_i) such that $B_i \in \underset{\sim}{B}_i$ and $B_i \subset B_{i+1}$. Put

$$B = \bigcup_{i=1}^{\infty} B_i \ .$$

Since the sequence (B_i) is increasing, every finite subset of B is contained in some B_i , hence in some translate of A_j . ∎

4. Proof of Theorem 2

Let B be a set of natural numbers of positive density such that $B-B$ is not a Bohr neighbourhood of 0 ; the existence of such a set follows from Theorem E and the observation that the sets $U(\underline{u}, \varepsilon)$ have bounded gaps. Put

$$C = \{4b+1 : b \in B\} \ .$$

Clearly $d(C) = d(B)/4 > 0$. Finally, let

$$A = C \cup (-C) \cup \{0\} \ ;$$

A will be our symmetric set.

We show that $A+A+A$ is not a Bohr neighbourhood of 0. Since the multiples of 4 form a neighbourhood, if $A+A+A$ were a neighbourhood, so would be

$$(A+A+A)\cap(4\underset{\sim}{Z}) .$$

Observe that an element of $A+A+A$ can be divisible by 4 only if it belongs to $C-C$. But $C-C=4(B-B)$ is not a neighbourhood, for if we had

$$C-C = 4(B-B) \supset U(u_1, \ldots u_k, \varepsilon) ,$$

then we would also have

$$B-B \supset U(4u_1, \ldots 4u_k, \varepsilon) ,$$

a contradiction. ∎

5. Proof of Theorem 3

This will be an easy deduction from Følner's Theorem G.

Choose a Bohr neighbourhood $U=U(\underline{u}, \varepsilon)$ such that $U\setminus(A-A)$ has density 0. Let $V=U(\underline{u}, \varepsilon/3)$. $\underset{\sim}{N}$ can be covered by a finite number of translates of V, so let

$$\underset{\sim}{N} \subset \bigcup_{j=1}^{k} (V+b_j) .$$

A, having positive upper density, intersects some of the sets $V+b_j$ in a set of positive upper density; say, $\bar{d}(A_j)>0$, where $A_j=A\cap(V+b_j)$. We now show that for every $a\in A_j$

$$A+A-A-a \supset V .$$

Let $v\in V$ be arbitrary. We want to find elements a_1, a_2, a_3

of A such that

$$a_1+a_2+a_3-a = v ,$$

that is,

(4.1) $$(a_1-a)-v = a_3-a_2 .$$

Let a_1 run over the elements of A_j. Since

$$a_1 \in V+b_j , \qquad a \in V+b_j , \qquad v \in V ,$$

we have

$$a_1-a-v \in V-V-V \subset U .$$

Thus the left-hand side of (4.1) runs over a subset of U of positive upper density. If equation (4.1) had no solution, this would be a part of $U \setminus (A-A)$ which is known to have density 0. Since this is impossible, (4.1) is solvable for every v, which just means $V \subset A+A-A-a$. □

6. Theorem E: the modular case

In Sections 6-9 we prove Kríz's Theorem E. The crucial step in the proof is establishing a version for the group $Z_m = \underset{\sim}{Z}/m\underset{\sim}{Z}$ of residue classes modulo m.

6.1 Definition. Let G be a commutative group. We call a set $H \subset G$ k-intersective, if for every partition $G = A_1 \cup \ldots \cup A_k$ of G into k subsets we have

$$H \cap (U\,(A_i-A_i)) \neq \emptyset .$$

For us the interesting cases are $G = \underset{\sim}{Z}$ or Z_m.

6.2 MAIN LEMMA. For every $\varepsilon>0$ and positive integer k there

are infinitely many integers m and sets A, $H \subset Z_m$ such that

$$|A| > (1/2-\varepsilon)m , \qquad H \cap (A-A) = \emptyset$$

and H is k-intersective.

Proof. m will be the product of $2r+k$ odd primes:

$$m = p_1 p_2 \cdots p_{2r+k} , \qquad p = p_1 < p_2 < \ldots < p_{2r+k} ,$$

r and the primes will be chosen later on.

We identify the elements of Z_m with the vectors

$$\underline{a} = (a_1, a_2, \ldots, a_{2r+k}) , \qquad 0 \le a_i \le p_i - 1 ,$$

where a_i denotes the residue modulo p_i. We call a residue $b \pmod{p_i}$ even, if it is one of $2, 4, \ldots, p_i-1$, odd, if it is one of $1, 3, \ldots, p_i-2$, while (like in the roulette) 0 is neither. The difference of two even (resp. two odd) residues cannot be equal to ± 1.

Now let A consist of the vectors $\underline{a}$ with the property that at most $r-1$ coordinates are even, and the rest is odd (none is 0). Let H be the set of elements with the property that at most k coordinates are different from ± 1. First we show

$$(A-A) \cap H = \emptyset .$$

Indeed, let $\underline{a}, \underline{a}' \in A$. Both $\underline{a}, \underline{a}'$ have at most $r-1$ even coordinates, thus there must be at least $k+2$ coordinates that are odd in both, and the corresponding coordinates of $\underline{a}-\underline{a}'$ cannot be equal to ± 1, hence $\underline{a}-\underline{a}' \notin H$.

Next we estimate the cardinality of A. Having chosen which of the coordinates should be odd and which even, the number of possible choices is

$$\prod \frac{p_i-1}{2} ,$$

thus we have

$$|A|/m = \frac{1}{m} \sum_{j=0}^{r-1} \binom{2r+k}{j} \prod \frac{p_i-1}{2}$$

$$> (1-1/p)^{2r+k} \, 2^{-(2r+k)} \sum_{j=0}^{r-1} \binom{2r+k}{j} .$$

If we choose r so large that

$$2^{-(2r+k)} \sum_{j=0}^{r-1} \binom{2r+k}{j} > (1-\varepsilon)/2 ,$$

and then p so large that

$$(1-1/p)^{2r+k} > 1-\varepsilon ,$$

then we shall indeed have

$$|A| > (1/2-\varepsilon)m .$$

Finally we show that H is k-intersective. To this end we need a result of Lovász [11] (see also Bárány [2] for a simple proof).

6.3 LEMMA. If we partition the r-element subsets of a set of cardinality $2r+k$ into $k+1$ classes, some of the classes contains two disjoint sets.

Now, to a set $X \subset \{1, 2, \ldots, 2r+k\}$, $|X|=r$, we assign an $\underline{a}(X) \in Z_m$ by putting $a_i=2$ if $i \in X$, $=1$ if $i \notin X$. Any partitioning of Z_m into k sets A_i induces a partition of the subsets of $\{1, \ldots, 2r+k\}$, thus by the Lemma there is an i , $1 \le i \le k$ and sets

$$X, Y \subset \{1, \ldots 2r+k\} , \qquad X \cap Y = \emptyset$$

such that $\underline{a}(X), \underline{a}(Y) \in A_i$. By $X \cap Y = \emptyset$, r coordinates of $\underline{a}(X)-\underline{a}(Y)$ are equal to $2-1=-1$, another r are $=1$ and k are $=0$, thus indeed $\underline{a}(X)-\underline{a}(Y) \in H$. This concludes the proof that H is k-intersective. □

7. Theorem E: the finite case

We get a step nearer to Theorem E.

7.1 LEMMA. Let $H \subset [1, m/2]$ be a set of integers. If the residues of H form a $2k$-intersective set in Z_m, then H is k-intersective.

Proof. Let

$$\underset{\sim}{N} = A_1 \cup \ldots \cup A_k$$

be a partition of the set of positive integers. We split Z_m into $2k$ classes as follows. Any element of Z_m is represented by an integer q, $1 \le q \le m$, and $q \in A_i$ for some i. Now we put q into B_{2i} if $q \le m/2$, into B_{2i+1} if $m/2 < q \le m$. For some j, $B_j - B_j$ contains a residue of H, that is,

$$b - b' \equiv h \pmod{m} .$$

By the construction we have $|b-b'| < m$, thus the congruence must be an equality. Since $B_j \subset A_i$ with $i = [j/2]$, this concludes the proof. ∎

7.2 LEMMA. For every $\varepsilon > 0$ and positive integer k there is a finite k-intersective set H of integers such that $\delta(H) > 1/2 - \varepsilon$.

Proof. We apply the Main Lemma of the previous section. Let H^* be a $2k$-intersective set of residues modulo m for a suitable m, such that $H^* \cap (A-A) = \emptyset$ for an $A \subset Z_m$, $|A| > (1/2-\varepsilon)m$. Let

$$H = \{h:\ 1 \le h \le m/2,\ h \text{ or } -h \text{ is represented in } H^*\} .$$

By the symmetry of difference sets and Lemma 7.1 we conclude that

H is k-intersective. Now let B be the set of positive integers whose residue modulo m is in A . We have

$$d(B)=|A|/m>1/2-\varepsilon\ , \qquad H\cap D(B)=\emptyset\ ,$$

which shows $\delta(H)>1/2-\varepsilon$. ∎

8. Properties of the measure of intersectivity

To combine the finite k-intersective sets of the previous section into a single infinite combinatorially intersective one we need some properties of the intersectivity measure.

8.1 LEMMA (Finitariness). *For every set* H *of integers and* $\varepsilon>0$ *there is a finite* $H'\subset H$ *such that*

$$\delta(H') < \delta(H)+\varepsilon\ .$$

8.2 LEMMA. *For every natural number* x *and set* H *of integers there is a set of integers* $A\subset[1, x]$ *such that*

$$(A-A)\cap H = \emptyset\ ,\quad |A| \geq \delta(H)x\ .$$

8.3 LEMMA. *For an arbitrary set* H *and natural number* m *we have* $\delta(mH)=\delta(H)$.

For proofs of lemmas 8.1-8.3, see Ruzsa [12].

8.4 LEMMA. *Let* H_1, H_2 *be nonempty sets of integers,* H_1 *finite. We have*

$$\liminf_{m\to\infty} \delta(H_1\cup mH_2) \geq 2\delta(H_1)\delta(H_2)\ . \tag{8.5}$$

Proof. Let A_2 be a sequence of density $\delta(H_2)$ whose difference set is disjoint to H_2 . (Such a set exists, see Ruzsa [12]; actually, for our present reasoning a set of upper density $\delta(H_2)-\varepsilon$ would also do.)

Let M be the maximal element of H_1, $m'=m-2M$ and $A_1 \subset [1, m']$ a set whose cardinality is

$$|A_1| \geq \delta(H_1)m'$$

(see Lemma 8.2), $D(A_1) \cap H_1 = \emptyset$.

Let h_1 and h_2 be arbitrary elements of H_1, resp. H_2. Let A be the set of natural numbers of the form $a=x+my$, where either $x \in A_1$ and $y \in A_2$, or $x \in A_1+h_1$ and $y \in A_2+h_2$. Observe that

$$A_1 \cap (A_1+h_1) = A_2 \cap (A_2+h_2) = \emptyset$$

by their very definition. Consequently

$$d(A) = 2^{\frac{|A1|}{m}} d(A_2) \geq 2\left(1-\frac{2M}{m}\right) \delta(H_1)\delta(H_2) . \tag{8.6}$$

If we can now show that $D(A)$ is indeed disjoint to $H_1 \cup mH_2$, then (8.6) immediately yields (8.5).

To see this, choose two elements of A, $a_j=x_j+my_j$ $(j=1, 2)$. Assume first $a_1-a_2 \in H_1$. Then

$$m(y_2-y_1) = x_1-x_2-h .$$

Since $|h| \leq M$ and $x_1, x_2 \in [1, m']$, the absolute value of the right hand side is smaller than m, thus in order to be divisible-$x_2 \in$ by m it must be 0. This means

$$y_1 = y_2 , \qquad x_1-x_2 \in H . \tag{8.7}$$

Recall that the elements of A are of two types:

(1) $x \in A_1$, $y \in A_2$; (2) $x \in A_1+h_1$, $y \in A_2+h_2$.

Now if a_1, a_2 are of the same type, then the second equation

of (8.7) is impossible; if they are of different types, then the first. This contradiction shows $a_1-a_2 \notin H_1$.

Assume now $a_1+a_2=mh$, $h \in H_2$. Then

$$m(y_1-y_2-h) = x_2-x_1 .$$

Again, the right hand side is less in absolute value than m , thus both sides must be equal to 0 . This leads to a contradiction in the same way as (8.7). ∎

9. Completion of the proof

9.1 LEMMA. *If* H *is* k-*intersective, so is* mH .

Proof. Let $A_1, \ldots A_k$ be a partition of $\underset{\sim}{N}$. Put

$$B_i = \{n: mn \in A_i\} .$$

$(B_1, \ldots B_k)$ is a partition of $\underset{\sim}{N}$ as well. By assumption, H intersects $D(B_i)$ for some i , and then mH intersects the corresponding $D(A_i)$. ∎

Proof of Theorem E. Choose a sequence (ε_k) of numbers, $0<\varepsilon_k<1$. For each k , let H_k be a k-intersective set with

$$\delta(H_k) > (1-\varepsilon_k)/2 \tag{9.1}$$

(Lemma 7.2).

We define a sequence of integers (m_k) recursively. Let $m_1=1$. Write

$$L_k = \bigcup_{j=1}^{k} m_j H_j .$$

Given $m_1, \ldots m_{k-1}$, select m_k so that

(9.2) $$\delta(L_k) = \delta(L_{k-1} \cup m_k H_k) > 2(1-\varepsilon_k)\delta(L_{k-1})\delta(H_k) ;$$

this is possible by Lemma 8.4.

(9.1) and (9.2) yield

$$\delta(L_k) > (1-\varepsilon_k)^2 \, \delta(L_{k-1}) ,$$

thus by induction

$$\delta(L_k) > \prod_{j=2}^{k} (1-\varepsilon_j)^2 \delta(L_1) > \frac{1}{2} \prod_{j=1}^{k} (1-\varepsilon_j)^2 .$$

Let

$$H = \bigcup_{j=1}^{\infty} L_j = \bigcup_{j=1}^{\infty} (m_j H_j) .$$

By Lemma 8.1 we have

$$\delta(H) = \lim \delta(L_k) > \frac{1}{2} \prod_{j=1}^{\infty} (1-\varepsilon_j)^2 ,$$

hence by a suitable choice of our (ε_k) we can achieve

$$\delta(H) > 1/2 - \varepsilon .$$

On the other hand, since H_k was k-intersective, so is $m_k H_k$. Consequently H is k-intersective for every k, that is, it is combinatorially intersective. ∎

10. Borsuk, Lovász, Kríz, and I

In the first version of the paper (spring 1985) I had the following result, which is weaker than Theorem E.

For every $\varepsilon>0$ there is an approximative set H of positive integers such that $\delta(H)>1/2-\varepsilon$.

For $u_1, \dots u_k \in Z_m$ and $\varepsilon>0$ put

$$U(u_1, \dots u_k, \varepsilon) = \{n\in Z_m: \quad \|nu_j/m\|<\varepsilon \text{ for all } 1\le j\le k\} .$$

Call a set $H\subset Z_m$ (k,ε)-approximative, if it intersects every $U(u_1, \dots u_k, \varepsilon)$.

The crucial step was a modular version, like the Main Lemma in §6:

For every positive integer k and $\varepsilon>0$ there are infinitely many integers m such that there are sets $H, A\subset Z_m$,

$$|A|>(1/2-\varepsilon)m , \qquad (A-A)\cap H=\emptyset ,$$

while H is (k,ε)-approximative.

The rest was essentially the same as here in §§7-9.

This was proved in the following way. Take $\alpha_1, \dots \alpha_q \in Z_m$ and for $x\in Z_m$ put

$$f(x) = \sum e(x\alpha_j/m) , \quad g(x) = \sum |1+e(x\alpha_j/m)| ,$$

where $e(t)=\exp 2\pi i t$. We have always

$$|f(x)+f(y)| \le g(x-y) ,$$

thus the sets

$$A = \{x: \text{Re } f(x)>L\} , \quad H = \{x: g(x)<L\}$$

satisfy $(A-A)\cap H=\emptyset$.

Now, for a "typical" choice of α_j , the functions $e(x\alpha_j/m)$ are "almost independent", thus $|A| \sim m/2$ if $L=o(\sqrt{q})$. I proved the (k,ε)-approximativity of H (for suitable choice of m, L, q, and for almost all choices of the coefficients α_j) by a complicated probabilistic-analytic argument.

I wanted to prove that this H is also k-intersective. For $x \in Z_m$ let

$$\varphi(x) = (e(x\alpha_1/m), \ldots e(x\alpha_q/m)) \in T^r ,$$

where $T = \{z: |z|=1\}$ is the unit circle. Again, for a 'typical' choice of α_j the values $\varphi(x)$ are 'dense' on the torus T^r .

Obsererve that a small value of $g(x-y)$ means that $\varphi(x)$ and $\varphi(y)$ are almost antipodal. The intersectivity of H would follow from the following assertion.

STATEMENT. <u>If we split the torus</u> T^q <u>into</u> k <u>sets</u> $X_1, \ldots X_k$, <u>then some set</u> X_j <u>contains two points</u> $\underline{x}=(x_1, \ldots x_q)$ <u>and</u> $\underline{y}=(y_1, \ldots y_q)$ <u>that are almost antipodal in the sense that</u> $x_j=-y_j$ <u>for all but</u> L <u>values of</u> j , <u>where</u> $L=L(k)$ <u>depends only on</u> k <u>and not on</u> q .

This sounds very similar to Borsuk's famous theorem [5].

<u>If we cover the unit sphere</u>

$$S_k = \{x \in R^{k+1}: \|x|=1\}$$

<u>with</u> $k+1$ <u>closed sets, then one of the sets contains two antipodal points.</u>

For a long time I tried, in vain, to find a direct link between the above Statement and Borsuk's theorem. Finally I realized that it follows from Lovász' theorem, here reproduced as Lemma 6.3, in the following way. Let $q=2r+k'$, where $k'=k$ or $k-1$ (the case $q\leq k$ is obvious). We map the sets $X\subset(1, 2, \ldots q)$ into T^q by putting

$$\Psi(X) = (x_1, \ldots x_q) , \qquad x_j = 1 \text{ if } j\in X , -1 \text{ otherwise.}$$

If $|X|=|Y|=r$ and $X\cap Y=\emptyset$, then $\Psi(X)$ and $\Psi(Y)$ are antipodal with the exception of $k'\leq k$ coordinates, hence the Statement follows from Lemma 6.3 with $L=k$.

The piquancy of the proof is that both Lovász and Bárány use Borsuk's theorem to obtain Lemma 6.3; the connection is particularly explicit in Bárány's version.

Problem. What is the real size of $L(k)$? I have a lower bound $c \log k$.

Having reduced everything to a combinatorial result, it was a natural idea to remove the analytical setup and replace the functions f and g by a discrete argument, as presented in §6. At this point, as I felt very satisfied, I learned that I had been preceded by Kríz, and that his proof also applies Lovász' Lemma 6.3.

This is not the only similarity between the proofs. Though he has a completely different perspective and terminology, there seems to be a strong strategical parallelism. Both proofs start with a multidimensional version; Kríz works in $\mathbb{Z}^k$, which cor-

responds to my handling of Z_m as a direct products of the Z_{p_j} (§6). The next step is a reduction to one dimension (§7), then a combination of two sets into one with a small loss in $\delta(H)$ (§8), finally a combination of infinitely many sets (§9). In my approach, the second step is simpler. Step 4 is seemingly longer in [9], but this is due to the fact that Kríz also proves (as Theorem 3.4) Stewart and Tijdeman's [15] result that in the definition of $\delta(H)$ (see §1) one can interchange upper and asymptotical density.

References

1. E. M. Alfsen, P. Holm, 'A note on compact representations and almost periodicity in topological groups', Math. Scandinavica 10(1962), 127-136.
2. I. Bárány, 'A short proof of Kneser's conjecture', J. Combinatorial Theory Ser. A. 25(1978), 325-326.
3. N. N. Bogolyubov, 'Some algebraical properties of almost periodes' (in Russian), Zapiski kafedry matematichnoi fiziki (Kiev) 4(1939), 185-194.
4. K. Borsuk, 'Drei Sätze über die n-dimensional euklidische sphäre', Fundamenta Mathematica 20(1933), 177-190
5. J. Bourgain, 'Ruzsa's problem on sets of recurrence', Israel J. Math. 59(1987), 150-166.
6. E. Følner, 'Generalization of a theorem of Bogoliuboff to topological Abelian groups. With an appendix on Banach mean values in non-Abelian groups', Math. Scandinavica 2(1954),

5-18.

7. E. Følner, 'Note on a generalization of a theorem of Bogoliuboff', Math. Scandinavica 2(1954), 224-226.

8. T. Kamae, M. Mendès France, 'Van der Corput's difference theorem', Israel J. Math. 31(1978), 335-342.

9. I. Kríz, 'Large independent sets in shift-invariant graphs', Graphs and Combinatorics 3(1987), 145-158.

10. M. B. Landstad, 'On the Bohr topology in amenable topological groups', Math. Scandinavica 28(1971),207-214.

11. L. Lovász, 'Kneser's conjecture, chromatic number and homotopy', J. Combinatorial Th. Ser. A. 25(1978), 325-326.

12. I. Z. Ruzsa, 'On difference sets', Studia Sci. Math. Hung. 13(1978), 319-326.

13. I. Z. Ruzsa, 'Connections between the uniform distribution of a sequence and its differences', Coll. Math. Soc. J. Bolyai 34, Topics in number theory, Budapest 1981 (Bp. 1984), 1419-1443

14. A. Sárközy, 'On difference sets of sequences of integers',
I. Acta Math. Acad. Sci. Hung. 31(1978), 125-149;
II. Annales Univ. Sci. Budapest 21(1978), 45-53;
III. Acta Math. Acad. Sci. Hung. 31(1978), 355-386.

15. C. L. Stewart, R. Tijdeman, 'On infinite difference sets', Canad. J. Math. 31(1979), 897-910.