SETS OF RECURRENCE OF $\mathbb{Z}^m$-ACTIONS AND PROPERTIES OF SETS OF DIFFERENCES IN $\mathbb{Z}^m$

VITALY BERGELSON

Introduction and definitions

In 1936, P. Erdos and P. Turan conjectured that if a set A of positive integers satisfies the condition

$$\limsup_n \frac{|A \cap [1,n]|}{n} > 0,$$

then A contains arbitrarily long arithmetic progressions. This conjecture was settled affirmatively by E. Szemerédi in 1975. In 1977 H. Furstenberg gave quite another proof using methods of ergodic theory (see **[1]**). Since then many other applications of ergodic theory and topological dynamics to Ramsey theory have appeared **[2, 3, 4]**. In this paper we use measure-theoretic and ergodic methods to obtain some new properties of difference sets in $\mathbb{Z}^m$. For $A \subset \mathbb{Z}^m$ the difference set $A - A$ is defined by

$$A - A = \{a_1 - a_2 \mid a_1, a_2 \in A\}.$$

Of course, $a \in A - A$ if and only if $A \cap (A + a) \neq \varnothing$. It often happens that it is easier to prove that the intersection $A \cap (A + a)$ is 'large' rather than to prove that it is non-empty. In what follows different notions of 'largeness' of sets in $\mathbb{Z}^m$ are used.

For $A \subset \mathbb{N}$ set $d(A) = \lim_n |A \cap [1,n]|/n$ if the limit exists and is positive; in this case $d(A)$ is called the density of A. In any case $\limsup |A \cap [1,n]|/n$ always exists; it is called the upper density of A and is denoted $d^*(A)$. Thus, Szemerédi's theorem is a statement about sets of positive upper density. What is really important for this type of result to hold is that there exist arbitrarily long intervals $[a_k, b_k]$ of $\mathbb{Z}$ in which the 'percentage' of elements of A is positive. The following definitions are taken from **[1]**.

A set $A \subset \mathbb{Z}$ is said to have positive upper Banach density if there exists a sequence of intervals $[a_k, b_k] \subset \mathbb{Z}$ such that $b_k - a_k \to \infty$ and

$$\limsup \frac{|A \cap [a_k, b_k]|}{(b_k - a_k + 1)} > 0.$$

The notion of upper Banach density extends naturally to $\mathbb{Z}^m$. By a block in $\mathbb{Z}^m$ we mean a product of intervals. The width of a block is the length of its shortest edge. A set $A \subset \mathbb{Z}^m$ is said to have positive upper Banach density if, for some sequence of blocks B_n whose widths approach infinity, $|A \cap B_n|/|B_n| > \delta > 0$. In the sequel we shall also need the notion of a measure-preserving system. A measure-preserving system will be a quadruple $(X, \mathscr{B}, \mu, G)$, where X is an abstract space, $\mathscr{B}$ is a σ-algebra of subsets of X, μ is a probability measure on $\mathscr{B}$, and G is a group of measure-preserving transformations of X.

Received 5 September 1984.

1980 *Mathematics Subject Classification* 28D05.

Acknowledgement. The author would like to thank Professors H. Furstenberg and Y. Katznelson for valuable discussions and suggestions.

1. *Combinatorial properties of intersections in sequences of sets of positive measure in a probability measure space*

THEOREM 1.1. *Let $(X, \mathscr{B}, \mu)$ be a probability measure space and suppose that $A_n \in \mathscr{B}$, $\mu(A_n) = a > 0$, for $n = 1, 2, \ldots$. Then there exists a set $P \subset \mathbb{N}$ such that $d^*(P) \geqslant a$ and for any finite subset $F \subset P$ we have*

$$\mu(\bigcap_{n \in F} A_n) > 0.$$

Proof. For a finite set $F \subset \mathbb{N}$ we denote the intersection $\bigcap_{n \in F} A_n$ by A_F.

First of all let us show that there exists a set $N \subset X$ of measure zero such that if $F \subset \mathbb{N}$ is finite and $(X \backslash N) \cap A_F \neq \varnothing$ then $\mu(A_F) > 0$. Let $\mathscr{C}$ be the (countable!) set of all finite products of characteristic functions 1_{A_n} of the sets A_n. For $f \in \mathscr{C}$ write

$$N_f = \{x \mid |f(x)| > \operatorname{sup\,ess} |f|\}, \quad N = \bigcup_{f \in \mathscr{C}} N_f.$$

Obviously $\mu(N_f) = 0$ and thus $\mu(N) = 0$. Suppose that $F \subset \mathbb{N}$ is a finite set and $(X \backslash N) \cap A_F \neq \varnothing$. We shall show that $\mu(A_F) > 0$.

Let $x \in (X \backslash N) \cap A_F$ and $f = \prod_{n \in F} 1_{A_n}$. If $\mu(A_F) = 0$, then $\|f\|_\infty = \operatorname{sup\,ess} |f| = 0$ and $x \in N_f$, which contradicts the fact that $x \in X \backslash N$. So, subtracting, if necessary, the set N from X we shall assume without loss of generality that if $A_F \neq \varnothing$ then $\mu(A_F) > 0$. Now, let $f_n(x) = 1/n \sum_{k=1}^{n} 1_{A_k}(x)$. Note that $0 \leqslant f_n(x) \leqslant 1$ for all x and $\int f_n \, d\mu = a > 0$. Let $f(x) = \limsup_n f_n(x)$. By Fatou's lemma we have

$$\int f \, d\mu = \int \limsup_n f_n \, d\mu \geqslant \limsup_n \int f_n = a > 0.$$

Thus $\int f \geqslant a$ and, as $\mu(X) = 1$, there exists $x_0 \in X$ such that $\limsup_n f_n(x_0) = f(x_0) \geqslant a$. Then there exists a sequence $\{n_i\}_{i=1}^{\infty}$ such that

$$f_{n_i}(x_0) = \frac{1}{n_i} \sum_{k=1}^{n_i} 1_{A_k}(x_0) \to f(x_0) \geqslant a. \tag{1.1}$$

Let $P = \{n \in \mathbb{N} \mid x_0 \in A_n\}$. It follows from (1.1) that $d^*(P) \geqslant a$ and as $x_0 \in A_n$ for all n in P we have $\mu(A_F) > 0$ for every finite subset $F \subset P$.

Suppose now that T is a measure-preserving transformation of $(X, \mathscr{B}, \mu)$. Let $A_0 \in \mathscr{B}$, $\mu(A_0) = a > 0$, and define $A_n = T^{-n} A_0$. It follows from the ergodic theorem that, for almost every x,

$$\lim \frac{1}{n} \sum_{k=1}^{n} 1_{A_k}(x) = f(x)$$

exists. As $\int f(x) = a$ we conclude that there exists a sequence $\{n_m\}_{m=1}^{\infty}$ of positive density $d(\{n_m\}) \geqslant a$ such that

$$\mu(T^{-n_1} A_0 \cap \ldots \cap T^{-n_m} A_0) > 0 \quad \text{for any } m \in \mathbb{N}.$$

Taking account of the fact that T is measure preserving and that sequences $\{n_m - n_1\}_{m=1}^{\infty}$ and $\{n_m\}_{m=1}^{\infty}$ have the same density, we obtain the following refinement of Poincaré's classical recurrence theorem.

THEOREM 1.2. *Let $(X, \mathscr{B}, \mu, T)$ be a measure-preserving system and let $A \in \mathscr{B}$, $\mu(A) = a > 0$. Then there exists a sequence $\{n_m\}_{m=1}^{\infty}$ with $d(\{n_m\}) \geqslant a$ such that, for any $m \in \mathbb{N}$, $\mu(A \cap T^{-n_1} A \cap \ldots \cap T^{-n_m} A) > 0$.*

2. *Applications to countable amenable groups*

Let G be a countable amenable group and let L_G be an invariant mean on the set $B(G)$ of all complex-valued bounded functions on G. Identifying subsets of G with their characteristic functions, let us assume that $L_G(A_n) \geqslant a > 0$ for a sequence $\{A_n\}_{n=1}^{\infty}$ of subsets of G.Then Theorem 1.1 implies the following.

THEOREM 2.1. *Suppose that subsets A_n, for $n = 1, 2, \ldots$, of an amenable group G satisfy the condition $L_G(A_n) \geqslant a > 0$. Then there exists a sequence $\{n_k\}_{k=1}^{\infty}$ such that $d^*(\{n_k\}) \geqslant a$ and for any $k \in \mathbb{N}$*

$$L_G(A_{n_1} \cap \ldots \cap A_{n_k}) > 0.$$

Proof. Denote by $\mathscr{A}$ the uniformly-closed and closed-under-conjugation algebra of functions on G, generated by characteristic functions 1_{A_n} of sets A_n. Then $\mathscr{A}$ is a separable C*-algebra with respect to the supremum norm, and by the Gelfand representation theorem we can represent $\mathscr{A}$ as $\mathscr{A} \cong C(X)$, where X is a compact metric space. The mean L_G extends to a positive linear functional $L_{\mathscr{A}}$ on $\mathscr{A}$, and $L_{\mathscr{A}}$ in its turn induces a positive linear functional L on $C(X)$. For $f \in \mathscr{A}$ let $\tilde{f}$ denote its image in $C(X)$. By a well-known theorem of F. Riesz there exists a regular Borel measure μ such that, for any $f \in C(X)$,

$$L_{\mathscr{A}}(f) = L(\tilde{f}) = \int \tilde{f} d\mu.$$

Note that images in $C(X)$ of characteristic functions of sets in $\mathscr{A}$ are also characteristic functions. For correspondence between $\mathscr{A}$ and $C(X)$ preserves algebraic operations and the characteristic functions are the only idempotents in $C(X)$. So there exist sets $\tilde{A}_n$, for $n \in \mathbb{N}$, such that for any $n_1 < n_2 < \ldots < n_k$ we have

$$L_G(A_{n_1} \cap \ldots \cap A_{n_k}) = \mu(\tilde{A}_{n_1} \cap \ldots \cap \tilde{A}_{n_k}).$$

The theorem now follows from Theorem 1.1.

Let us consider the special case in which $G = \mathbb{Z}$ and $E_n = E + n$, where E is a set of positive upper Banach density. Proceeding as in the proof of Theorem 2.1 and taking into account that a shift on $\mathbb{Z}$ induces a measure-preserving transformation of X, we obtain as a consequence of Theorem 1.2 the following statement.

THEOREM 2.2. *Let $E \subset \mathbb{Z}$ be a subset of positive upper Banach density. Then there exists a set $R \subset \mathbb{Z}$ such that for any $n_1, \ldots, n_k \in R$ the upper Banach density of the set $E \cap E + n_1 \cap \ldots \cap E + n_k$ is positive and R is a set whose density exists and is not less than the upper Banach density of E.*

This gives us the following proposition which is attributed in [1] to R. Ellis.

COROLLARY 2.2.1. *Let $E \subset \mathbb{Z}$ be a subset of positive upper Banach density. There exists a set $R \subset \mathbb{Z}$ with the property that if F is any finite subset of R, then some translate $F + h \subset E$ where $h \in \mathbb{Z}$, and R is a set whose density exists and is positive.*

REMARK. It follows from Theorem 2.2 that h can be an element of E.

3. *A property of difference sets in* $\mathbb{Z}^2$

THEOREM 3.1. *If* $(X, \mathscr{B}, \mu)$ *is a probability measure space, and* T, S *are commuting invertible measure-preserving transformations of* $(X, \mathscr{B}, \mu)$ *then for any set* $A \in \mathscr{B}$ *with* $\mu(A) > 0$ *there exists a sequence* $\{k_i\}_{i=1}^{\infty}$ *of positive upper density such that, for all* $i, j \in \mathbb{N}$,

$$\mu(A \cap T^{k_i} S^{k_j} A) > 0.$$

Proof. A subset $P \subset \mathbb{Z}$ is called syndetic if there exists a finite set $F \subset \mathbb{Z}$ such that $P+F = \mathbb{Z}$. In other words the complement of P does not contain too long intervals of integers. It is an apparently well-known fact (referred to as Khintchine's recurrence theorem) that if T is an invertible measure-preserving transformation of a probability measure space $(X, \mathscr{B}, \mu)$ and $A \in \mathscr{B}$, $\mu(A) > 0$, then the set

$$\{n \mid \mu(A \cap T^n A) > \mu(A)^2 - \varepsilon\}$$

is syndetic for any $\varepsilon > 0$. For instance, one can obtain it as a consequence of von Neumann's uniform ergodic theorem.

Applying Khintchine's recurrence theorem to the transformation ST we obtain a syndetic sequence $\{m_n\}_{n=1}^{\infty}$ such that for some α, with $0 < \alpha < \mu(A)^2$,

$$\mu(A \cap (ST)^{m_n} A) \geqslant \alpha, \quad n = 1, 2, \ldots.$$

As S is an invertible measure-preserving transformation and T, S commute we can rewrite this expression as

$$\mu(S^{-m_n} A \cap T^{m_n} A) \geqslant \alpha.$$

Writing $A_n = S^{-m_n} A \cap T^{m_n} A$ and applying Theorem 1.1 we obtain a sequence $\{n_i\}_{i=1}^{\infty}$ with $d^*(\{n_i\}) > 0$ such that, for any $k \in \mathbb{N}$,

$$\mu(A_{n_1} \cap A_{n_2} \cap \ldots \cap A_{n_k}) > 0. \tag{3.1}$$

It follows from (3.1) that

$$\mu(S^{-m_{n_i}} A \cap T^{m_{n_j}} A) > 0 \quad \text{for any } i, j \in \mathbb{N}. \tag{3.2}$$

As $\{m_n\}$ is a syndetic sequence and $\{n_i\}$ has positive upper density we conclude that the sequence $\{m_{n_i}\}_{i=1}^{\infty}$ has positive upper density. Writing $m_{n_i} = k_i$ we obtain from (3.2) that

$$\mu(A \cap S^{k_i} T^{k_j} A) > 0 \quad \text{for any } i, j \in \mathbb{N},$$

where $d^*(\{k_i\}) > 0$.

COROLLARY 3.1.1. *Let* $A \subset \mathbb{Z}^2$ *and suppose that* A *has positive upper Banach density. Then there exists* $B \subset \mathbb{Z}$ *such that* $d^*(B) > 0$ *and*

$$A - A \supset B \times B.$$

Here $A - A$ *denotes the set of differences of elements of* A *and* $B \times B$ *is the Cartesian square of* B.

Proof. Define $\Omega = \{0, 1\}^{\mathbb{Z}^2}$. Then Ω is the space of all double sequences with entries 0 or 1. Now Ω can be made into a compact metric space, taking as metric

$$\rho(\omega, \omega') = \inf\left\{\frac{1}{k+1} \,\middle|\, \omega(i_1, i_2) = \omega'(i_1, i_2) \text{ for } |i_1|, |i_2| < k\right\}.$$

Define transformations T, S of Ω by

$$T\omega(i_1, i_2) = \omega(i_1+1, i_2), \quad S\omega(i_1, i_2) = \omega(i_1, i_2+1).$$

Of course $TS = ST$ and we see that powers of these transformations generate in a natural way a $\mathbb{Z}^2$-action on Ω. We shall regard the characteristic functions of subsets of $\mathbb{Z}^2$ as points of Ω.

Let $\xi = 1_A(n,m)$, where $A \subset \mathbb{Z}^2$ is a subset of positive upper Banach density, and let X be the closure in Ω of all translates of ξ:

$$X = \overline{\{T^n S^m \xi \mid (n,m) \in \mathbb{Z}^2\}}.$$

Let $A_1 = \{\omega \in X \mid \omega(0,0) = 1\}$. One can show that there exists a probability measure μ on the Borel sets of X satisfying $\mu(A_1) > 0$ and invariant with respect to T and S (see for example [**1**, p. 152]).

By Theorem 3.1 there exists a sequence of positive upper density $\{n_i\} \subset \mathbb{Z}$ such that for all $i,j \in \mathbb{N}$ we have

$$\mu(A_1 \cap T^{n_i} S^{n_j} A_1) > 0.$$

Let $\omega \in A_1 \cap T^{n_i} S^{n_j} A_1$. Then $\omega(0,0) = \omega(n_i, n_j) = 1$. But ω is in the orbit closure of ξ. Thus we can find $(n_0, m_0) \in \mathbb{Z}^2$ such that $T^{n_0} S^{m_0} \xi$ and ω have the same coordinates at the point (n_i, n_j). Then

$$1_A(n_0, m_0) = 1_A(n_0+n_i, m_0+n_j) = 1.$$

It follows that $(n_i, n_j) \in A - A$ and the theorem is proved.

Corollary 3.1.2. *If $A \subset \mathbb{Z}$ and A has positive upper Banach density then there exists a set $B \subset \mathbb{Z}$ of positive upper density such that*

$$A - A \supset B + B.$$

Proof. Let $A \subset \mathbb{Z}$ be a set of positive upper Banach density. We can regard the characteristic function $1_A(n)$ as a point in $\{0,1\}^{\mathbf{Z}}$. Let X be the closure in $\{0,1\}^{\mathbf{Z}}$ of the set of all translates of $\xi = 1_A(n)$. Define $A_1 = \{x \in X \mid x(0) = 1\}$. Let μ be a probability measure on Borel sets of X satisfying $\mu(A_1) > 0$. Taking $T = S$ in Theorem 3.1 we see that there exists a set $\{n_i\} \subset \mathbb{Z}$ of positive upper density such that

$$\mu(A_1 \cap T^{n_i+n_j} A_1) > 0 \quad \text{for any } i,j \in \mathbb{N}.$$

Taking account of the facts that if $x \in A_1 \cap T^{n_i+n_j} A_1$, then

$$x(0) = x(n_i+n_j) = 1,$$

and that x lies in the orbit closure of ξ, we conclude that there exists m such that

$$T^m \xi(0) = T^m \xi(n_i+n_j) = 1,$$

or

$$\xi(m) = \xi(m+n_i+n_j) = 1.$$

This gives us the desired result.

Remark. We do not know the answer to the following questions.

Question 1. Let $A \subset \mathbb{Z}^3$ be a set of positive upper Banach density. Is it true that there exists a set $B \subset \mathbb{Z}$ of positive upper density such that $A - A \supset B \times B \times B$?

Question 2. Let $A \subset \mathbb{Z}$ be a set of positive upper Banach density. Is it true that there exists a set $B \subset \mathbb{Z}$ of positive upper density such that $A-A \supset B+B+B$?

On the other hand we have the following.

THEOREM 3.2. *Let $A \subset \mathbb{Z}^m$ be a set of positive upper Banach density. Then there exists an infinite set $B \in \mathbb{Z}$ such that*

$$A-A \supset B^m$$

(*where B^m stands for the m-fold Cartesian product of B with itself*).

Proof. We shall show that for any m invertible and commuting measure-preserving transformations $T_1, T_2, \ldots, T_m$ of a probability measure space $(X, \mathscr{B}, \mu)$ and any $A \in \mathscr{B}$ with $\mu(A) > 0$ there exists an infinite set $B \subset \mathbb{N}$ such that, for any $(n_1, n_2, \ldots, n_m) \in B^m$,

$$\mu(A \cap T_1^{n_1} T_2^{n_2} \ldots T_m^{n_m} A) > 0. \tag{3.3}$$

The reduction of this result to the desired combinatorial statement can be made in complete analogy with the proof of Corollary 3.1.1.

We shall use the multidimensional ergodic Szemerédi theorem of Furstenberg and Katznelson [3] which states that if $S_1, S_2, \ldots, S_k$ are invertible commuting measure-preserving transformations of a probability measure space $(X, \mathscr{B}, \mu)$ and $A \in \mathscr{B}$ with $\mu(A) > 0$ then

$$\liminf_{N\to\infty} \frac{1}{N} \sum_{n-1}^{N} \mu(A \cap S_1^n A \cap \ldots \cap S_k^n A) > 0.$$

To avoid cumbersome notation we shall show (3.3) for $m = 3$. The same proof holds for any $m \in \mathbb{N}$.

By the theorem of Furstenberg and Katznelson there exists $b_1 \in \mathbb{N}$ such that the set

$$A_1 = A \cap T_1^{b_1} A \cap T_2^{b_1} A \cap T_3^{b_1} A \cap T_1^{b_1} T_2^{b_1} A \cap T_1^{b_1} T_3^{b_1} A \cap T_2^{b_1} T_3^{b_1} A \cap T_1^{b_1} T_2^{b_1} T_3^{b_1} A$$

has positive measure. Applying the theorem to the set A_1, we can find b_2 such that the set

$$A_2 = A_1 \cap T_1^{b_2} A_1 \cap T_2^{b_2} A_1 \cap T_3^{b_2} A_1 \cap T_1^{b_2} T_2^{b_2} A_1 \cap T_1^{b_2} T_3^{b_2} A_1 \cap T_2^{b_2} T_3^{b_2} A_1 \cap T_1^{b_2} T_2^{b_2} T_3^{b_2} A_1$$

has positive measure. It is clear that all triples made from elements of the set $\{b_1, b_2\}$ satisfy (3.3). Continuing in this manner we find an infinite sequence of sets A_k of positive measure such that $A_k \subset A_{k-1}$ for all $k \in \mathbb{N}$ (here $A_0 = A$) and an infinite sequence $\{b_i\}_{i=1}^{\infty}$ such that, for any k,

$$A_k = A_{k-1} \cap T_1^{b_k} A_{k-1} \cap T_2^{b_k} A_{k-1} \cap T_3^{b_k} A_{k-1} \cap T_1^{b_k} T_2^{b_k} A_{k-1} \cap T_1^{b_k} T_3^{b_k} A_{k-1}$$
$$\cap T_2^{b_k} T_3^{b_k} A_{k-1} \cap T_1^{b_k} T_2^{b_k} T_3^{b_k} A_{k-1}$$

has positive measure.

We see that (3.3) holds for any m-tuple made from elements of $B = \{b_1, b_2, \ldots\}$. This completes the proof of Theorem 3.2.

Taking $T_1 = T_2 = \ldots = T_m = T$ we see that for any measure-preserving transformation T of a probability measure space $(X, \mathscr{B}, \mu)$ and for any $A \in \mathscr{B}$ with $\mu(A) > 0$

there exists an infinite set B such that for any (not necessarily distinct!) $n_1, n_2, \ldots, n_m \in B$ we have

$$\mu(A \cap T^{n_1+n_2+\ldots+n_m} A) > 0.$$

This gives the following result.

COROLLARY 3.2.1. *Let $A \subset \mathbb{Z}$ be a set of positive upper Banach density. Then for any $m \in \mathbb{N}$ there exists an infinite set $B \subset \mathbb{Z}$ such that*

$$A - A \supset \{b_{i_1} + b_{i_2} + \ldots + b_{i_m} \mid b_{i_j} \in B, j = 1, 2, \ldots, m\}.$$

REMARK. The set B in Theorem 3.2 and Corollary 3.2.1. can be chosen to be symmetric about the origin. To see this one applies the Furstenberg–Katznelson theorem to products of transformations $T_1, T_2, \ldots, T_m, T_1^{-1}, T_2^{-1}, \ldots, T_m^{-1}$.

4. *Sets of recurrence*

Let G be a countable group with $E \subset G$ an infinite subset of G. We call E a *set of recurrence* if for any measure-preserving system $(X, \mathscr{B}, \mu, T_g, g \in G)$ and any $A \in \mathscr{B}$, $\mu(A) > 0$ there exists $g \in E$ such that

$$\mu(A \cap T_g^{-1} A) > 0.$$

We shall say that E is a *set of strong recurrence* if, for any measure-preserving system $(X, \mathscr{B}, \mu, T_g, g \in G)$, any $A \in \mathscr{B}$ with $\mu(A) > 0$ and any positive sufficiently small α there exists an infinite subset $E' \subset E$ such that

$$\mu(A \cap T_g^{-1} A) > \alpha \quad \text{for any } g \in E'.$$

REMARK. We know of no example of a set of recurrence which is not a set of strong recurrence.

We pose the following question.

Question. Is it true that the notions of recurrence and strong recurrence coincide?

We now give some examples of sets of (strong!) recurrence in $\mathbb{Z}$. Proofs can be found in [**1**].

1. *Thick sets.* A set $R \subset \mathbb{Z}$ is called thick if it contains arbitrarily long intervals.

2. *IP-sets.* A subset of $\mathbb{Z}$ is called an *IP*-set if it consists of a sequence of (not necessarily distinct) integers $n_1, n_2, \ldots$ together with all sums of these for distinct indices.

3. Sets of the form $\{p(n) \mid n \in \mathbb{Z}\}$, where $p(n)$ is a polynomial with integer coefficients and with $p(0) = 0$.

Theorem 3.18 of [**1**] states that if $A \subset \mathbb{Z}$ is a set of positive upper Banach density and $W \subset \mathbb{Z}$ is a set of recurrence then $A - A \cap W$ contains non-zero integers. An analogous statement holds also for more general groups. The following theorem points out the connection between difference sets in $\mathbb{Z}^2$ and sets of strong recurrence in $\mathbb{Z}$.

THEOREM 4.1. *Let $D \subset \mathbb{Z}$ be a set of strong recurrence and let $A \subset \mathbb{Z}^2$ be a set of positive upper Banach density. Then there exists an infinite set $B \subset D$ such that*

$$A - A \supset B \times B.$$

Proof. First of all one can prove (analogously to the proof of Theorem 3.1) that if $D \subset \mathbb{Z}$ is a set of strong recurrence and T, S are commutative invertible measure-preserving transformations of a probability measure space (X, B, μ), then for any $A \in B$ with $\mu(A) > 0$ there exists an infinite subset $B \subset D$ such that for any $n, m \in B$ we have

$$\mu(A \cap T^n S^m A) > 0.$$

The rest of the proof follows the lines of the proof of Corollary 3.3.1.

COROLLARY 4.1.1. *Let $p(n)$ be a polynomial with integer coefficients and with $p(0) = 0$, and let $A \subset \mathbb{Z}^2$ be a set of positive upper Banach density. Then there exists an infinite sequence $\{n_k\}_{k=1}^{\infty}$ such that*

$$A - A \supset B \times B,$$

where $B = \{p(n_k) \mid k = 1, 2, \ldots\}$.

The proof of this corollary is immediate since if a polynomial $p(n)$ satisfies the conditions above then $p(\mathbb{Z})$ is a set of strong recurrence. A proof of this fact can be given similarly to the proof of [**4**, Theorem 3.5]. The following consequence of it is given in [**4**, Proposition 3.6].

PROPOSITION. *Let $S \subset \mathbb{Z}$ be a set of positive upper Banach density and let $p(n)$ be a polynomial taking integer values at the integers and including 0 in its range on the integers. Then there exists a solution to the equation*

$$x - y = p(z), \quad x, y \in S,\ z \in \mathbb{Z},\ x \neq y.$$

This proposition was also proved independently by Sarkozy and Conze. We remark that Corollary 4.1.1 can be regarded as a generalization of this proposition. We shall see later that an even stronger result holds (see Corollary 4.2.1 below).

The following theorem can be proved analogously to [**4**, Theorem 3.5].

THEOREM 4.2. *Let $T_1, T_2, \ldots, T_k$ be invertible commuting transformations of a probability measure space $(X, \mathscr{B}, \mu)$. Suppose that $p_1(n), \ldots, p_k(n)$ are polynomials with integer coefficients such that $p_i(0) = 0$, for $i = 1, 2, \ldots, k$. Let $A \in \mathscr{B}$, $\mu(A) > 0$. Then there exists $n \in \mathbb{Z}$, $n \neq 0$, such that*

$$\mu(A \cap T_1^{p_1(n)} T_2^{p_2(n)} \ldots T_k^{p_k(n)} A) > 0.$$

In other words, the set

$$\{(p_1(n), \ldots, p_k(n)) \mid n \in \mathbb{Z}\} \subset \mathbb{Z}^k$$

is a set of recurrence.

COROLLARY 4.2.1. *Suppose that $S \subset \mathbb{Z}^k$ is a set of positive upper Banach density and let $p_1(n), p_2(n), \ldots, p_k(n)$ be polynomials with integer coefficients such that $p_i(0) = 0$, for $i = 1, 2, \ldots, k$. Then there exists a solution to the equation*

$$x - y = (p_1(n), p_2(n), \ldots, p_k(n)),$$

where $x, y \in S$, $x \neq y$, $n \in \mathbb{Z}$.

Proof. Let $\Omega = \{0, 1\}^{\mathbb{Z}^k}$ and denote by

$$v_1 = (1, 0, \ldots, 0),\ v_2 = (0, 1, \ldots, 0) \ldots,\ v_k = (0, \ldots, 1)$$

the basis vectors in $\mathbb{Z}^k$. Define $T_i:\Omega \to \Omega$ by

$$T_i\,\omega(n) = \omega(n+v_i), \quad n\in\mathbb{Z}^k,\ i = 1,2,\dots,k.$$

Obviously, the T_i commute. Let $\xi(n)$ be the characteristic function of the set S, and let X be the closure in Ω of the set of all translates of ξ:

$$X = \overline{\{T_1^{n_1}T_2^{n_2}\dots T_k^{n_k}\xi \mid (n_1,\dots,n_k)\in\mathbb{Z}^k\}}.$$

Let $A = \{x\in X \mid x(0) = 1\}$. In complete analogy with the one-dimensional situation one can show that there exists a probability measure μ on the Borel sets of X, satisfying $\mu(A) > 0$. It follows from Theorem 4.2 that there exists $n\in\mathbb{Z}$, $n \neq 0$, such that

$$\mu(A \cap T_1^{p_1(n)}T_2^{p_2(n)}\dots T_k^{p_k(n)}A) > 0.$$

If $x\in A \cap T_1^{p_1(n)}T_2^{p_2(n)}\dots T_k^{p_k(n)}A$, then

$$x(0) = 1 = x(p_1(n), p_2(n), \dots, p_k(n)).$$

As x lies in the orbit closure of ξ, there exists $(m_1, m_2, \dots, m_k)\in\mathbb{Z}^k$ such that

$$T_1^{m_1}T_2^{m_2}\dots T_k^{m_k}\xi(0) = T_1^{m_1}T_2^{m_2}\dots T_k^{m_k}\xi(p_1(n),\dots,p_k(n)) = 1$$

or $\xi(m_1,\dots,m_k) = \xi(m_1+p_1(n),\dots,m_k+p_k(n)) = 1$, and this proves the corollary.

5. *Generalizations and concluding remarks*

(i) The results obtained in this paper for sets of differences $A-A$, where A is a set of positive upper Banach density in $\mathbb{Z}^m$, are also valid for finite intersections of such sets. To illustrate this we shall indicate how the following generalization of Corollary 3.1.1 can be proved.

THEOREM 5.1. *Suppose that $A_1, A_2, \dots, A_k$ are sets of positive upper Banach density in $\mathbb{Z}^2$. Then there exists a set $B \subset \mathbb{Z}$ of positive upper density such that*

$$(A_1-A_1)\cap(A_2-A_2)\cap\dots\cap(A_k-A_k) \supset B\times B.$$

Sketch of the proof. First of all we need an appropriate version of Theorem 3.1. Let $(X_i, \mathscr{B}_i, \mu_i)$ be probability measure spaces and $C_1\in\mathscr{B}_i$, $\mu_i(C_i) > 0$. Suppose that T_i, S_i are commuting invertible measure-preserving transformations of $(X_i, \mathscr{B}_i, \mu_i)$, for $i = 1,2,\dots,k$. Let

$$(X, \mathscr{B}, \mu) = \prod_{i-1}^{k}(X_i, \mathscr{B}_i, \mu_i)$$

be the product measure space. This means that X is the Cartesian product of X_i, $\mathscr{B}$ is the σ-algebra generated by Cartesian products of sets from $\mathscr{B}_i$, and $\mu = \mu_1\times\mu_2\times\dots\times\mu_k$ is the product measure on $\mathscr{B}$. Define the product maps $T = T_1\times T_2\times\dots\times T_k$ and $S = S_1\times S_2\times\dots\times S_k$ by

$$T(x_1,\dots,x_k) = (T_1x_1, T_2x_2,\dots,T_kx_k), \quad S(x_1,x_2,\dots,x_k) = (S_1x_1, S_2x_2,\dots,S_kx_k).$$

Let $C = \prod_{i-1}^k C_i\in\mathscr{B}$. Obviously $\mu(C) = \prod_{i-1}^k \mu(C_i) > 0$ and $TS = ST$. Applying Theorem 4.1 to C, T and S we obtain a sequence $\{n_j\}_{j=1}^\infty$ of positive upper density such that, for any $j, l\in\mathbb{N}$,

$$(C\cap T^{n_j}S^{n_l}C) > 0. \tag{5.1}$$

Remembering that $C = \prod_{i=1}^{k} C_i$ we obtain from (5.1) that for any $j, l \in \mathbb{N}$ and all $i = 1, 2, \ldots, k$

$$\mu_i(C_i \cap T_i^{n_j} S_i^{n_l} C_i) > 0. \tag{5.2}$$

Now let $\Omega = \{0,1\}^{\mathbb{Z}^2}$, $\xi_i = 1_{A_i}$, for $i = 1, 2, \ldots, k$, and let T, S be as in the proof of Corollary 3.1.1. Define

$$X_i = \overline{\{T^n S^m \xi_i \mid (n,m) \in \mathbb{Z}^2\}}, \quad C_i = \{\omega \in X_i \mid \omega(0,0) = 1\}.$$

For each i, $1 \leqslant i \leqslant k$, let μ_i be a probability measure on X_i such that $\mu_i(C_i) > 0$. Forming the appropriate product space and applying (5.2) we obtain the desired result.

(ii) The following generalization of Theorem 3.1 can be obtained by using Furstenberg's and Katznelson's multidimensional ergodic Szemerédi theorem instead of Khintchine's recurrence theorem.

THEOREM 5.2. *If $(X, \mathscr{B}, \mu)$ is a probability measure space and $T_1, T_2, \ldots, T_k$ are commuting invertible measure-preserving transformations of $(X, \mathscr{B}, \mu)$, then for any $A \in \mathscr{B}$ with $\mu(A) > 0$ there exists a sequence $\{n(i)\}_{i=1}^{\infty}$ of positive upper density such that for any $i_1, i_2, \ldots, i_k \in \mathbb{N}$ we have*

$$(A \cap T_1^{n(i_1)} A \cap T_2^{n(i_2)} A \cap \ldots \cap T_k^{n(i_k)} A) > 0.$$

A combinatorial consequence of Theorem 5.2 is the following.

THEOREM 5.3. *Let $A \subset \mathbb{Z}^m$ be a set of positive upper Banach density and let $v_1, v_2, \ldots, v_n \in \mathbb{Z}^m$. Then there exists a set $B \subset \mathbb{N}$ of positive upper density such that for any $k_1, k_2, \ldots, k_n \in B$ the set A contains a congruent image of the set $\{0, k_1 v_1, k_2 v_2, \ldots, k_n v_n\}$.*

(iii) We were not interested in quantitative statements about the density of sets which appear in our discussion. In most cases such statements can be formulated and rather precise bounds can be given. For example one can show that if $A \subset \mathbb{Z}$ with $d^*(A) = a > 0$, then there exists a sequence of integers $\{n_k\}_{k=1}^{\infty}$ such that $d^*(\{n_k\}) > \frac{1}{4}a^4$ and, for any i, j, $n_i^2 + n_j^2 \in A - A$.

References

1. H. FURSTENBERG, *Recurrence in ergodic theory and combinatorial number theory* (University Press, Princeton 1981).
2. H. FURSTENBERG and B. WEISS, 'Topological dynamics and combinatorial number theory, *J. Analyse Math.* 34 (1978) 61–85.
3. H. FURSTENBERG and Y. KATZNELSON, 'An ergodic Szemerédi theorem for commuting transformations', *J. Analyse Math.* 34 (1978) 275–291.
4. H. FURSTENBERG, 'Poincaré recurrence and number theory', *Bull. Amer. Math. Soc.* 5 (1981) 211–234.

Institute of Mathematics
Hebrew University
Jerusalem
Israel