Squarefree numbers, IP sets and ergodic theory

Vitaly Bergelson * and Imre Z. Ruzsa **

Department of Mathematics
Ohio State University
Columbus, Ohio, 43210
USA
e-mail: vitaly@math.ohio-state.edu

Alfréd Rényi Mathematical Institute, Hungarian Academy of Sciences,
Budapest, Pf. 127, H–1364 Hungary.
e-mail: ruzsa@math-inst.hu

1. Introduction

In this paper we deal mainly with the set S of squarefree numbers and its shifts, namely, sets of the form

$$S - a = \{x - a : x \in S\}.$$

The questions we ask intertwine combinatorial number theory with ergodic theory of multiple recurrence and are motivated by the natural curiosity related to an important subset of $\mathbb{N}$ as well as by the desire to gain, through the study of S, some additional (heuristic) insight about the set of primes.

We start this introduction by mentioning some known facts and conjectures about primes which the reader is invited to juxtapose with the results about S brought up in this paper.

One of the outstanding open problems related to the set $P = \{2, 3, 5, ...\}$ of primes is the conjecture that it contains arbitrarily long arithmetic progressions. In this direction it is known that P contains infinitely many 3-term arithmetic progressions (Chowla, 1944). In contrast we remark that one can show with relative ease that S contains arbitrarily long arithmetic progressions (see Theorem 2.8 below). (This also immediately

* Supported by NSF under grants DMS-9706057 and DMS-0070566
** Supported by Hungarian National Foundation for Scientific Research, Grants No. T 25617 and T 29759

follows from a celebrated theorem of Szemerédi (1975), which states that every set of positive upper density has this property.)

Another important type of configurations that we are interested in are the *sets of finite sums*. Given a nonempty set $E \subset \mathbb{N}$, the set of its finite sums, $\mathrm{FS}(E)$ is defined as the collection of all sums of elements of finite nonempty subsets of E. (The exclusion of the empty sum, that is, the number 0 from $\mathrm{FS}(E)$ helps to avoid some trivial complications. We could also include it here and modify the statements accordingly.) For infinite E the sets $\mathrm{FS}(E)$ are called IP-sets and play a prominent role in ergodic theory of multiple recurrence and its applications. (See, for instance, Furstenberg (1981), Furstenberg and Katznelson (1985), Bergelson, Furstenberg and McCutcheon (1996), Bergelson and McCutcheon (2000)).

We say that a set D of positive integers has IP_0 *property*, if for every $k \in \mathbb{N}$ there exists an $E \subset D$ with $|E| = k$ such that $\mathrm{FS}(E) \subset D$. It is known that for any t the set of shifted primes, $P - t$, does not contain an IP-set (Hegyváry and Sárközy, 1999). It is an open problem whether the set $P - 1$ has IP_0 property. (We believe it does. It follows from easy divisibility considerations that $P - t$ does not have this property if $t \neq \pm 1$, see Statement 2.12. A positive answer for $t = \pm 1$ would follow from the prime tuple conjecture. This asserts that for any finite collection $a_1, ..., a_k$ of integers, which do not contain a complete residue system modulo m for any $m \geq 2$, there are infinitely many integers t such that each $t + a_i$ is prime – the simplest case is the twin prime conjecture. The IP_0 property for $P - 1$ is equivalent to the solvability of certain systems of linear equations in the set of primes. The best known unconditional results in this direction, due to Balog (1992), are still too weak for our purposes, but perhaps not hopelessly so.) We will show that for any $a \in S$ the set $S - a$ contains an IP set (see Lemma 2.10 below). It is easy to see that if $a \notin S$, then $S - a$ does not even have the IP_0 property, see Statement 2.12.

A set $H \subset \mathbb{N}$ is called *intersective*, if for any set E which has positive upper density, defined as

$$\overline{\mathbf{d}}(E) = \limsup_{n \to \infty} \frac{|E \cap \{1, 2, ..., n\}|}{n},$$

one has $(E - E) \cap H \neq \emptyset$. As a nontrivial example of an intersective set we mention $P - 1$ (Sárközy, 1978b). ($P + 1$ is also intersective and $P - t$ is not for any $t \neq \pm 1$, as it does not intersect $E - E$ for, say, $E = 2|t|\mathbb{N}$.)

The notion of intersectivity has an equivalent formulation in the language of abstract ergodic theory. Following Furstenberg, let us call a set $R \subset \mathbb{Z}$ a *set of recurrence* (or *Poincaré set*) if for any measure-preserving transformation T of a probability space $(X, \mathcal{B}, \mu)$ and for any $A \in \mathcal{B}$ with $\mu(A) > 0$ there exists an $n \in R$, $n \neq 0$ such that $\mu(A \cap T^n A) > 0$. A set $R \subset \mathbb{N}$ is a set of recurrence if and only if it is intersective (Bertrand-Mathis (1986)), see also Appendix.

We list some further examples of sets of recurrence:

(i) $\{f(n)\}_{n\in\mathbb{N}}$, where $f(x)\in\mathbb{Z}[x]$ is such that $f(0)=0$. (Sárközy (1978a), Kamae and Mendès France (1978), Furstenberg (1977, 1981)).

(ii) $\{f(n)\}_{n\in P-1}$, where f is as above. (Wierdl, 1989.)

(iii) $\{f(n)\}_{n\in\Gamma}$, where f is as above and Γ is any IP set. (Bergelson, Furstenberg, McCutcheon, 1996.)

As was already mentioned, it will be shown in this paper that any set of the form $S-a$, $a\in S$ contains an IP set. It follows from (iii) above that for any $a\in S$ the set $\{f(n)\}_{n\in S-a}$ is a set of recurrence. We shall see below that actually a stronger fact pertaining to *multiple* recurrence is also true.

Definition 1.1. Fix $d\in\mathbb{N}$ and let $E\subset\mathbb{Z}^d$. The *upper Banach density* $\mathbf{d}^*(E)$ is defined as

$$\mathbf{d}^*(E)=\limsup_{n\to\infty}\left(\sup\frac{|E\cap\Pi|}{|\Pi|}\right),$$

where the supremum in parentheses is taken over all parallelopipeds

$$\Pi=[a_1,b_1]\times\ldots\times[a_d,b_d]$$

satisfying $b_i-a_i\geq n$ for all i.

Definition 1.2. A set $H\subset\mathbb{Z}^d$ is called *intersective*, if for any $E\subset\mathbb{Z}^d$ with $\mathbf{d}^*(E)>0$ one has $(E-E)\cap H\neq\emptyset$.

Given d commuting measure-preserving transformations $T_1,\ldots,T_d$ acting on a probability measure space $(X,\mathcal{B},\mu)$, we shall use the notation

$$T^{\mathbf{n}}=T_1^{n_1}\ldots T_d^{n_d},$$

where $\mathbf{n}=(n_1,\ldots,n_d)$. We call this family $(T^{\mathbf{n}})_{\mathbf{n}\in\mathbb{Z}^d}$ a *measure-preserving $\mathbb{Z}^d$-action.*

Definition 1.3. A set $R\subset\mathbb{Z}^d$ is called a *set of recurrence* (for $\mathbb{Z}^d$-actions), if for any measure-preserving $\mathbb{Z}^d$-action on a probability space $(X,\mathcal{B},\mu)$ and any $A\in\mathcal{B}$ with $\mu(A)>0$ there exists an $\mathbf{n}\in R$, $\mathbf{n}\neq\mathbf{0}$, such that $\mu(A\cap T^{\mathbf{n}}A)>0$.

The examples of sets of recurrence in $\mathbb{Z}$ admit natural extensions to $\mathbb{Z}^d$. Let $f_1(x),\ldots,f_d(x)\in\mathbb{Z}[x]$, $f_i(0)=0$. (Our statements about polynomials work in general for the wider class of polynomials $f(x)\in\mathbb{Q}[x]$ satisfying $f(\mathbb{Z})\subset\mathbb{Z}$, which includes natural examples like $n(n+1)/2$. However, for a finite collection $f_1,\ldots,f_d$ of such polynomials one can always find a positive integer m such that all the polynomials $g_i(x)=f_i(mx)$ have integral coefficients, thus the results would not be truly more general.)

The following are examples of sets of $\mathbb{Z}^d$-recurrence.

(a) $\{\big(f_1(n),\ldots,f_d(n)\big)\}_{n\in S-a}$, where $a\in S$;

(b) $\{\big(f_1(n),...,f_d(n)\big)\}_{n\in\Gamma}$, where Γ is an IP set;

(c) $\{\big(f_1(n),...,f_d(n)\big)\}_{n\in P-1}$.

For more about (a) and (b), see Proposition 3.4 and afterwards. (c) can be shown by some modifications of the method of Kamae and Mendès France, and we plan to give details in another paper.

One can show that the notions of $\mathbb{Z}^d$-intersectivity and $\mathbb{Z}^d$-recurrence coincide (see Appendix).

A related stronger concept got its name after some results of van der Corput on uniform distribution.

Definition 1.4. A set $H \subset \mathbb{Z}^d$ is called *van der Corput set*, if it has the following property: whenever for a real sequence $(u_{\mathbf{n}})_{\mathbf{n}\in\mathbb{Z}^d}$ all the difference sequences $(u_{\mathbf{n}+\mathbf{h}} - u_{\mathbf{n}})_{\mathbf{n}\in\mathbb{Z}^d}$ formed with any $\mathbf{h} \in H$ are uniformly distributed modulo 1, then $(u_{\mathbf{n}})_{\mathbf{n}\in\mathbb{Z}^d}$ itself is uniformly distributed.

The van der Corput property implies intersectivity (this is easy, but prehaps not completely obvious; we plan to return to this and related questions in another paper.) For $d = 1$ it is known to be equivalent to various other properties, see Ruzsa (1981/82, 1984). It is also known that (for $d = 1$) intersectivity does not imply the van der Corput property (Bourgain 1987, Forrest 1991). One can show that examples (a) and (c) above are actually van der Corput sets. It is an open problem whether, for a general Γ, (b) is van der Corput or not.

2. Some properties of squarefree numbers

In this section we prove some properties of certain sets formed from the set of squarefree numbers. We do not claim originality for any of these simple results. In lack of a reference we list and prove what we need for our applications.

We will use $S = \{s_1, s_2, ...\}$ to denote the set of squarefree numbers.

In the sequel we formulate some properties of sets of integers. We allow these sets to contain 0 or negative numbers (our sets will have only finitely many such elements), however, we define density by considering the number of elements in $[1, N]$ and letting $N \to \infty$, so the possible negative elements do not affect it.

Definition 2.1. We say that a set $A \subset \mathbb{Z}$ is *rational*, if for every $\varepsilon > 0$ there is a set B which is a union of finitely many arithmetic progressions and

$$\overline{\mathbf{d}}\big((A \setminus B) \cup (B \setminus A)\big) < \varepsilon. \tag{2.1}$$

Lemma 2.2.

i) The class of rational sets forms a set algebra (it is closed under taking finite unions, intersections and forming the complement).

ii) A rational set has an asymptotic density.

Proof. (i) is obvious.

(ii) Indeed, (2.1) implies that the difference between upper and lower density is at most ε. ■

Sometimes we will need a stronger property.

Definition 2.3.

i) A set $A \subset \mathbb{Z}$ is (m, ε)-*regular*, if its intersection with a residue class modulo m has always either upper density $< \varepsilon/m$, or lower density $> (1-\varepsilon)/m$.

ii) A set $A \subset \mathbb{Z}$ is *inner* (m, ε)-*regular*, if its intersection with a residue class modulo m is either empty, or has lower density $> (1-\varepsilon)/m$.

Definition 2.4. A set $A \subset \mathbb{N}$ is *regular* (*inner regular*), if for every $\varepsilon > 0$ there is an $m \in \mathbb{N}$ such that A is (m, ε)-regular (or inner (m, ε)-regular, respectively).

The difference between regularity and inner regularity is that a regular set may contain a few "exceptional" elements (say only one even number), and an inner regular one cannot. This property will be heavily utilized below during the proof of Theorem 2.8.

Lemma 2.5.

A regular set always has a density. The density of a nonempty inner regular set is always positive.

Proof. A regular set is rational, hence has a density. If a set is $(m, 1/2)$ inner regular, the density must be clearly at least $1/(2m)$. ■

We do not know whether the classes of regular and inner regular sets are closed under finite union and intersection. We expect that they are not, and it would be interesting to modify the definition to have these properties while still including the examples to be described below. However, an important special case can be easily shown.

Lemma 2.6.

(i) Let A be an inner regular set. Any set, formed from finitely many translations of A via the operations of union and itersection is also inner (or outer) regular, respectively.

(ii) Let A be a regular set. Any element of the set algebra, generated by the translations of A, is also regular.

Proof. (i) The only point to be observed is that if A is inner (m, ε)-regular, then so are all its translates, with the same m. Take an intersection B of k translations of A. If the intersection of B with a residue class modulo m is not empty, then each of the translations of A involved intersect it, then each contains it save a set of upper density $\leq \varepsilon/m$, thus B contains it save a set of upper density $\leq k\varepsilon/m$.

Consider now a union C of l sets, say $B_1, ..., B_l$, each of which is formed as an intersection of at most k translations of A. Take a residue class modulo m. If some B_i intersects it, then the intersection has density $\geq 1 - k\varepsilon/m$ by the previous argument, so C intersects it with density $\geq 1 - k\varepsilon/m$; if no B_i intersects it, then C does not intersect it either. Consequently C is inner $(m, k\varepsilon)$-regular.

(ii) The proof follows that of (i) with obvious changes. ■

Lemma 2.7.

Let $B \subset \mathbb{N}$ be a set such that $1 \notin B$, any two elements of B are coprime and

$$\sum_{b \in B} 1/b < \infty.$$

Define A as the set of natural numbers that are not divisible by any element of B. Then A is an inner regular set of positive density. In particular, S is inner regular (its density is well known to be $6/\pi^2$).

Proof. Take an $\varepsilon > 0$, and choose K so that

$$\sum_{b \in B, b > K} 1/b < \varepsilon. \tag{2.3}$$

Let

$$m = \prod_{b \in B, b \leq K} b.$$

We claim that A is inner (m, ε)-regular. Indeed, consider a residue class $a \pmod m$. If the gcd (a, m) is divisible by any $b \in B$, then clearly no integer $\equiv a \pmod m$ belongs to A.

Assume that (a,m) has no divisor from B. We show that the density of the numbers in this residue class and not in A is $< \varepsilon/m$. We estimate the number of such integers up to N.

Such an integer satisfies

$$n \equiv a \pmod{m}, \quad n \equiv 0 \pmod{b}$$

with some $b \in B$. This congruence is impossible if $b \leq K$, and it is equivalent to a single congruence

$$n \equiv r_b \pmod{mb}$$

for $b > K$. The number of solutions up to N is hence $\leq 1 + N/(bm)$. Also, there is no such number if $b > N$. Thus the total cardinality of such numbers up to N is

$$\leq \sum_{b\in B, K<b\leq N} \left(1 + \frac{N}{bm}\right) \leq \frac{\varepsilon N}{m} + \sum_{b\in B, b\leq N} 1 = \left(\frac{\varepsilon}{m} + o(1)\right) N$$

as claimed. Above, in the firs inequality we applied (2.3), in the second we used the fact that a set whose sum of reciprocals converges always has density 0. ■

We cannot decide whether the condition of coprimality is necessary. It is easy to see that for a set B with a convergent sum of reciprocals the corresponding set A will always be rational.

Now we look for IP sets in regular sets. We will find slightly more general configurations. An IP set can be thought of as an infinite dimensional cube of side 2; we will find cubes whose sides tend to infinity. More exactly, given a sequence $E = \{e_1, e_2, ..., \}$ of integers, we define $\overline{\mathrm{FS}}(E)$ as the set of all sums of the form $\sum x_i e_i$ with integer coefficients x_i satisfying $0 \leq x_i \leq i$, not all $x_i = 0$. (The additional requirement $x_i \leq 1$ gives $\mathrm{FS}(E)$.) We will call a set of the form $\overline{\mathrm{FS}}(E)$ with infinite E an $\overline{\mathrm{IP}}$ set.

Theorem 2.8.

Every inner regular set A such that $0 \in A$ contains an $\overline{\mathrm{IP}}$ set (hence a fortiori it contains an IP set).

Lemma 2.9.

Let A be an inner regular set, $a_1, ..., a_k \in A$, $l \in \mathbb{N}$. There are infinitely many positive integers e with the property that all the integers $a_i + je$, $1 \leq i \leq k$, $1 \leq j \leq l$ are in A.

Proof. Consider the set

$$B = \bigcap_{i=1}^{k} (A - a_i).$$

It is inner regular by Lemma 2.6, and $0 \in B$ by definition. Take $\varepsilon = 1/4l^2$, and choose an m for which it is (m, ε)-regular. Write

$$X = m\mathbb{Z} \setminus B;$$

we know that $\mathbf{d}(X) \le \varepsilon/m$.

We will show at least half of the multiples of m can serve as a value of e. To do this we will estimate the number of integers $t \le T$ for which mt does not work. This means that $jmt \notin B$ for some $1 \le j \le l$, so $jmt \in X$. As $jmt \le lmT$, the number of such integers (for a fixed j) is $< 2(\varepsilon/m)lmT = 2\varepsilon lT$ for $T > T_0$. Since there are l possible choices for j, the total number of excluded values of t is $< 2\varepsilon l^2 T < T/2$ as claimed. ■

Proof of the Theorem. We find integers e_i inductively so that always

$$\overline{\mathrm{FS}}\,(e_1, ..., e_j) \subset S.$$

If $e_1, ..., e_{j-1}$ are already found, we apply the Lemma with $l = j$, with k replaced by $(j-1)!$ and $a_1, ..., a_k$ replaced by the elements of $\overline{\mathrm{FS}}\,(e_1, ..., e_{j-1}) \cup \{0\}$. Any of the integers e provided by the lemma is a suitable choice for e_j. ■

We state separately those corollaries for squarefree numbers that we will need.

Lemma 2.10.

For any $a_1, ..., a_k \in S$, the set $\bigcap(S - a_i)$ contains an IP set. In particular, each $S - a$, where $a \in S$, contains an IP set.

Lemma 2.11.

If $E \subset S - a$ is such that $\overline{\mathbf{d}}\big((S-a) \setminus E\big) = 0$, then E contains an IP set.

Proof. Indeed, if we omit a set of density 0 from an inner regular set, the remaining set still will be inner regular. ■

We complement the above positive results by a negative one which shows why the assumption $a \in S$ was necessary, and also explains a remark in the Introduction about primes.

Statement 2.12.

(i) If a is not squarefree, then the set $S - a$ does not have the IP_0 property.

(ii) If $t \ne \pm 1$, then the set $P - t$ does not have the IP_0 property.

Proof. Consider a set A with $\overline{\mathrm{IP}}$ property. We show that for every m, A contains infinitely many multiples of m. Indeed, take an E such that $|E| = km$ and $\mathrm{FS}\,(E) \subset A$.

By the box principle, there is a residue class modulo m in which E has at least k elements. The sum of any m of these numbers is a multiple of m, and (by fixing the first $m-1$ summands and varying the last) we see that there are at least $k-m+1$ different m-term sums.

Now to deduce (i), observe that $S-a$ cannot contain a multiple of $|a|$ if a is not squarefree. To obtain (ii), observe that if $t \neq \pm 1$, then the only multiples of $|t|$ in the set $P-t$ are $\pm t$ if t is itself prime, and there is no such multiple at all if t is composite. ■

3. Application to intersection problems with squarefree numbers

We shall derive now some corollaries from Theorem 2.8 . We present first some results which will be needed for the derivation of these corollaries.

First we formulate a version of Furstenberg's correspondence principle, which was introduced by him in order to derive combinatorial facts, such as Szemerédi's theorem, from multiple recurrence results in ergodic theory. For a proof of the particular version that we are giving here see Bergelson and McCutcheon (2000), Proposition 7.2. See also Furstenberg (1981), p. 152.

Proposition 3.1.

Let $E \subset \mathbb{Z}^r$ be a set satisfying $\mathbf{d}^*(E) > 0$ ($\mathbf{d}^*$ denotes upper Banach density). Then there exists a probability measure preserving system $(X, \mathcal{B}, \mu, \{T^{\mathbf{n}}\}_{\mathbf{n}\in\mathbb{Z}^r})$ and a set A with $\mu(A) > 0$ such that for all $k \in \mathbb{N}$ and $\mathbf{n}_1, ..., \mathbf{n}_k \in \mathbb{Z}^r$ one has

$$\mathbf{d}^*\big(E \cap (E-\mathbf{n}_1) \cap ... \cap (E-\mathbf{n}_k)\big) \geq \mu\big(A \cap T^{\mathbf{n}_1}A \cap ... \cap T^{\mathbf{n}_k}A\big).$$

Next we formulate Hindman's finite sets theorem (Hindman, 1974), which has greatly influenced our work.

Proposition 3.2.

If we partition an IP set into finitely many classes, one of them will contain an IP set. Equivalently, if we color the finite subsets of an infinite set with finitely many colors, then there is an infinite collection of disjoint finite subset with the property than all the finite unions formed from these subsets are all of the same color.

Another tool which will be utilized in the sequel is the IP polynomial Szemerédi theorem, proved by Bergelson and McCutcheon (2000).

Definition 3.3. A set $E \subset \mathbb{Z}^d$ is called an IP* set, if for every IP set $\Gamma \subset \mathbb{Z}^d$ one has $E \cap \Gamma \neq \emptyset$.

Hindman's theorem (Prosition 3.2 above) immediately implies that any IP* set contains an IP subset of any IP set.

Proposition 3.4.

Suppose we are given r comuting invertible measure preserving transformation $T_1, ..., T_r$ of a probability space $(X, \mathcal{B}, \mu)$. Let $d, t \in \mathbb{N}$ and let

$$p_{ij}(x_1, ..., x_d) \in \mathbb{Z}[x_1, ..., x_d]$$

with $p_{ij}(0, ..., 0) = 0$, $1 \leq i \leq r$, $1 \leq j \leq t$. Then for every $A \in \mathcal{B}$ with $\mu(A) > 0$ the set

$$\left\{ (n_1, ..., n_d) \in \mathbb{Z}^d : \mu \left(\bigcap_{j=1}^{t} \prod_{i=1}^{r} T_i^{p_{ij}(n_1, .., n_d)} A \right) > 0 \right\}$$

is an IP set in $\mathbb{Z}^d$.*

See Bergelson and McCutcheon (2000).

In view of Furstenberg's correspondence principle, one has the following result (ibid.)

Corollary 3.5.

Suppose that $r, k, t \in \mathbb{N}$, $E \subset \mathbb{Z}^r$ with $\mathbf{d}^*(E) > 0$ and $p_i : \mathbb{Z}^k \to \mathbb{Z}^d$ are polynomials with $p_i(\mathbf{0}) = \mathbf{0}$, $1 \leq i \leq t$. Then

$$R_E = \left\{ \mathbf{n} \in \mathbb{Z}^k : \mathbf{d}^* \big(E \cap (E - p_1(\mathbf{n})) \cap ... \cap (E - p_t(\mathbf{n})) \big) > 0 \right\}$$

is an IP set in $\mathbb{Z}^k$.*

The following proposition follows from Lemma 2.10.

Proposition 3.6.

The set R_E in Corollary 3.4 has nonempty intersection with $S - a$ for any $a \in S$. Moreover, for any $a_1, ..., a_k \in S$ the set $R_E \cap \left(\bigcap_{i=1}^{k} (S - a_i) \right)$ contains an IP set.

We mention an interesting special case.

Corollary 3.7.

For any $E \subset \mathbb{Z}$ with $\mathbf{d}^*(E) > 0$, any $a_1, ..., a_k \in S$ and any $f_1, ..., f_k \in \mathbb{Z}[x]$ such that $f_i(0) = 1$ for $i = 1, ..., k$ one can find integers $n \in \bigcap_{i=1}^{k} (S - a_i)$ such that

$$E \cap \big(E - f_1(n) \big) \cap ... \cap \big(E - f_k(n) \big) \neq \emptyset.$$

Moreover, there is an infinite IP set consisting of such integers n.

There is a less straightforward application of partitional nature.

Theorem 3.8.

Let $k, r \in \mathbb{N}$, $a \in S$. Let $f_1, ..., f_k \in \mathbb{Z}[x]$ satisfy $f_i(0) = 1$ for $i = 1, ..., k$. If $S - a = \bigcup_{i=1}^{r} C_i$, then at least one C_i has the following property: there are arbitrarily large $x, y \in C_i$ such that

$$\{x, x + f_1(y), ..., x + f_k(y)\} \subset C_i.$$

Proof. Reindexing if necessary, we can assume that $C_1, ..., C_{r'}$ have positive upper density and the C_i, $r' < i \leq r$ have density 0, for some $1 \leq r' \leq r$. By Lemma 2.11 the set $\bigcup_{i=1}^{r'} C_i$ contains an IP set, and hence, by Hindman's theorem, so does one of the C_i, $1 \leq i \leq r'$. The set $C = C_i$ has the following crucial properties: it has positive upper density, and it ontains an IP set. Now the claim follows from Corollary 3.6. ■

4. Appendix: Multidimensional recurrence and intersectivity

Theorem 4.1.

A set $E \subset \mathbb{Z}^d$ is a set of recurrence if and only if it is a set of $\mathbb{Z}^d$-intersectivity.

Proof. In one direction the result follows immediately from Furstenberg's correspondence principle (quoted above as Proposition 3.1). We need only the case $k = 2$.

We outline the proof in the other direction. We define the density (if it exists) of a set $E \subset \mathbb{Z}^d$ by the formula

$$\mathbf{d}(E) = \lim_{n \to \infty} n^{-d} |E \cap [1, n]^d|.$$

Lemma 4.2.

Let $(T^{\mathbf{n}})_{\mathbf{n} \in \mathbb{Z}^d}$ be a measure-preserving $\mathbb{Z}^d$-action on a probability measure space $(X, \mathcal{B}, \mu)$. Let $A \in \mathcal{B}$ with $\mu(A) = a > 0$. Then there exists a set $E \subset \mathbb{Z}^d$ with $\mathbf{d}(E) \geq a$ such that for any $m \in \mathbb{N}$ and any $\mathbf{n}_1, ..., \mathbf{n}_m \in E$ one has

$$\mu(A \cap T^{\mathbf{n}_1} \cap ... \cap T^{\mathbf{n}_m}) > 0.$$

The case $d = 1$ is Theorem 1.2 in Bergelson (1985). The proof for general d is practically the same.

We now deduce that if a set R is $\mathbb{Z}^d$-intersective, then it is a set of $\mathbb{Z}^d$-recurrence. To this end take a set E as in Lemma 4.2 above. Then $(E-E)\cap R\neq\emptyset$ by the intersectivity. This means that we have $\mathbf{n}_1-\mathbf{n}_2=\mathbf{r}$ with some $\mathbf{n}_1,\mathbf{n}_2\in E$ and $\mathbf{r}\in R$. From the Lemma we conclude that

$$\mu(T^{\mathbf{n}_1}A\cap T^{\mathbf{n}_2}A)>0.$$

This is equivalent to

$$\mu(A\cap T^{\mathbf{n}_1-\mathbf{n}_2}A)>0,$$

that is, $\mu(A\cap T^{\mathbf{r}}A)>0$ for some $\mathbf{r}\in R$ as wanted. ■

Theorem 4.1 could also be proved along the lines of Theorem 2.2 from Bergelson and McCutcheon (1998).

References

Balog, A. (1992), Linear equations in primes, *Mathematika* **39**, 367–378.

Bergelson, V. (1985), Sets of recurrence of $\mathbb{Z}^m$-actions and properties of sets of differences in $\mathbb{Z}^m$, *J. London Math. Soc. (2)* **31**, 295–304.

Bergelson, V., Furstenberg, H., McCutcheon, R. (1996), IP-sets and polynomial recurrence, *Ergodic Theory and Dynamical Systems* **16**, 963–974.

Bergelson, V., McCutcheon, R. (1998), Recurrence for semigroup actions and a non-commutative Schur theorem, *Contemporary Math.* **215**, 205-222.

Bergelson, V., McCutcheon, R. (2000), An ergodic IP polynomial Szemerédi theorem, *Memoirs of Amer. Math. Soc.* **146**, No. 695, vii + 106 pp..

Bertrand-Mathis, A. (1986), Ensembles intersectifs et récurrence de Poincaré, *Israel J. Math.* **55**, 184–198.

Bourgain, J. (1987), Ruzsa's problem on sets of recurrence, *Israel J. Math.* **59**, 150–166.

Chowla, S. (1944), There exists an infinity of 3-combinations of primes in A. P., *Proc. Lahore Philos. Soc.* **6**, 15–16.

Forrest, A. (1991), The construction of a set of recurrence which is not a set of strong recurrence, *Israel J. Math* **76**, 215–228.

Furstenberg, H. (1977), Ergodic hehaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. d'Analyse Math.* **31**, 204–256.

Furstenberg, H. (1981), *Recurrence in ergodic theory and combinatorial number theory*, Princeton University Press.

Furstenberg, H., Katznelson, Y. (1985), An ergodic Szemerédi theorem for IP-systems and combinatorial theory, *J. d'Analyse Math.* **45**, 117–168.

Hegyváry, N., Sárközy, A. (1999), Hilbert cubes in certain sets, *Ramanujan J.* **3**, 303–304.

Hindman, N. (1974), Finite sums from sequences within cells of a partition of $\mathbb{N}$, *J. Combin. Th. (Ser. A)* **17**, 1-11.

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

Ruzsa, I. Z. (1981/82), Uniform distribution, positive trigonometric polynomials and difference sets, in: *Semin. on Number Theory*, Univ. Bordeaux I (1981/82), No. 18, 1–18.

Ruzsa, I. Z. (1984), Connections between the uniform distribution of a sequence and its differences, in: *Coll. Math. Soc. J. Bolyai 34, Topics in Number Theory, Budapest 1981*, Akadémiai Kiadó, Budapest (1984), 1419–1443.

A. Sárközy (1978a), On difference sets of sequences of integers I., *Acta Math. Acad. Sci. Hung.* **31**, 125-149.

Sárközy, A. (1978b), On difference sets of sequences of integers III., *Acta Math. Acad. Sci. Hung.* **31**, 355-386.

Szemerédi, E. (1975), On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27**, 199–245.

Wierdl, M. (1989), *Almost everywhere convergence and recurrence along subsequences in ergodic theory*, PhD. Thesis, Ohio State University.