Ergodic theorem involving additive and multiplicative groups of a field and $\{x + y, xy\}$ patterns

VITALY BERGELSON and JOEL MOREIRA

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

Abstract. We establish a 'diagonal' ergodic theorem involving the additive and multiplicative groups of a countable field K and, with the help of a new variant of Furstenberg's correspondence principle, prove that any 'large' set in K contains many configurations of the form $\{x + y, xy\}$. We also show that for any finite coloring of K there are many $x, y \in K$ such that $x, x + y$ and xy have the same color. Finally, by utilizing a finitistic version of our main ergodic theorem, we obtain combinatorial results pertaining to finite fields. In particular, we obtain an alternative proof for a result obtained by Cilleruelo [Combinatorial problems in finite fields and Sidon sets. *Combinatorica* **32**(5) (2012), 497–511], showing that for any finite field F and any subsets $E_1, E_2 \subset F$ with $|E_1| \, |E_2| > 6|F|$, there exist $u, v \in F$ such that $u + v \in E_1$ and $uv \in E_2$.

1. Introduction

Schur's theorem [**17**] asserts that, given a finite coloring of $\mathbb{N} = \{1, 2, \ldots\}$, there exist $x, y \in \mathbb{N}$ such that x, y and $x + y$ all have the same color. A multiplicative version of this theorem is also true: given a finite coloring of $\mathbb{N}$, we can find $x, y \in \mathbb{N}$ such that x, y and xy all have the same color. To see this, consider, for instance, the induced coloring of the set $\{2^n; n \in \mathbb{N}\}$. However, very little is known regarding partition regularity of configurations involving both addition and multiplication. For some results in this direction see [**2**], [**7**, §6], [**5**, **8**, **10**, **12**, **15**].

In particular, the following question is still unanswered (cf. [**16**, Question 3]).

Question 1.1. Given a finite coloring of $\mathbb{N}$, is it true that there exist distinct $x, y \in \mathbb{N}$ such that both $x + y$ and xy have the same color?†

---

† In fact it is believed that one can find a monochromatic configuration of the form $\{x, y, x + y, xy\}$ for any finite coloring of $\mathbb{N}$.

While replacing $\mathbb{N}$ by $\mathbb{Z}$ does not seem to make the question easier, replacing $\mathbb{N}$ by $\mathbb{Q}$ does and this allows for the introduction of useful ergodic techniques. In this paper we show that any 'large'† set in $\mathbb{Q}$ contains the sought-after configurations, which leads to a partition result involving three-element sets having the form $\{x, y + x, yx\}$. Actually, the ergodic method that we employ works equally well in the framework of arbitrary countable‡ fields§.

Here is the formulation of the main partition result obtained in this paper.

THEOREM 1.2. (See Theorem 4.1 for a more precise formulation) *Let K be a countable field. Given a finite coloring $K = \bigcup C_i$, there exists a color C_i and x, $y \in K$ such that $\{x, x + y, xy\} \subset C_i$.*

We remark that it follows from Theorem 4.1 below that x and y can in fact be chosen from outside any prescribed finite set. We will derive Theorem 1.2 from a 'density' statement which, in turn, follows from an ergodic result dealing with measure preserving actions of the affine group $\mathcal{A}_K = \{ux + v : u, v \in K^*, u \neq 0\}$ of the field K (cf. Definition 2.2). To formulate these results, we first need to introduce the notion of double Følner sequences in K.

Definition 1.3. Let K be a countable field. A sequence of non-empty finite sets $(F_N) \subset K$ is called a *double Følner sequence* if for each $x \in K^* := K \setminus \{0\}$ we have

$$\lim_{N \to \infty} \frac{|F_N \cap (F_N + x)|}{|F_N|} = \lim_{N \to \infty} \frac{|F_N \cap (xF_N)|}{|F_N|} = 1.$$

See Proposition 2.4 for the proof of the existence of double Følner sequences in any countable field.

Here is the formulation of the main ergodic result in this paper and its combinatorial corollary (which is derived via a version of the Furstenberg correspondence principle - see Theorem 2.8).

THEOREM 1.4. *Let K be a countable field and let $\mathcal{A}_K$ be the group of affine transformations of K. Let $(\Omega, \mathcal{B}, \mu)$ be a probability space and let $(T_g)_{g \in \mathcal{A}_K}$ be a measure preserving action of $\mathcal{A}_K$ on Ω. For each $u \in K^*$, let $A_u = T_g$ where $g \in \mathcal{A}_K$ is defined by $g : x \mapsto x + u$ and let $M_u = T_h$ where $h \in \mathcal{A}_K$ is defined by $h : x \mapsto ux$. Let (F_N) be a double Følner sequence in K. Then for each $B \in \mathcal{B}$ we have*

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u}B \cap M_{1/u}B) \geq \mu(B)^2$$

and, in particular, the limit exists.

It is not hard to see that the quantity $\mu(B)^2$ in the right hand side of the displayed formula is the largest possible (consider, for example, the case when the action of $\mathcal{A}_K$ is strongly mixing).

† Here large means to have positive upper density with respect to some *double* Følner sequence in $\mathbb{Q}$. This will be defined in §2.3.
‡ We use the word 'countable' to mean infinitely countable.
§ And indeed in the framework of finite fields, this is explored in §5.

THEOREM 1.5. *Let K be a countable field, let (F_N) be a double Følner sequence in K and let $E \subset K$ be such that $\bar{d}_{(F_N)}(E) := \lim \sup_{N \to \infty} |E \cap F_N|/|F_N| > 0$. Then there are an infinite number of pairs $x, y \in K^*$ with $x \neq y$ such that*

$$\{x + y, xy\} \subset E. \tag{1}$$

A precise formulation of the size of the set of pairs (x, y) that satisfy equation (1) is given by Theorem 2.5 below.

We also obtain similar results for finite fields. For example, we have the following result (see also Theorem 5.1 for a dynamical formulation).

THEOREM 1.6. *For any finite field F and any subsets $E_1, E_2 \subset F$ with $|E_1| \, |E_2| > 6|F|$, there exist $x, y \in F$, $y \neq 0$, such that $x + y \in E_1$ and $xy \in E_2$.*

Theorem 1.6 has also been obtained for fields of prime order by Shkredov [**18**], for general finite fields by Cilleruelo [**11**, Corollary 4.2] and, with some additional quantitative estimates, by Hanson [**14**].

The paper is organized as follows. In §2 we introduce some notation, discuss basic facts about the affine group of a countable field, explore some properties of double Følner sequences, state our main results more precisely and obtain a general correspondence principle. In §3 we prove our main ergodic theoretical results. In §4 we deduce the main partition result for infinite fields, Theorem 1.2. In §5 we adapt our methods to prove an analogue of Theorems 1.2 and 1.4 for finite fields. Section 6 is devoted to some general remarks.

2. *Preliminaries*

2.1. *The group $\mathcal{A}_K$ of affine transformations.* We will work with a fixed countable field K. The set of non-zero elements of K will be denoted by K^*. It is not hard to see that for a set $E \subset K$, the statement that E contains a configuration of the form $\{u + v, uv\}$ is equivalent to the statement that $(E - u) \cap (E/u)$ is non-empty for some $u \in K^*$. To study this intersection we need to understand how the additive and the multiplicative groups of K interact. Hence, it is natural to work with the subgroup of all bijections of K generated by these two groups, which brings us to the group of all affine transformations of K as defined below.

Definition 2.2. The *affine group* of K is the set

$$\mathcal{A}_K = \{g : x \mapsto ux + v \mid u, v \in K, u \neq 0\}$$

with the operation of composition of functions. The *additive subgroup* of $\mathcal{A}_K$ is the set S_A of affine transformations of the form $A_u : x \mapsto x + u$, with $u \in K$. Note that S_A is isomorphic to the additive group $(K, +)$. The *multiplicative subgroup* of $\mathcal{A}_K$ is the set S_M of affine transformations of the form $M_u : x \mapsto ux$, with $u \in K^*$. Note that S_M is isomorphic to the multiplicative group $(K^*, \times)$.

Note also that the map $x \mapsto ux + v$ can be represented as the composition $A_v M_u$. We have the following identity, which will be utilized frequently in this paper, namely

$$M_u A_v = A_{uv} M_u. \tag{2}$$

Note that equation (2) expresses the fact that S_A is a normal subgroup of $\mathcal{A}_K$. Since both S_A and $S_M \cong \mathcal{A}_K/S_A$ are abelian groups, we conclude that $\mathcal{A}_K$ is a solvable group.

We can now represent the intersection $(E - u) \cap (E/u)$ as $A_{-u}E \cap M_{1/u}E$, where $A_{-u}E = \{x - u : x \in E\}$ and $M_{1/u}E = \{x/u : x \in E\}$. With this notation, a set $E \subset K$ contains a configuration of the form $\{u + v, uv\}$ if and only if there is some $u \in K^*$ such that $A_{-u}E \cap M_{1/u}E$ is non-empty. Also, the statement that there exist $u, v \in K^*$ such that $\{v, u + v, uv\} \subset E$ is equivalent to the statement that there exists some $u \in K^*$ such that $E \cap A_{-u}E \cap M_{1/u}E \neq \emptyset$.

2.3. *Double Følner sequences.* The first step in the proof of Theorem 1.2 is to prove that the intersection $A_{-u}E \cap M_{1/u}E$ is non-empty (for many choices of $u \in K$) when E is a large subset of K in a suitable sense. In this section, we will make this statement more precise.

As mentioned before, $\mathcal{A}_K$ is solvable and hence it is a (discrete) countable amenable group. This suggests the existence of a sequence of finite sets (F_N) in K, asymptotically invariant under the action of $\mathcal{A}_K$. Indeed, we have the following proposition.

PROPOSITION 2.4. *Let K be a countable field. There exists a sequence of non-empty finite sets (F_N) in K which forms a Følner sequence for the actions of both the additive group $(K, +)$ and the multiplicative group $(K^*, \times)$. In other words, for each $u \in K^*$ we have*

$$\lim_{N \to \infty} \frac{|F_N \cap (F_N + u)|}{|F_N|} = \lim_{N \to \infty} \frac{|F_N \cap (u F_N)|}{|F_N|} = 1.$$

We call such a sequence (F_N) a double Følner sequence.

Proof. Let $(G_N)_{N \in \mathbb{N}}$ be a (left) Følner sequence in $\mathcal{A}_K$. This means that G_N is a non-empty finite subset of $\mathcal{A}_K$ for each $N \in \mathbb{N}$, and that for each $g \in \mathcal{A}_K$ we have

$$\lim_{N \to \infty} \frac{|G_N \cap (g G_N)|}{|G_N|} = 1.$$

Note that for $g_1, g_2 \in \mathcal{A}_K$, if $g_1 \neq g_2$, then there is at most one solution $x \in K$ to the equation $g_1 x = g_2 x$. Thus, for each $N \in \mathbb{N}$, we can find a point x_N in the (infinite) field K such that $g_i x_N \neq g_j x_N$ for all pairs $g_i, g_j \in G_N$ with $g_i \neq g_j$. It follows that $F_N := \{g x_N : g \in G_N\}$ has $|G_N|$ elements.

Since $F_N \cap g F_N \supset \{h x_N : h \in G_N \cap g G_N\}$, we have $|F_N \cap g F_N| \geq |\{h x_N : h \in G_N \cap g G_N\}| = |G_N \cap g G_N|$. Therefore

$$1 \geq \limsup_{N \to \infty} \frac{|F_N \cap g F_N|}{|F_N|} \geq \liminf_{N \to \infty} \frac{|F_N \cap g F_N|}{|F_N|} \geq \lim_{N \to \infty} \frac{|G_N \cap g G_N|}{|G_N|} = 1.$$

Finally, putting $g = M_u$ and $g = A_u$ in the previous equation we get that (F_N) is a Følner sequence for $(K^*, \times)$ and for $(K, +)$. $\qquad \square$

From now on we fix a double Følner sequence (F_N) in K. For a set $E \subset K$, the lower density of E with respect to (F_N) is defined by the formula

$$\underline{d}_{(F_N)}(E) := \liminf_{N \to \infty} \frac{|F_N \cap E|}{|F_N|},$$

and the upper density of E with respect to (F_N) is defined by the formula

$$\bar{d}_{(F_N)}(E) := \limsup_{N \to \infty} \frac{|F_N \cap E|}{|F_N|}.$$

Note that both the upper and lower densities, $\underline{d}_{(F_N)}$ and $\bar{d}_{(F_N)}$, are invariant under affine transformations. In particular, for every $u \in K^*$ we have $\underline{d}_{(F_N)}(E/u) = \underline{d}_{(F_N)}(E - u) = \underline{d}_{(F_N)}(E)$ and $\bar{d}_{(F_N)}(E/u) = \bar{d}_{(F_N)}(E - u) = \bar{d}_{(F_N)}(E)$.

The following is the first step towards the proof of Theorem 1.2.

THEOREM 2.5. *Let $E \subset K$ be such that $\bar{d}_{(F_N)}(E) > 0$. Then for each $\epsilon > 0$ there is a set $D \subset K^*$ such that*

$$\underline{d}_{(F_N)}(D) \geq \frac{\epsilon}{\epsilon + \bar{d}_{(F_N)}(E) - \bar{d}_{(F_N)}(E)^2}$$

and for all $u \in D$ we have

$$\bar{d}_{(F_N)}((E - u) \cap (E/u)) > \bar{d}_{(F_N)}(E)^2 - \epsilon.$$

This result is of independent interest and does not follow from Theorem 1.2, because here we just need E to satisfy $\bar{d}_{(F_N)}(E) > 0$, not that it is a cell in a finite coloring. Theorem 2.5 will be proved in §2.9 as a consequence of Corollary 2.13, which in turn is proved in §3.

We will need the following lemma, which, roughly speaking, asserts that certain transformations of Følner sequences are still Følner sequences.

LEMMA 2.6. *Let (F_N) be a double Følner sequence in a field K and let $b \in K^*$. Then the sequence (bF_N) is also a double Følner sequence. Also, if (F_N) is a Følner sequence for the multiplicative group $(K^*, \times)$, then the sequence (F_N^{-1}), where $F_N^{-1} = \{g^{-1} : g \in F_N\}$, is still a Følner sequence for that group.*

Proof. The sequence (bF_N) is trivially a Følner sequence for the multiplicative group. To prove that it is also a Følner sequence for the additive group, let $x \in F$. Then we have

$$\lim_{N \to \infty} \frac{|bF_N \cap (x + bF_N)|}{|bF_N|} = \lim_{N \to \infty} \frac{|b(F_N \cap (x/b + F_N))|}{|F_N|} = 1.$$

To prove that (F_N^{-1}) is a Følner sequence for the multiplicative group note that for any finite sets $A, B \subset K$ we have $|A^{-1}| = |A|$, $(A \cap B)^{-1} = A^{-1} \cap B^{-1}$ and, if $x \in K^*$, then $(xA)^{-1} = x^{-1}A^{-1}$. Putting this all together we conclude that

$$\lim_{N \to \infty} \frac{|F_N^{-1} \cap (xF_N^{-1})|}{|F_N^{-1}|} = \lim_{N \to \infty} \frac{|(F_N \cap (x^{-1}F_N))^{-1}|}{|F_N|}$$

$$= \lim_{N \to \infty} \frac{|F_N \cap (x^{-1}F_N)|}{|F_N|} = 1. \qquad \square$$

2.7. *A correspondence principle.* To prove Theorem 2.5 we need an extension of Furstenberg's correspondence principle for an action of a group on a set (the classical versions deal with the case when the group acts on itself by translations, cf. [13]).

THEOREM 2.8. *Let X be a set, let G be a countable group and let $(\tau_g)_{g \in G}$ be an action of G on X. Assume that there exists a sequence (G_N) of finite subsets of X such that for each $g \in G$ we have the property*

$$\frac{|G_N \cap (\tau_g G_N)|}{|G_N|} \to 1 \quad as \ N \to \infty. \tag{3}$$

Let $E \subset X$ and assume that $\bar{d}_{(G_N)}(E) := \limsup_{N \to \infty} |G_N \cap E|/|G_N| > 0$.

Then there exists a compact metric space Ω, a probability measure μ on the Borel sets of Ω, a μ-preserving G-action $(T_g)_{g \in G}$ on Ω, a Borel set $B \subset \Omega$ such that $\mu(B) = \bar{d}_{(G_N)}(E)$, and for any $k \in \mathbb{N}$ and $g_1, \ldots, g_k \in G$ we have

$$\bar{d}_{(G_N)}(\tau_{g_1} E \cap \cdots \cap \tau_{g_k} E) \geq \mu(T_{g_1} B \cap \cdots \cap T_{g_k} B).$$

Proof. Define the family of sets

$$\mathcal{S} := \left\{ \bigcap_{j=1}^{k} \tau_{g_j} E : k \in \mathbb{N}, \ g_j \in G \forall j = 1, \ldots, k \right\} \cup \{X\}.$$

Note that $\mathcal{S}$ is countable, so using a diagonal procedure we can find a subsequence $(\tilde{G}_N)$ of the sequence (G_N) such that $\bar{d}_{(G_N)}(E) = \lim_{N \to \infty}(|E \cap \tilde{G}_N|/|\tilde{G}_N|)$ and, for each $S \in \mathcal{S}$, the following limit exists

$$\lim_{N \to \infty} \frac{|S \cap \tilde{G}_N|}{|\tilde{G}_N|}.$$

Note that (3) holds for any subsequence of (G_N), and in particular for $(\tilde{G}_N)$. Let $B(X)$ be the space of all bounded complex-valued functions on X. The space $B(X)$ is a Banach space with respect to the norm $\|f\| = \sup_{x \in X} |f(x)|$. Let $\rho \in \ell^\infty(\mathbb{N})^*$ be a Banach limit†.

Define the linear functional $\lambda : B(X) \to \mathbb{C}$ by

$$\lambda(f) = \rho\left(\left(\frac{1}{|\tilde{G}_N|} \sum_{x \in \tilde{G}_N} f(x) \right)_{N \in \mathbb{N}} \right).$$

The functional λ is positive (i.e. if $f \geq 0$, then $\lambda(f) \geq 0$) and $\lambda(1) = 1$. For any $f \in B(X)$, $g \in G$ and $x \in X$, the equation $f_g(x) = f(\tau_g x)$ defines a new function $f_g \in B(X)$. By (3), we have that $\lambda(f_g) = \lambda(f)$ for all $g \in G$, so λ is an invariant mean for the action $(\tau_g)_{g \in G}$. Moreover, $\bar{d}_{(G_N)}(E) = \lambda(1_E)$ and, for any $S \in \mathcal{S}$, we have $\bar{d}_{(G_N)}(S) \geq \lambda(1_S)$.

Note that the Banach space, $B(X)$, is a commutative C^*-algebra (with the involution being pointwise conjugation). Now, let $Y \subset B(X)$ be the (closed) subalgebra generated by the indicator functions of sets in $\mathcal{S}$. Then Y is itself a C^*-algebra. It has an identity (the constant function equal to 1) because $X \in \mathcal{S}$. If $f \in Y$, then $f_g \in Y$ for all $g \in G$. Moreover, since $\mathcal{S}$ is countable, Y is separable. Thus, by the Gelfand representation theorem (cf. [**1**, Theorem 1.1.1]), there exists a compact metric space Ω and a map $\Phi : Y \to C(\Omega)$ which is simultaneously an algebra isomorphism and a homeomorphism.

---

† This means that $\rho : \ell^\infty(\mathbb{N}) \to \mathbb{C}$ is a shift invariant positive linear functional such that for any convergent sequence $\mathbf{x} = (x_n) \in \ell^\infty(\mathbb{N})$ we have $\rho(\mathbf{x}) = \lim x_n$.

The linear functional λ induces a positive linear functional L on $C(\Omega)$ by $L(\Phi(f)) = \lambda(f)$. Applying the Riesz Representation theorem we have a measure μ on the Borel sets of Ω such that

$$\lambda(f) = L(\Phi(f)) = \int_\Omega \Phi(f) \, d\mu \quad \text{for all } f \in B(X).$$

The action $(\tau_g)_{g \in G}$ induces an anti-action (or right action) $(U_g)_{g \in G}$ on $C(\Omega)$ by $U_g \Phi(f) = \Phi(f_g)$, where $f_g(x) = f(\tau_g x)$ for all $g \in G$, $f \in Y$ and $x \in X$. It is not hard to see that, for each $g \in G$, U_g is a positive invertible isometry of $C(\Omega)$. By the Banach–Stone theorem [19], for each $g \in G$, there is a homeomorphism $T_g : \Omega \to \Omega$ such that $U_g \phi = \phi \circ T_g$ for all $\phi \in C(\Omega)$. Moreover, for all $g, h \in G$ we have $\phi \circ T_{gh} = U_{gh}\phi = U_h U_g \phi = U_h(\phi \circ T_g) = \phi \circ (T_g \circ T_h)$. This means that $(T_g)_{g \in G}$ is an action of G on Ω. For every $f \in Y$, we have $\lambda(f_g) = \lambda(f)$ and hence

$$\int_\Omega \Phi(f) \circ T_g \, d\mu = \int_\Omega U_g \Phi(f) \, d\mu = \int_\Omega \Phi(f_g) \, d\mu$$

$$= \lambda(f_g) = \lambda(f) = \int_\Omega \Phi(f) \, d\mu.$$

Therefore the action (T_g) preserves measure μ.

Note that the only idempotents of the algebra $C(\Omega)$ are indicator functions of sets. Therefore, given any set $S \in \mathcal{S}$, the Gelfand transform $\Phi(1_S)$ of the characteristic function 1_S of S is the characteristic function of some Borel subset (which we denote by $\Phi(S)$) in Ω. In other words, $\Phi(S)$ is such that $\Phi(1_S) = 1_{\Phi(S)}$. Let $B = \Phi(E)$. We have

$$\bar{d}_{(G_N)}(E) = \lambda(1_E) = \int_\Omega \Phi(1_E) \, d\mu = \int_\Omega 1_B \, d\mu = \mu(B).$$

Since the indicator function of the intersection of two sets is the product of the indicator functions, we conclude that for any $k \in \mathbb{N}$ and any $g_1, \ldots, g_k \in G$ we have

$$\bar{d}_{(G_N)}\left(\bigcap_{i=1}^k \tau_{g_i} E\right) \geq \lambda\left(\prod_{i=1}^k 1_{\tau_{g_i} E}\right) = \int_\Omega \Phi\left(\prod_{i=1}^k 1_{\tau_{g_i} E}\right) d\mu$$

$$= \int_\Omega \prod_{i=1}^k \Phi(1_{\tau_{g_i} E}) \, d\mu = \int_\Omega \prod_{i=1}^k U_{g_i^{-1}} \Phi(1_E) \, d\mu$$

$$= \int_\Omega \prod_{i=1}^k 1_B \circ T_{g_i^{-1}} \, d\mu = \int_\Omega \prod_{i=1}^k 1_{T_{g_i} B} \, d\mu = \mu\left(\bigcap_{i=1}^k T_{g_i} B\right). \quad \square$$

2.9. *Deriving Theorem 2.5 from ergodic results.* In this subsection we state the main ergodic results of the paper and use them to derive Theorem 2.5. The proof of the ergodic results will be given in §3. We begin by recalling Theorem 1.4 stated in the introduction.

THEOREM 2.10. (Cf. Theorem 1.4 in the Introduction) *Let $(\Omega, \mathcal{B}, \mu)$ be a probability space and suppose that $\mathcal{A}_K$ acts on Ω by measure preserving transformations. Let (F_N)*

be a double Følner sequence on K. Then for each $B \in \mathcal{B}$ we have†

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u}B \cap M_{1/u}B) \geq \mu(B)^2$$

and, in particular, the limit exists.

In the case when the action of $\mathcal{A}_K$ is ergodic, we can replace one of the sets B with another set C. This is the content of the next theorem.

THEOREM 2.11. *Let $(\Omega, \mathcal{B}, \mu)$ be a probability space and suppose that $\mathcal{A}_K$ acts ergodically on Ω by measure preserving transformations. Let (F_N) be a double Følner sequence on K. Then for any $B, C \in \mathcal{B}$ we have*

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u}B \cap M_{1/u}C) = \mu(B)\mu(C)$$

and, in particular, the limit exists.

Remark 2.12. We note that Theorem 2.11 fails without ergodicity. Indeed, take the normalized disjoint union of two copies of the same measure preserving system. Choosing B to be one of the copies and C the other we get

$$A_{-u}B \cap M_{1/u}C = \emptyset \quad \text{for all } u \in K^*.$$

We can extract some quantitative bounds from Theorems 2.10 and 2.11. This is summarized in the next corollary.

COROLLARY 2.13. *Let $(\Omega, \mathcal{B}, \mu)$ be a probability space and suppose that $\mathcal{A}_K$ acts on Ω by measure preserving transformations. Let (F_N) be a double Følner sequence on K, let $B \in \mathcal{B}$ and let $\epsilon > 0$. Then we have*

$$\underline{d}_{(F_N)}(\{u \in K^* : \mu(A_{-u}B \cap M_{1/u}B) > \mu(B)^2 - \epsilon\}) \geq \frac{\epsilon}{\epsilon + \mu(B) - \mu(B)^2}.$$

Moreover, if the action of $\mathcal{A}_K$ is ergodic and $B, C \in \mathcal{B}$, the set

$$D_\epsilon := \{u \in K^* : \mu(A_{-u}B \cap M_{1/u}C) > \mu(B)\mu(C) - \epsilon\}$$

satisfies

$$\underline{d}_{(F_N)}(D_\epsilon) \geq \max\left(\frac{\epsilon}{\epsilon + \mu(B)(1 - \mu(C))}, \frac{\epsilon}{\epsilon + \mu(C)(1 - \mu(B))}\right). \tag{4}$$

Corollary 2.13 will be proved in §3. We will use it now, together with the correspondence principle, to deduce Theorem 2.5.

Proof of Theorem 2.5. Let $X = K$, let $G = \mathcal{A}_K$ and let $(G_N) = (F_N)$. Applying the correspondence principle (Theorem 2.8), we obtain, for each $E \subset K$, a measure preserving action $(T_g)_{g \in \mathcal{A}_K}$ of $\mathcal{A}_K$ on a probability space $(\Omega, \mathcal{B}, \mu)$, a set $B \in \mathcal{B}$ such that $\mu(B) = \bar{d}_{(F_N)}(E)$, and, for all $u \in K^*$, we have $\bar{d}_{(F_N)}(A_{-u}E \cap M_{1/u}E) \geq \mu(T_{A_{-u}}B \cap T_{M_{1/u}}B)$.

---

† By slight abuse of language we use the same symbol to denote the elements (such as $M_{1/u}$ and A_{-u}) of $\mathcal{A}_K$ and the measure preserving transformation they induce on Ω.

To simplify notation we will denote the measure preserving transformations $T_{A_{-u}}$ and $T_{M_{1/u}}$ on Ω by just A_{-u} and $M_{1/u}$. Also, recalling that $A_{-u}E = E - u$ and $M_{1/u}E = E/u$ we can rewrite the previous equation as

$$\bar{d}_{(F_N)}(E - u \cap E/u) \geq \mu(A_{-u}B \cap M_{1/u}B) \quad \text{for all } u \in K^*.$$

Now assume that $\bar{d}_{(F_N)}(E) > 0$ and let $\epsilon > 0$. Let

$$D_\epsilon := \{u \in K^* : \bar{d}_{(F_N)}((E - u) \cap (E/u)) > \bar{d}_{(F_N)}(E)^2 - \epsilon\}.$$

By Corollary 2.13 we have

$$\underline{d}_{(F_N)}(D_\epsilon) \geq \underline{d}_{(F_N)}(\{u \in K^* : \mu(A_{-u}B \cap M_{1/u}B) > \mu(B)^2 - \epsilon\})$$
$$\geq \frac{\epsilon}{\epsilon + \mu(B) - \mu(B)^2}$$
$$= \frac{\epsilon}{\epsilon + \bar{d}_{(F_N)}(E) - \bar{d}_{(F_N)}(E)^2}. \qquad \square$$

2.14. *Some classical results.* We will need to use two results that are already in the literature. The first is a version of the classical van der Corput trick for unitary representations of countable abelian groups. For a proof see [**9**, Lemma 2.9].

PROPOSITION 2.15. *Let H be an Hilbert space and let $(a_u)_{u \in K^*}$ be a bounded sequence in H, indexed by K^*. If, for all b in a co-finite subset of K^*, we have*

$$\limsup_{N \to \infty} \left| \frac{1}{|F_N|} \sum_{u \in F_N} \langle a_{bu}, a_u \rangle \right| = 0,$$

then also

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} a_u = 0.$$

Another result we will need is von Neumann's mean ergodic theorem. See, for instance [**6**, Theorem 5.5] for a proof of this version.

THEOREM 2.16. *Let G be a countable abelian group and let (F_N) be a Følner sequence in G. Let H be a Hilbert space and let $(U_g)_{g \in G}$ be a unitary representation of G on H. Let P be the orthogonal projection onto the subspace of vectors fixed under G. Then*

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{g \in F_N} U_g f = Pf \quad \text{for all } f \in H$$

in the strong topology of H.

3. *Proof of the main theorem*

In this section we will prove Theorems 2.10 and 2.11 and Corollary 2.13. Throughout this section let K be a countable field, let $(\Omega, \mathcal{B}, \mu)$ be a probability space, let $(T_g)_{g \in \mathcal{A}_K}$ be a measure preserving action of $\mathcal{A}_K$ on Ω and let (F_N) be a double Følner sequence on K.

Let $H = L^2(\Omega, \mu)$ and let $(U_g)_{g \in \mathcal{A}_K}$ be the unitary Koopman representation of $\mathcal{A}_K$ (this means that $(U_g f)(x) = f(g^{-1}x)$). By a slight abuse of notation we will write $A_u f$ instead of $U_{A_u} f$ and $M_u f$ instead of $U_{M_u} f$.

Let P_A be the orthogonal projection from H onto the subspace of vectors which are fixed under the action of the additive subgroup S_A and let P_M be the orthogonal projection from H onto the subspace of vectors which are fixed under the action of the multiplicative subgroup S_M.

We will show that the orthogonal projections P_A and P_M commute, which is surprising considering that the subgroups S_A and S_M do not. The reason for this is that, for each $k \in K^*$, the map $M_k : K \to K$ is an isomorphism of the additive group.

LEMMA 3.1. *For any $f \in H$ we have*

$$P_A P_M f = P_M P_A f.$$

Proof. First, we prove that, for any $k \in K^*$, the projection P_A commutes with M_k. For this, we will use Theorem 2.16, Lemma 2.6 and equation (2). We have

$$M_k P_A f = M_k \left(\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} A_u f \right) = \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_k A_u f$$

$$= \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} A_{ku} M_k f = \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in k F_N} A_u M_k f = P_A M_k f.$$

Now we can conclude the result. It follows that

$$P_M P_A f = \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_u P_A f = P_A \left(\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_u f \right) = P_A P_M f. \quad \square$$

Lemma 3.1 implies that $P_M P_A f$ is invariant under both S_A and S_M. Since those two subgroups generate $\mathcal{A}_K$, this means that $P_M P_A$ is the orthogonal projection onto the space of functions invariant under $\mathcal{A}_K$.

Let $P : H \to H$ be the orthogonal projection onto the space of functions invariant under the action of the group $\mathcal{A}_K$. We have $P = P_A P_M = P_M P_A$.

The bulk of the proofs of Theorems 2.10 and 2.11 comes from the next lemma.

LEMMA 3.2. *Let $f \in H = L^2(\Omega, \mu)$. We have*

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_u A_{-u} f = Pf.$$

In particular, the limit exists.

Proof. First, we assume that $P_A f = 0$. For $u \in K^*$, let $a_u = M_u A_{-u} f$. Then, for each $b \in K^*$ we have

$$\langle a_{ub}, a_u \rangle = \langle M_{ub} A_{-ub} f, M_u A_{-u} f \rangle$$
$$= \langle M_b A_{-ub} f, A_{-u} f \rangle$$
$$= \langle A_{-ub} f, M_{1/b} A_{-u} f \rangle$$
$$= \langle A_{-ub} f, A_{-u/b} M_{1/b} f \rangle$$
$$= \langle A_{-u(b-1/b)} f, M_{1/b} f \rangle,$$

where we used equation (2) and the fact that the operators are unitary. Now, if $b \neq \pm 1$, then $b - 1/b = (b^2 - 1)/b \neq 0$ and so the sequence of sets $(-((b^2 - 1)/b)F_N)_N$ is again a double Følner sequence on K, by Lemma 2.6. Thus, applying Theorem 2.16 we get (keeping $b \neq \pm 1$ fixed)

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \langle a_{ub}, a_u \rangle = \left\langle \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} A_{-u(b-1/b)} f, M_{1/b} f \right\rangle$$

$$= \left\langle \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in -((b^2-1)/b)F_N} A_u f, M_{1/b} f \right\rangle$$

$$= \langle P_A f, M_{1/b} f \rangle = 0.$$

Thus, it follows from Proposition 2.15 that

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_u A_{-u} f = 0.$$

Now, for a general $f \in H$, we can write $f = f_1 + f_2$, where $f_1 = P_A f$ and $f_2 = f - P_A f$ satisfies $P_A f_2 = 0$. Note that f_1 is invariant under A_u. Therefore

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_u A_{-u} f = \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_u A_{-u} f_1$$

$$= \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} M_u f_1$$

$$= P_M f_1 = P_M P_A f = P f. \qquad \square$$

Remark 3.3. Lemma 3.2 can be interpreted as an ergodic theorem along a sparse subset of $\mathcal{A}_K$ (namely the subset $\{M_u A_{-u} : u \in K^*\}$).

Proof of Theorem 2.10. Let $B \in \mathcal{B}$. By Lemma 3.2 applied to the characteristic function 1_B of B we get that

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u} B \cap M_{1/u} B) = \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \int_\Omega A_{-u} 1_B M_{1/u} 1_B \, d\mu$$

$$= \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \int_\Omega (M_u A_{-u} 1_B) 1_B \, d\mu$$

$$= \int_\Omega (P 1_B) 1_B \, d\mu.$$

We can use the Cauchy–Schwartz inequality with the functions $P 1_B$ and the constant function 1, and the trivial observation that $P 1 = 1$, to get

$$\int_\Omega (P 1_B) 1_B \, d\mu = \|P 1_B\|^2 \geq \langle P 1_B, 1 \rangle^2 = \langle 1_B, P 1 \rangle^2 = \langle 1_B, 1 \rangle^2 = \mu(B)^2.$$

Putting everything together we obtain

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u} B \cap M_{1/u} B) \geq \mu(B)^2. \qquad \square$$

Proof of Theorem 2.11. Let $B, C \in \mathcal{B}$. By Lemma 3.2 applied to the characteristic function 1_B of B we get that

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u}B \cap M_{1/u}C) = \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \int_\Omega A_{-u}1_B M_{1/u}1_C \, d\mu$$

$$= \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \int_\Omega (M_u A_{-u}1_B)1_C \, d\mu$$

$$= \int_\Omega (P1_B)1_C \, d\mu.$$

Since the action of $\mathcal{A}_K$ is ergodic, $P1_B = \mu(B)$ and hence

$$\lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u}B \cap M_{1/u}C) = \mu(B) \int_\Omega 1_C \, d\mu = \mu(B)\mu(C). \qquad \square$$

Proof of Corollary 2.13. Let $B, C \subset \mathcal{B}$. Note that trivially $\mu(A_{-u}B \cap M_{1/u}B) \le \mu(M_{1/u}B) = \mu(B)$. For each $\epsilon > 0$, let D_ϵ be the set $D_\epsilon := \{u \in K : \mu(A_{-u}B \cap M_{1/u}B) > \mu(B)^2 - \epsilon\}$.

Now let $(\tilde{F}_N)_{N \in \mathbb{N}}$ be a subsequence of $(F_N)_{N \in \mathbb{N}}$ such that

$$\underline{d}_{(F_N)}(D_\epsilon) = \lim_{N \to \infty} \frac{|D_\epsilon \cap \tilde{F}_N|}{|\tilde{F}_N|}.$$

Thus, $\underline{d}_{(F_N)}(D_\epsilon) = \underline{d}_{(\tilde{F}_N)}(D_\epsilon) = \bar{d}_{(\tilde{F}_N)}(D_\epsilon)$. By Theorem 2.10, we now have

$$\mu(B)^2 = \lim_{N \to \infty} \frac{1}{|F_N|} \sum_{u \in F_N} \mu(A_{-u}B \cap M_{1/u}B)$$

$$= \lim_{N \to \infty} \frac{1}{|\tilde{F}_N|} \sum_{u \in \tilde{F}_N} \mu(A_{-u}B \cap M_{1/u}B)$$

$$= \lim_{N \to \infty} \frac{1}{|\tilde{F}_N|} \left(\sum_{u \in \tilde{F}_N \cap D_\epsilon} \mu(A_{-u}B \cap M_{1/u}B) + \sum_{u \in \tilde{F}_N \setminus D_\epsilon} \mu(A_{-u}B \cap M_{1/u}B) \right)$$

$$\le \mu(B)\bar{d}_{(\tilde{F}_N)}(D_\epsilon) + (\mu(B)^2 - \epsilon)(1 - \underline{d}_{(\tilde{F}_N)}(D_\epsilon))$$

$$= \mu(B)\underline{d}_{(F_N)}(D_\epsilon) + (\mu(B)^2 - \epsilon)(1 - \underline{d}_{(F_N)}(D_\epsilon)).$$

From this we conclude that $\underline{d}_{(F_N)}(D_\epsilon) \ge \epsilon/(\epsilon + \mu(B)(1 - \mu(B)))$.

Now assume that the action of $\mathcal{A}_K$ is ergodic. Note that trivially $\mu(A_{-u}B \cap M_{1/u}C) \le \mu(M_{1/u}C) = \mu(C)$. For each $\epsilon > 0$ let D_ϵ be the set $D_\epsilon := \{u \in K : \mu(A_{-u}B \cap M_{1/u}C) > \mu(B)\mu(C) - \epsilon\}$.

Now let $(\tilde{F}_N)_{N \in \mathbb{N}}$ be a subsequence of $(F_N)_{N \in \mathbb{N}}$ such that

$$\underline{d}_{(F_N)}(D_\epsilon) = \lim_{N \to \infty} \frac{|D_\epsilon \cap \tilde{F}_N|}{|\tilde{F}_N|}.$$

Thus, $\underline{d}_{(F_N)}(D_\epsilon) = \underline{d}_{(\tilde{F}_N)}(D_\epsilon) = \bar{d}_{(\tilde{F}_N)}(D_\epsilon)$. By Theorem 2.11, we now have

$$\mu(B)\mu(C) = \lim_{N\to\infty} \frac{1}{|F_N|} \sum_{u\in F_N} \mu(A_{-u}B \cap M_{1/u}C)$$

$$= \lim_{N\to\infty} \frac{1}{|\tilde{F}_N|} \sum_{u\in\tilde{F}_N} \mu(A_{-u}B \cap M_{1/u}C)$$

$$= \lim_{N\to\infty} \frac{1}{|\tilde{F}_N|} \left(\sum_{u\in\tilde{F}_N\cap D_\epsilon} \mu(A_{-u}B \cap M_{1/u}C) + \sum_{u\in\tilde{F}_N\setminus D_\epsilon} \mu(A_{-u}B \cap M_{1/u}C) \right)$$

$$\leq \mu(C)\bar{d}_{(\tilde{F}_N)}(D_\epsilon) + (\mu(B)\mu(C) - \epsilon)(1 - \underline{d}_{(\tilde{F}_N)}(D_\epsilon))$$

$$= \mu(C)\underline{d}_{(F_N)}(D_\epsilon) + (\mu(B)\mu(C) - \epsilon)(1 - \underline{d}_{(F_N)}(D_\epsilon)).$$

From this we conclude that $\underline{d}_{(F_N)}(D_\epsilon) \geq \epsilon/(\epsilon + \mu(C)(1 - \mu(B)))$. Switching the roles of B and C we obtain equation (4). □

Remark 3.4. Note that the lower bound on $\underline{d}_{(F_N)}(D_\epsilon)$ does not depend on the set B, only on the measure $\mu(B)$. Moreover, it does not depend on the double Følner sequence (F_N).

4. *Proof of Theorem 1.2*

In this section we give a proof of Theorem 1.2. We start by giving a more precise statement.

THEOREM 4.1. *For any finite coloring $K = \bigcup C_i$ there exists a color C_i, a subset $D \subset K$ satisfying $\bar{d}_{(F_N)}(D) > 0$ and, for each $u \in D$, there is a set $D_u \subset K$ also satisfying $\bar{d}_{(F_N)}(D_u) > 0$ such that, for any $v \in D_u$, we have $\{u, u + v, uv\} \subset C_i$.*

Definition 4.2. Let G be a group. A set $R \subset G$ is a *set of recurrence* if, for all probability preserving actions $(\Omega, \mu, (T_g)_{g\in G})$ and every measurable set $B \subset \Omega$ with positive measure, there exists some non-identity, $g \in R$, such that $\mu(B \cap T_g B) > 0$.

The proof of Theorem 4.1 uses the fact that sets of recurrence are partition regular. For other similar applications of this phenomenon see for instance [3], the discussion before [4, Question 11] and [10, Theorem 0.4].

The following lemma is well known; we include the proof for the convenience of the reader.

LEMMA 4.3. *Let G be a group and let $R \subset G$ be a set of recurrence. Then for every finite partition $R = R_1 \cup \cdots \cup R_r$, one of the sets R_i is also a set of recurrence.*

Proof. The proof goes by contradiction. Assume that none of the sets $R_1, \ldots, R_r$ is a set of recurrence. Then, for each $i = 1, \ldots, r$, there is some probability preserving action $(\Omega_i, \mu_i, (T_g)_{g\in G}^{(i)})$ and a set $B_i \subset \Omega_i$ with $\mu_i(B_i) > 0$, such that $\mu_i(B_i \cap T_g^{(i)}B_i) = 0$ for all $g \in R_i$.

Let $\Omega = \Omega_1 \times \cdots \times \Omega_r$, let $\mu = \mu_1 \otimes \cdots \otimes \mu_r$, let $B = B_1 \times \cdots \times B_r$ and, for each $g \in G$, let $T_g(\omega_1, \ldots, \omega_r) = (T_g^{(1)}\omega_1, \ldots, T_g^{(r)}\omega_r)$. Then $(T_g)_{g\in G}$ is a probability preserving action of G on Ω and $\mu(B) = \mu_1(B_1) \cdots \mu_r(B_r) > 0$.

Since R is a set of recurrence, there exists some $g \in R$ such that $\mu(B \cap T_g B) > 0$. Since $\mu(B \cap T_g B) = \prod_{i=1}^{r} \mu_i(B_i \cap T_g B_i)$, we conclude that $\mu_i(B_i \cap T_g B_i) > 0$ for all

$i = 1, \ldots, r$. But this implies that $g \notin R_i$ for all $i = 1, \ldots, r$, which contradicts the fact that $g \in R = R_1 \cup \cdots \cup R_r$. □

Proof of Theorem 4.1. Let $K = C_1 \cup C_2 \cup \cdots \cup C_{r'}$ be a finite partition of K. Assume without loss of generality that, for some $r \leq r'$, the upper density $\bar{d}_{(F_N)}(C_i)$ is positive for $i = 1, \ldots, r$ and $\bar{d}_{(F_N)}(C_i) = 0$ for $i = r + 1, \ldots, r'$.

For a set $C \subset K$ and each $u \in C$, define the set $D_u(C) = (C - u) \cap (C/u)$. Let $D(C) = \{u \in C : \bar{d}_{(F_N)}(D_u(C)) > 0\}$. We want to show that, for some $i = 1, \ldots, r$, we have $\bar{d}_{(F_N)}(D(C_i)) > 0$.

If, for some $1 \leq i \leq r$, we have $\bar{d}_{(F_N)}(D(C_i)) = 0$ but $D(C_i) \neq \emptyset$, we can consider the more refined coloring obtained by distinguishing between $D(C_i)$ and $C_i \setminus D(C_i)$. Since

$$D(C_i \setminus D(C_i)) \subset (C_i \setminus D(C_i)) \cap D(C_i)$$

we conclude that $D(C_i \setminus D(C_i)) = \emptyset$. Thus, without loss of generality, we can assume that either $D(C_i) = \emptyset$ or $\bar{d}_{(F_N)}(D(C_i)) > 0$. Therefore, it suffices to show that for some $i = 1, \ldots, r$ we have $D(C_i) \neq \emptyset$.

For each $i = 1, \ldots, r$, let $R_i = \{M_u A_{-u} : u \in C_i\} \subset \mathcal{A}_K$ and let $R = R_1 \cup \cdots \cup R_r$. We claim that R is a set of recurrence. Indeed, given any probability preserving action $(\Omega, \mu, (T_g)_{g \in \mathcal{A}_K})$ of $\mathcal{A}_K$ and any measurable set $B \subset \Omega$ with positive measure, by Theorem 2.10, we find that the set $\{u \in K^* : \mu(A_{-u}B \cap M_{1/u}B) > 0\}$ has positive upper density. In particular, for some $u \in C_1 \cup \cdots \cup C_r$, we have that $\mu(M_u A_{-u}B \cap B) = \mu(A_{-u}B \cap M_{1/u}B) > 0$. Since $M_u A_{-u} \in R$, we conclude that R is a set of recurrence.

By Lemma 4.3, we conclude that for some $i = 1, \ldots, r$ the set R_i is a set of recurrence. We claim that $D(C_i) \neq \emptyset$.

To see this, apply the correspondence principle (Theorem 2.8), with $X = K$, $G = \mathcal{A}_K$, $G_N = F_N$ and $E = C_i$, to find a probability preserving action $(T_g)_{g \in \mathcal{A}_K}$ of $\mathcal{A}_K$ on some probability space (Ω, μ) and a measurable set $B \subset \Omega$ satisfying $\mu(B) = \bar{d}_{(F_N)}(C_i)$ and

$$\bar{d}_{(F_N)}(A_{-u}C_i \cap M_{1/u}C_i) \geq \mu(T_{A_{-u}}B \cap T_{M_{1/u}}B)$$

for all $u \in K^*$. Since R_i is a set of recurrence, there is some $u \in C_i$ such that

$$0 < \mu(T_{M_u A_{-u}}B \cap B) = \mu(T_{A_{-u}}B \cap T_{M_{1/u}}B)$$
$$\leq \bar{d}_{(F_N)}(A_{-u}C_i \cap M_{1/u}C_i) = \bar{d}_{(F_N)}(D_u(C_i)).$$

We conclude that $u \in D(C_i)$ and hence $\bar{d}_{(F_N)}(D^i) > 0$.

Let $D = D(C_i) \subset C_i$ and for each $u \in D$ let $D_u = D_u(C_i)$. Now, let $v \in D_u$. Then we have $u + v \in C_i$ and $uv \in C_i$. We conclude that $\{u, u + v, uv\} \subset C_i$ as desired. □

5. *Finite fields*

The main result of this section is an analogue of Theorem 2.10 for finite fields.

For a finite field F, let $F^* = F \setminus \{0\}$ be the multiplicative subgroup. The group of affine transformations, which we denote by $\mathcal{A}_F$, is the group of maps of the form $x \mapsto ux + v$, where $u \in F^*$ and $v \in F$. Again, we will use the notation $A_u \in \mathcal{A}_F$ to denote the map $x \mapsto x + u$ and $M_u \in \mathcal{A}_F$ to denote the map $x \mapsto ux$, and we will use the subgroups S_A and S_M as defined in Definition 2.2. The next result is an analogue of Theorem 2.10 for finite fields.

THEOREM 5.1. *Let F be a finite field and assume that the affine group $\mathcal{A}_F$ acts by measure preserving transformations on a probability space $(\Omega, \mathcal{B}, \mu)$. Then for each $B \in \mathcal{B}$ such that $\mu(B) > \sqrt{6/|F|}$, there exists $u \in F^*$ such that $\mu(B \cap M_u A_{-u} B) > 0$.*

Moreover, if the action of $\mathcal{A}_F$ on Ω is ergodic (this is the case, for instance, when $\Omega = F$) and if $B, C \in \mathcal{B}$ are such that $\mu(B)\mu(C) > 6/|F^*|$, then there exists $u \in F^*$ such that $\mu(B \cap M_u A_{-u} C) > 0$.

For an estimation of how many $u \in F^*$ satisfy Theorem 5.1, see Corollary 5.2 below. The proof of Theorem 5.1, is a 'finitization' of the proof of Theorem 2.10.

Proof. Let $H = L^2(\Omega, \mu)$. We consider the Koopman representation $(U_g)_{g \in \mathcal{A}_F}$ of $\mathcal{A}_F$ on H by defining $(U_g f)(x) = f(g^{-1}x)$. By an abuse of notation, we will denote $U_{A_u} f$ by just $A_u f$ and $U_{M_u} f$ by just $M_u f$. Let P_A be the orthogonal projection onto the space of all functions invariant under the additive subgroup S_A, so that $P_A f(x) = (1/|F|) \sum_{u \in F} A_u f$, and let P_M be the orthogonal projection onto the space of all functions invariant under the multiplicative subgroup S_M, so that $P_M f(x) = (1/|F^*|) \sum_{u \in F^*} M_u f$. We claim that $P_M P_A f = P_A P_M f$, in analogy with Lemma 3.1. Indeed, by equation (2) we have

$$P_M P_A f = \frac{1}{|F^*|} \sum_{u \in F^*} \frac{1}{|F|} \sum_{v \in F} M_u A_v f = \frac{1}{|F| |F^*|} \sum_{u \in F^*} \sum_{v \in F} A_{uv} M_u f.$$

Since, for each $u \in F^*$, we have $\{uv : v \in F\} = F$, we conclude that

$$P_M P_A f = \frac{1}{|F| |F^*|} \sum_{u \in F^*} \sum_{v \in F} A_v M_u f = P_A P_M f,$$

proving the claim. Let $B, C \in \mathcal{B}$ be such that $\mu(B)\mu(C) > 6/|F^*|$ and let $f = 1_C - P_A 1_C$. Note that $P_A f = 0$ and $A_u P_A 1_C = P_A 1_C$. Since we are in a finite setting now, we will need to bound error terms that are not 0 (but asymptotically go to 0 as $|F|$ increases to ∞). For that, we will need an estimation on the norm of f.

We have, for every $u \in F^*$, that $|A_u 1_C - 1_C|$ is the indicator function of a set with measure no larger than $2\mu(C)$. Hence, $\|1_C - A_u 1_C\| \leq \sqrt{2\mu(C)}$. Therefore

$$\|f\| = \left\| \frac{1}{|F|} \sum_{u \in F} 1_C - A_u 1_C \right\| \leq \frac{1}{|F|} \sum_{u \in F} \|1_C - A_u 1_C\| \leq \sqrt{2\mu(C)}.$$

We need to estimate the sum of the measures of the intersections $B \cap M_u A_{-u} C$ with u running over all possible values in F^*. We have that

$$\sum_{u \in F^*} \mu(B \cap M_u A_{-u} C) = \sum_{u \in F^*} \langle 1_B, M_u A_{-u} P_A 1_C \rangle + \sum_{u \in F^*} \langle 1_B, M_u A_{-u} f \rangle. \quad (5)$$

Also, by the Cauchy–Schwartz inequality we have that

$$\left| \sum_{u \in F^*} \langle 1_B, M_u A_{-u} f \rangle \right| = \left| \left\langle 1_B, \sum_{u \in F^*} M_u A_{-u} f \right\rangle \right| \leq \sqrt{\mu(B)} \left\| \sum_{u \in F^*} M_u A_{-u} f \right\|. \quad (6)$$

Using linearity of the inner product, the fact that the operators A_u and M_u are unitary, equation (2) and the fact that F^* is a multiplicative group (so that we can change the

variables in the sums while still adding over the whole group) we get

$$\left\| \sum_{u \in F^*} M_u A_{-u} f \right\|^2 = \sum_{u,d \in F^*} \langle M_u A_{-u} f, M_d A_{-d} f \rangle$$

$$= \sum_{u,d \in F^*} \langle A_{d^2/u-u} f, M_{d/u} f \rangle$$

$$= \sum_{u,d \in F^*} \langle A_{u(d^2-1)} f, M_d f \rangle.$$

Now we separate the sum when $d = \pm 1$ and note that when $d \neq \pm 1$ we have

$$\sum_{u \in F^*} \langle A_{u(d^2-1)} f, M_d f \rangle = \langle |F| P_A f - f, M_d f \rangle = -\langle f, M_d f \rangle.$$

So putting this together we obtain

$$\left\| \sum_{u \in F^*} M_u A_{-u} f \right\|^2 = |F^*|(\langle f, M_1 f + M_{-1} f \rangle) - \sum_{d \neq \pm 1} \langle f, M_d f \rangle.$$

Applying the Cauchy–Schwartz inequality again and using the bound $\|f\| \leq \sqrt{2\mu(C)}$, we get the estimate

$$\left\| \sum_{u \in F^*} M_u A_{-u} f \right\|^2 \leq 3|F^*|\|f\|^2 \leq 6|F^*|\mu(C). \tag{7}$$

Combining this with (5) and (6) we have

$$\sum_{u \in F^*} \mu(B \cap M_u A_{-u} C) \geq \sum_{u \in F^*} \langle 1_B, M_u P_A 1_C \rangle - \sqrt{6|F^*|\mu(B)\mu(C)}.$$

Normalizing we conclude that

$$\frac{1}{|F^*|} \sum_{u \in F^*} \mu(B \cap M_u A_{-u} C) \geq \langle 1_B, P_M P_A 1_C \rangle - \sqrt{\frac{6\mu(B)\mu(C)}{|F^*|}}. \tag{8}$$

Note that $P_M P_A 1_C = P_A P_M 1_C$ is a function invariant under $\mathcal{A}_F$. Thus, if the action of $\mathcal{A}_F$ is ergodic then $P_M P_A 1_C = \mu(C)$. Therefore, the right hand side of the previous inequality is $\mu(B)\mu(C) - \sqrt{6\mu(B)\mu(C)/|F^*|}$, so when $\mu(B)\mu(C) > 6/|F^*|$ it is positive and hence for some $n \in F^*$ we have $\mu(B \cap M_u A_{-u} C) > 0$.

When $C = B$, and without assuming ergodicity, we have that $P_M P_A 1_B = P_A P_M 1_B$ is the projection of 1_B onto the subspace of invariant functions under the action of $\mathcal{A}_F$. Therefore

$$\langle 1_B, P_M P_A 1_B \rangle = \|P_M P_A 1_B\|^2 \geq \langle P_M P_A 1_B, 1 \rangle^2 = \langle 1_B, 1 \rangle^2 = \mu(B)^2. \tag{9}$$

So, if $\mu(B) > \sqrt{6/|F^*|}$, the average above is positive and hence $\mu(B \cap M_u A_{-u} B) > 0$ for some $u \in F^*$. $\square$

As a Corollary of the proof we get the following estimates.

COROLLARY 5.2. *Let F be a finite field and assume that the affine group $\mathcal{A}_F$ acts by measure preserving transformations on a probability space $(\Omega, \mathcal{B}, \mu)$. Then for each $B \in \mathcal{B}$ and for each $\delta < \mu(B)$, the set $D := \{u \in F^* : \mu(B \cap M_u A_{-u} B) > \delta\}$ satisfies*

$$\frac{|D|}{|F^*|} \geq \frac{\mu(B)^2 - \mu(B)\sqrt{6/|F^*|} - \delta}{\mu(B) - \delta}.$$

Moreover, if the action of $\mathcal{A}_F$ on Ω is ergodic, then for all $B, C \in \mathcal{B}$ and for each $\delta < \min\{\mu(B), \mu(C)\}$, the set $D := \{u \in F^* : \mu(B \cap M_u A_{-u} C) > \delta\}$ satisfies

$$\frac{|D|}{|F^*|} \geq \frac{\mu(B)\mu(C) - \sqrt{6\mu(B)\mu(C)/|F^*|} - \delta}{\min(\mu(B), \mu(C)) - \delta}.$$

Proof. Let $B \in \mathcal{B}$ and let $\delta < \mu(B)$. Let $D := \{u \in F^* : \mu(B \cap M_u A_{-u} B) > \delta\}$. From equations (8) and (9) we have

$$\frac{1}{|F^*|} \sum_{u \in F^*} \mu(B \cap M_u A_{-u} B) \geq \mu(B)^2 - \mu(B)\sqrt{\frac{6}{|F^*|}}.$$

On the other hand, since $\mu(B \cap M_u A_{-u} B) \leq \mu(B)$ we have

$$\frac{1}{|F^*|} \sum_{u \in F^*} \mu(B \cap M_u A_{-u} B) \leq \frac{|D|}{|F^*|}\mu(B) + \left(1 - \frac{|D|}{|F^*|}\right)\delta = \delta + \frac{|D|}{|F^*|}(\mu(B) - \delta).$$

Putting both together, we obtain the conclusion of Corollary 5.2. The case when the action is ergodic follows similarly, using equation (8) and the fact that $P1_C = \mu(C)$ is a constant function. $\qquad\square$

An application of Theorem 5.1 is the following finitistic analogue of Theorem 2.5.

THEOREM 5.3. *For any finite field F and any subsets $E_1, E_2 \subset F$ with $|E_1|\,|E_2| > 6|F|$, there exist $u, v \in F$, $v \neq 0$, such that $u + v \in E_1$ and $uv \in E_2$.*
More precisely, for each $s < \min(|E_1|, |E_2|)$ there is a set $D \subset F^*$ with cardinality

$$|D| \geq \frac{|E_1|\,|E_2|\,|F^*|/|F| - \sqrt{6|E_1|\,|E_2|\,|F^*|} - s|F^*|}{\min(|E_1|, |E_2|) - s}$$

such that for each $u \in D$ there are s choices of $v \in F$ such that $u + v \in E_1$ and $uv \in E_2$.

Since the action of $\mathcal{A}_F$ on F is always ergodic, we get a slightly stronger result than Theorem 2.5, in that we have two sets E_1 and E_2. Unfortunately, we were unable to apply the methods of §4 used to derive Theorem 1.2 from Theorem 2.10 in the finitistic situation.

Proof of Theorem 5.3. Let $\Omega = F$, let μ be the normalized counting measure on F and let $\mathcal{A}_F$ act on F by affine transformations. Note that this action is ergodic. Let $\delta = s/|F|$ and let $D = \{u \in F^* : \mu(E_2 \cap M_u A_{-u} E_1) > \delta\}$. By Corollary 5.2 we have that

$$\frac{|D|}{|F^*|} \geq \frac{\mu(E_1)\mu(E_2) - \sqrt{6\mu(E_1)\mu(E_2)/|F^*|} - \delta}{\min(\mu(E_1), \mu(E_2)) - \delta}$$

$$= \frac{|E_1|\,|E_2|/|F| - \sqrt{6|E_1|\,|E_2|/|F^*|} - s}{\min(|E_1|, |E_2|) - s}$$

and hence
$$|D| \geq \frac{|E_1|\,|E_2|\,|F^*|/|F| - \sqrt{6|E_1|\,|E_2|\,|F^*|} - s|F^*|}{\min(|E_1|, |E_2|) - s}.$$

For each $u \in D$ we have
$$\frac{s}{|F|} = \delta \leq \mu(E_2 \cap M_u A_{-u} E_1) = \mu(M_{1/u} E_2 \cap A_{-u} E_1) = \frac{|M_{1/u} E_2 \cap A_{-u} E_1|}{|F|}.$$

Thus, we have s choices for v inside $M_{1/u} E_2 \cap A_{-u} E_1$ and, for each such v, we have both $uv \in E_2$ and $u + v \in E_1$. □

Theorem 5.1 implies also the following combinatorial result in finite dimensional vector spaces over finite fields.

COROLLARY 5.4. *Let $d \in \mathbb{N}$ and let F be a finite field. Then for each set $B \subset F^d$ with $|B| > \sqrt{6}|F|^{d-1/2}$ and any $\alpha = (\alpha_1, \ldots, \alpha_d) \in (F^*)^d$ there exists $v = (v_1, \ldots, v_d) \in F^d$ and $u \in F^*$ such that both $v + u\alpha := (v_1 + u\alpha_1, \ldots, v_d + u\alpha_d)$ and $vu := (v_1 u, \ldots, v_d u)$ are in B.*

Proof. Let $\Omega = F^d$ and let μ be the normalized counting measure on Ω. Note that $\mu(B) > \sqrt{6/|F|}$. Consider the action of the affine group $\mathcal{A}_F$ on Ω defined coordinate-wise.

By Theorem 5.1, we obtain $u \in F^*$ such that $\mu(B \cap M_u A_{-u} B) = \mu(M_{1/u} B \cap A_{-u} B) > 0$. Let $v \in M_{1/u} B \cap A_{-u} B$. We conclude that both $uv \in B$ and $u + v\alpha \in B$. □

Theorem 5.3 was obtained by different methods by Cilleruelo [11] and by Hanson [14]. It should also be mentioned that, for fields of prime order, Shkredov obtained a stronger result, as stated in the following theorem.

THEOREM 5.5. [18] *Let F be a finite field of prime order and let A, B, $C \subset F$ be such that $|A|\,|B|\,|C| > 40|F|^{5/2}$. Then there are x, $y \in F$ such that $x + y \in A$, $xy \in B$ and $x \in C$.*

6. *Some concluding remarks*

6.1. Iterating Theorem 2.5 one can obtain more complex configurations. For instance, if $E \subset K^*$ is such that $\bar{d}_{(F_N)}(E) > 0$, then there exist x, $y \in K^*$ such that
$$\bar{d}_{(F_N)}(((((E - x) \cap (E/x)) - y) \cap (((E - x) \cap (E/x))/y))$$
$$= \bar{d}_{(F_N)}((E - x - y) \cap (E/x - y) \cap ((E - x)/y) \cap (E/(xy))) > 0.$$

In particular there exist x, y, $z \in K^*$ such that $\{z + y + x, (z + y)x, zy + x, zyx\} \subset E$. Iterating once more we get x, y, z, $t \in K^*$ such that
$$\begin{cases} ((t + z) + y) + x \;\; ((t + z) + y) \times x \;\; ((t + z) \times y) + x \;\; ((t + z) \times y) \times x \\ ((t \times z) + y) + x \;\; ((t \times z) + y) \times x \;\; ((t \times z) \times y) + x \;\; ((t \times z) \times y) \times x \end{cases} \subset E.$$

More generally, for each $k \in \mathbb{N}$, applying Theorem 2.5 k times we find, for a given set $E \subset K^*$ with $\bar{d}_{(F_N)}(E) > 0$, a finite sequence $x_0, x_2, \ldots, x_k$ such that
$$(\ldots (((x_0 \circ_1 x_1) \circ_2 x_2) \circ_3 x_3) \ldots) \circ_k x_k \in E$$

for each of the 2^k possible choices of operations $\circ_i \in \{+, \times\}$. Note that the sequence $x_0, \ldots, x_k$ depends on k, so we do not necessarily have an infinite sequence $x_0, x_1, \ldots$

that works for every k (in the same way that we have arbitrarily long arithmetic progressions on a set of positive density but not an infinite arithmetic progression).

6.2. While the main motivation for this paper was Question 1.1, our methods do not work in $\mathbb{N}$, at least without some new ideas. The crucial difference between the field set-up and that of $\mathbb{N}$ (or $\mathbb{Z}$) is that the affine group $\mathcal{A}_K$ of a field K is amenable, whereas the semigroup $\{ax + b : a, b \in \mathbb{Z}, a \neq 0\}$ is not. In particular, it is not difficult to see that no double Følner sequence can exist for $\mathbb{N}$ (or $\mathbb{Z}$). Indeed, the set $2\mathbb{N}$ of even numbers must have density 1 with respect to any multiplicative Følner sequence because it is a (multiplicative) shift of $\mathbb{N}$. On the other hand, $2\mathbb{N}$ must have density $1/2$ with respect to any additive Følner sequence, because $\mathbb{N}$ is the disjoint union of two (additive) shifts of $2\mathbb{N}$.

Even if, for a ring R, there exists a double Følner sequence, we are not guaranteed to have Lemma 2.6, which is used to prove Lemma 3.1. Another interesting question is whether Lemma 3.1 holds for measure preserving actions of the semigroup of affine transformations of $\mathbb{N}$.

6.3. Note that the stipulation about arbitrarily 'large' in Theorem 1.2 is essential since we want to avoid the case when the configuration $\{x + y, xy\}$ degenerates to a singleton. To better explain this point, let $x \in K$, $x \neq 1$ and let $y = x/(x - 1)$. Then $xy = x + y$ and hence the configuration $\{x + y, xy\}$ is rather trivial. We just showed that for any finite coloring of K there are an infinite number of (trivial) monochromatic configurations of the form $\{x + y, xy\}$. Note that our Theorem 4.1 is much stronger than this statement, not only because we have configurations with 3 terms $\{x, x + y, xy\}$, but also because, for each of 'many' x (indeed a set of positive lower density with respect to any double Følner sequence), there is not only one but 'many' y (indeed a set of positive upper density with respect to any double Følner sequence) such that $\{x, x + y, xy\}$ is monochromatic.

6.4. Our main ergodic result (Theorem 2.10) raises the question of whether, under the same assumptions, one has a triple intersection of positive measure $\mu(B \cap A_{-u}B \cap M_{1/u}B) > 0$ for some $u \in K^*$. This would imply that, given any set $E \subset K$ with $\bar{d}_{(F_N)}(E) > 0$, one can find $u, y \in K^*$ such that $\{y, y + u, yu\} \subset E$. Using the methods of §4, one could then show that for every finite coloring of K, one color contains a configuration of the form $\{u, y, y + u, yu\}$.

On the other hand, not every set $E \subset K$ with $\bar{d}_{(F_N)}(E) > 0$ contains a configuration $\{u, y, y + u, yu\}$. In fact, in every abelian group there exists a syndetic set (hence of positive density for any Følner sequence) not containing a configuration of the form $\{u, y, y + u\}$. Indeed, let G be an abelian group and let $\chi : G \to \mathbb{R}/\mathbb{Z}$ be a non-principal character (a non-zero homomorphism; it exists by Pontryagin duality). Then the set $E := \{g \in G : \chi(g) \in [1/3, 2/3)\}$ has no triple $\{u, y, y + u\}$. However, it is syndetic because the intersection $[1/3, 2/3) \cap \chi(G)$ is syndetic in the group $\chi(G)$. (This is true and easy to check with $\chi(G)$ replaced by any subgroup of $\mathbb{R}/\mathbb{Z}$.)

REFERENCES

[1] W. Arveson. *An Invitation to C*-algebras (Graduate Texts in Mathematics, 39)*. Springer, New York, 1976, p. 2.

[2] M. Beiglböck, V. Bergelson, N. Hindman and D. Strauss. Multiplicative structures in additively large sets. *J. Combin. Theory Ser.* A **113**(7) (2006), 1219–1242.

[3] V. Bergelson. A density statement generalizing Schur's theorem. *J. Combin. Theory Ser.* A **43**(2) (1986), 338–343.

[4] V. Bergelson. Ergodic Ramsey theory—an update. *Ergodic Theory of $\mathbf{Z}^d$ Actions (Warwick, 1993–1994) (London Mathematical Society Lecture Note Series, 228)*. Cambridge University Press, Cambridge, 1996, pp. 1–61.

[5] V. Bergelson. Multiplicatively large sets and ergodic Ramsey theory. *Israel J. Math.* **148** (2005), 23–40.

[6] V. Bergelson. Combinatorial and diophantine applications of ergodic theory. *Handbook of Dynamical Systems.* 1B. Eds. B. Hasselblatt and A. Katok. Elsevier, Amsterdam, 2006, pp. 745–841.

[7] V. Bergelson. Ultrafilters, IP sets, dynamics, and combinatorial number theory. *Ultrafilters Across Mathematics (Contemporary Mathematics, 530)*. American Mathematical Society, Providence, RI, 2010, pp. 23–47.

[8] V. Bergelson, H. Furstenberg and R. McCutcheon. IP-sets and polynomial recurrence. *Ergod. Th. & Dynam. Sys.* **16**(5) (1996), 963–974.

[9] V. Bergelson, A. Leibman and R. McCutcheon. Polynomial Szemerédi theorems for countable modules over integral domains and finite fields. *J. Anal. Math.* **95** (2005), 243–296.

[10] V. Bergelson and R. McCutcheon. Uniformity in the polynomial Szemerédi theorem. *Ergodic Theory of $\mathbf{Z}^d$ Actions (Warwick, 1993–1994) (London Mathematical Society Lecture Note Series, 228)*. Cambridge University Press, Cambridge, 1996, pp. 273–296.

[11] J. Cilleruelo. Combinatorial problems in finite fields and Sidon sets. *Combinatorica* **32**(5) (2012), 497–511.

[12] N. Frantzikinakis and B. Host. Uniformity of multiplicative functions and partition regularity of some quadratic equations. *Preprint*, 2013, arXiv:1303.4329.

[13] H. Furstenberg. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Anal. Math.* **31** (1977), 204–256.

[14] B. Hanson. Capturing forms in dense subsets of finite fields. *Acta Arith.* **160**(3) (2013), 277–284.

[15] N. Hindman. Monochromatic sums equal to products in $\mathbb{N}$. *Integers* **11**(4) (2011), 431–439.

[16] N. Hindman, I. Leader and D. Strauss. Open problems in partition regularity. *Combin. Probab. Comput.* **12**(5–6) (2003), 571–583; Special issue on Ramsey theory.

[17] I. Schur. Über die kongruenz $x^m + y^m = z^m \pmod{p}$. *Jahresber. Dtsch. Math.-Ver.* **25** (1916), 114–117.

[18] I. D. Shkredov. On monochromatic solutions of some nonlinear equations in $\mathbb{Z}/p\mathbb{Z}$. *Mat. Zametki* **88**(4) (2010), 625–634.

[19] M. H. Stone. Applications of the theory of Boolean rings to general topology. *Trans. Amer. Math. Soc.* **41**(3) (1937), 375–481.