

# The structure of sets with cube-avoiding sumsets

Thomas Karam\*      Peter Keevash†

November 22, 2024

## Abstract

We prove that if  $d \geq 2$  is an integer,  $G$  is a finite abelian group,  $Z_0$  is a subset of  $G$  not contained in any strict coset in  $G$ , and  $E_1, \dots, E_d$  are dense subsets of  $G^n$  such that the sumset  $E_1 + \dots + E_d$  avoids  $Z_0^n$  then  $E_1, \dots, E_d$  essentially have bounded dimension. More precisely, they are almost entirely contained in sets  $E'_1 \times G^{I^c}, \dots, E'_d \times G^{I^c}$ , where the size of  $I \subset [n]$  is non-zero and independent of  $n$ , and  $E'_1, \dots, E'_d$  are subsets of  $G^I$  such that the sumset  $E'_1 + \dots + E'_d$  avoids  $Z_0^I$ .

## 1 Introduction

An important direction in combinatorial number theory and geometry considers questions that are broadly of the following kind: given two subsets  $A, B$  of some ambient (abelian) group, what may be deduced about the structure of  $A, B$  if the sumset  $A + B$  is somehow constrained?

Among various constraints that may be considered for  $A + B$ , the most basic and most studied is bounding  $|A + B|$  in terms of  $|A|$  and  $|B|$ . For example, when  $A = B$ , there is a long line of research describing the structure of finite sets  $A \subset \mathbb{Z}$  with  $|A + A| \leq K|A|$  for some fixed  $K$ . Here the landmark result is Freiman's theorem, which shows that such  $A$  must be contained in some multidimensional arithmetic progression  $P$  with  $\dim(P)$  and  $|P|/|A|$  both bounded by a constant depending only on  $K$ . Further milestones in this direction are an extension to general (not necessarily abelian) groups by Breuillard, Green and Tao [3] and a resolution of Marton's Conjecture (aka the Polynomial Freiman-Ruzsa Conjecture) on a polynomial quantitative improvement for abelian groups with bounded torsion by Gowers, Green, Manners and Tao [5].

It is also natural to constrain  $A + B$  not by placing an upper bound on its size, but by requiring that it avoids a specific structured set. For instance, a theorem of Sárközy [11] provides upper bounds on the size of a subset  $A \subset [n]$  such that  $A - A$  does not contain any prime integer, and Green [6] recently obtained a related result for shifted primes. Another well-studied example is that of subsets  $A \subset [n]$  such that  $A - A$  does not contain any perfect square, for which bounds were obtained by Sárközy [11] and Furstenberg [4], with a more recent improvement by Bloom and Maynard [2].

Our own focus in the present paper will be on high-dimensional subsets  $E, F$  of a large power  $G^n$  of some fixed finite abelian group  $G$ , satisfying the constraint that for some fixed

---

\*Mathematical Institute, University of Oxford. Email: [thomas.karam@maths.ox.ac.uk](mailto:thomas.karam@maths.ox.ac.uk). Supported by ERC Advanced Grant 883810.

†Mathematical Institute, University of Oxford. Email: [keevash@maths.ox.ac.uk](mailto:keevash@maths.ox.ac.uk). Supported by ERC Advanced Grant 883810.

$Z_0 \subset G$  the sumset  $E + F$  avoids the power  $Z_0^n$ . To illustrate this, we consider two subsets  $A, B$  of  $\mathbb{Z}^n$  with constraints according to residues modulo some integer  $N$ . Here we give two examples, the first being trivial, and the second already capturing the main difficulties of the question. Suppose first that  $N = 2$  and we require that there is no  $(a, b) \in A \times B$  with  $a_i + b_i$  even for every  $i \in [n]$ . Equivalently, projecting  $A, B$  modulo 2 to subsets  $E, F$  of  $\mathbb{Z}_2^n$ , we require that  $E + F$  does not contain  $\{0\}^n \in \mathbb{Z}_2^n$ , or equivalently that  $F$  is disjoint from  $-E$ . In this example, we do not obtain any non-trivial structure for  $E$  and  $F$ .

Now suppose that  $N > 2$  and  $A + B$  avoids  $(N\mathbb{Z} \cup (N\mathbb{Z} + 1))^n$ . Equivalently, projecting  $A, B$  modulo  $N$  to subsets  $E, F$  of  $\mathbb{Z}_N^n$ , we require  $E + F$  to be disjoint from  $\{0, 1\}^n$ . Here it is not clear what structure this imposes on  $E$  and  $F$ . Furthermore, one may hope that an answer to this question may lead to progress on the longstanding Additive Basis Conjecture of Jaeger, Linial, Payan and Tarsi (reported by Alon, Linial and Meshulam [1]), which is equivalent to the statement that for any prime  $p$  there is a constant  $C = C(p)$  such that for any invertible linear maps  $A_i \in GL(n, \mathbb{Z}_p)$  for  $1 \leq i \leq C$  we have  $A_1(\{0, 1\}^n) + \dots + A_C(\{0, 1\}^n) = \mathbb{Z}_p^n$ .

In a companion paper [8] we solve the corresponding continuous extremal problem for  $E$  and  $F$  in the torus  $(\mathbb{R}/\mathbb{Z})^n$ , which can be rephrased in terms of extremal expansions by cubes: given  $m, \ell \in (0, 1)$  we describe the extremal examples (and show stability) for minimising  $\mu(E + [0, \ell]^n)$  among all  $E \subset (\mathbb{R}/\mathbb{Z})^n$  with  $\mu(E) = m$ . One application of our extremal result is another proof of the known bound  $C < O(\log n)$  for the Additive Basis Conjecture. The present paper concerns structural properties of  $E, F$  with  $(E + F) \cap \{0, 1\}^n = \emptyset$  that have density bounded below but may be quite far from any extremal example.

## 1.1 Results

Next we make three basic observations that motivate our structural result for subsets  $E, F$  of  $\mathbb{Z}_N^n$  such that  $E + F$  avoids  $\{0, 1\}^n$  (or more generally  $Z_0^n$  for some  $Z_0 \subset \mathbb{Z}_N$ ).

1. Many natural examples are low-dimensional, e.g.  $E = F = \{x \in \mathbb{Z}_3^n : x_1 = 1\}$ .
2. Any example in some dimension can be extended to any higher dimension: if  $E', F'$  are subsets of  $\mathbb{Z}_N^k$  such that  $E' + F'$  avoids  $\{0, 1\}^k$  then we can extend  $E', F'$  to subsets  $E, F$  of  $\mathbb{Z}_N^n$  for any  $n > k$  simply by taking  $E = E' \times \mathbb{Z}_N^{n-k}$  and  $F = F' \times \mathbb{Z}_N^{n-k}$ .
3. If  $E + F$  avoids  $\{0, 1\}^n$  then so does  $E' + F'$  for any  $E' \subset E$  and  $F' \subset F$ .

Conversely, our main result will state that any  $E, F$  with  $(E + F) \cap Z_0^n$  empty can be approximated by sets obtained by these three moves (starting with a low-dimensional set, extending to a higher dimension, taking arbitrary subsets). We start with the formulation when  $N$  is prime and  $E + F$  avoids  $Z_0^n$  for some  $Z_0 \subset \mathbb{Z}_N$  with  $|Z_0| > 1$  (as illustrated above, if  $|Z_0| = 1$  then  $E, F$  need not have any non-trivial structure). Throughout, if  $I$  is a subset of  $[n]$  we write  $I^c$  for the complement of  $I$  in  $[n]$ .

**Theorem 1.1.** *Let  $p$  be a prime, let  $\varepsilon > 0$ , and let  $Z_0 \subset \mathbb{Z}_p$  with  $|Z_0| > 1$ . Then there exists  $C = C(p, \varepsilon)$  such that for any subsets  $E, F$  of  $\mathbb{Z}_p^n$  with  $(E + F) \cap Z_0^n = \emptyset$  there exist  $I \subset [n]$  with  $0 < |I| < C$  and subsets  $E', F'$  of  $\mathbb{Z}_p^I$  satisfying*

$$|E \setminus (E' \times \mathbb{Z}_p^{I^c})| \leq \varepsilon |\mathbb{Z}_p^n|, \quad |F \setminus (F' \times \mathbb{Z}_p^{I^c})| \leq \varepsilon |\mathbb{Z}_p^n|, \quad (E' + F') \cap Z_0^I = \emptyset.$$

We note that in Theorem 1.1 we require the set  $I$  of structured coordinates to have bounded size, be non-empty (for non-triviality) and be the same for both  $E$  and  $F$ . If instead we showed that  $E$  and  $F$  are structured with respect to some unrelated sets  $I_E$  and  $I_F$  then we could recover the formulation above by taking  $I = I_E \cup I_F$ , but in the converse direction we cannot allow unrelated sets (e.g. if  $I_E \cap I_F = \emptyset$  then we may have  $E + F = \mathbb{Z}_p^n$ ).

Next we suppose that the modulus  $N$  is not necessarily prime. Compared to the case of cyclic groups  $\mathbb{Z}_N$  it will cost us little to tackle the case of finite abelian groups, so we shall present the corresponding generalisation of Theorem 1.1 in the latter setting. Throughout, if  $G$  is a finite abelian group, then we will say that a *strict coset in  $G$*  is a set of the type  $H + \{x\}$  where  $H$  is a subgroup of  $G$  with  $H \neq G$ , and  $x$  is an element of  $G$ .

**Theorem 1.2.** *Let  $G$  be a finite abelian group and let  $\varepsilon > 0$ . Then there exists  $C = C(G, \varepsilon)$  such that if  $Z_0 \subset G$  is not contained in any strict coset in  $G$  and  $E, F$  are subsets of  $G^n$  with  $(E + F) \cap Z_0^n = \emptyset$  then there exist  $I \subset [n]$  with  $0 < |I| < C$  and subsets  $E', F'$  of  $G^I$  satisfying*

$$|E \setminus (E' \times G^{I^c})| \leq \varepsilon |G^n|, \quad |F \setminus (F' \times G^{I^c})| \leq \varepsilon |G^n|, \quad (E' + F') \cap Z_0^I = \emptyset.$$

The assumption on  $Z_0$  cannot be weakened, as if  $Z_0$  is contained in a coset of some strict subgroup  $H$  of  $G$  then under the projection  $\pi : G \rightarrow G/H$  we have  $|\pi(Z_0)| \leq 1$ , which leads to a lack of structure similarly to the case  $|Z_0| = 1$  (see Example 3.1 for details).

Finally, we give a further extension of Theorem 1.2 that considers several summands.

**Theorem 1.3.** *Let  $d \geq 2$  be an integer, let  $G$  be a finite abelian group, and let  $\varepsilon > 0$ . Then there exists  $C = C(d, G, \varepsilon)$  such that if  $Z_0 \subset G$  is not contained in any strict coset in  $G$  and  $E_1, \dots, E_d$  are subsets of  $G^n$  with  $(E_1 + \dots + E_d) \cap Z_0^n = \emptyset$  then there exist  $I \subset [n]$  with  $0 < |I| < C$  and subsets  $E'_1, \dots, E'_d$  of  $G^I$  satisfying*

$$|E_j \setminus (E'_j \times G^{I^c})| \leq \varepsilon |G^n| \text{ for all } j \in [d], \quad (E'_1 + \dots + E'_d) \cap Z_0^I = \emptyset.$$

In Section 2 we will prove Theorem 1.1. Section 3 discusses the necessary modifications to prove its two successive generalisations, Theorem 1.2 and Theorem 1.3. The final Section 4 contains some potential further generalisations and remaining open questions.

## 1.2 Notation and conventions

If  $X$  is a finite set,  $I$  is a subset of  $[n]$ , and  $E$  is a subset of  $X^I$ , then we refer to the ratio  $|E|/|X^I|$  as the *density of  $E$  inside  $X^I$* . Usually there will be no ambiguity as to which set  $X^I$  is being considered and we will denote this density by  $d(E)$ . If  $y$  is an element of  $X^I$  and  $E$  is a subset of  $X^n$ , then we write  $E_{I \rightarrow y}$  for the set of points  $x \in E$  such that  $x_i = y_i$  for every  $i \in I$ . Although the set  $E_{I \rightarrow y}$  is a subset of  $\mathbb{Z}_p^n$  rather than a subset of  $\mathbb{Z}_p^{I^c}$ , we can also view it as a subset of  $\mathbb{Z}_p^{I^c}$ , and the notation  $d(E_{I \rightarrow y})$  will always refer to the density of  $E_{I \rightarrow y}$  as a subset of  $\mathbb{Z}_p^{I^c}$ . If  $I, J$  are disjoint subsets of  $[n]$ ,  $y$  and  $z$  are elements of  $X^I$  and  $X^J$  respectively, and  $E$  is a subset of  $\mathbb{Z}_p^n$ , then we write  $E_{I \rightarrow y, J \rightarrow z}$  for the set  $E_{I \cup J, w}$  where  $w$  is the element of  $X^{I \cup J}$  defined by  $w_i = y_i$  for each  $i \in I$  and  $w_i = z_i$  for each  $i \in J$ .

## 2 Two summands and prime modulus

In the present section we prove Theorem 1.1. The two main technical ingredients of the proof are (i) a simultaneous regularity lemma for two sets, and (ii) a result of Hażła, Holenstein

and Mossel on product space models of correlation. We present the first ingredient in the first subsection, which is a minor modification of an existing result, although we include a proof for the convenience of the reader. In the second subsection we prove Theorem 1.1 assuming a lemma on summands in dense pseudorandom sets. We then conclude the proof in the third subsection by using the second ingredient mentioned above to prove this lemma.

## 2.1 Pseudorandom sets and a simultaneous regularity lemma

In our context, a regularity lemma is a result on decomposing any subset of a product set  $X^n$  into a bounded number of pieces, most of which are pseudorandom, in the following sense.

**Definition 2.1.** *Let  $X$  be a finite set, let  $r$  be a nonnegative integer and let  $\beta > 0$ . We say that a subset  $E$  of  $X^n$  is  $(r, \beta)$ -pseudorandom if for any subset  $I$  of  $[n]$  with size at most  $r$  and every  $y \in X^I$  we have  $|d(E_{I \rightarrow y}) - d(E)| \leq \beta$ .*

The following formulation is similar to that in [9, Lemma 3.2], with the slight complication of simultaneously decomposing two sets; the required modification of the proof is straightforward, but we give the details for the convenience of the reader.

**Lemma 2.2.** *Let  $X$  be a finite set, let  $r$  be a nonnegative integer, and let  $\beta, \alpha > 0$ . Then there exists  $C = \text{Psr}_2(X, r, \beta, \alpha)$  such that for any subsets  $E, F$  of  $X^n$  there exists  $I \subset [n]$  with  $0 < |I| < C$  which simultaneously satisfies*

$$\mathbb{P}_{y \in X^I}(E_{I \rightarrow y} \text{ not } (r, \beta)\text{-pseudorandom}) \leq \alpha, \quad (1)$$

$$\mathbb{P}_{y \in X^I}(F_{I \rightarrow y} \text{ not } (r, \beta)\text{-pseudorandom}) \leq \alpha. \quad (2)$$

*Proof.* We construct the set  $I$  using an inductive process. Let us begin by ignoring the requirement that  $I$  is non-empty (which will be easy to also ensure). For a positive integer  $s$ , at the  $s$ th iteration we proceed as follows, unless we have stopped before then.

Having obtained a set  $I_s$ , if the inequalities (1) and (2) hold for  $I = I_s$  then we stop. Let us now assume that (1) fails (if instead (2) fails, then we proceed similarly with  $E$  replaced by  $F$ ). We then define the set

$$E_s^{\text{psr}} = \{y \in X^{I_s} : E_{I_s \rightarrow y} \text{ not } (r, \beta)\text{-pseudorandom}\}.$$

For each  $y \in E_s^{\text{psr}}$  we can find some  $I_{s+1, y} \subset I_s^c$  with size at most  $r$  satisfying

$$|d(E_{I_s \rightarrow y, I_{s+1, y} \rightarrow z}) - d(E_{I_s \rightarrow y})| > \beta$$

for some  $z \in I_{s+1, y}$ . To complete the inductive step we set

$$I_{s+1} = I_s \cup \bigcup_{y \in E_s^{\text{psr}}} I_{s+1, y}.$$

We next show that the process terminates after a number of iterations that is bounded above depending on  $p, r, \beta, \alpha$  only. We will do so by an energy-increment argument. For each step  $s$  of the induction we define the energies

$$\mathcal{E}_s(E) = \mathbb{E}_{y \in X^{I_s}} d(E_{I_s \rightarrow y})^2, \quad \mathcal{E}_s(F) = \mathbb{E}_{y \in X^{I_s}} d(F_{I_s \rightarrow y})^2.$$

The sets  $I_s$  constitute an increasing sequence (with respect to inclusion), so the sequences  $\mathcal{E}_s(E)$  and  $\mathcal{E}_s(F)$  are nondecreasing by the Cauchy-Schwarz inequality. If some step  $s$  of the induction involves  $E$ , then we may lower bound the difference

$$\mathcal{E}_{s+1}(E) - \mathcal{E}_s(E) = \mathbb{E}_{y \in X^{I_s}} \left( \mathbb{E}_{z \in X^{I_{s+1} \setminus I_s}} d(E_{I_s \rightarrow y, I_{s+1} \setminus I_s \rightarrow z})^2 - d(F_{I_s \rightarrow y})^2 \right)$$

by interpreting for every  $y \in X^{I_s}$  the inner expectation as the variance of the variable  $d(E_{I_s \rightarrow y, I_{s+1} \setminus I_s \rightarrow z})$  when  $z$  is chosen uniformly at random in  $X^{I_{s+1} \setminus I_s}$ . For every  $y \in E_s^{\text{psr}}$ , the variance of the variable  $d(E_{I_s \rightarrow y, I_{s+1} \setminus I_s \rightarrow z})$  when  $z$  is chosen uniformly at random in  $X^{I_{s+1} \setminus I_s}$  is again (by the Cauchy-Schwarz inequality) at least the variance of the variable  $d(E_{I_s \rightarrow y, I_{s+1} \setminus I_s \rightarrow z})$  when  $z$  is chosen uniformly at random in  $X^{I_{s+1} \setminus I_s}$ , which is always at least  $p^{-r} \beta^2$  by definition of  $E_s^{\text{psr}}$ . Hence we obtain the lower bound

$$\mathcal{E}_{s+1}(E) - \mathcal{E}_s(E) \geq p^{-r} \alpha \beta^2,$$

which is independent of  $s$ . Thus the sum of the energies  $\mathcal{E}_s(E) + \mathcal{E}_s(F)$  increases by at least  $p^{-r} \alpha \beta^2$  at each step, and since it is always bounded above by 2, the number of steps is at most  $2p^r \alpha^{-1} \beta^{-2}$ . At every step, the set  $I_{s+1} \setminus I_s$  has size bounded above by  $p^{|I_s| r}$ .

To ensure that  $I$  is non-empty, at the very first iteration we continue (rather than stop) regardless of whether (1) or (2) holds, and for that iteration the difference  $(\mathcal{E}_1(E) + \mathcal{E}_1(F)) - (\mathcal{E}_0(E) + \mathcal{E}_0(F))$  is lower bounded by 0 rather than by  $p^{-r} \alpha \beta^2$ .  $\square$

## 2.2 Reducing to pseudorandom summands

Here we will reduce the structure theorem to the following proposition on pseudorandom dense summands  $E$  and  $F$ , showing that not only does  $E + F$  meet  $Z_0^n$  but  $E \times F$  contains a positive proportion of the pairs with sum in  $Z_0^n$ . In what follows, we will continue to refer to subsets  $E, F \subset \mathbb{Z}_p^n$  for simplicity of notation, but the upcoming considerations will in fact be applied to subsets  $E_{I \rightarrow x'}$  and  $F_{I \rightarrow y'}$  of  $\mathbb{Z}_p^{I^c}$  obtained by applying Lemma 2.2.

**Proposition 2.3.** *Let  $p$  be a prime, let  $\varepsilon > 0$  and let  $Z_0$  be a subset of  $\mathbb{Z}_p$  with  $|Z_0| > 1$ . Let  $S = \{(x, y) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n : x + y \in Z_0^n\}$ . Then there exist  $\beta > 0$ ,  $c > 0$ , and a positive integer  $r$  such that whenever  $E, F$  are  $(r, \beta)$ -pseudorandom subsets of  $\mathbb{Z}_p^n$  with density at least  $\varepsilon$  we have  $|(E \times F) \cap S| \geq c|S|$ . In particular, there exist  $x \in E$ ,  $y \in F$  satisfying  $x + y \in Z_0^n$ .*

Let us now explain how Theorem 1.1 follows from Lemma 2.2 and Proposition 2.3.

*Proof of Theorem 1.1.* Let  $\varepsilon > 0$ , and let  $E, F$  be subsets of  $\mathbb{Z}_p^n$  satisfying  $(E + F) \cap Z_0^n = \emptyset$ . First we consider the trivial case that one of  $E$  or  $F$  is sparse, say  $d(E) \leq \varepsilon$ . Then taking  $I = \{1\}$  (say),  $E' = \emptyset$  and  $F' = \mathbb{Z}_p$  satisfies all three required conclusions. Likewise if  $d(F) \leq \varepsilon$  by exchanging the roles of  $E$  and  $F$ , so we may now assume both  $d(E) \geq \varepsilon$  and  $d(F) \geq \varepsilon$ .

We then let  $r, \beta$  be the parameters given by Proposition 2.3 for  $p, Z_0, \varepsilon/2$ . Applying Lemma 2.2 with  $X = \mathbb{Z}_p$ , these  $r, \beta$  and  $\alpha = \varepsilon/2$ , we obtain a non-empty subset  $I$  of  $[n]$  with size at most  $\text{Psr}_2(\mathbb{Z}_p, r, \beta, \varepsilon/2)$  satisfying both (1) and (2). We then consider the sets

$$\begin{aligned} E^{\text{psr}} &= \{x' \in \mathbb{Z}_p^I : E_{I \rightarrow x'} \text{ is } (r, \beta)\text{-pseudorandom}\}, & E' &= \{x' \in E^{\text{psr}} : d(E_{I \rightarrow x'}) > \varepsilon/2\}, \\ F^{\text{psr}} &= \{y' \in \mathbb{Z}_p^I : F_{I \rightarrow y'} \text{ is } (r, \beta)\text{-pseudorandom}\}, & F' &= \{y' \in F^{\text{psr}} : d(F_{I \rightarrow y'}) > \varepsilon/2\}. \end{aligned}$$

We note that any  $(x', x'')$  in  $E \setminus (E' \times \mathbb{Z}_p^{I^c})$  satisfies  $x' \in (E^{\text{psr}})^c$  or  $d(E_{I \rightarrow x'}) \leq \varepsilon/2$ , so the density of such  $(x', x'')$  in  $\mathbb{Z}_p^n$  is at most  $\alpha + \varepsilon/2 = \varepsilon$ , as required for the first conclusion of Theorem 1.1. Similarly,  $F \setminus (F' \times \mathbb{Z}_p^{I^c})$  has density at most  $\varepsilon$ .

It remains to show that  $(E' + F') \cap Z_0^I = \emptyset$ . To see this, suppose on the contrary that we have  $(x', y') \in E' \times F'$  with  $x' + y' \in Z_0^I$ . By definition of  $E'$  and  $F'$  we can apply Proposition 2.3 to  $E_{I \rightarrow x'}$  and  $F_{I \rightarrow y'}$ , thus obtaining  $(x'', y'') \in E_{I \rightarrow x'} \times F_{I \rightarrow y'}$  with  $x'' + y'' \in Z_0^{I^c}$ . However, we then have  $x = (x', x'') \in E$  and  $y = (y', y'') \in F$  with  $x + y \in Z_0^n$ . This contradicts our assumption on  $(E, F)$ , so  $(E' + F') \cap Z_0^I = \emptyset$ , as required.  $\square$

### 2.3 Pseudorandom summands via correlation

To complete the proof of Theorem 1.1, it remains to establish Proposition 2.3, which we will deduce from a result of Hażła, Holenstein and Mossel [7]. We will state it in the simplified setting of two correlated variables, deferring the more general setting to Section 3 where we will use it extended to more summands.

Let  $(U, V)$  be random variables following some probability distribution  $\mathcal{P}$  on  $\Omega^2$ , where  $\Omega$  is some finite set. The *correlation* of  $\mathcal{P}$  is

$$\rho(\mathcal{P}) = \sup\{\text{Cov}(\lambda(U), \sigma(V)) : \text{Var } \lambda(U) = \text{Var } \sigma(V) = 1\},$$

where the supremum is over functions  $\lambda, \sigma : \Omega \rightarrow \mathbb{R}$  with  $\text{Var } \lambda(U) = \text{Var } \sigma(V) = 1$ . We have  $\rho(\mathcal{P}) \leq 1$  by the Cauchy-Schwarz inequality, and we may characterise the equality case as follows.

**Lemma 2.4.** *Let  $\Omega$  be a finite set and  $(U, V)$  be random variables following some probability distribution  $\mathcal{P}$  on  $\Omega^2$ . Then  $\rho(\mathcal{P}) = 1$  if and only if there exist non-constant  $\lambda, \sigma : \Omega \rightarrow \mathbb{R}$  such that  $\lambda(U) = \sigma(V)$  with probability 1.*

*Proof.* Since the quantities  $\text{Cov}(\lambda(U), \sigma(V)), \text{Var } \lambda(U), \text{Var } \sigma(V)$  are unchanged after subtracting constants from  $\lambda$  and  $\sigma$ , we can view  $\rho(\mathcal{P})$  as the supremum of  $\text{Cov}(\lambda(U), \sigma(V))$  over all  $\lambda, \sigma$  with expectation 0 and variance 1. This supremum is a maximum, as the set of such pairs  $(\lambda, \sigma)$  is compact (since the set  $\Omega$  is finite). We consider  $(\lambda, \sigma)$  attaining the maximum and apply the Cauchy-Schwarz inequality

$$\rho(\mathcal{P}) = \text{Cov}(\lambda(U), \sigma(V))^2 \leq \text{Var } \lambda(U) \text{Var } \sigma(V) = 1.$$

If  $\rho(\mathcal{P}) = 1$  then we have equality in this inequality, so  $\lambda(U) = \sigma(V)$  with probability 1; this gives the required conclusion, as  $\lambda, \sigma$  are non-constant (they have non-zero variance). Conversely, if we can find non-constant  $\lambda, \sigma$  satisfying  $\lambda(U) = \sigma(V)$  with probability 1, then  $\text{Var } \lambda(U) > 0$ , so after multiplying  $\lambda$  and  $\sigma$  by  $(\text{Var } \lambda(U))^{-1/2}$  we get  $\text{Var } \lambda(U) = \text{Var } \sigma(V) = 1$  as well as  $\text{Cov}(\lambda(U), \sigma(V)) = \text{Var } \lambda(U) = 1$ , so  $\rho(\mathcal{P}) = 1$ .  $\square$

We now state the required result from [7] and deduce Proposition 2.3.

**Theorem 2.5.** *[[7], Theorem 7.1, special case] For every  $\mu > 0$  and  $\rho < 1$  there exist a positive integer  $r$  and some  $\beta, c > 0$  such that the following holds. Let  $(X, Y)$  be a pair of random variables taking values in  $\Omega^n \times \Omega^n$  for some finite set  $\Omega$ , such that the pairs  $(X_i, Y_i)$  with  $i \in [n]$  follow the same distribution  $\mathcal{P}$  on  $\Omega^2$  independently. Let  $f, g : \Omega^n \rightarrow \{0, 1\}$  satisfying the following three assumptions.*

(i) The sets  $\{f=1\}$  and  $\{g=1\}$  are  $(r, \beta)$ -pseudorandom,

(ii)  $\mathbb{E} f(X) \geq \mu$  and  $\mathbb{E} g(Y) \geq \mu$ ,

(iii)  $\rho(\mathcal{P}) \leq \rho$ .

Then we have the lower bound

$$\mathbb{E} f(X)g(Y) \geq c. \quad (3)$$

*Proof of Proposition 2.3.* Let  $E, F$  be as in Proposition 2.3, for some  $r, \beta, c$  to be determined below. In Theorem 2.5 we take  $\Omega$  to be  $\mathbb{Z}_p$ , take  $f = 1_E$  and  $g = 1_F$ , and take  $\mathcal{P}$  to be the probability distribution on  $\mathbb{Z}_p^2$  where each pair  $(x, y)$  with  $x + y \in Z_0$  has probability  $(p|Z_0|)^{-1}$  and all other pairs  $(x, y)$  have probability 0. Setting  $\mu = \varepsilon$ , as  $\mathcal{P}$  has uniform marginals on  $\mathbb{Z}_p$  we have  $\mathbb{E} f(X) = d(E) \geq \mu$  and  $\mathbb{E} g(Y) = d(F) \geq \mu$ .

The remaining condition  $\rho := \rho(\mathcal{P}) < 1$  follows from Lemma 2.4. To see this, consider any  $\lambda, \sigma : \mathbb{Z}_p \rightarrow \mathbb{R}$  such that  $\lambda(U) = \sigma(V)$  with probability 1 when  $(U, V) \sim \mathcal{P}$ . As  $|Z_0| > 1$  we can fix distinct elements  $u, v$  of  $Z_0$ . For each  $x \in \mathbb{Z}_p$ , there is a non-zero probability that  $(U, V) = (u - x, x)$ , so we must have  $\lambda(u - x) = \sigma(x)$ . Similarly, we must have  $\lambda(v - x) = \sigma(x)$ . Thus  $\lambda(u - x) = \lambda(v - x)$ , so  $\lambda$  is a constant function, and so is  $\sigma$ . Thus  $\rho < 1$  by Lemma 2.4.

We can therefore apply Theorem 2.5, which provides the required parameters  $r, \beta, c$  for the assumptions on  $E, F$  in Proposition 2.3. Recalling that  $S = \{(x, y) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n : x + y \in Z_0^n\}$ , the conclusion (3) of Theorem 2.5 is equivalent to  $|(E \times F) \cap S| \geq c|S|$ .  $\square$

### 3 Extensions

In the present section we will generalise our result successively from cyclic groups of prime order to finite abelian groups and then from two summands to several summands. The main ideas of the proofs will be the same, although some non-trivial modifications are needed, and the second generalisation will require more of the framework developed in [7].

#### 3.1 Extending to finite abelian groups

We begin with an extension of Theorem 1.1 replacing  $\mathbb{Z}_p$  for  $p$  prime by any finite abelian group  $G$ . As mentioned in the introduction, we will need to strengthen our assumption on  $Z_0$  to not being contained in any strict coset in  $G$ . The following construction shows that this assumption on  $Z_0$  is necessary for us to obtain any non-trivial structure for  $E, F$ .

**Example 3.1.** Let  $G$  be a finite abelian group and let  $Z_0 \subset H + \{x\}$ , where  $H$  is a strict subgroup of  $G$  and  $x \in G$ . Let  $K$  be the quotient group  $G/H$  and let  $\pi : G \rightarrow K$  be the projection from  $G$  to  $K$ . Then  $\pi(Z_0) = \{\kappa\}$  for some  $\kappa \in K$ .

Let  $E_K, F_K$  be two subsets of  $K^n$  such that for any  $x_K \in E_K$  and  $y_K \in F_K$  we have  $x_K + y_K \neq \kappa$ . Consider any  $E \subset (\pi^{\otimes n})^{-1}(E_K)$  and  $F \subset (\pi^{\otimes n})^{-1}(F_K)$ . Then for any  $x \in E$  and  $y \in F$  we have  $\pi^{\otimes n}(x) + \pi^{\otimes n}(y) \in E_K + F_K$ , so  $x + y \notin Z_0^n$ . However, the sets  $E_K, F_K$  are fairly arbitrary: e.g. if  $\kappa = 0$  then the only condition is that  $E_K$  and  $-F_K$  are disjoint.

Now we modify the proof of Theorem 1.1 to prove Theorem 1.2.

*Proof of Theorem 1.2.* The proof of Theorem 1.1 also proves Theorem 1.2, assuming that we have the corresponding analogue of Proposition 2.3, so it suffices to show that the above proof of Proposition 2.3 also works replacing ‘ $Z_0 \subset \mathbb{Z}_p$  with  $|Z_0| > 1$ ’ by ‘ $Z_0 \subset G$  not contained in any strict coset in  $G$ ’. We will apply Theorem 2.5 similarly to before: we take  $\Omega = G$ ,  $f = 1_E$ ,  $g = 1_F$  and the distribution  $\mathcal{P}$  on  $G^2$  where each pair  $(x, y)$  with  $x + y \in Z_0$  has probability  $(|G||Z_0|)^{-1}$ . Similarly to before this satisfies conditions (i) and (ii) of Theorem 2.5, so it remains to check condition (iii), that is  $\rho(\mathcal{P}) < 1$ .

We suppose for contradiction that  $\rho(\mathcal{P}) = 1$ . By Lemma 2.4 we then have non-constant  $\lambda, \sigma : G \rightarrow \mathbb{R}$  such that  $\lambda(U) = \sigma(V)$  with probability 1 when  $(U, V) \sim \mathcal{P}$ . For every  $x, y \in G$  with  $x + y \in Z_0$  the probability of the event  $\{U = x, V = y\}$  is positive, so  $\lambda(x) = \sigma(y)$ . Thus for any  $y_1, y_2 \in Z_0$  we have  $\sigma(y_1 - x) = \lambda(x) = \sigma(y_2 - x)$  for every  $x \in G$ . Equivalently,  $\sigma(x) = \sigma(x + y)$  for all  $x \in G$  and all  $y \in Z_0 - Z_0$ . Taking  $x = 0$  and iterating this identity, we see that  $\sigma$  is constant on the subgroup  $H$  generated by  $Z_0 - Z_0$ . Furthermore,  $Z_0$  is contained in a coset of  $H$ , as for any  $x \in Z_0$  we have  $Z_0 - \{x\} \subset Z_0 - Z_0 \subset H$ . By assumption on  $Z_0$ , we therefore have  $H = G$ , so  $\sigma$  is constant. This is a contradiction, so  $\rho(\mathcal{P}) < 1$ .  $\square$

As a sanity check, it may be helpful to observe where the above proof fails (as it must) in the case where  $Z_0$  is contained in a strict coset  $H + \{x\}$  of  $G$ , that is  $\pi(Z_0) = \{\kappa\}$  with notation as in Example 3.1. Fix any reals  $(a_k : k \in K)$  and consider  $\lambda, \sigma : G \rightarrow \mathbb{R}$  defined by  $\lambda(x) = a_{\pi(x)}$ ,  $\sigma(x) = a_{\kappa - \pi(x)}$ . These functions are not constant in general, but satisfy  $\lambda(x) = \sigma(y)$  whenever  $x + y \in Z_0$ .

### 3.2 Extending to several summands

In this subsection we obtain our most general result, extending the previous result from two summands to any number of summands. As for two summands, we need to assume that  $Z_0 \subset G$  is not contained in any strict coset in  $G$ . We start with a construction to show that this assumption is necessary (in the case of two summands it reduces to a special case of Example 3.1).

**Example 3.2.** Let  $K = G/H$  with  $H$  a strict subgroup of  $G$  and  $Z_0 \subset H + \{x\}$  with  $\pi(Z_0) = \{\kappa\}$  be as in Example 3.1. Define  $S : K^n \rightarrow K$  by  $S(y_1, \dots, y_n) = y_1 + \dots + y_n$ . Fix  $a_1, \dots, a_d \in K$  such that  $a_1 + \dots + a_d \neq n\kappa$ , and define subsets  $K_1, \dots, K_d$  of  $K^n$  and  $E_1, \dots, E_d$  of  $G^n$  by  $K_i = S^{-1}(a_i)$  and  $E_i = (\pi^{\otimes n})^{-1}(K_i)$  for each  $i \in [d]$ . Then clearly  $(K_1 + \dots + K_d) \cap \{\kappa\}^n = \emptyset$  and so  $(E_1 + \dots + E_d) \cap Z_0^n$ . However, the subsets  $E_i$  each have density  $1/|K|$  but do not satisfy the conclusion of Theorem 1.3 in general.

The remainder of this subsection will be devoted to the proof of Theorem 1.3. We start by stating the appropriate generalisation of Lemma 2.2 (we omit the proof, as it is a straightforward adaptation of Lemma 2.2, considering the sum of energies of the  $d$  sets  $E_1, \dots, E_d$ ).

**Lemma 3.3.** *Let  $X$  be a finite set, let  $d, r$  be positive integers, and let  $\beta, \alpha > 0$ . Then there exists  $C = \text{Psr}_d(X, r, \beta, \alpha)$  such that for any subsets  $E_1, \dots, E_d$  of  $X^n$  there exists  $I \subset [n]$  with  $0 < |I| < C$  which simultaneously satisfies*

$$\mathbb{P}_{y \in X^I}((E_j)_{I \rightarrow y} \text{ not } (r, \beta)\text{-pseudorandom}) \leq \alpha \quad \text{for every } j \in [d]. \quad (4)$$

Next we formulate the appropriate generalisation of Proposition 2.3.



**Proposition 3.4.** *Let  $d \geq 2$  be an integer, let  $G$  be a finite abelian group, let  $Z_0$  be a subset of  $G$  that is not contained in any strict coset in  $G$ , and let  $\varepsilon > 0$ . Let*

$$S = \{(x^1, \dots, x^d) \in (G^n)^d : x^1 + \dots + x^d \in Z_0^n\}.$$

*Then there exist  $\beta > 0$ ,  $c > 0$ , and a positive integer  $r$  such that whenever  $E_1, \dots, E_d$  are  $(r, \beta)$ -pseudorandom subsets of  $G^n$  with density at least  $\varepsilon$  we have  $|S \cap \prod_{i=1}^d E_i| \geq c|S|$ . In particular, there exist  $x^1 \in E_1, \dots, x^d \in E_d$  satisfying  $x^1 + \dots + x^d \in Z_0^n$ .*

Before proving Proposition 3.4, we present the deduction of Theorem 1.3, which is very similar to the case of two summands, but we nonetheless write it in full for clarity.

*Proof of Theorem 1.3.* Let  $\varepsilon > 0$ , and let  $E_1, \dots, E_d$  be subsets of  $G^n$  such that  $E_1 + \dots + E_d$  avoids  $Z_0^n$ . As for two summands, the case where some  $E_i$  has density at most  $\varepsilon$  is trivial, so we may assume  $d(E_i) \geq \varepsilon$  for all  $i \in [d]$ .

We take  $r, \beta$  to be the parameters given by Proposition 3.4 applied with  $d, G, Z_0, \varepsilon/2$ . Applying Lemma 3.3 with  $X = G$ , these  $r, \beta$  and  $\alpha = \varepsilon/2$ , we obtain a non-empty subset  $I$  of  $[n]$  with size at most  $\text{Psr}_d(G, r, \beta, \varepsilon/2)$  satisfying (4). For each  $j \in [d]$  we consider

$$\begin{aligned} E_j^{\text{psr}} &= \{x' \in G^I : (E_j)_{I \rightarrow x'} \text{ is } (r, \beta)\text{-pseudorandom}\}, \text{ and} \\ E'_j &= \{x' \in E_j^{\text{psr}} : d((E_j)_{I \rightarrow x'}) > \varepsilon/2\}. \end{aligned}$$

We note that any  $(x', x'')$  in  $E_j \setminus (E'_j \times G^{I^c})$  satisfies  $x' \in (E_j^{\text{psr}})^c$  or  $d((E_j)_{I \rightarrow x'}) \leq \varepsilon/2$ , so the density of such  $(x', x'')$  in  $G^n$  is at most  $\alpha + \varepsilon/2 = \varepsilon$ .

It remains to show that  $(E'_1 + \dots + E'_d) \cap Z_0^I = \emptyset$ . To see this, suppose on the contrary that we have  $((x^1)', \dots, (x^d)') \in E'_1 \times \dots \times E'_d$  with  $(x^1)' + \dots + (x^d)' \in Z_0^I$ . By definition of  $E'_1, \dots, E'_d$  we can apply Proposition 3.4 to  $(E_1)_{I \rightarrow (x^1)'}, \dots, (E_d)_{I \rightarrow (x^d)'}$ , thus obtaining  $((x^1)'', \dots, (x^d)'') \in (E_1)_{I \rightarrow (x^1)'} \times \dots \times (E_d)_{I \rightarrow (x^d)'}$  with  $(x^1)'' + \dots + (x^d)'' \in Z_0^{I^c}$ . However, we then have  $x^j = ((x^j)', (x^j)'') \in E_j$  for each  $j \in [d]$  with  $x^1 + \dots + x^d \in Z_0^n$ . This contradicts our assumption on  $(E_1, \dots, E_d)$ , so  $(E'_1 + \dots + E'_d) \cap Z_0^I = \emptyset$ , as required.  $\square$

To complete the proof of Theorem 1.3, it remains to establish Proposition 3.4, via the result of [7], which we will now state in more generality. Let  $(U_1, \dots, U_d)$  be random variables following some probability distribution  $\mathcal{P}$  on  $\Omega^d$ , where  $\Omega$  is some finite set. Let

$$\rho(\mathcal{P}) = \max_{j \in [d]} \sup \{\text{Cov}(\lambda(U_j), \sigma(\overline{U}_j)) : \text{Var } \lambda(U_j) = \text{Var } \sigma(\overline{U}_j) = 1\},$$

where we write  $\overline{U}_j$  for  $(U_1, \dots, U_{j-1}, U_{j+1}, \dots, U_d)$  and consider functions  $\lambda : \Omega \rightarrow \mathbb{R}$  and  $\sigma : \Omega^{[d] \setminus \{j\}} \rightarrow \mathbb{R}$ . We now state the required result from [7] and deduce Proposition 3.4.

**Theorem 3.5.** *[[7], Theorem 7.1, special case] For every integer  $d \geq 2$ ,  $\mu > 0$  and  $\rho < 1$  there exists a positive integer  $r$  and some  $\beta, c > 0$  such that the following holds.*

*Let  $(X^1, \dots, X^d)$  be random variables taking values in  $(\Omega^n)^d$  for some finite set  $\Omega$ , such that  $(X_i^1, \dots, X_i^d)$  with  $i \in [n]$  follow the same distribution  $\mathcal{P}$  on  $\Omega^d$  independently.*

*Suppose  $\rho(\mathcal{P}) \leq \rho$  and  $f_1, \dots, f_d : \Omega^n \rightarrow \{0, 1\}$  are such that for every  $j \in [d]$  the set  $\{f_j = 1\} \subset \Omega^n$  is  $(r, \beta)$ -pseudorandom and  $\mathbb{E} f_j(X^j) \geq \mu$ . Then  $\mathbb{E} f_1(X^1) \dots f_d(X^d) \geq c$ .*

*Proof of Proposition 3.4.* Let  $E_1, \dots, E_d$  be as in Proposition 3.4. In Theorem 3.5 we take  $\Omega$  to be  $G$  and  $\mathcal{P}$  to be the probability distribution on  $G^d$  where each  $(x^1, \dots, x^d)$  with  $x^1 + \dots + x^d \in Z_0$  has probability  $(|G|^{d-1}|Z_0|)^{-1}$  and all other  $d$ -tuples  $(x^1, \dots, x^d)$  have probability 0. Each marginal of  $\mathcal{P}$  is uniform, so taking  $f_j = 1_{E_j}$  we have  $\mathbb{E} f_j(X^j) = d(E_j) \geq \mu := \varepsilon$  for every  $j \in [d]$ .

As in the proof of Proposition 2.3, the proposition will follow from Theorem 3.5 once we verify the remaining condition  $\rho(\mathcal{P}) < 1$ . We can use the characterisation from Lemma 2.4 even for  $\lambda : G \rightarrow \mathbb{R}$  and  $\sigma : G^{[d] \setminus \{i\}} \rightarrow \mathbb{R}$  with  $i \in [d]$ , since its proof did not rely on the domains on which  $\lambda, \sigma$  are defined. The roles of the  $d$  coordinates are interchangeable, so it suffices to show that if  $\lambda : G \rightarrow \mathbb{R}$  and  $\sigma : G^{d-1} \rightarrow \mathbb{R}$  satisfy  $\lambda(U_1) = \sigma(U_2, \dots, U_d)$  with probability 1 when  $(U_1, \dots, U_d) \sim \mathcal{P}$  then  $\lambda, \sigma$  are constant.

Fix any  $(x^3, \dots, x^d) \in G^{d-2}$  and consider the event  $A = \{U_3 = x^3, \dots, U_d = x^d\}$ . (We can assume  $d > 2$ , or regard  $A$  as the trivial event that always holds if  $d = 2$ .) Then  $\mathcal{P}(A) > 0$ , so we can consider the conditional distribution  $\mathcal{P}_{(x^3, \dots, x^d)}$  of  $(U^1, U^2)$  under  $\mathcal{P}$  conditioned on  $A$ , which satisfies  $\lambda(U_1) = \sigma(U_2, x^3, \dots, x^d)$  with probability 1.

We note that  $\mathcal{P}_{(x^3, \dots, x^d)}$  is the distribution on  $G^2$  that is uniformly distributed on pairs  $(x^1, x^2)$  with  $x^1 + x^2$  in the translate  $Z_0 - \{x^3 + \dots + x^d\}$  of  $Z_0$ . Applying the  $d = 2$  case (which we proved in Proposition 2.3) to  $\mathcal{P}_{(x^3, \dots, x^d)}$ , which is valid as  $Z_0 - \{x^3 + \dots + x^d\}$  is not contained in any strict coset in  $G$ , we have  $\rho(\mathcal{P}_{(x^3, \dots, x^d)}) < 1$ .

We then define  $\sigma_{(x^3, \dots, x^d)} : G \rightarrow \mathbb{R}$  by  $\sigma_{(x^3, \dots, x^d)}(x^2) = \sigma(x^2, x^3, \dots, x^d)$  and apply Lemma 2.4 to  $\lambda$  and  $\sigma_{(x^3, \dots, x^d)}$ . As  $\lambda(U_1) = \sigma_{(x^3, \dots, x^d)}(U_2)$  with probability 1 for  $(U_1, U_2) \sim \mathcal{P}_{(x^3, \dots, x^d)}$ , we deduce that  $\lambda$  and  $\sigma_{(x^3, \dots, x^d)}$  are constant, always taking some fixed value  $c$ .

It remains to show that  $\sigma$  is constant. Consider any  $(x^2, x^3, \dots, x^d) \in G^{d-1}$  and  $x^1 \in Z_0 - \{x_2 + x_3 + \dots + x_d\}$ . Then  $(x^1, x^2)$  is in the support of  $(U_1, U_2) \sim \mathcal{P}_{(x^3, \dots, x^d)}$ , so  $c = \lambda(x^1) = \sigma_{(x^3, \dots, x^d)}(x^2) = \sigma(x^2, x^3, \dots, x^d)$ .  $\square$

## 4 Further discussion

Our first open problem is to improve the bound in our main theorems, starting with the simplest setting.

**Question 4.1.** *Can we for each prime  $p$  require  $|I| \leq O(\log(\varepsilon^{-1}))$  in Theorem 1.1?*

Such a bound would be optimal, as is shown by the example of  $Z_0 = \{0, 1\}$ ,  $\varepsilon = p^{-(k+1)}$ ,  $E = (\mathbb{Z}_p^k \setminus \{0, 1\}^k) \times \mathbb{Z}_p^{n-k}$ , and  $F = \{0\}^k \times \mathbb{Z}_p^{n-k}$  for some integer  $k$ . Indeed, if  $E', F'$  satisfy the conclusion of Theorem 1.1 for some non-empty  $I \subset [n]$  then  $F' \neq \emptyset$  and  $E' \neq \mathbb{Z}_p^I$ , so  $E_0 := E \setminus (E' \times \mathbb{Z}_p^{I^c})$  satisfies  $\varepsilon \geq d(E_0) \geq p^{-|I|} - (p/2)^{-k}$ , giving  $|I| = \Omega(k)$ .

Our second problem is to consider other directions of generalising Theorem 1.1, besides the extensions to finite abelian groups and more summands considered in this paper. Our general setting (with two inputs for simplicity) is an arbitrary function  $f : X \times Y \rightarrow Z$  and its tensor product  $f^{\otimes n} : X^n \times Y^n \rightarrow Z^n$ , where  $X, Y, Z$  are finite sets. We would like to characterise pairs  $(f, Z_0)$  with  $Z_0 \subset Z$  satisfying the following statement analogous to that in Theorem 1.1: for every  $\varepsilon > 0$  there is some  $C = C(f, \varepsilon)$  such that for any  $E \subset X^n$  and  $F \subset Y^n$  with  $f^{\otimes n}(E, F) \cap Z_0^n = \emptyset$  there exist  $I \subset [n]$  with  $0 < |I| < C$  and  $E' \subset X^I$ ,  $F' \subset Y^I$  satisfying

$$|E \setminus (E' \times X^{I^c})| \leq \varepsilon |X^n|, \quad |F \setminus (F' \times Y^{I^c})| \leq \varepsilon |Y^n|, \quad f^{\otimes I}(E', F') \cap Z_0^I = \emptyset.$$

The following result gives a general condition on  $(f, Z_0)$  that guarantees the existence of the desired sets  $I, E', F'$ , for the trivial reason that there are almost complete sets  $E_n$  and  $F_n$  such that  $f^{\otimes n}(E_n, F_n) \cap Z_0^n = \emptyset$ . (To be formal, consider any  $\varepsilon > 0$ , let  $n'$  be such that we can find  $E_{n'}, F_{n'}$  as below with densities at least  $1 - \varepsilon$ , and take  $I = [n], E' = E, F' = F$  if  $n < n'$ , or  $I = [n'], E' = E_{n'}, F' = F_{n'}$  if  $n \geq n'$ .)

**Proposition 4.2.** *Let  $X, Y, Z$  be finite sets, let  $f : X \times Y \rightarrow Z$  and let  $Z_0 \subset Z$ . Suppose that there exist  $A \subset X$  and  $B \subset Y$  such that  $f(A \times B) \cap Z_0 = \emptyset$  and  $|A|/|X| + |B|/|Y| > 1$ .*

*Then there exist subsets  $E_n \subset X^n$  and  $F_n \subset Y^n$  for every positive integer  $n$  such that  $f^n(E_n \times F_n) \cap Z_0^n = \emptyset$  and  $\min(d(E_n), d(F_n)) \rightarrow 1$  as  $n \rightarrow \infty$ .*

The condition in Proposition 4.2 is satisfied by some natural functions, such as the minimum function  $[2k] \times [2k] \rightarrow [2k]$  for some  $k \geq 2$  with  $Z_0 = [2k] \setminus [k+1]$ . On the other hand, it contrasts heavily with the case that  $f : G \times G \rightarrow G$  is addition on a finite abelian group  $G$ , as for any  $A, B \subset G$  with  $A + B \neq G$  we have  $A$  disjoint from some translate of  $-B$ , so  $d(A) + d(B) \leq 1$ , and similarly  $d(E) + d(F) \leq 1$  for any  $E, F \subset G^n$  with  $E + F \neq G^n$ .

*Proof.* Let  $r, s, n$  be positive integers such that  $rs \leq n$ . We consider the ‘tribe-like’ sets

$$\begin{aligned} E_n &= \{x_1 \in A \vee \cdots \vee x_r \in A\} \wedge \cdots \wedge \{x_{r(s-1)+1} \in A \vee \cdots \vee x_{rs} \in A\}, \\ F_n &= \{y_1 \in B \wedge \cdots \wedge y_r \in B\} \vee \cdots \vee \{y_{r(s-1)+1} \in B \wedge \cdots \wedge y_{rs} \in B\}. \end{aligned}$$

We claim that  $f^{\otimes n}(E_n \times F_n) \cap Z_0^n = \emptyset$ . To see this, consider any  $(x, y) \in E_n \times F_n$ . By definition of  $F_n$ , there is some  $s' \in [s]$  such that  $y_i \in B$  for all  $i \in [r(s'-1)+1, rs']$ . By definition of  $E_n$ , there is some  $i \in [r(s'-1)+1, rs']$  such that  $x_i \in A$ , so  $(x_i, y_i) \in A \times B$ . As  $f(A \times B) \cap Z_0 = \emptyset$ , we deduce  $f^{\otimes n}(x, y) \notin Z_0^n$ , so the claim holds.

It remains to estimate the densities of  $E_n$  and  $F_n$ . We have

$$\begin{aligned} 1 - d(E_n) &= 1 - (1 - (1 - |A|/|X|)^r)^s \leq s(1 - |A|/|X|)^r, \\ 1 - d(F_n) &= (1 - (|B|/|Y|)^r)^s \leq \exp(-s(|B|/|Y|)^r). \end{aligned}$$

As  $1 - |A|/|X| < |B|/|Y|$ , for any  $\varepsilon > 0$  we can choose  $r$  such that  $(1 - |A|/|X|)^r (|Y|/|B|)^r < \varepsilon$ . Then choosing  $s = \lceil (|Y|/|B|)^r \log(\varepsilon^{-1}) \rceil$  gives  $1 - d(F_n) \leq \varepsilon$  and  $1 - d(E_n) \leq 2\varepsilon \log(\varepsilon^{-1})$ , which can be both arbitrarily small, as required.  $\square$

For further insight on the problem for general functions  $f$ , it seems natural to generalise from addition in abelian groups, to multiplication in general groups, and then further to latin squares, namely functions  $f : X \times X \rightarrow X$  (for some finite set  $X$ ) such that for every  $x, y$  in  $X$  there is a unique  $z$  such that  $f(x, z) = y$  and a unique  $z'$  such that  $f(z', x) = y$ .

**Question 4.3.** *Does some analogue of Theorem 1.1 hold for latin squares?*

## References

- [1] N. Alon, N. Linial, R. Meshulam, *Additive bases of vector spaces over prime fields*, J. Combin. Theory Ser. A **57** (1991), 203-210.
- [2] T. Bloom, J. Maynard, *A new upper bound for sets with no square differences*, Compos. Math. **158** (2022), 1777-1798.

- [3] E. Breuillard, B. J. Green, T. Tao, *The structure of approximate groups*, Publ. Math. IHES **116** (2012), 115-221.
- [4] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Anal. Math. **31** (1977), 204-256.
- [5] W. T. Gowers, B. J. Green, F. Manners, T. Tao, *Marton’s Conjecture in abelian groups with bounded torsion*, arXiv:2404.02244 (2024).
- [6] B. J. Green, *On Sárközy’s theorem for shifted primes*, J. Amer. Math. Soc. **37** (2024), 1121-1201.
- [7] J. Hażła, T. Holenstein, E. Mossel, *Product space models of correlation: Between noise stability and additive combinatorics*, Discrete Anal. **19** (2018).
- [8] T. Karam, P. Keevash, *Extremal expansions by cubes in the torus*, in preparation.
- [9] P. Keevash, N. Lifshitz, E. Long, D. Minzer, *Forbidden intersection for codes*, Jour. London. Math. Soc. **108** (2023), 2037-2083.
- [10] A. Sárközy, *On difference sets of sequences of integers. I*, Acta Math. Acad. Sci. Hungar. **31** (1978), 125-149.
- [11] A. Sárközy, *On difference sets of sequences of integers. III*, Acta Math. Acad. Sci. Hungar. **31** (1978), 355–386.