ON PRODUCT OF DIFFERENCE SETS FOR SETS OF POSITIVE DENSITY

ALEXANDER FISH

Abstract. In this paper we prove that given two sets $E_1, E_2 \subset \mathbb{Z}$ of positive density, there exists $k \geq 1$ which is bounded by a number depending only on the densities of E_1 and E_2 such that $k\mathbb{Z} \subset (E_1 - E_1) \cdot (E_2 - E_2)$. As a corollary of the main theorem we deduce that if $\alpha, \beta > 0$ then there exist N_0 and d_0 which depend only on α and β such that for every $N \geq N_0$ and $E_1, E_2 \subset \mathbb{Z}_N$ with $|E_1| \geq \alpha N, |E_2| \geq \beta N$ there exists $d \leq d_0$ a divisor of N satisfying $d\mathbb{Z}_N \subset (E_1 - E_1) \cdot (E_2 - E_2)$.

1. INTRODUCTION

One of the main themes of additive combinatorics is sum-product estimates. It goes back to Erdös and Szemerédi [3] who conjectured that for any finite set $A \in \mathbb{Z}$ (or in $\mathbb{R}$), for every $\varepsilon > 0$ we have

$$|A + A| + |A \cdot A| \gg |A|^{2-\varepsilon},$$

where the $A + A = \{a + b \,|\, a, b \in A\}$, and $A \cdot A = \{ab \,|\, a, b \in A\}$. Currently the best known estimate is due to Konyagin-Shkredov [7] and it is based on the beautiful previous breakthrough work by Solymosi [8]:

$$|A + A| + |A \cdot A| \gg |A|^{4/3+c},$$

for any $c < 5/9813$.

In this paper we study a slightly twisted, but nevertheless related, sum-product phenomenon. Namely, we address the following

Question 1. *For a given **infinite** set $E \subset \mathbb{Z}$, how much structure does possess the set $(E - E) \cdot (E - E)$?*

We will restrict our attention to sets having positive density, see the definition below.

Furstenberg [6] noticed a strong connection between difference sets for sets of positive density, and the sets of return times of a set of positive measure in measure-preserving systems. In this paper we will establish an arithmetic richness of a set of return times of a set of a positive measure to itself within a measure-preserving system. Recall that a triple (X, μ, T) is a measure-preserving system if X is a compact metric space, μ is a probability measure

Date: 8 February 2017.

2010 *Mathematics Subject Classification.* Primary: 37A45; Secondary: 11E25, 11T30.

Key words and phrases. Difference sets, sum-product estimates.

on the Borel σ-algebra of X, and $T : X \to X$ is a bi-measurable map which preserves μ. For a measurable set $A \subset X$ with $\mu(A) > 0$ the set of return times from A to itself is:

$$R(A) = \{n \in \mathbb{Z} \,|\, \mu(A \cap T^n A) > 0\}.$$

We will denote by $E^2 = \{e^2 \,|e \in E\}$ the set of squares of $E \subset \mathbb{Z}$. It has been proved by Björklund and the author [2] that for any three sets of positive measure A, B, and C in measure-preserving systems there exists $k \geq 1$ (depending on the sets A, B, and C) such that $k\,\mathbb{Z} \subset R(A) \cdot R(B) - R(C)^2$. One of the motivations for this work was to show that k in the latter statement depends only on the measures of the sets A, B, and C. We prove the latter, and even more surprisingly, we show that $R(C)$ can be omitted. We have

Theorem 1.1. *Let (X, μ, T) and (Y, ν, S) be measure-preserving systems, and let $A \subset X, B \subset Y$ be measurable sets with $\mu(A) > 0$, and $\nu(B) > 0$. Then there exist k_0 depending only on $\mu(A)$ and $\nu(B))$, and $k \leq k_0$ such that $k\,\mathbb{Z} \subset R(A) \cdot R(B)$.*

This result has a few combinatorial consequences. To state the first application, we recall that the upper Banach density of a set $E \subset \mathbb{Z}$ is defined by

$$d^*(E) = \limsup_{N\to\infty} \sup_{a\in\mathbb{Z}} \frac{|E \cap \{a, a+1, \ldots, a+(N-1)\}|}{N}.$$

Through Furstenberg's correspondence principle [6], we obtain

Corollary 1.1. *Let $E_1, E_2 \subset \mathbb{Z}$ be sets of positive upper Banach density. Then there exist k_0 which depends only on the densities of E_1 and E_2 and $k \leq k_0$ such that*

$$k\,\mathbb{Z} \subset (E_1 - E_1) \cdot (E_2 - E_2).$$

Another application of Theorem 1.1 is the following result.

Corollary 1.2. *For any $\alpha, \beta > 0$ there exist N_0 and d_0, depending only on α and β, such that for every $N \geq N_0$ and $E_1, E_2 \subset \mathbb{Z}_N$ with $|E_1| \geq \alpha N, |E_2| \geq \beta N$ there exists $d \leq d_0$ which is a divisor of N and $d\,\mathbb{Z}_N \subset (E_1 - E_1) \cdot (E_2 - E_2)$.*

Corollary 1.2 implies also that if p is a large enough prime and $E_1, E_2 \subset \mathbb{Z}_p$ satisfy $|E_1| \geq \alpha p, |E_2| \geq \beta p$, then $(E_1 - E_1) \cdot (E_2 - E_2) = \mathbb{Z}_p$. This also follows from a result by Hart-Iosevich-Solymosi [4] who proved that if $E \subset \mathbf{F}_q$ (where $\mathbf{F}_q$ is a field with q elements) with $|E| \geq q^{3/4+\varepsilon}$ then for q large enough $(E - E) \cdot (E - E) = \mathbf{F}_q$.

Acknowledgment: The work has been carried out during a research visit to Weizmann Institute, Israel. The author would like to thank Feinberg visiting program and Mathematics Department at Weizmann Institute for their support. The author is indebted to Omri Sarig for his constant encouragement

and support, Eliran Subag and Igor Shparlinski for enlightening discussions.

2. Proof of Theorem 1.1

Let us assume that (X, μ, T) is a measure-preserving system, and let $A \subset X$ be a measurable set with $\mu(A) > 0$. Recall that the set of return times of A is defined by

$$R(A) = \{n \in \mathbb{Z} \,|\, \mu(A \cap T^n A) > 0\}.$$

The theorem will follow from the following statement.

Lemma 2.1. *For every $\ell \geq 1$ there exists n which depends only on ℓ and $\mu(A)$ such that for every $b \in \mathbb{Z} \setminus \{0\}$ there exists $m \leq n$ with*

$$\{mb, 2mb, \ldots, \ell mb\} \subset R(A).$$

Indeed, let $R(A)$ and $R(B)$ be sets of return times for measurable sets A and B of positive measures. Then choose $N = \lceil \frac{1}{\nu(B)} \rceil + 1$. Then for every $b \in \mathbb{Z} \setminus \{0\}$ there exist $1 \leq i < j \leq N$ such that $\nu((S^b)^i B \cap (S^b)^j B) > 0$. Then by S-invariance of ν it follows that there exists $1 \leq m \leq N$ ($m = j - i$) such that $mb \in R(B)$.

Let us define $X = N!$. By Lemma 2.1 there exists $n = n(X, \mu(A))$ such that for every $b \in \mathbb{Z} \setminus \{0\}$ there exists $m \leq n$ with $\{mb, 2mb, \ldots, Xmb\} \in R(A)$.

Let us define $k = X \cdot n!$. Take any $b \in \mathbb{Z} \setminus \{0\}$. By the choice of n, there exists $m \leq n$ such that $\{mb, 2mb, \ldots, Xmb\} \in R(A)$. By the choice of N it follows that there exists $1 \leq j \leq N$ such that $j \cdot \frac{k}{Xm} \in R(B)$. Also, $\frac{Xm}{j}$ is an integer less or equal than Xm, therefore $\frac{Xm}{j} b \in R(A)$. Thus $kb = \frac{Xm}{j} b \cdot j \frac{k}{Xm} \in R(A) \cdot R(B)$. This finishes the proof of Theorem 1.1.

Proof of Lemma 2.1. Given measurable sets $A_1, A_2, \ldots, A_n \subset X$ with $\mu(A_i) = \mu(A), i = 1, \ldots, n$, there exists a set $C \subset \{1, \ldots, n\}$ with $|C| \geq \mu(A)n$ such that

$$\mu(\bigcap_{i \in C} A_i) > 0.$$

Indeed, take $f = \sum_{i=1}^n 1_{A_i}$. Then $\int f d\mu = \mu(A)n$. Therefore there exists a set of positive measure $D \subset X$ such that for all $x \in D$ we have $f(x) \geq \mu(A)n$. Countable additivity of μ implies the statement.

By Szemerédi's theorem there exists $N(\ell, \mu(A))$ such that for every $N \geq N(\ell, \mu(A))$ and any set $F \subset \{1, 2, \ldots, N\}$ with $|F| \geq \mu(A)N$ contains an arithmetic progression of length $\ell + 1$.

Let $n = N(\ell, \mu(A))$. For any $b \in \mathbb{Z} \setminus \{0\}$, let $A_i = (T^b)^i A$. Then there exists $C \subset \{1, 2, \ldots, n\}$ such that $|C| \geq \mu(A)n$, and $\mu(\cap_{i \in C} (T^b)^i A) > 0$. Then by Szemerédi's theorem we can find arithmetic progression of length

$\ell+1$ within C, i.e., for some $1 \leq m \leq n$ and $1 \leq a \leq n$ we have $\{a, a+m, a+2m, \dots, a+\ell m\} \in C$. In particular, we have for all $0 \leq i < j \leq \ell$:

$$\mu((T^b)^{a+im}A \cap (T^b)^{a+jm}A) > 0.$$

Thus we have $\mu(A \cap (T^{bm})^{(j-i)}A) > 0$. Therefore, we have $\mu(A \cap (T^{bm})^k A) > 0$ for all $k = 1, 2, \dots, \ell$. Thus, by definition of $R(A)$:

$$\{bm, 2bm, \dots, \ell bm\} \in R(A).$$

□

3. Proofs of Corollaries 1.1 and 1.2

Furstenberg [6] in his seminal work on Szemerédi's theorem showed:

Correspondence Principle. *Given a set $E \subset \mathbb{Z}$ there exists a measure-preserving system (X, μ, T) and a measurable set $A \subset X$ such that for all $n \in \mathbb{Z}$ we have*

$$d^*\left(E \cap (E+n)\right) \geq \mu(A \cap T^n A),$$

and

$$d^*(E) = \mu(A).$$

Proof of Corollary 1.1. Let $E_1, E_2 \subset \mathbb{Z}$ be sets of positive densities. Then by Furstenberg's correspondence principle there exist measure-preserving systems (X, μ, T) and (Y, ν, S) and measurable sets $A \subset X$, $B \subset Y$ that satisfy

$$\mu(A) = d^*(E_1),\ \nu(B) = d^*(E_2)$$

and

$$R(A) \subset E_1 - E_1,\ R(B) \subset E_2 - E_2.$$

By Theorem 1.1 there exist $k(\mu(A), \nu(B))$ and $k \leq k(\mu(A), \nu(B))$ such that $k\,\mathbb{Z} \subset R(A) \cdot R(B)$. The latter statement implies the conclusion of the corollary.

□

Proof of Corollary 1.2. Let $\alpha > 0$, and $\beta > 0$ and let $E_1, E_2 \subset \mathbb{Z}_N$ with $|E_1| \geq \alpha N$, and $|E_2| \geq \beta N$. It is clear that $X = \mathbb{Z}_N$ with the shift map $Tx = x+1 (\mathrm{mod}\ N)$ and the uniform measure μ on X defined by $\mu(E) = \frac{|E|}{N}$ for any $E \subset X$ is a measure-preserving system. It is also clear that for (X, μ, T) and the sets $E_1, E_2 \subset X$ we have[1] $R(E_1) = (E_1 - E_1) + N\,\mathbb{Z}$ and $R(E_2) = (E_2 - E_2) + N\,\mathbb{Z}$. Then by Theorem 1.1 it follows that if $N \geq N_0$, where N_0 depends only on α and β, then there exist $k(\alpha, \beta)$ and $k \leq k(\alpha, \beta)$ such that $k\,\mathbb{Z} \subset R(E_1) \cdot R(E_2)$. Then by the Chinese Remainder theorem for $d = \gcd(k, N) \leq k$ we have $d\,\mathbb{Z} \subset (E_1 - E_1) \cdot (E_2 - E_2) + N\mathbb{Z}$, which implies the statement of the corollary.

□

[1] We identify here the ring $\mathbb{Z}_N$ with the set $\{0, 1, \dots, N-1\}$.

4. Further problems

It might be of interest to have a relatively small bound on k_0 in terms of $\mu(A)$ and $\nu(B)$ in Theorem 1.1. In the proof we use the Szemerédi theorem [9], as a result, the bound on k depends on the bound of Szemerédi's number $N(\lceil \frac{1}{\nu(B)} \rceil !, \mu(A))$. The current record is due to Gowers [5] who proved the following upper bound on $N(\ell, \delta)$:

$$N(\ell, \delta) = \exp\left(\delta^{-c(\ell)}\right), \text{ where } c(\ell) = 2^{2^{\ell+9}}.$$

So, our current bound on k is five times exponential in $\frac{1}{\mu(A)}$ and $\frac{1}{\nu(B)}$.

Problem 1. *Can we avoid Szemerédi's theorem in the proof of Theorem 1.1 and obtain a much better bound on k? For instance, is it possible to obtain an exponential bound on k in the variables $\frac{1}{\mu(A)}$ and $\frac{1}{\nu(B)}$?*

To formulate the next problem, we mention a recent result by Björklund-Bulinski [1], who proved, in particular, that for any $E \subset \mathbb{Z}^3$ of positive density there exists $k \geq 1$, depending on the set E and not only on its density, such that

$$k\,\mathbb{Z} \subset \{x^2 - y^2 - z^2 \,|\, (x, y, z) \in E - E\}.$$

Problem 2. *Is it true that given $E_1, E_2 \subset \mathbb{Z}$ of positive density there exist k_0, which depends only on $d^*(E_1)$ and $d^*(E_2))$, and $k \leq k_0$ such that $k\,\mathbb{Z} \subset (E_1 - E_1)^2 - (E_2 - E_2)^2$? If yes, can we show that for any set $E \subset \mathbb{Z}^2$ of positive density there exist k_0, which depends only on $d^*(E)$, and $k \leq k_0$ such that $k\,\mathbb{Z} \subset \{x^2 - y^2 \,|\, (x, y) \in E - E\}$?*

The next two problems arise naturally by Theorem 1.1 and the following result proved by Björklund and the author in [2]:

Theorem 4.1. *Let $E \subset Mat_d^0(\mathbb{Z}) = \{(a_{ij}) \in \mathbb{Z}^{d \times d} \,|\, tr(a_{ij}) = 0\}$ be a set of positive density. Then there exists $k \geq 1$ (which a priori depends on the set E and not only on its density) such that for any matrix $A \in k \cdot Mat_d^0(\mathbb{Z})$ there exists $B \in E - E$ such that the characteristic polynomial of B coincides with the characteristic polynomial of A.*

Problem 3. *Is it true that given $E \subset \mathbb{Z}^2$ of positive upper Banach density, i.e.,*

$$d^*(E) = \limsup_{b-a \to \infty, d-c \to \infty} \frac{|E \cap [a, b) \times [c, d)|}{(b - a)(d - c)} > 0,$$

there exist k_0 that depends only on $d^*(E)$ and $k \leq k_0$ such that

$$k\,\mathbb{Z} \subset \{xy \ , | \, (x, y) \in E - E\}?$$

We also would like to establish the quantitative version of Theorem 4.1:

Problem 4. *Is it true that the parameter k in Theorem 4.1 depends only on the density of the set $E \subset Mat_d^0(\mathbb{Z})$?*

In view of Corollary 1.2 we believe that a similar statement holds true for any finite commutative ring.

Conjecture 1. *Let $\alpha > 0$. Then there exist N and k depending only on α such that for any finite commutative ring R with $|R| \geq N$ and any set $E \subset R$ satisfying $|E| \geq \alpha|R|$ the set $(E-E)\cdot(E-E)$ contains a subring R_0 such that $|R|/|R_0| \leq k$.*

References

[1] M. Björklund, K. Bulinski, *Twisted patterns in large subsets of $\mathbb{Z}^N$*. Preprint.

[2] M. Björklund, A. Fish, *Characteristic polynomial patterns in difference sets of matrices*, Bull. London Math. Soc. (2016) 48 (2): 300-308.

[3] P. Erdös, E. Szemerédi, *On sums and products of integers.* Studies in pure mathematics, 213-218, Birkhäuser, Basel, 1983.

[4] D. Hart, Derrick, A. Iosevich, J. Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Not. IMRN 2007, no. 5

[5] W.T. Gowers, *A new proof of Szemerédi's theorem.* Geom. Funct. Anal. 11 (2001), no. 3, 465-588.

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

[7] S.V. Konyagin, I.D. Shkredov, *New results on sum-products in $\mathbb{R}$*, Preprint, arXiv:1602.03473.

[8] J. Solymosi, *Bounding multiplicative energy by the sumset*, Advances in Mathematics Volume 222, Issue 2, (2009), 402-408.

[9] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Collection of articles in memory of Juriĭ Vladimirovič Linnik, Acta Arith.

School of Mathematics and Statistics, University of Sydney, Australia
E-mail address: alexander.fish@sydney.edu.au