PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 146, Number 8, August 2018, Pages 3449–3453
http://dx.doi.org/10.1090/proc/14078
Article electronically published on May 2, 2018

ON PRODUCT OF DIFFERENCE SETS FOR SETS OF POSITIVE DENSITY

ALEXANDER FISH

(Communicated by Alexander Iosevich)

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 $A \subset \mathbb{Z}$ (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 [6] and it is based on the beautiful previous breakthrough work by Solymosi [7]:

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

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 the set $(E - E) \cdot (E - E)$ possess?

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

Furstenberg [5] noticed an intimate 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 on the Borel σ-algebra of X, and

Received by the editors February 26, 2017, and, in revised form, November 21, 2017.
2010 *Mathematics Subject Classification.* Primary 37A45; Secondary 11E25, 11T30.
Key words and phrases. Difference sets, sum-product estimates.

$T : X \to X$ 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 [5], 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 depending 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 exist $d \leq d_0$ 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 $(E-E)\cdot(E-E) = \mathbf{F}_q$.

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 $L \geq 1$ and every $b \in \mathbb{Z} \setminus \{0\}$ there exists $m \leq \lfloor \frac{1}{\mu(A)^L} \rfloor + 1$ such that*

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

Indeed, let $R(A)$ and $R(B)$ be sets of return times for measurable sets A and B of positive measures. Then choose $N = \lfloor \frac{1}{\nu(B)} \rfloor + 1$. 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 $L = N!$. By Lemma 2.1 there exists $n = n(L, \mu(A))$ such that for every $b \in \mathbb{Z} \setminus \{0\}$ there exists $m \leq n$ with $\{mb, 2mb, \ldots, Lmb\} \subset R(A)$.

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

Proof of Lemma 2.1. [1] Let (X, μ, T) be a measure-preserving system, and let $A \subset X$ be a measurable set, and let $b \in \mathbb{Z} \setminus \{0\}$. We introduce a new product system $Z = \prod_{i=1}^{L} X$ with the transformation $S = \prod_{i=1}^{L} T^{ib}$ and the product measure $\nu = \prod_{i=1}^{L} \mu$. Then (Z, ν, S) is a measure-preserving system, and the set $\tilde{A} = \prod_{i=1}^{L} A$ has measure

$$\nu\left(\tilde{A}\right) = \mu(A)^L > 0.$$

Then by the Poincaré lemma there exists $m \leq \lfloor \frac{1}{\mu(A)^L} \rfloor + 1$ such that

$$\nu(\tilde{A} \cap S^m \tilde{A}) > 0.$$

The latter means that for every $1 \leq i \leq L$ we have

$$\mu(A \cap T^{ibm} A) > 0.$$

Therefore, we have $\{bm, 2bm, \ldots, Lbm\} \in R(A)$ for $m \leq \lfloor \frac{1}{\mu(A)^L} \rfloor + 1$. □

3. Proofs of Corollaries 1.1 and 1.2

Furstenberg [5] 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

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

and

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

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. □

[1] This proof has been proposed to the author by I. Shkredov. The original proof used Szemerédi's theorem and provided a much worse bound on m.

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 $Tx = x + 1 (\bmod N)$ 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[2] $R(E_1) = (E_1 - E_1) + N\,\mathbb{Z}$ 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, 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. ☐

4. Further problems

To formulate the first 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

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

Recall the definition of the upper Banach density of a set $E \subset \mathbb{Z}^2$:

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

Problem 1. 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 $k\,\mathbb{Z} \subset \{x^2 - y^2 \mid (x, y) \in E - E\}$?

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 $E \subset Mat_d^0(\mathbb{Z}) = \{(a_{ij}) \in \mathbb{Z}^{d \times d} \mid tr(a_{ij}) = 0\}$ 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 2. Is it true that given $E \subset \mathbb{Z}^2$ of positive upper Banach density, there exist k_0 depending only on $d^*(E)$ and $k \leq k_0$ such that

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

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

Problem 3. 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 $|R|/|R_0| \leq k$.*

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

Acknowledgments

The work was carried out during a research visit to Weizmann Institute, Israel. The author would like to thank the Feinberg visiting program and the 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, and Ilya Shkredov for his useful comments on the first version of the paper and for allowing us to reproduce his simplified proof of Lemma 2.1.

References

[1] Michael Björklund and Kamil Bulinski, *Twisted patterns in large subsets of* $\mathbb{Z}^N$, Comment. Math. Helv. **92** (2017), no. 3, 621–640. MR3682781

[2] Michael Björklund and Alexander Fish, *Characteristic polynomial patterns in difference sets of matrices*, Bull. Lond. Math. Soc. **48** (2016), no. 2, 300–308. MR3483067

[3] P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in pure mathematics, Birkhäuser, Basel, 1983, pp. 213–218. MR820223

[4] Derrick Hart, Alex Iosevich, and Jozsef Solymosi, *Sum-product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Not. IMRN **5** (2007), Art. ID rnm007, 14 pp. MR2341599

[5] Harry Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204–256. MR0498471

[6] S. V. Konyagin and I. D. Shkredov, *New results on sums and products in* $\mathbb{R}$ (Russian), Tr. Mat. Inst. Steklova **294** (2016), 87–98. Sovremennye Problemy Matematiki, Mekhaniki i Matematicheskoĭ Fiziki. II. MR3628494

[7] József Solymosi, *Bounding multiplicative energy by the sumset*, Adv. Math. **222** (2009), no. 2, 402–408. MR2538014

[8] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression,* Collection of articles in memory of Juriĭ Vladimirovič Linnik, Acta Arith. **27** (1975), 199–245. MR0369312

School of Mathematics and Statistics, University of Sydney, Sydney, NSW, 2006 Australia

Email address: alexander.fish@sydney.edu.au