ON SUM-PRODUCT BASES

NORBERT HEGYVÁRI

ABSTRACT. We investigate a sum-product result says in special case that $\sum_{i=1}^{s} \lambda_i A^2 = \mathbb{F}_p,\ \lambda_i \in \mathbb{F}_p^*$ provided $|A| > p^{\frac{1}{2}+\frac{1}{2(s-1)}}$.

In the second part other sum-product basis is investigated.

2000 Mathematics Subject Classification:11B75,05D10.

Keywords: Thin bases, sum-product bases

1. INTRODUCTION

A classical theorem of Lagrange states that every natural number is the sum of four square numbers. A related question can be considered in $\mathbb{Z}_p$ too; Cauchy observed (and perhaps it motivated the Cauchy-Davenport lemma) that the squares (including 0) form a basis of order two.

A generalization of this question would be the following: let $A \subseteq \mathbb{F}_p$, denote by A^2 the set

$$A^2 = \{a \cdot a' : a, a' \in A\}.$$

Bourgain investigated the following question: what is the minimum of the cardinality of A which ensures that $3A^2 = A^2+A^2+A^2 = \mathbb{F}_p$ (see (see [B]) and [TV]). He concluded that $|A| > p^{3/4}$ is sufficient.

In [GK] Glibichuk and Konyagin proved a more general question: it is proved that if $A, B \subseteq \mathbb{F}_p, \quad |A||B| > p$ then $16AB = \mathbb{F}_p$.

In section 2 we give mild generalization of a result of Bourgain which is related to the question of Glibichuk and Konyagin. Our proof will be similar to the proof in [B] with some additional ingredients.

2. SUM-PRODUCT BASES I

Proposition 2.1. *Let $A, B \subseteq \mathbb{F}_p^*,\ s > 2,$ and $\lambda_1, \lambda_2, \dots, \lambda_s \in \mathbb{F}_p^*$.*

Then every element $x \in \mathbb{F}_p$ can be represented as an element of $\sum_{i=1}^{s} \lambda_i AB$, i.e.

$$\sum_{i=1}^{s} \lambda_i AB = \mathbb{F}_p,$$

provided

$$\min\{|B|^{s/2}|A|^{(s-2)/2}, |A|^{s/2}|B|^{(s-2)/2}\} > p^{s/2}. \tag{2.2}$$

In particular if $B = A$, *or* $B = \frac{1}{A}$ *respectively we have*

$$\sum_{i=1}^{s} \lambda_i A^2 = \mathbb{F}_p,$$

and

$$\sum_{i=1}^{s} \lambda_i \frac{A}{A} = \mathbb{F}_p,$$

resp., assuming

$$|A| > p^{\frac{1}{2}+\frac{1}{2(s-1)}}. \tag{2.3}$$

Remark:

Our result gives a new result in cases $4 \le s \le 15$. Similar and general result obtained later and independently by Hart and Iosevich (see [HI])

Proof. Let $B(x)$ be the indicator function of B, i.e. $B(x) = 1$ if $x \in B$ and 0 otherwise. If $u : \mathbb{Z}_p \to \mathbb{C}$ is any function then its Fourier coefficient is defined as $\widehat{u}(r) = \frac{1}{p}\sum_x u(x)e(-xr)$, where as usual $e(x) = exp(2\pi ix/p)$. We shall use some elementary fact on Fourier transforms.

Let $\varphi_i(x) = |A|^{-1}\sum_{a\in A} B(\frac{x}{\lambda_i a})$, $i = 1, 2, \dots, s$. Since A and the set $\{\lambda_i\}$ are in $\mathbb{F}_p^*$ hence $\frac{x}{\lambda_i a}$ is well-defined. Clearly for every i, $0 \le \varphi_i(x) \le 1$ and $\varphi_i(x) \ne 0$ if and only if for some $a \in A$ $B(\frac{x}{\lambda_i a}) \ne 0$, i.e. there exists a $b \in B$ such that $\frac{x}{\lambda_i a} = b$, or equivalently $x = \lambda_i ab \in \lambda_i AB$. Hence $\varphi_(x)$ also indicates elements of $\lambda_i AB$ (although it is not necessary an indicator).

Let the convolution of two functions is defined by $u(x) * v(x) = \sum_y u(y)v(x-y)$ (i.e. if $u(x), v(x)$ are indicators then the convolution is the number of solution to $x = u + v;\ u \in U, v \in V$.) Convolution for terms more than two is defined inductively. Thus $\varphi_1(x) * \varphi_2(x) * \dots * \varphi_s(x)$ is positive for $x \in \sum_{i=1}^{s} \lambda_i AB$.

By the definition it is not too hard to check that for every $u(x), v(x)$, $\widehat{u * v(r)} = \widehat{u}(r) \cdot \widehat{v}(r)$. By the inversion-formula we obtain that

$$\varphi_1(x) * \varphi_2(x) * \dots * \varphi_s(x) = \sum_r \widehat{(\varphi_1(x) * \varphi_2(x) * \dots * \varphi_s)}(x)e(rx) =$$

$$= \sum_r \widehat{\varphi_1}(x) \cdot \widehat{\varphi_2}(x) \cdots \widehat{\varphi_s}(x)e(rx).$$

Now for every i we express $\widehat{\varphi_i}(r)$ by

$$\widehat{\varphi_i}(r) = \frac{1}{p}\sum_x \varphi_i(x)e(-xr) = \frac{1}{p}\sum_x (|A|^{-1}\sum_{a\in A} B(\frac{x}{\lambda_i a}))e(-xr) =$$

$$= |A|^{-1} \sum_{a\in A} (\frac{1}{p} \sum_{x} B(\frac{x}{\lambda_i a}) e(-xr)).$$

Use $z = \frac{x}{\lambda_i a}$, and thus $x = z\lambda_i a$, and if x runs in $\mathbb{Z}_p$ then z so is, thus we have

$$\widehat{\varphi_i}(r) = |A|^{-1} \sum_{a\in A} (\frac{1}{p} \sum_{z} B(z) e(-r\lambda_i a \cdot z) =$$

$$= |A|^{-1} \sum_{a\in A} \widehat{B}(r\lambda_i a).$$

For $r = 0$

$$\widehat{\varphi_i}(0) = |A|^{-1} \sum_{a\in A} \widehat{B}(0) = |A|^{-1} \sum_{a\in A} \frac{|B|}{p} = \frac{|B|}{p}.$$

Separating the the term $r = 0$ and using the triangle inequality we have the estimation

$$\varphi_1(x) * \varphi_2(x) * \cdots * \varphi_s(x) \geq \frac{|B|^s}{p^s} - \sum_{r\in \mathbb{F}_p^*} \prod_{i=1}^{s} |\widehat{\varphi}(r)|.$$

Now we give an upper bound for $\widehat{\varphi_i}(r)$ if r differs from 0. By the triangle and Cauchy inequalities

$$|\widehat{\varphi_i}(r)| = |A|^{-1} | \sum_{a\in A} \widehat{B}(r\lambda_i a)| \leq$$

$$\leq |A|^{-1} \sum_{a\in A} |\widehat{B}(r\lambda_i a)| \leq |A|^{-1} |A|^{1/2} \sum_{a\in A} (|\widehat{B}(r\lambda_i a)|^2)^{1/2} \leq$$

which can be estimated by the Parseval formula as

$$\leq |A|^{-1/2} \sum_{a\in A} (|\widehat{B}(r\lambda_i a)|^2)^{1/2} \leq |A|^{-1/2} \sum_{r} (|\widehat{B}(r)|^2)^{1/2} = \sqrt{\frac{|B|}{|A|p}}. \tag{2.4}$$

Now we bound $\varphi_1(x) * \varphi_2(x) * \cdots * \varphi_s(x)$ as follows:

$$\varphi_1(x) * \varphi_2(x) * \cdots * \varphi_s(x) \geq \frac{|B|^s}{p^s} - \sum_{r\in \mathbb{F}_p^*} \prod_{i=1}^{s} |\widehat{\varphi_i}(r)| \geq$$

by the Hölder inequality we get

$$\geq \frac{|B|^s}{p^s} - \max_{r\in \mathbb{F}_p^*} (\prod_{i=1}^{s} |\widehat{\varphi_i}(r)|)^{(s-2)/s} \cdot \prod_{i=1}^{s} (\sum_{r} |\widehat{\varphi_i}(r)|^2)^{1/s}.$$

By the Parseval formula

$$\sum_{r} |\widehat{\varphi_i}(r)|^2 = \frac{1}{p} \sum_{x} |\varphi_i(x)|^2 \leq \frac{1}{p} |B| \max |\varphi_i(x)|^2 = \frac{|B|}{p}, \tag{2.5}$$

since $|\varphi_i(x)| \leq 1$.

Finally by (2.4) and (2.5) we have

$$\varphi_1(x) * \varphi_2(x) * \cdots * \varphi_s(x) \geq \frac{|B|^s}{p^s} - (\frac{|B|}{|A|p})^{(s-2)/2}\frac{|B|}{p} > 0,$$

assuming

$$|B|^{s/2}|A|^{(s-2)/2} > p^{s/2},$$

which gives (by a similar conclusion changing the role of A and B) (2.2) .

When $B = A$ or $B = A^{-1}$, we have that $|A| = |B|$ and hence (2.2) gives in this special case

$$|A| > p^{\frac{s}{2(s-1)}}.$$

□

3. Sum-product bases II

Note that for $\lambda, \mu \in \mathbb{F}_p^*$ the multiplication $(\lambda + \mu)A$ is not necesaary distributive, i.e. $(\lambda + \mu)A = \lambda A + \mu A$ does not hold for every $A \subseteq \mathbb{F}_p^*$. (We can assert just $(\lambda + \mu)A \subseteq \lambda A + \mu A$.)

Hence for $B = \{b_1, b_2, \ldots, b_t\} \subseteq \mathbb{F}_p^*$, and $A \subseteq \mathbb{F}_p^*$ it is reasonable to introduce the multiplication $B * A$ as

$$B * A := \sum_{i=1}^{t} b_i A.$$

(Remark that this multiplication is also not necessary commutative.) We will ask that for a given set A which condition of B implies

$$B * A = \mathbb{F}_p.$$

In the present section we consider a well-structured set of B; it will be a set of *multiplicative* Hilbert-cube. It is defined in an analogous way as the *additive* Hilbert cube. Generally if X is a subset of a given semigroup $\{L, \circ\}$ then the cube H generated by X is

$$H(X) := \{\bigcirc_{x\in Y} x : Y \subseteq X,\ |Y| < \infty\}.$$

So when $\circ = +$, then we get the *additive* Hilbert cube, i.e.

$$H_{add}(X) := \{\sum_{x\in Y} x : Y \subseteq X,\ |Y| < \infty\},$$

and when $\circ = \cdot$, then the *multiplicative* Hilbert-cube is

$$H_{mult}(X) := \{\prod_{x\in Y} x : Y \subseteq X,\ |Y| < \infty\}.$$

In this section we prove:

Theorem 3.1. *Let $A \subseteq \mathbb{F}_p$, $|A| > 2$, and let $q(x) = 1 + u_1 x + \cdots + u_D x^D$ be a polynomial, and let $Q = \{q(r) : r \in \mathbb{F}_p\}$ be a multi-set of the values.*

There exist a multi-subset B of Q, $c_1 > 0$ for which

$$|B| < c_1 \log \frac{\log p/D}{log|A|} + 2D + 3, \tag{3.1}$$

and

$$H_{mult}(B) * A = \sum_{h \in H_{mult}(B)} h \cdot A = \mathbb{F}_p.$$

Proof of Theorem 3.1. For the proof we need the following lemma:

Lemma 3.2. *Let $A, B \subseteq \mathbb{F}_p$. Let $S(r) := |\{A + B \cdot q(r)\}|$. We have*

$$\max_{r \in \mathbb{F}_p} S(r) \geq \frac{p|A||B|}{p + D|A||B|}, \tag{3.2}$$

where $D = \deg q(x)$.

A similar idea as this lemma is used in [K].

Proof of Lemma 3.2. Denote by $R(r, m)$ the number of representation of m in the form $m = a + q(r) \cdot b$. By the Cauchy inequality we have

$$(\sum_m R(r, m))^2 \leq S(r)(\sum_m R^2(r, m)),$$

and clearly $\sum_m R(r, m) = |A||B|$, hence we obtain

$$|A|^2|B|^2 \leq S(r)(\sum_m R^2(r, m)). \tag{3.3}$$

Since $R^2(r, m)$ counts the number of quadruples (a, a', b, b') for which $m = a + q(r) \cdot b = a' + q(r) \cdot b'$, we argue, that r solves the equation $q(r) = \frac{a'-a}{b-b'}$, which has at most $D = \deg q(x)$ solutions. Take

$$\sum_r \sum_m R^2(r, m) = \sum_r \sum_{m;a=a'} R^2(r, m) + \sum_r \sum_{m;a \neq a'} R^2(r, m),$$

(clearly $a = a' \Leftrightarrow b = b'$). Now $\sum_r \sum_{m;a=a'} R^2(r, m) = \sum_r |A||B| = p \cdot |A||B|$, furthermore since there are at most D solutions of $q(r) = \frac{a'-a}{b-b'}$, we get $\sum_r \sum_{m;a \neq a'} R^2(r, m) \leq D \cdot |A|^2|B|^2$.

Now by (3.3)

$$p \cdot |A|^2|B|^2 \leq \sum_r S(r)(\sum_m R^2(r, m)) \leq$$

$$\leq p \cdot \max_r S(r) \cdot (\sum_m R^2(r, m)) \leq p \cdot \max_r S(r) \cdot (p \cdot |A||B| + D \cdot |A|^2|B|^2),$$

from which estimating $\max_r S(r)$ we obtain (3.2). □

Now we follow an iteration step. We define a sequence of sets $A_0, A_1, \dots$ and sequence $b_0, b_1, \dots$ of the values of the range of Q as follows: let $A_0 = A$ and $b_0 = q(0) = 1$. By Lemma (3.2) we obtain an r_1, such that $S(r_1) \geq \frac{p|A|^2}{p+D|A|^2}$; so let $A_1 = A_0 + q(r_1) \cdot A_0$ and thus

$$|A_1| \geq \frac{p|A_0|^2}{p + D|A_0|^2}.$$

Generally assume the sets $A_0, A_1, \dots A_k$ and the sequence $b_0, b_1, \dots b_k$ have been defined, then by Lemma (3.2) we have an r_{k+1}, such that for the set $A_{k+1} := A_k + q(r_{k+1})A_k$ we get

$$|A_{k+1}| \geq \frac{p|A_k|^2}{p + D|A_k|^2}. \tag{3.4}$$

Repeat this process unless we have $\frac{p}{p+D|A_n|^2} < \frac{9}{10}$, or equivalently

$$|A_n| > \sqrt{\frac{p}{9D}}. \tag{3.5}$$

We prove that this process is terminated, i.e. there exists an n for which (3.5) holds. From (3.4) and from the definition of n we conclude that for $1 \leq k < n$

$$|A_{k+1}| \geq \frac{p|A_k|^2}{p + D|A_k|^2} \geq \frac{9}{10}|A_k|^2,$$

and by induction it is not too hard to check that

$$|A_{k+1}| \geq \frac{10}{9} \cdot \big(9|A|/10\big)^{2^k}. \tag{3.6}$$

By (3.5) and (3.6) we have that

$$n \leq c_1 \log \frac{\log p/D}{log|A|} \tag{3.7}$$

for some $c_1 > 0$.

Repeat once more this process any easy calculation shows that $|A_{n+1}| \geq \frac{p}{2D}$. Finally let $r_{n+2} = \dots = r_{n+2+2D} = 0$, and then by the Cauchy Davenport lemma we obtain that

$$A_{n+2+2D} = \mathbb{F}_p.$$

In the rest of the proof we check that for the set B (3.1) holds and $A_{n+2+2D} = H_{mult}(B) \cdot A$. For $0 \leq k \leq n+2+D$, $b_k = q(r_k)$, $B = \{b_k : 0 \leq k \leq n+2+D\}$ hence by (3.7) we obtain (3.1).

Finally by induction we prove that

$$A_k = H_{mult}(b_0, \dots, b_k)A. \tag{3.8}$$

For $k = 0$ $A_0 = q(0)A = A$. From (3.8)

$$A_{k+1} = A_k + b_{k+1}A_k = H_{mult}(b_0, \dots, b_k)A + b_{k+1} \cdot H_{mult}(b_0, \dots, b_k)A,$$

in the first term there are those $h \in H_{mult}(b_0, \dots, b_{k+1})$ which do not contain b_{k+1}, while in the second which do. □

Acknowledgement: This note is supported by "Balaton Program Project" and OTKA grants T0 43623,49693,38396.

References

[B] J. Bourgain: Mordell's exponential sum estimate reviseted, J. of the Amer. Math. Soc. 18, N.2 p. 477-499

[GK] A.A. Glibichuk, S.V. Konyagin: Additive properties of product sets in fields of prime order, Centre de Recherches Mathmatiques CRM Proceedings and Lecture Notes AMS 2006 (1-8)

[TV] T. Tao, V. Vu: Additive Combinatorics, Cambridge Univ. Press, Cambridge, 2006

[HI] D. Hart, A. Iosevich: Sums and products in finite fields: an integral geometric viewpoint, arXiv 0705,4256v4 (math. NT)

[K] S. Konyagin: A Sum-Product Estimate in Fields of Prime Order, arXiv:math.NT/0304217 v1

Norbert Hegyvári
ELTE TTK
Eötvös University
Institute of Mathematics
H-1117 Pázmány st. 1/c
Budapest
Hungary
e-mail: hegyvari@elte.hu