SOME REMARKS ON MULTILINEAR EXPONENTIAL SUMS WITH AN APPLICATION

NORBERT HEGYVÁRI

Abstract. A sum-product equation is considered in prime fields. We bound a multilinear exponential sum with an additional requirement for some sets.

2000 Mathematics Subject Classification:11L07, 11B75.

Keywords: Multilinear exponential sum, sum-product problem, Sárközy's type sum-product equations

1. Introduction

Let $\mathbb{F}_p$ be the prime field with multiplicative subgroup denoted by $\mathbb{F}_p^*$. A well-known estimation for the double exponential sums is the following upper bound

$$\Big|\sum_{x\in X,y\in Y} e(xy)\Big| < \sqrt{p|X||Y|}, \tag{0.1}$$

noted by Vinogradov. One of an interesting application of (0.1) is due to Sárközy [6]. He proved that for $A, B, C, D \subseteq \mathbb{F}_p$, the equation

$$a + b = cd,\ (a, b, c, d) \in A \times B \times C \times D$$

has a solution, provided

$$|A||B||C||D| > p^3. \tag{1.1}$$

A new proof avoids exponential sums was found by Cilleruelo (see [4]).

In [6] the author derived some corollary of this equation; for instance he investigated the Schur type equation

$$a + b = x^k, \tag{1.2}$$

$a \in A,\ b \in B, x \in \mathbb{F}_p$ i.e. a sumset intersects a subgroup of $\mathbb{F}_p$:

$$A + B \cap H \neq \emptyset;\ H < \mathbb{F}_p. \tag{1.3}$$

Let us remark here that a deep theorem of Bourgain (see [1]) yields that for every k there exists an $\varepsilon = \varepsilon(k) > 0$ such that (1.3) is solvable when $|A||B| > p^{2-\varepsilon}$ (ε is ineffective).

In [6] it is also noted that (1.1) is best possible apart the constant factor.

Date: September 8, 2010.

A more general question would be the investigation of the equations type

$$a + b = F_p(c, d).$$

Let us mention that it is close to the problem of *complete expander polynomials.* A polynomial $f(x_1, \dots, x_r)$ is said to be complete expander, if there exist fix $\delta > 0, \varepsilon = \varepsilon(\delta) > 0$ such that $|f(A_1, \dots, A_r)| \geq \min\{p, |A_r|)^{1+\varepsilon}\}$, provided $|A_1| \leq \cdots \leq |A_r|, |A_r| \gg p^{\delta}$.

Indeed it is not too hard to see that the solvability of the equation

$$a + b = F_p(c, d), |A||B||C||D| > p^{\gamma};\ \gamma > 0$$

implies that $f(x, y, z, w) = x+y+F(z, w)$ is a complete expander when $|A||B||C||D| > p^{\gamma}$, (namely $f(A, B, C, D)$ covers $\mathbb{F}_p$.)

We merely mention that a result of Bourgain also comes from (1.1); he 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 [8], [9] and [10]). He concluded that $|A| > p^{3/4}$ is sufficient.

In [5] we investigate this problem for functions $F_p(x, y) = x^{1+u}y + x^{2-u}h(y)$ for any p, where we fix $u \in \{0, 1\}$ and any non constant polynomial $h(y) \in \mathbb{Z}[y]$, furthermore for $F_p(x, y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^*$ and $u \in \{0, 1\}$ is fixed. We proved that if F_p is one of the two families of functions defined above, then there exist real numbers $0 < \delta, \delta' < 1$ such that for any p and for any sets $A, B, C, D \subseteq \mathbb{F}_p$ fulfilling the conditions

$$|C| > p^{1/2-\delta}, \quad |D| > p^{1/2-\delta} \quad |A||B| > p^{2-\delta'},$$

there exist $a \in A, b \in B, c \in C, d \in D$ solving the equation $a + b = F_p(c, d)$.

In [7] Shparlinski proved that restricting the region of possible values for $|A|, |B|, |C|, |D|$ one can relax the condition (1.1). He proved that for any fixed $\varepsilon > 0$, there exists $\delta > 0$ such that if

$$|A| > p^{1/2+\varepsilon},\ |B| > p^{\varepsilon},\ |C||D| > p^{2-\delta},$$

then the equation $a+b = cd$ can be solved, roughly speaking; restricting the possible region of the sets the power 3 in (1.2) can be decrease to $\approx 5/2$. (His proof works actually in arbitrary finite fields.)

In section 2 we investigate any other possibilities to restrict the cardinalities of the sets. We will investigate the 'opposite' of Shparlinski's case; namely when $|A||B| > p^{2-\alpha}$, (α runs $0 < \alpha < 3/16$) and we decrease the cardinalities of C and D under some conditions for the sets (in this case we decrease (1.2) to $\approx 8/3$).

A strong generalization of (0.1) is proved recently by Bourgain. He proved in [1] the following result:

Theorem 1.1. *There is a constant $C > 1$ such that for every $0 < \delta < 1$, and $r \in \mathbb{N},\ r > C/\delta$, if $A_1, A_2, \ldots, A_r \subseteq \mathbb{F}_p$, $|A_i| > p^\delta$ for $1 \leq i \leq r$, p is a prime which is large enough, then*

$$\Big|\sum_{x_1 \in A_1, \ldots, x_r \in A_r} e(x_1 x_2 \cdots x_r)\Big| < p^{-\delta'} |A_1||A_2| \cdots |A_r|,$$

where $\delta' > C^{-r}$.

This important theorem is related to extractors with $\delta-$entropy (see e.g. [3] and [5]).

In Theorem 1.1 when r approaches to infinity then C^{-r} tends to 0 and we can conclude that $\delta' > 0$.

In section 3 we will show that some restriction for three sets of the collection of $A_1, A_2, \ldots, A_r$ we obtain a δ' depending only on the ratio of the cardinalities of these given three sets.

At this estimation will play a crucial rule to give an upper bound for multiplicative energy defined by $E_\times(X, Y) = \sum_z r^2_{X,Y}(z)$, where $r_{X,Y}(z) := |\{(x, y) \in X \times Y : z = x \cdot y\}|$.

2. Sárközy's type sum-product equations

In this section we will consider the following case; let $A, B \subseteq \mathbb{F}_p$ and let $H < \mathbb{F}_p^*$. We ask the solvability of the equation

$$a + b = h;\ (a, b, h) \in A \times B \times H.$$

Restricting the cardinality of H to some region we improve the result of Sárközy:

Theorem 2.1. *Let $A, B \subseteq \mathbb{F}_p$, $H < \mathbb{F}_p$. Write $|A||B| = p^{2-2\alpha}; |H| = p^\beta$. Then the equation*

$$a + b = h;\ (a, b, h) \in A \times B \times H$$

is solvable, provided

$$\beta > \frac{8\alpha + 1}{3}.$$

Essentially in the same way we can prove a more general result. Assume that $C, D \subseteq \mathbb{F}_p^*$, and assume that the cardinality of the generating subgroups of C and D are close to $|C|$ and $|D|$ respectively. We have

Theorem 2.2. *Assume that $C, D \subseteq \mathbb{F}_p^*$, $A, B \subseteq \mathbb{F}_p$. Let $|A||B| = p^{2-2\alpha}; |C| = p^\beta,\ |D| = p^\gamma,\ \langle C\rangle = G_1, \langle D\rangle = G_2, |G_1| = p^\delta, |G_2| = p^\theta, \max\{\delta, \theta\} < 3/4$. Then the equation*

$$a + b = cg \quad (a, b, c, g) \in A \times B \times G_1 \times G_2,$$

is solvable, provided

$$\frac{5}{16}(\beta+\gamma) > \alpha + \frac{1+\delta+\theta}{8}.$$

Corollary 1. *Let $A, B \subseteq \mathbb{F}_p$, $H < \mathbb{F}_p$. Write $|H| = p^{\beta}$. Then the equation*

$$a+b=h;\ \ (a,b,h) \in A \times B \times H$$

is solvable, provided

$$|A||B||H|^2 > p^{\frac{9+5\beta}{4}}.$$

Note when $0 < \beta < \frac{3}{5}$, then it improves the Sárközy's result.

Proof of Theorem 2.1

For the proof we need some lemmas. Recall that E_s^+, the additive energy is defined by $E_s^+(X) = |\{(x_1,\dots,x_s,x_1',\dots,x_s') \in X^{2s} : x_1 + \dots + x_s = x_1' + \dots + x_s'\}|$.

Lemma 2.3. *Let $C, D \subseteq \mathbb{F}_p$, and let $S(r) = \sum_{c\in C, g\in D} e(r(c\cdot g))$, $r \in \mathbb{F}_p^*$. Then*

$$|S(r)| \le |C|^{1/2}|D|^{1/2}(pE_2^+(C)E_2^+(D))^{1/8}.$$

Remark: 1. One can prove by induction the more general estimation which sounds as follows: for every $m, n \in \mathbb{N}$

$$|S(r)| \ll_k |C|^{1-1/2^{n+1}}|D|^{1-1/2^m}(pE_{2^{n+1}}^+(C)E_{2^m}^+(D))^{1/2^{n+m+1}}.$$

For $n=0; m=1$ it is Lemma 7.1 in [3]. For convenience of the readers we present here the short proof. Note that in the case when $|C||D| < p$, this estimation is sharper for $|S(r)|$ than (0.1) and this estimation can be improved if we have an extra information for the additive energy for the sets C, and D (and some cases the above mentioned generalization also can be applied). Indeed using the fact that for every set X the bound $E_2^+(X) < |X|^3$ holds we obtain

$$|C|^{1/2}|D|^{1/2}(pE_2^+(C)E_2^+(D))^{1/8} < |C|^{1/2}|D|^{1/2}p^{1/2}.$$

Proof. By the triangle inequality and the Cauchy-Schwarz inequality we obtain

$$|S(r)|^2 \le |C| \sum_{c\in C} \sum_{g,g'\in D} e(r(c\cdot(g-g'))).$$

Changing the order of the summation and again by the Cauchy-Schwarz

$$|S(r)|^4 \le |C|^2|D|^2 \sum_{g,g'\in D} \sum_{c,c'\in C} e(r((c-c')\cdot(g-g'))).$$

Finally using the Vinogradov estimation for the last sum, we obtain the claim of the lemma.

∎

A nice application of Stepanov-method ([8] Ch. 9) one can find the following estimation:

Lemma 2.4. *Let $G < \mathbb{F}_p^*$, $|G| \ll p^{3/4}$, $Y \subseteq G$, then*

$$E_2^+(Y) \ll |G||Y|^{3/2}.$$

We note that for the proof of Theorem 2.1 we will use the case $Y = G$; i.e. we use $E_2^+(Y) \ll |G|^{5/2}$. For the proof of Theorem 2.2 is necessary the sharper form.

Finally we get

Lemma 2.5. *Assume that for some $M > 0$, $\max_{r \neq 0} |S(r)| \leq M$. If*

$$\sqrt{|A||B|}|C||D| > pM,$$

then the equation $a + b = cd$ $(a, b, c, d) \in A \times B \times C \times D$, is solvable.

The proof of the lemma is simple writing the indicated exponential sum of equation $a + b = cd$ (see [6]).

Now we are going to give a bound for M.

Firstly we will do it under the condition of Theorem 2.2 and after for the simplicity we end the proof under the condition of Theorem 2.1. Assume that $C, D \subseteq \mathbb{F}_p^*$ and let the generating subgroup of C and D, $\langle C \rangle = G_1, \langle D \rangle = G_2$ respectively.

By Lemma 2.1 and 2.2 we conclude that

$$|S(r)| \leq |C|^{1/2}|D|^{1/2}(pE_4^+(C)E_4^+(D))^{1/8} \ll$$

$$\ll p^{1/8}|C|^{11/16}|D|^{11/16}|G_1|^{1/8}|G_2|^{1/8}. \tag{2.1}$$

By Lemma 2.3 we obtain that the equation $a + b = cd$ $(a, b, c, d) \in A \times B \times C \times D$, is solvable, provided

$$|A|^{1/2}|B|^{1/2}|C|^{5/16}|D|^{5/16} \gg p^{9/8}|G_1|^{1/8}|G_2|^{1/8}. \tag{2.2}$$

Writing $|A||B| = p^{2-2\alpha}; |C| = p^\beta,\ |D| = p^\gamma, |G_1| = p^\delta, |G_2| = p^\theta$ (2.2) is equivalent to

$$1 - \alpha + \frac{5}{16}(\beta + \gamma) > \frac{9 + \delta + \theta}{8},$$

which gives Theorem 2.2. When $|A||B| = p^{2-2\alpha}; |H| = p^\beta$, it gives the constraint

$$\beta > \frac{8\alpha + 1}{3}.$$

and we obtain Theorem 2.1.

3. Multilinear exponential sum with restricted sets

In this section we prove that under some restriction for three sets of the sets $A_1, A_2, A_3, \dots A_n$ we obtain some explicit bound for a multilinear exponential sum.

Theorem 3.1. *Let $\varepsilon > 0, p > p(\varepsilon),\ A_1, A_2, A_3, \dots A_n \subseteq \mathbb{F}_p, n \geq 3$. Assume that for $i = 2, 3$ $|A_i| \geq c_i\sqrt{p} > 0$,*

$$|A_i - A_i| \leq 8c_i^2|A_i|, \tag{3.1}$$

and

$$0 < \alpha \leq \frac{\ln\{|A_1|/(|A_2||A_3|)^{13/8+\varepsilon}\}}{2\ln p} + 5/8. \tag{3.2}$$

Then

$$|S| := \Big|\sum_{x_1\in A_1, x_2\in A_2, \dots, x_n\in A_n} e(x_1\cdots x_n)\Big| < p^{-\alpha}\cdot\prod_{i=1}^{n}|A_i|.$$

Corollary 2. *Let $|A_2|, |A_3| \asymp \sqrt{p}$, $|A_1| > p^{3/8}$ and assume* (3.1) *holds. Then*

$$|S| := |\sum_{x_1\in A_1, x_2\in A_2, \dots, x_n\in A_n} e(x_1\cdots x_n)| < p^{-\alpha}\cdot\prod_{i=1}^{n}|A_i|,$$

where $0 < \alpha < \frac{\ln|A_1|}{2\ln p} - \frac{3}{16}$.

Proof of Theorem 3.1

We use the notation $\widehat{f}(y) = \sum_x f(x)\cdot e(xy)$.
Write the sum

$$S = \sum_{x_1\in A_1, x_2\in A_2, \dots, x_n\in A_n} e(x_1\cdots x_n) = \sum_{x_2\in A_2, x_3\in A_3, \dots, x_n\in A_n}\sum_{x_1\in A} e(x_1(x_2\cdots x_n)) =$$

$$= \sum_{x_2\in A_2, x_3\in A_3, \dots, x_n\in A_n} \widehat{A}_1(x_2\cdots x_n) = \sum_{x_2, x_3 \dots, x_n\in\mathbb{F}_p} A_2(x_2)\cdots A_n(x_n)\widehat{A}_1(x_2\cdots x_n),$$

where $A_i(x_i)$ is the indicator of the set A_i. Write $z = x_2\cdots x_n$, then we have

$$S = \sum_{z\in\mathbb{F}_p} r(z)\widehat{A}_1(z),$$

where

$$r(z)_{A_1,\dots,A_n} = r(z) =$$

$$= |\{(x_2, \dots, x_n) : x_2 \in A_2, x_3 \in A_3, \dots, x_n \in A_n;\ z = x_2\cdots x_n\}|.$$

Thus by the Cauchy-Schwarz and the Parseval

$$|S| \leq \sqrt{\sum_{z\in\mathbb{F}_p} r^2(z)} \cdot \sqrt{\sum_{z\in\mathbb{F}_p} |\widehat{A}_1(z)|^2} = \sqrt{E_\times(A_2, A_3, \dots, A_n)} \cdot \sqrt{p|A_1|},$$

where $E_\times(A_2, A_3, \dots, A_n)$ is the multiplicative energy of the sets $A_2, A_3, \dots, A_n$. The n terms multiplicative energy is defined by

$$E_\times(X_1, \dots, X_n) =$$
$$= |\{(x_1, \dots, x_n, x'_1, \dots, x'_n) \in (X_1 \times \cdots \times X_n)^2 : x_1 \cdots x_n = x'_1 \cdots x'_n\}|.$$

Lemma 3.2. *Let $X_1, X_2, \dots X_n \subseteq \mathbb{F}_p$ and denote the multiplicative energy of them by $E_\times(X_1, \dots, X_n)$.*

We have

$$E_\times(X_1, \dots, X_n) \leq |X_1|^2 E_\times(X_2, \dots, X_n).$$

Proof. By the definition of the multiplicative energy

$$E_\times(X_1, \dots, X_n) =$$
$$= |\{(x_1, \dots, x_n, x'_1, \dots, x'_n) \in (X_1 \times \cdots \times X_n)^2 : x_1 \cdots x_n = x'_1 \cdots x'_n\}|$$

hence

$$E_\times(X_1, \dots, X_n) =$$
$$= |\bigcup_{x_1, x'_1 \in X_1} \{(x_2, \dots, x_n, x'_2, \dots, x'_n) \in (X_2 \times \cdots \times X_n)^2 : x_1 \cdots x_n = x'_1 \cdots x'_n\}|.$$

Fix a pair $x_1, x'_1 \in X_1$. Now the set

$$\{(x_2, \dots, x_n, x'_2, \dots, x'_n) \in (X_2 \times \cdots \times X_n)^2 : x_1 \cdots x_n = x'_1 \cdots x'_n\}|$$

can be written as

$$\{(x_2, \dots, x_n, x'_2, \dots, x'_n) \in (X_2 \times \cdots \times X_n)^2 : x_2 \cdots x_n = (x_1^{-1} x'_1) x_2 \cdots x'_n\}$$

Hence

$$|\{(x_2, \dots, x_n, x'_2, \dots, x'_n) \in (X_2 \times \cdots \times X_n)^2 : x_2 \cdots x_n = (x_1^{-1} x'_1) x_2 \cdots x'_n\}| =$$
$$= \sum_{z\in\mathbb{F}_p} r'(z) r'(x_1^{-1} x'_1 z)$$

where $r'(u) = |\{(x_2, \dots, x_n) : x_2 \in A_2, x_3 \in A_3, \dots, x_n \in A_n;\ u = x_2 \cdots x_n\}|$.

Finally by using Cauchy-Schwarz we obtain

$$E_\times(X_1, \dots, X_n) \leq$$
$$\leq \sum_{x_1, x'_1 \in X_1} |\{(x_2, \dots, x_n, x'_2, \dots, x'_n) \in (X_2 \times \cdots \times X_n)^2 : x_1 \cdots x_n = x'_1 \cdots x'_n\}| \leq$$
$$\leq \sum_{x_1, x'_1 \in X_1} \sum_{z\in\mathbb{F}_p} r'(z) r'(x_1^{-1} x'_1 z) \leq |X_1|^2 \sqrt{\sum_{z\in\mathbb{F}_p} r'^2(z)} \sqrt{\sum_{z\in\mathbb{F}_p} r'^2((x_1^{-1} x'_1) z)} =$$

$$= |X_1|^2 \sum_{z\in\mathbb{F}_p} r'^2(z) = |X_1|^2 E_\times(X_2,\dots,X_n),$$

using the fact if z runs on $\mathbb{F}_p$ then $(x_1^{-1}x_1')z$ so does. $\square$

Iterating the result of Lemma 3.2 we can estimate $|S| \le \sqrt{E_\times(A_2,A_3,\dots,A_n)}\cdot\sqrt{p|A_1|}$ as

$$|S| \le \prod_{i=4}^{n} |A_i| \sqrt{E_\times(A_2,A_3)} \cdot \sqrt{p|A_1|}.$$

Lemma 3.3. *Let $B,C \subseteq \mathbb{F}_p^*$. Then*

$$E_\times(B,C) \le \sqrt{E_\times(B,B)E_\times(C,C)}.$$

This lemma is Corollary 2.10 in [8] proved for additive energy. The proof for multiplicative energy is the same and short, so we prove for seek of completeness.

Proof. Let $q_{U,V}(n) := |\{(u,v)\in U\times V : n = u/v\}|$. Clearly

$$\sum_z q_{B,C}^2(z) = \sum_z q_{C,B}^2(z) = \sum_z r_{B,B}(z) r_{C,C}(z),$$

since

$$\sum_z q_{B,C}^2(z) = \sum_z q_{C,B}^2(z) = \sum_z r_{B,C}(z) r_{C,B}(z) =$$

$$= |\{(b,,b',c,c')\in B\times B\times C\times C : b/c = b'/c'\}| =$$

$$= |\{(b,,b',c,c')\in B\times B\times C\times C : c/b = c'/b'\}| =$$

$$= |\{(b,,b',c,c')\in B\times B\times C\times C : cb' = bc'\}|.$$

By the Cauchy-Schwarz inequality we obtain the result. $\square$

Now by Lemma 3.3 we have with $B = A_2, C = A_3$,

$$|S| \le \prod_{i=4}^{n} |A_i| (E_\times(A_2,A_2))^{1/4} \cdot (E_\times(A_3,A_3))^{1/4} \cdot \sqrt{p|A_1|}. \tag{3.3}$$

Lemma 3.4. *Let $U \subseteq \mathbb{F}_p$. Assume that $|U-U| \le 8\frac{|U|^3}{p}$*

$$E_\times(U,U) \le 2^9 \frac{|U|^{29/4}}{p^{9/4}} \ln|U|. \tag{3.4}$$

Proof. For the proof of (3.4) we use Theorem 1.1 in [3]:

Let $U \subseteq \mathbb{F}_p$. We have

$$E_\times(U,U) \le 2\sqrt{2}\sqrt[4]{|U-U| + \frac{8|U|^3}{p}}|U|^{5/4}|U-U|\sqrt[4]{|2U-2U|}\ln|U|. \tag{3.5}$$

Now by the Plünnecke-Ruzsa inequality and the bound $|U-U| \le 8\frac{|U|^3}{p}$ we have

$$|2U-2U| \le \frac{|U-U|^4}{|U|^3} \le \frac{2^{12}|U|^9}{p^4}.$$

and using the bound $|U-U| \le 8\frac{|U|^3}{p}$ again in (3.5) an easy calculation gives the upper estimation for $E_\times(U,U)$.

□

Now we turn to the estimation of $|S|$. By (3.1) we can use (3.5) for the sets A_2 and A_3. We obtain

$$|S| \le \prod_{i=4}^n |A_i|(E_\times(A_2,A_2))^{1/4} \cdot (E_\times(A_3,A_3))^{1/4} \cdot \sqrt{p|A_1|} \le$$

$$\le 4\prod_{i=4}^n |A_i|\sqrt{p|A_1|}\frac{(|A_2||A_3|)^{29/16}}{p^{9/8}}\ln|A_2|\ln|A_3| =$$

$$= 4\prod_{i=4}^n |A_i||A_1||A_2||A_3|p^{-\alpha}p^{\alpha-5/8}|A_1|^{-1/2}(|A_2||A_3|)^{13/16}\ln|A_2|\ln|A_3|.$$

Thus from

$$p^{\alpha-5/8}|A_1|^{-1/2}(|A_2||A_3|)^{13/16}\ln|A_2|\ln|A_3| \le 1, \tag{3.6}$$

we obtain

$$|S| \le 4\prod_{i=4}^n |A_i||A_1||A_2||A_3|p^{-\alpha} = 4\prod_{i=1}^n |A_i|p^{-\alpha}.$$

(3.6) holds if

$$|A_1| \ge p^{2\alpha-5/4}(|A_2||A_3|)^{13/8}\ln^2|A_2|\ln^2|A_3|. \tag{3.7}$$

When $|A_2|, |A_3| \asymp \sqrt{p}$ we obtain

$$|A_1| \ge p^{2\alpha+3/8+\varepsilon}. \tag{3.8}$$

From (3.7) and (3.8) an easy calculation gives (3.2) and the Corollary.

Acknowledgement: This note is supported by "Balaton Program Project" and OTKA grants K 61908, K 67676.

References

[1] J. Bourgain, Multilinear Exponential Sums in Prime Fields Under Optimal Entropy Condition on the Source, GAFA Vol 18 (2009) 1477-1502

[2] J. Bourgain, More on the sum-product phenomenon in prime fields and its application, Int. J. of Number Theory **1** (2005), 1–32.

[3] J. Bourgain, M.Z. Garaev: On a Variant of Sum-Product Estimates and explcit exponential sum bounds in prime fields, Math. Proc. of the Cambridge Phil. Soc. Vol. 146, p.1-21 (2009)

[4] J. Cilleruelo: Combinatorial Problems in finite fields and Sidon sets arXiv:1003.3576v1

[5] N. Hegyvári, F. Hennecart: Explicit Constructions of Extractors and Expanders, Acta Arithmetica, 140(2009), p. 233-249

[6] A. Sárközy: On sums and products of residues modulo p, Acta Arith. (2005), 118.4 p 403-409

[7] I. Shparlinski: On the solvability of bilinear equations in finite fields, Glasgow Math. J. 2008. v. 50 p. 523-539

[8] T.Tao, V.Vu: Additive Combinatorics, Cambridge University Press, Cambridge 2006

[9] J. Bourgain: Mordell's exponential sum estimate revisited, J. of the Amer. Math. Soc. 18, N.2 p. 477-499 (2005)

[10] N. Hegyvári On Sum-Product Bases, Ramanujan Journal, (2009), 19; p. 1-8

Norbert Hegyvári, ELTE TTK, Eötvös University, Institute of Mathematics, H-1117 Pázmány st. 1/c, Budapest, Hungary

E-mail address: hegyvari@elte.hu