

NONLINEAR ROTH TYPE THEOREMS IN FINITE FIELDS

J. BOURGAIN AND M.-C. CHANG

ABSTRACT. We obtain smoothing estimates for certain nonlinear convolution operators on prime fields, leading to quantitative nonlinear Roth type theorems. For instance, we produce triplets $x, x + y, x + y^2$ and $x, x + y, x + \bar{y}$ in proportional subsets of \mathbb{F}_p .

Compared with the usual linear setting (i.e. arithmetic progressions), the nonlinear nature of the operators leads to different phenomena, both qualitatively and quantitatively. The methods used are purely analytical.

1. INTRODUCTION

In this note, we study in the setting of prime fields certain nonlinear averages, motivated by the non-conventional ergodic averages considered in particular in [FK]. While the results from [FK] are of a more general nature, our emphasis are the quantitative aspects that also are in sharp contrast with the linear case corresponding to arithmetic progressions. As discussed below, this phenomenon leads to several questions related to generalization in various directions, worth further investigation.

For $f : \mathbb{F}_p \rightarrow \mathbb{C}$. Denote

$$\begin{aligned}\mathbb{E}[f] &= \mathbb{E}_x[f] = \frac{1}{p} \sum_{x=0}^{p-1} f(x) \\ \|f\|_r &= \left(\frac{1}{p} \sum_x |f(x)|^r \right)^{\frac{1}{r}} \\ \|f\|_{\ell^r} &= \left(\sum_x |f(x)|^r \right)^{\frac{1}{r}} \\ \hat{f}(z) &= \frac{1}{p} \sum_x e_p(-xz) f(x).\end{aligned}$$

We also recall that the notations $A \gtrsim B$ means $A \geq cB$ and $A \sim B$ means $A \leq c_1 B \leq c_2 A$ for some constant $c, c_1, c_2 > 0$.

Thus with this notation, Parseval's identity reads thus

$$\|f\|_2 = \|\hat{f}\|_{\ell^2}.$$

The authors were partially supported by NSF grants DMS-1301619 and DMS 1600154.

Our first result is the following inequality for a certain nonlinear convolution.

Theorem 1.1. *Let $f_1, f_2 : \mathbb{F}_p \rightarrow \mathbb{C}$. Define*

$$(1.1) \quad F(x) = \frac{1}{p} \sum_{y \in \mathbb{F}_p} f_1(x+y) f_2(x+y^2).$$

Then

$$(1.2) \quad \|F - \mathbb{E}[f_1] \cdot \mathbb{E}[f_2]\|_2 \leq cp^{-\frac{1}{10}} \|f_1\|_2 \cdot \|f_2\|_2.$$

Corollary 1.2. *(quadratic Roth theorem on \mathbb{F}_p).*

Let $A \subset \mathbb{F}_p$, $|A| = \delta p$ with $\delta > c_1 p^{-\frac{1}{15}}$ and $c_1 > 0$ an appropriate constant.

Then there are $x \in A, y \in \mathbb{F}_p^*$ such that $x, x+y, x+y^2 \in A$

(and in fact $\gtrsim \delta^3 p^2$ such triplets).

Proof of Corollary 1.2.

Let f be the indicator function of A . Then $\|f\|_2 = \delta^{\frac{1}{2}}$ and $\mathbb{E}(f) = \delta$.

Let F be as in (1.1) with $f_1 = f_2 = f$. Then Cauchy-Schwarz and (1.2) imply

$$(1.3) \quad \begin{aligned} \mathbb{E}_x \mathbb{E}_y [f(x) f(x+y) f(x+y^2)] &= \mathbb{E}_x [fF] \\ &= \mathbb{E}_x [f \cdot \mathbb{E}[f^2]] + \mathbb{E}_x [f \cdot (F - \mathbb{E}[f^2])] \\ &\geq \mathbb{E}[f]^3 - \|f\|_2 \|F - \mathbb{E}[f^2]\|_2 \\ &\geq \mathbb{E}[f]^3 - cp^{-\frac{1}{10}} \|f\|_2^3 \\ &\geq \delta^3 - cp^{-\frac{1}{10}} \delta^{\frac{3}{2}} \sim \delta^3. \quad \square \end{aligned}$$

Remarks

- (i) Recall Behrend's construction [Be] providing a subset $A \subset \{0, 1, \dots, p-1\}$ or $A \subset \mathbb{F}_p$, $|A| > \delta p$ with $\delta = e^{-c\sqrt{\log p}}$ and containing no non-trivial triples $x, x+y, x+2y \in A$. Thus Corollary 1.2 in the non-linear setting allows δ to be much smaller.
- (ii) Theorem 1.1 is indeed a non-linear phenomenon, both qualitatively and quantitatively. It was proven by N. Frantzikinakis and B. Kra [FK] that if (X, μ, T) is totally ergodic measure preserving probability system and $\{p_1(n), \dots, p_k(n)\}$ a linearly independent family of integer polynomials with $p_j(0) = 0$, then for $f_1, \dots, f_k \in L^\infty(\mu)$

$$(1.4) \quad \lim_{N \rightarrow \infty} \left\| \frac{1}{N} \sum_{n=0}^{N-1} f_1(T^{p_1(n)}x) \cdots f_k(T^{p_k(n)}x) - \prod_{i=1}^k \int f_i d\mu \right\|_{L^2(\mu)} = 0.$$

The case $k = 2, p_1(n) = n, p_2(n) = n^2$ (corresponding to Theorem 1.1) is due to Furstenberg and Weiss. Thus what makes (1.4) a non-linear phenomenon (compared with the linear case $p_1(n) = n, p_2(n) = 2n, \dots, p_k(n) = kn$, i.e. Szemerédi's theorem) is that the characteristic factor in the situation (1.4) turns out to be trivial (this was first conjectured by V. Bergelson). On the quantitative side, the approach in [FK] (based on the work of Host-Kra [HK]) does not seem to provide any estimates however, which is the main interest of Theorem 1.1.

We also refer to [BP] for a (quantitative) Roth type theorem for the squares.

- (iii) The proof of Theorem 1.1 relies on Fourier analysis, much in the spirit of [B]. Compared with [B], some differences occur due to the fact that oscillatory integrals are replaced by certain exponential sums that allow simple (and optimal) bounds (by use of Weil's estimate). A natural question is of course to what extent Theorem 1.1 generalizes to other non-linear settings (see discussion at the end).

We will also prove the following theorem which is less elementary than Theorem 1.1, and uses deep results of [FKM] on multilinear Kloosterman sums.

Theorem 1.3. *Define*

$$(1.5) \quad F(x) = \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} f_1(x+y) f_2(x+\bar{y}),$$

where \bar{y} stands for the multiplicative inverse of $y \in \mathbb{F}_p^*$. Then the following inequality holds

$$(1.6) \quad \|F - \mathbb{E}[f_1] \mathbb{E}[f_2]\|_2 \leq cp^{-\frac{1}{10}} \|f_1\|_2 \cdot \|f_2\|_2.$$

Corollary 1.4.

Let $A \subset \mathbb{F}_p$, $|A| = \delta p$ with $\delta > c_1 p^{-\frac{1}{15}}$ and $c_1 > 0$ an appropriate constant.

Then there are $x \in A, y \in \mathbb{F}_p^$ such that $x, x+y, x+\bar{y} \in A$*

(and in fact $\gtrsim \delta^3 p^2$ such triplets).

2. PROOF OF THEOREM 1.1

The structure of the argument follows closely the proof of Lemma 5 of [B]. But while [B] involves averages over \mathbb{R} , the present analysis is over a prime field leading to exponential sums.

Expanding f_1, f_2 in Fourier sum gives

$$(2.1) \quad F(x) = \mathbb{E}_y[f_1(x+y)f_2(x+y^2)] = \sum_{n_1, n_2=0}^{p-1} \hat{f}_1(n_1)\hat{f}_2(n_2)c_{n_1, n_2}e_p((n_1+n_2)x)$$

with (using quadratic Gauss sums evaluation. [IK])

$$(2.2) \quad \begin{aligned} c_{n_1, n_2} &= \mathbb{E}_y[e_p(n_1y + n_2y^2)] \\ &= \begin{cases} 1 & \text{if } n_1 = n_2 = 0 \\ 0 & \text{if } n_2 = 0, n_1 \neq 0 \\ \frac{1}{\sqrt{p}}\left(\frac{n_2}{p}\right)e_p(-n_1^2\overline{4n_2})\sigma_p & \text{if } n_2 \neq 0 \end{cases} \end{aligned}$$

and where

$$\sigma_p = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ i & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

and \bar{x} stands for the multiplicative inverse of $x \in \mathbb{F}_p^*$.

Denote

$$(2.3) \quad K(x, y) = \begin{cases} e_p(-x^2\overline{4y}) & \text{if } y \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$F(x) = \mathbb{E}[f_1] \cdot \mathbb{E}[f_2] + \frac{1}{\sqrt{p}} \sum_{s=0}^{p-1} e_p(sx) \sum_{n=1}^{p-1} \hat{f}_1(s-n)\hat{f}_2(n)\left(\frac{n}{p}\right)K(s-n, n)\sigma_p,$$

and by Parseval,

$$(2.4) \quad \|F(x) - \mathbb{E}[f_1] \cdot \mathbb{E}[f_2]\|_2 = \frac{1}{\sqrt{p}} \left\{ \sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n)\hat{f}_2(n)\left(\frac{n}{p}\right)K(s-n, n) \right|^2 \right\}^{\frac{1}{2}}.$$

Since we are aiming for an estimate of (2.4) in terms of $\|f_1\|_2 \cdot \|f_2\|_2$, the factor $\left(\frac{n}{p}\right)$ may be absorbed in $\hat{f}_2(n)$. Thus we need to analyze further

$$(2.5) \quad \left(\sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n)\hat{f}_2(n)K(s-n, n) \right|^2 \right)^{\frac{1}{2}}$$

with K given by (2.3).

Our goal is to bound (2.5) non-trivially. Note that the trivial bound by $\sqrt{p} \|f_1\|_2 \cdot \|f_2\|_2$ is just insufficient and we need to gain an extra $p^{-\gamma}$ from additional cancellation exploiting (2.3). The first step is to invoke the following very general inequality, identical to Lemma 7 in [B]. We also use the notation $\int dx$ for \sum_x .

Lemma 2.1. *Let $f, g : \mathbb{F}_p \rightarrow \mathbb{C}$ and $K : \mathbb{F}_p \times \mathbb{F}_p \rightarrow \mathbb{C}$. Then*

$$\begin{aligned}
(2.6) \quad & \left\| \sum_x K(s-x, x) f(s-x) g(x) \right\|_{\ell_s^2} =: I \\
& \leq \|f\|_{\ell^2}^{1/2} \|f\|_{\ell^4}^{1/2} \|g\|_{\ell^2} \cdot \\
& \quad \left\| \sum_x K(x, s-x) \overline{K(x+u, s-x)} \overline{K(x, s+v-x)} K(x+u, s+v-x) \right\|_{\ell_{s,u,v}^2}^{1/4}.
\end{aligned}$$

We repeat the argument for selfcontainedness.

Proof. The proof follows from consecutive linearizations and applications of the Cauchy-Schwarz inequality.

Linearization of the ℓ_s^2 -norm yields

$$\begin{aligned}
(2.7) \quad I & \leq \|g\|_2 \left\| \sum_s K(s-x, x) f(s-x) \varphi(s) \right\|_{\ell_x^2} \quad (\text{for some } \varphi \text{ with } \|\varphi\|_{\ell^2} = 1) \\
& \leq \|g\|_2 \left\| \sum_x K(s-x, x) \overline{K(s'-x, x)} f(s-x) \overline{f(s'-x)} \right\|_{\ell_{s,s'}^2}^{1/2}.
\end{aligned}$$

Make the change of variable $x \leftrightarrow s-x$ and put $u = s' - s$. Thus

$$\begin{aligned}
(2.8) \quad & \left\| \sum_x K(s-x, x) \overline{K(s'-x, x)} f(s-x) \overline{f(s'-x)} \right\|_{\ell_{s,s'}^2} \\
& = \left\| \sum_x K(x, s-x) \overline{K(x+u, s-x)} f(x) \overline{f(x+u)} \right\|_{\ell_{s,u}^2}
\end{aligned}$$

Fixing the u -variable and again linearizing the ℓ_s^2 -norm gives

$$\begin{aligned}
& \left\| \sum_x K(x, s-x) \overline{K(x+u, s-x)} f(x) \overline{f(x+u)} \right\|_{\ell_s^2} \\
& \leq \left\| \sum_x K(x, s-x) \overline{K(x+u, s-x)} \overline{K(x, s+v-x)} \right. \\
& \quad \left. K(x+u, s+v-x) \right\|_{\ell_{s,v}^2}^{1/2} \|f \cdot \bar{f}_u\|_{\ell_x^2}.
\end{aligned}$$

Hence, by Cauchy-Schwarz again expression (2.8) is bounded by

$$\begin{aligned}
(2.9) \quad & \left\| \sum_x K(x, s-x) \overline{K(x+u, s-x)} \overline{K(x, s+v-x)} \right. \\
& \quad \left. \times K(x+u, s+v-x) \right\|_{\ell_{s,u,v}^2}^{1/2} \left\| \|f \cdot \bar{f}_u\|_{\ell_x^2} \right\|_{\ell_u^4}.
\end{aligned}$$

Since the last factor in (2.9) is bounded by

$$\max_u \mathbb{E}_x [|f|^2 |f_u|^2]^{1/4} \cdot \|f\|_{\ell^2} \leq \|f\|_{\ell^2} \|f\|_{\ell^4}$$

(2.6) follows from (2.7)-(2.9). This proves Lemma 2.1. \square

Returning to (2.5), we prove inequality (2.16) below using an interpolation argument. Let $M > 0$ be a parameter and perform a level set decomposition

$$(2.10) \quad \begin{aligned} \hat{f}_1(n) &= \hat{f}_{1,0}(n) + \hat{f}_{1,1}(n), \quad \text{with} \\ \hat{f}_{1,0}(n) &= \begin{cases} \hat{f}_1(n) & \text{if } \hat{f}_1(n) < \frac{M}{\sqrt{p}} \|f_1\|_2 \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Applying Lemma 2.6 with $f = \hat{f}_{1,0}$ and $g = \hat{f}_2$ implies

$$(2.11) \quad \left(\sum_s \left| \sum_{n \neq 0} \hat{f}_{1,0}(s-n) \hat{f}_2(n) K(s-n, n) \right|^2 \right)^{\frac{1}{2}} \leq \|\hat{f}_{1,0}\|_{\ell^2}^{\frac{1}{2}} \|\hat{f}_{1,0}\|_{\ell^4}^{\frac{1}{2}} \|\hat{f}_2\|_{\ell^2} \Omega^{\frac{1}{4}},$$

where

$$(2.12) \quad \Omega = \left\| \sum_x [K(x, s-x) \overline{K(x+u, s-x)} \overline{K(x, s+v-x)} K(x+u, s+v-x)] \right\|_{\ell_{s,u,v}^2}.$$

Also

$$\|\hat{f}_{1,0}\|_{\ell^2} \leq \|\hat{f}_1\|_{\ell^2} = \|f_1\|_2, \quad \|\hat{f}_2\|_{\ell^2} = \|f_2\|_2$$

while by (2.10)

$$\|\hat{f}_{1,0}\|_{\ell^4} = \left(\sum |\hat{f}_{1,0}(n)|^4 \right)^{\frac{1}{4}} \leq \left(\frac{M}{\sqrt{p}} \right)^{\frac{1}{2}} \|f_1\|_2^{\frac{1}{2}} \left(\sum |\hat{f}_1(n)|^2 \right)^{\frac{1}{4}} = \left(\frac{M}{\sqrt{p}} \right)^{\frac{1}{2}} \|f_1\|_2.$$

Thus the right hand side of (2.11) is bounded by

$$(2.13) \quad \left(\frac{M}{\sqrt{p}} \right)^{\frac{1}{4}} \|f_1\|_2 \cdot \|f_2\|_2 \Omega^{\frac{1}{4}}.$$

The contribution of $\hat{f}_{1,1}$ in (2.5) is estimated trivially as follows

$$(2.14) \quad \left(\sum_s \left| \sum_{n \neq 0} \hat{f}_{1,1}(s-n) \hat{f}_2(n) K(s-n, n) \right|^2 \right)^{\frac{1}{2}} \leq \left(\sum_s \left(\sum_n |\hat{f}_{1,1}(s-n)| |\hat{f}_2(n)| \right)^2 \right)^{\frac{1}{2}}$$

and noting that since $\hat{f}_{1,1}(n) = 0$ or $|\hat{f}_{1,1}(n)| \geq \frac{M}{\sqrt{p}} \|f_1\|_2$, it follows $\|f_1\|_2^2 \left(\frac{M}{\sqrt{p}} \right)^2 |\text{supp } \hat{f}_{1,1}| \leq \|\hat{f}_{1,1}\|_{\ell^2}^2 \leq \|f_1\|_2^2$ implying $|\text{supp } \hat{f}_{1,1}| \leq \left(\frac{\sqrt{p}}{M} \right)^2$. By Cauchy-Schwarz

$$\sum_n |\hat{f}_{1,1}(s-n)| |\hat{f}_2(n)| \leq \frac{\sqrt{p}}{M} \left(\sum_n |\hat{f}_{1,1}(s-n)|^2 |\hat{f}_2(n)|^2 \right)^{\frac{1}{2}}$$

and (2.14) is bounded by

$$(2.15) \quad \frac{\sqrt{p}}{M} \|\hat{f}_{1,1}\|_{\ell^2} \cdot \|\hat{f}_2\|_{\ell^2} \leq \frac{\sqrt{p}}{M} \|f_1\|_2 \cdot \|f_2\|_2.$$

Adding (2.13), (2.15) shows that

$$\left(\sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n) \hat{f}_2(n) K(s-n, n) \right|^2 \right)^{\frac{1}{2}} \leq \left[\left(\frac{M}{\sqrt{p}} \right)^{\frac{1}{4}} \Omega^{\frac{1}{4}} + \frac{\sqrt{p}}{M} \right] \|f_1\|_2 \cdot \|f_2\|_2$$

and choosing M appropriately, we have a bound on (2.5)

$$(2.16) \quad \left(\sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n) \hat{f}_2(n) K(s-n, n) \right|^2 \right)^{\frac{1}{2}} \leq \Omega^{\frac{1}{5}} \|f_1\|_2 \cdot \|f_2\|_2.$$

Next, recalling (2.4), we will establish a non-trivial bound on (2.13), exploiting cancellation in \sum_x in the definition of Ω in (2.12).

We have by (2.4), for $s \neq x, s+v \neq x$

$$K(x, s-x) \overline{K(x+u, s-x)} = e_p \left(-\frac{x^2}{4(s-x)} + \frac{(x+u)^2}{4(s-x)} \right) = e_p \left(\frac{(2x+u)u}{4(s-x)} \right).$$

Hence

$$(2.17) \quad \begin{aligned} & \mathcal{K}_{x,s,u,v} \\ & := K(x, s-x) \overline{K(x+u, s-x)} \overline{K(x, s+v-x)} K(x+u, s+v-x) \\ & = e_p \left(\frac{(2x+u)u}{4} \left(\frac{1}{s-x} - \frac{1}{s+v-x} \right) \right) \\ & = e_p \left(\frac{uv(2x+u)}{(s-x)(s+v-x)} \right), \end{aligned}$$

and assuming $u, v \neq 0, u \neq -2s, -2s-2v$, we will prove

$$(2.18) \quad \left| \sum_{\substack{x=0 \\ x \neq s, s+v}}^{p-1} \mathcal{K}_{x,s,u,v} \right| \leq 3\sqrt{p}.$$

In order to establish (2.18) we make use of the following result from [Bom] (Theorem 5).

Proposition 2.2. *Let $f_1, f_2 \in \mathbb{Z}[X]$, $(f_1, f_2) = 1$ and $\tilde{f}_1, \tilde{f}_2 \in \mathbb{F}_p[X]$ the corresponding polynomials over \mathbb{F}_p , $\tilde{f}(x) = \frac{\tilde{f}_1(x)}{\tilde{f}_2(x)}$ where x is to take only values with $p \nmid f_2(x)$. Define*

$$(2.19) \quad S(\tilde{f}) = \sum_x e_p(\tilde{f}(x)).$$

Then, assuming $\deg(\tilde{f}) := \deg(\tilde{f}_1) + \deg(\tilde{f}_2) \geq 1$, we have

$$(2.20) \quad |S(\tilde{f})| \leq (n-2 + \deg(\tilde{f})_\infty) p^{\frac{1}{2}} + 1$$

where n is the number of the poles and $(\tilde{f})_\infty$ is the divisor of the poles of \tilde{f} over the algebraic closure $\overline{\mathbb{F}_p}$ (including ∞ if necessary).

Applying Proposition 2.2 with $\tilde{f}(x)$ as in (2.17), $n = 2$, $\deg(\tilde{f})_\infty = 2$ so that indeed

$$|S(f)| \leq 2p^{\frac{1}{2}} + 1 < 3\sqrt{p}.$$

If the assumptions in (2.18) are not fulfilled, estimate trivially $|\sum_x \mathcal{K}_{x,s,u,v}| \leq p$. Using (2.18), it follows that

$$(2.21) \quad \Omega \leq c\{p^3(\sqrt{p})^2 + p^2 \cdot p^2\}^{\frac{1}{2}} \leq cp^2.$$

Substituting in (2.16) gives

$$(2.22) \quad \left(\sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n) \hat{f}_2(n) K(s-n, n) \right|^2 \right)^{\frac{1}{2}} \leq cp^{2/5} \|f_1\|_2 \|f_2\|_2.$$

Hence by (2.4)

$$\|F - \mathbb{E}[f_1] \cdot \mathbb{E}[f_2]\|_2 \leq cp^{-\frac{1}{10}} \|f_1\|_2 \|f_2\|_2$$

which is (1.2). This proves Theorem 1.1.

Remark. One may wonder about the sharpness of inequality (1.2) in Theorem 1.1. Although we did not attempt to optimize our approach, it almost surely will not answer this presumably difficult question. We only note a few examples below.

Example 1. Take $f_1(x) = f_2(x) = e_p(x)$. Then $F(x) = e_p(2x) \left(\frac{1}{p} \sum_y e_p(y + y^2) \right)$, hence $|F(x)| = \frac{1}{\sqrt{p}}$ and $\|F - \mathbb{E}[f_1] \mathbb{E}[f_2]\|_2 = p^{-\frac{1}{2}} \|f_1\|_2 \|f_2\|_2$.

Example 2. For $i = 1, 2$, define

$$f_i(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Thus $\mathbb{E}[f_i] = \frac{1}{p}$, $\|f_i\|_2 = p^{-\frac{1}{2}}$ and

$$F(x) = \begin{cases} \frac{1}{p} & \text{if } x = 0, -1 \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, $\|F - \mathbb{E}[f_1] \mathbb{E}[f_2]\|_2 = O(p^{-\frac{3}{2}}) = O(p^{-\frac{1}{2}} \|f_1\|_2 \|f_2\|_2)$ again.

The next example is slightly more interesting as it shows that (1.2) cannot hold with $p^{-\frac{1}{10}}$ replaced by $p^{-\frac{1}{2}}$.

Example 3. Recall the Fourier formulation (2.4) and (2.3). The left hand side of (1.2) equals

$$\frac{1}{\sqrt{p}} \left\{ \sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n) \hat{f}_2(n) \left(\frac{n}{p} \right) e_p(-4n) e_p(-4ns^2) \right|^2 \right\}^{\frac{1}{2}}$$

and absorbing $\left(\frac{n}{p} \right) e_p(-4n)$ in the $\hat{f}_2(n)$ -factor, one obtains

$$(2.23) \quad \frac{1}{\sqrt{p}} \left\{ \sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n) \hat{f}_2(n) e_p(-4ns^2) \right|^2 \right\}^{\frac{1}{2}}.$$

Next, we will define \hat{f}_1 and \hat{f}_2 . Let D be the product of the primes less than $\frac{1}{10} \log p$ and \mathcal{D} the set of divisors of D . Hence

$$D < p^{\frac{1}{9}} \quad \text{and} \quad |\mathcal{D}| > \exp\left(c \frac{\log p}{\log \log p}\right).$$

Define

$$(2.24) \quad \hat{f}_1(x) = \begin{cases} (2D)^{-\frac{1}{2}} & \text{if } x \in 4D \cdot \{1, 2, \dots, 2D\} \\ 0 & \text{otherwise} \end{cases}$$

and

$$(2.25) \quad \hat{f}_2(x) = \begin{cases} |\mathcal{D}|^{-\frac{1}{2}} & \text{if } x \in 4D \cdot \mathcal{D} \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\|f_1\|_2 = 1 = \|f_2\|_2$.

Setting $s = 4Ds_1$ and $n = 4Dn_1$, we have a lower bound on $\sqrt{p} \cdot (2.23)$ as follows.

$$(2.26) \quad \begin{aligned} & \left\{ \sum_s \left| \sum_{n \neq 0} \hat{f}_1(s-n) \hat{f}_2(n) e_p(-4\bar{n}s^2) \right|^2 \right\}^{\frac{1}{2}} \\ & \geq \left\{ \sum_{D < s_1 \leq 2D} \left| \sum_{n_1 \in \mathcal{D} \cap (s_1 - \{1, \dots, 2D\})} (2D)^{-\frac{1}{2}} |\mathcal{D}|^{-\frac{1}{2}} e_p(-D\bar{n}_1 s_1^2) \right|^2 \right\}^{\frac{1}{2}} \\ & \geq \frac{1}{2} |\mathcal{D}|^{-\frac{1}{2}} \min_{D < s_1 \leq 2D} \left| \sum_{n_1 \in \mathcal{D}} e_p(-D\bar{n}_1 s_1^2) \right|. \end{aligned}$$

Note that by the definitions of D and \mathcal{D} , $D\bar{n}_1 \in \{1, \dots, D\}$ for $n_1 \in \mathcal{D}$ and $D\bar{n}_1 s_1^2$ is an integer bounded by $4D^3 < p^{\frac{1}{2}}$ for $D < s_1 < 2D$, recalling that $D < p^{\frac{1}{9}}$. It follows that the inner sum in (2.26) is of size $|\mathcal{D}|$ and therefore (2.23) is

$$(2.27) \quad \gtrsim |\mathcal{D}|^{\frac{1}{2}} p^{-\frac{1}{2}} > \exp\left(c \frac{\log p}{\log \log p}\right) p^{-\frac{1}{2}}.$$

Hence this example shows that the exponent $\frac{1}{10}$ in (1.2) cannot be replaced by a clean $\frac{1}{2}$, though we are unable to rule out the validity of this inequality with exponent $\frac{1}{2} + \epsilon$.

3. COMMENTS AND PROOF OF THEOREM 1.3

The phenomenon described in Theorem 1.1 opens the door to a number of questions on possible generalizations in different directions.

Question 1. Let $\varphi_1, \varphi_2 \in \mathbb{Z}[X]$, $\varphi_1(0) = \varphi_2(0) = 0$ be linearly independent polynomials and define for $f_1, f_2 : \mathbb{F}_p \rightarrow \mathbb{C}$

$$(3.1) \quad F(x) = \frac{1}{p} \sum_{y \in \mathbb{F}_p} f_1(x + \varphi_1(y)) f_2(x + \varphi_2(y)).$$

Is an inequality of the type (1.2) valid?

Question 1'. Same question as above with φ_1, φ_2 a pair of rational functions, and excluding the poles in the summation (3.1).

Likely Theorem 1.1 and its proof extend to the case φ_1, φ_2 are linearly independent quadratic polynomials. Note that in the above analysis not only a bound

$$(3.2) \quad \left| \sum_y e_p(a\varphi_1(y) + b\varphi_2(y)) \right| < c\sqrt{p}$$

for $ab \neq 0$ (the latter being obtainable from Weil) is involved but also the exact evaluation of the above exponential sum (which is possible only in special cases).

Beyond the bilinear case, one may also ask

Question 2. Is there a multilinear generalization of Theorem 1.1? In particular if we define

$$(3.3) \quad F(x) = \frac{1}{p} \sum_{y \in \mathbb{F}_p} f_1(x+y)f_2(x+y^2)f_3(x+y^3)$$

does an inequality of the form

$$(3.4) \quad \|F - \mathbb{E}[f_1] \mathbb{E}[f_2] \mathbb{E}[f_3]\|_1 \leq cp^{-\delta} \|f_1\|_\infty \|f_2\|_\infty \|f_3\|_\infty.$$

hold for some $\delta < 0$?

The main theorem in [FK] would imply that the left hand side of (3.4) is bounded by $o(1) \|f_1\|_\infty \|f_2\|_\infty \|f_3\|_\infty$ but without any quantitative specification (that would be awkward to extract from their approach) and certainly not a power gain $p^{-\delta}$ as in Theorem 1.1. The explicit calculation based on the standard Fourier transform used above in the bilinear case does not seem to succeed for the trilinear average (3.3) that likely would require higher order Fourier analysis.

Next, returning to Question 1', we establish another result in the spirit of Theorem 1.1, taking $\varphi_1(x) = x, \varphi_2(x) = \frac{1}{x}$. Thus we prove Theorem 1.3.

Proof of Theorem 1.3.

Following the initial steps in the proof of Theorem 1.1, the left hand side of (1.6) is bounded by

$$(3.5) \quad \frac{1}{\sqrt{p}} \left\{ \sum_{s=0}^{p-1} \left| \sum_{n=0}^{p-1} \hat{f}_1(n-s)\hat{f}_2(n)K(s-n,n) \right|^2 \right\}^{\frac{1}{2}}$$

where now

$$(3.6) \quad K(x,y) = \begin{cases} \frac{1}{\sqrt{p}} \sum_{z \in \mathbb{F}_p^*} e_p(xz + y\frac{1}{z}) & \text{if } y \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

is given by a Kloosterman sum. (See [IK].)

Note that by change of variables

$$(3.7) \quad \frac{1}{\sqrt{p}} \sum_{z \in \mathbb{F}_p^*} e_p \left(xz + y \frac{1}{z} \right) = \frac{1}{\sqrt{p}} \sum_{z \in \mathbb{F}_p^*} e_p \left(xyz + \frac{1}{z} \right) = K\ell(xy)$$

denoting the Kloosterman sum (cf. [FKM]).

$$(3.8) \quad \frac{1}{\sqrt{p}} \sum_{z \in \mathbb{F}_p^*} e_p \left(az + \frac{1}{z} \right) = K\ell_2(a; p) = K\ell(a).$$

(Note that $\overline{K\ell(a)} = K\ell(a)$.)

It is well-known that

$$(3.9) \quad |K\ell(a)| < c$$

but $K\ell(a)$ does not allow an explicit evaluation.

Instead, we will rely on results from [FKM] to bound Ω given by (2.13). Thus, by (3.10)

$$(3.10) \quad \Omega = \left\| \sum_x K\ell(x(s-x)) K\ell((x+u)(s-x)) K\ell(x(s'-x)) K\ell((x+u)(s'-x)) \right\|_{\ell^2_{s,s',u}}$$

and hence

$$(3.11) \quad \Omega^2 = \sum_{x,y,s,s',u} K\ell(x(s-x)) K\ell((x+u)(s-x)) K\ell(x(s'-x)) K\ell((x+u)(s'-x)) \\ \times K\ell(y(s-y)) K\ell((y+u)(s-y)) K\ell(y(s'-y)) K\ell((y+u)(s'-y)).$$

We will perform the summations in s, s' with x, y, u fixed. Thus we bound

$$(3.12) \quad \sum_{s=0}^{p-1} K\ell(x(s-x)) K\ell((x+u)(s-x)) K\ell(y(s-y)) K\ell((y+u)(s-y))$$

which, in order to invoke [FKM], we rewrite as

$$(3.13) \quad \sum_s K\ell(\gamma_1 \cdot s) K\ell(\gamma_2 \cdot s) K\ell(\gamma_3 \cdot s) K\ell(\gamma_4 \cdot s)$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL_2(\mathbb{F}_p)$ acts by linear fractional transformation

$$(3.14) \quad \gamma \cdot s = \frac{as + b}{cs + d}$$

and in our case (3.12) these transformations are affine

$$(3.15) \quad \gamma_1 = \begin{pmatrix} x & -x^2 \\ 0 & 1 \end{pmatrix} \quad \gamma_2 = \begin{pmatrix} x+u & -x(x+u) \\ 0 & 1 \end{pmatrix} \\ \gamma_3 = \begin{pmatrix} y & -y^2 \\ 0 & 1 \end{pmatrix} \quad \gamma_4 = \begin{pmatrix} y+u & -y(y+u) \\ 0 & 1 \end{pmatrix}$$

It follows in particular from Corollary 3.3 in [FKM] that if $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in PGL_2(\mathbb{F}_p)$ are pairwise distinct, then

$$(3.16) \quad \left| \sum_s K\ell(\gamma_1.s)K\ell(\gamma_2.s)K\ell(\gamma_3.s)K\ell(\gamma_4.s) \right| < c\sqrt{p}.$$

By (3.16) the latter condition will be satisfied if $x \neq y$ and $u \neq 0$.

Returning to (3.11), we fix $x, y, u, x \neq y, u \neq 0$ and bound the s, s' summations using (3.16). If $x = y$ or $u = 0$, bound (3.13) trivially by p . This gives a bound on (3.11).

$$\Omega^2 < c(\sqrt{p})^2 p^3 + cp^2 \cdot p^2 \leq cp^4.$$

Therefore,

$$(3.17) \quad \Omega < cp^2.$$

Substituting again the bound on Ω in (3.10) shows that

$$(3.18) \quad \frac{1}{\sqrt{p}} \left\{ \sum_{s=0}^{p-1} \left| \sum_{n=0}^{p-1} \hat{f}_1(n-s)\hat{f}_2(n)K(s-n, n) \right|^2 \right\}^{\frac{1}{2}} \\ \leq c \frac{1}{\sqrt{p}} p^{2/5} \|f_1\|_2 \cdot \|f_2\|_2 \leq cp^{-\frac{1}{10}} \|f_1\|_2 \|f_2\|_2$$

proving (1.6). \square

Acknowledgement. The second author would like to thank the Mathematics Department of the University of California at Berkeley for its hospitality while the paper was under revision.

REFERENCES

- [Be] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Natl. Acad. Sci. USA, 32(12), 331-332, (1946).
- [B] J. Bourgain, *A nonlinear version of Roth's theorem for sets of positive density in the real line*, J. Analyze Math., Vol. 50, 1988, 169–181.
- [Bom] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math., Vol. 88, No 1 (1966), 71–10
- [BP] T. D. Browning, S. M. Prendiville, *A Transference Approach to a Roth-Type Theorem in the Squares*, Int Math Res Notices (to appear).
- [FK] H. Frantzikinakis, B. Kra, *Polynomial averages converge to the product of integrals*, Israel J. Math., Vol. 148, 2005, 267–276.
- [FKM] E. Fouvry, E. Kowalski, P. Michel, *A study in sums of products*, Phil. Trans. Royal Soc. A, Vol. 373, No 2040 (2015).
- [HK] B. Host, B. Kra, *Convergence of polynomial ergodic averages*, Israel J. Math., Vol. 149, 2005, 1–19.
- [IK] H. Iwaniec, E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, (2004).

J. BOURGAIN, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NJ 08540

E-mail address: `bourgain@math.ias.edu`

M.-C. CHANG, UNIVERSITY OF CALIFORNIA, RIVERSIDE, CA 92521

E-mail address: `mcc@math.ucr.edu`