Uniform Distribution Theory **9** (2014), no.2, 103–123

uniform distribution theory

# ON THE DISTRIBUTION OF THE VALUES OF MULTIVARIATE RATIONAL FUNCTIONS

Norbert Hegyvári — François Hennecart

ABSTRACT. We investigate the distribution of the values taken by multivariate rational functions with integral coefficients in different directions. Firstly we consider the problem of estimating the maximum of a nonnegative multivariate polynomial on the $n$-dimensional hypercube $[0,1]^n$ in terms of the arithmetical properties of the exponents of their constituting monomials. Secondly we are interested by the distribution of the values of expander polynomials in prime fields. And finally we focus on some multivariate covering rational functions on prime fields.

*Communicated by Ilya Shkredov*

## 1. Introduction

In the present paper we investigate the distribution of values of multivariate rational functions.

Firstly we consider $n$-variables polynomials $f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ with integral coefficients. Consider the simplest case: let $f \in \mathbb{Z}[x]$, and assume that $f(x)$ is nonnegative on $[0,1]$ and not identically the zero polynomial. It is expected that $f$ could not be too 'flat' depending on the degree of $f$. More precisely there exists a positive bound $\beta(d)$ such that for any such polynomial $f \in \mathbb{Z}[x]$ with degree $d$, we have $\max_{x\in[0,1]} f(x) \geq \beta(d)$. In the next section we give a bound for the multivariate case, showing that it depends both on the degree of the multivariate polynomial and on the arithmetical structure of the sequence of exponents occurring in each monomial of $f$.

In the third and fourth sections we will consider multivariate functions on prime fields. As a first task, we shall concentrate our attention to 2-variable polynomials called *expanders*. A polynomial $f(x,y)$ is said to be expander,

2010 Mathematics Subject Classification: 11B75, 11C08.
Keywords: Uniform distribution, expanders.

if for fixed $0 < \alpha < 1$, $f : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$, there exists a $\beta = \beta(\alpha) > \alpha$ such that for all $A, B \subseteq \mathbb{F}_p$, $|B| \asymp |A| \sim p^\alpha$ we have

$$|f(A,B)| > p^\beta.$$

Expander maps have a rather long story. In 2004, Barak, Implagliazzo, Wigderson asked to find an 'explicit' (algebraic) expander polynomial (see [1]). One year later Bourgain proved that $f = f(x,y) = x^2 + xy$ is an expander (see [2]).

**Theorem 1.1** (Bourgain)**.** *The polynomial $f(x,y) = x^2 + xy$ is an expander: for all $0 < \alpha < 1$, there exists a number $\delta = \delta(\alpha) > 0$, such that if $|B| \asymp |A| \sim p^\alpha$ then*

$$|f(A,B)| > p^{\alpha+\delta}.$$

An expander map blows up its argument set, so one can expect that its values are well-distributed on $\mathbb{F}_p$. In section 3 we formally explicite this notion of well-distribution.

In 2008 the authors gave a wide family of expanders (see [6] and [7] and see also [16] and [15], and details in the third section). We will consider distribution in two different meanings as well (cf. section 3).

The converse problem arises as a natural question: if the images of all sufficiently big 'bricks' $A \times B$ by a given map $F(x,y)$ are well-distributed, can we conclude that the map $F(x,y)$ is an expander? Surprisingly the answer is negative. J. Bourgain showed in [2] the following

**Theorem 1.2** (Bourgain)**.** *Let $G(x,y) := x^2y^2 + xy$, and $A, B \subseteq \mathbb{F}_p \setminus \{0\}$ with $|A| \sim |B| \sim p^{1/2}$. Then there exists a real number $\gamma > 0$, such that for all $r \in \mathbb{F}_p \setminus \{0\}$*

$$\Big| \sum_{x \in A; y \in B} \exp\Big(\frac{2\pi i r G(x,y)}{p}\Big) \Big| \leq p^{1-\gamma}.$$

So the image set of any brick $A \times B$ with prescribed size by the function $G(x,y)$ is well-distributed (see section 3 for the links between equidistribution and the size of the Fourier coefficients). In the same time, we may write

$$x^2y^2 + xy = \frac{(2xy+1)^2 - 1}{4},$$

hence by considering $A$ and $B$ both being geometric sequences with common ratio and with length $\sim \sqrt{p}$, we plainly conclude that $G(x,y)$ cannot be an expander.

## 2. On integral polynomials being nonnegative in the unit hypercube

Let $N, n$ be two positive integers. Let $f = f(x_1, x_2, \dots, x_n) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ and write $f$ under the form

$$f(x_1, \dots, x_n) \ = \sum_{\underline{k}=(k_1,\dots,k_n)\in\mathbb{N}^n} a_{\underline{k}} x_1^{k_1} x_2^{k_2} \dots x_n^{k_n},$$

where we assume that $a_{\underline{k}} \neq 0$ implies $N \geq k_1 + k_2 + \cdots + k_n + n$, *i.e.,* the degree of $f$ is at most $N - n$. Denote by

$$\mathcal{A}_f := \{\underline{k} \in \mathbb{N}^n \text{ such that } a_{\underline{k}} \neq 0\},$$

and for each $\underline{k} \in \mathcal{A}_f$, let

$$K_{\underline{k}} := \prod_{i=1}^{n} (k_i + 1).$$

We define $\mathcal{F}_{N,n}$ to be the set of all $n$-variable non zero integral polynomials $f$ satisfying

$$\begin{cases} \deg f \leq N - n \text{ and} \\ \forall (x_1, x_2, \dots, x_n) \in [0,1]^n, \ f(x_1, x_2, \dots, x_n) \geq 0. \end{cases}$$

Let $P^*$ be any subsequence of all primes with relative positive upper density $\alpha$. More precisely if we write $\pi^*(x) := P^* \cap [1, x]$, then we define

$$\alpha := \limsup_{x\to\infty} \frac{\pi^*(x)}{\pi(x)}$$

and we assume $\alpha > 0$.

We thus make the assumption that $f$ is nonnegative and is not identically zero on the hypercube $[0,1]^n$, has degree less than or equal to $N - n$ and is such that all prime divisors of its exponents incremented by one belong to $P^*$, *i.e.,*

$$P^* \supseteq \{p \text{ prime such that } p \mid K_{\underline{k}} \text{ for some } \underline{k} \in \mathcal{A}_f\}.$$

We denote the set of these polynomials by $\mathcal{F}^*_{N,n}$. We are interested in how small could be the maximum $M_f$ of $f$ in the unit hypercube. We prove

**Theorem 2.1.** *We have*

$$\min_{f\in\mathcal{F}^*_{N,n}} \max_{\underline{x}\in[0,1]^n} f(\underline{x}) \geq e^{-(1+o(1))\alpha N \mathcal{H}_n}, \quad \text{as } N \to \infty,$$

*where* $\mathcal{H}_n = \sum_{\ell=1}^{n} 1/\ell$ *is the nth harmonic number.*

P r o o f. We let

$$I := \int_0^1 \int_0^1 \dots \int_0^1 f(x_1, x_2, \dots, x_n)\, dx_1 dx_2 \dots dx_n.$$

Calculating this integral gives

$$I = \left[ \sum_{\underline{k} \in \mathcal{A}_f} \frac{a_{\underline{k}} x_1^{k_1+1} x_2^{k_2+1} \dots x_n^{k_n+1}}{(k_1+1)(k_2+1)\dots(k_n+1)} \right]_{x_1,\dots,x_n=0}^{x_1,\dots,x_n=1},$$

hence

$$I = \sum_{\underline{k} \in \mathcal{A}_f} \frac{a_{\underline{k}}}{K_{\underline{k}}}.$$

Since $f$ is nonnegative (not identically zero), we know that $I$ is positive, then for some positive integer $A$ we have

$$I = \frac{A}{\operatorname{lcm}\{K_{\underline{k}},\ \underline{k} \in \mathcal{A}_f\}} \geq \frac{1}{\operatorname{lcm}\{K_{\underline{k}},\ \underline{k} \in \mathcal{A}_f\}}.$$

Let $\ell \in \{1, 2, \dots, n-1\}$ and $p \in P^*$ a prime number in the interval

$$\frac{N}{\ell+1} < p \leq \frac{N}{\ell}.$$

We first prove that if $p^\beta \mid K_{\underline{k}}$ for some $\underline{k} \in \mathcal{A}_f$, then $\beta \leq \ell$. Indeed

$$\beta \leq \sum_{i=1}^n v_p(k_i+1) \ = \sum_{\substack{i=1 \\ p \leq k_i+1}}^n v_p(k_i+1) \ = \sum_{\substack{i=1 \\ N/(\ell+1) < k_i+1}}^n v_p(k_i+1),$$

where we denote $v_p(k)$ to be the greater exponent $\beta$ such that $p^\beta \mid k$. By taking $N$ large enough, namely $N > n^2$, we cannot have $v_p(k_i+1) > 1$, hence we infer

$$\beta \ \leq \sum_{\substack{i=1 \\ N/(\ell+1) < k_i+1}}^n 1 < \ell + 1$$

by the condition $\sum_{i=1}^n (k_i+1) \leq N$. We now consider the prime numbers $p$ such that $p \leq N/n$. For any such prime $p$ and any exponent $\beta$ such that $p^\beta \mid K_{\underline{k}}$ one has

$$\beta \leq \sum_{i=1}^n v_p(k_i+1) \leq \frac{1}{\log p} \sum_{i=1}^n \log(k_i+1).$$

By investigating the maximum of the multivariate function

$$(x_1, \dots, x_n) \mapsto \sum_{i=1}^n \log x_i$$

subject to the condition $x_1 + \cdots + x_n \le N$, one easily deduces that

$$\beta \le \frac{n \log(N/n)}{\log p}.$$

It follows that $p^\beta \le (N/n)^n$. By collecting the preceding bounds we obtain

$$L_f^* := \prod_{p \in P^*} p^{\max_{\underline{k} \in \mathcal{A}_f} v_p(K_{\underline{k}})} \le \Big(\frac{N}{n}\Big)^{n\pi^*(N/n)} \times \prod_{\ell=1}^{n-1} \prod_{\substack{p \in P^* \\ N/(\ell+1) < p \le N/\ell}} p^\ell.$$

Taking the logarithm we get the bound

$$\log L_f^* \le n\pi^*(N/n)\log(N/n) + \sum_{\ell=1}^{n-1} \ell\Big(\theta^*(N/\ell) - \theta^*\big(N/(\ell+1)\big)\Big)$$

where $\theta^*(x) = \sum_{\substack{p \in P^* \\ p \le x}} \log p$. Hence rearranging the summation we finally infer

$$\log L_f^* \le \big(1 + o(1)\big) \sum_{\ell=1}^{n} \theta^*(N/\ell) \le \big(1 + o(1)\big)\alpha N \mathcal{H}_n.$$

since $\pi^*(x)\log x \le (1 + o(1))\theta^*(x) \le (1 + o(1))\alpha x$. Clearly

$$\operatorname{lcm}\{K_{\underline{k}},\ \underline{k} \in \mathcal{A}_f\} \le L_f^*.$$

Comparing the deduced lower bound $I \ge e^{-(1+o(1))\alpha N \mathcal{H}_n}$ with the plain upper bound $I \le M_f$ we get the desired result. □

**Remark.** Our argument is related to a similar reasoning that Gelfond followed in [5], the interesting being that it is used in the reverse direction.

## 3. The case: $F = F(x, y) \in \mathbb{F}_p[x, y]$

The analogous question in prime fields would be the following: any function from a given family of maps could not concentrated to some room of $\mathbb{F}_p$.

In the present section we will focus expander polynomials with two variables. Firstly we quote our result which gives an infinite family of expanders [6].

**Theorem 3.1.** *Let $k \ge 1$ be an integer and $f$, $g$ be polynomials with integer coefficients, and define for any prime number $p$, the map $F$ from $\mathbb{Z}^2$ onto $\mathbb{Z}$ by*

$$F(x, y) = f(x) + x^k g(y)$$

*Furthermore assume that $f(x)$ is affinely independent to $x^k$. Then $F$ is an expander.*

*Moreover if $\delta > 1/2$, then for any pair $(A,B)$ of subsets of $\mathbb{F}_p$ such that $|A| \asymp |B| \asymp p^\delta$, we have*

$$|F(A,B)| \gg |A|^{1+\frac{\min\{2\delta-1;2-2\delta\}}{2\delta}}.$$

Here two maps $f(x)$ and $h(x)$ are affinely independent if there is no $(u,v) \in \mathbb{Z}^2$ such that $f(x) = uh(x)+v$ or $h(x) = uf(x)+v$. Let us denote by $\mathcal{H}$ our infinite family of expanders.

We will show that each map in $\mathcal{H}$ is well-distributed in two meanings as well.

### 3.1. Equidistribution for mutisubset in $\mathbb{F}_p$

Let $M$ be a multisubset of $\mathbb{F}_p$. The usual meaning for equidistribution in the arithmetic progression of $\mathbb{F}_p$ could be stated as follows. A subset $I$ of $\mathbb{F}_p$ is called an interval if it is an arithmetic progression $\{u+kv,\ k=0,\dots,|I|-1\}$ with $u \in \mathbb{F}_p$ and $v \in \mathbb{F}_p \setminus \{0\}$. We denote by $\|M\|$ the size of the multiset $M$. The intersection $M \cap I$ is simply the multiset formed by the terms of $M$ which belongs to $I$, each of them counted according to its multiplicity in $M$.

**Definition.** Let $\epsilon > 0$ be a real number. The multiset $M$ is said to be $\epsilon$-equidistributed (in the arithmetic way) if for any interval $I$ of $\mathbb{F}_p$ we have

$$\left| \frac{\|M \cap I\|}{\|M\|} - \frac{|I|}{p} \right| < \epsilon.$$

Observe that if $M$ is $\epsilon$-equidistributed, then $M \cap I \neq \varnothing$ whenever $|I| > \epsilon p$.

We will use Fourier method. Recall some well-known facts: Let $\phi : \mathbb{F}_p \to \mathbb{C}$ and $x \in \mathbb{F}_p$, let $\hat{\phi}(x) := \sum_{y\in\mathbb{F}_p} \phi(y) e\big(\frac{yx}{p}\big)$, where $e(t) := \exp(2i\pi t)$. Briefly we write $e\big(\frac{\cdot}{p}\big) = e_p(\cdot)$. We also recall the Parseval identity

$$\sum_{y\in\mathbb{F}_p} |\hat{\phi}(y)|^2 = p \sum_{y\in\mathbb{F}_p} |\phi(y)|^2.$$

It appears that the notion of equidistribution can be reduced to bounding the associated Fourier coefficients

$$\max_{r\in\mathbb{F}_p\setminus\{0\}} \Big| \sum_{x\in M} e_p(rx) \Big|$$

by $\delta\|M\|$ for some sufficiently small positive number $\delta(\epsilon)$. It comes from the Weyl approach for the famous eponymous criterion for equiditribution modulo 1.

**Definition.** Let $\delta > 0$ be a real number. The multiset $M$ is said to be $\delta$-trignonometrically-equidistributed (in the arithmetic way) if we have

$$\max_{r\in\mathbb{F}_p\setminus\{0\}} \Big| \sum_{x\in M} e_p(rx) \Big| < \delta\|M\|.$$

In [4] the author verifies the effective equivalence of these two definitions: if $M$ is $\epsilon$-equidistributed, then $M$ is $\sqrt{\epsilon}$-trigonometrically-equiditributed; conversely if $M$ is $\epsilon$-trigonometrically-equidistributed, then $M$ is $O(\sqrt{\epsilon})$-equidistributed.

### 3.2. First meaning

**Definition.** Let $\alpha$ and $\varrho$ be two real numbers in $(0,1)$. We say that the map $F(x,y)$ is arithmetically well-distributed (a.w.d.) in order $(\alpha,\varrho)$, if for every $A\subseteq\mathbb{F}_p$ with $|A|\geq p^\alpha$ and for every interval $I=\{u+kv,\ k=0,\dots,|I|-1\}\subseteq\mathbb{F}_p$ with $|I|\gg p^\varrho$, we have $F(A,A)\cap I\neq\varnothing$.

We shall first prove

**Proposition 3.2.** *Let $F(x,y)\in\mathcal{H}$. Let $1/2<\alpha<1$ and let $\varrho$ such that $\varrho\geq 9/8-\alpha/4$. Then $F(x,y)$ is arithmetically well-distributed in order $(\alpha,\varrho)$.*

In the next we will show

$$\max_{r\in\mathbb{F}_p\setminus\{0\}}\Big|\sum_{x,y\in A}e_p\big(rF(x,y)\big)\Big|\ll\frac{p^{1/4}}{|A|^{1/2}}|A|^2. \tag{1}$$

It is clear from the preceding subsection that it is sufficient for the announced result.

P r o o f. Let

$$T_r:=\sum_{(x,y)\in A^2}e_p\Big(r\big(f(x)+x^kg(y)\big)\Big). \tag{2}$$

Using the triangle and the Cauchy-Schwarz inequalities,

$$|T_r|\leq\sum_{x\in A}\Big|\sum_{y\in A}e_p\big(rx^kg(y)\big)\Big|\leq|A|^{1/2}\cdot\bigg(\sum_{x\in\mathbb{F}_p}\sum_{y,y'\in A}e_p\Big(rx^k\big(g(y)-g(y')\big)\Big)\bigg)^{1/2}.$$

Letting $S_k(h)=\sum_{x\in\mathbb{F}_p}e_p(hx^k)$ and intervenrting summations on $x$ and $y,y'$, we infer

$$|T_r|\leq|A|^{1/2}\cdot\bigg(\sum_{y,y'\in A}S_k\Big(r\big(g(y)-g(y')\big)\Big)\bigg)^{1/2}.$$

When $g(y)\neq g(y')$ the Gauss sum can be bounded by $k\sqrt{p}$. Otherwise it is plainly equal to $p$. For a given $z$ the number of solutions $y$ in the equation $z=g(y)$ is bounded by some constant $C(g)$. Thus

$$|T_r|\leq|A|^{1/2}\cdot\big(k|A|^2\sqrt{p}+C(g)p|A|\big)^{1/2}\ll\frac{p^{1/4}}{|A|^{1/2}}|A|^2, \tag{3}$$

as requested. □

In fact we proved that if $|A| \gg p^\alpha$ and $|I| \gg p^\varrho$ with $\varrho \geq 9/8 - \alpha/2$, then

$$\|F(A,A) \cap I\| \gg \frac{|A|^2|I|}{p} \tag{4}$$

where $F(A,A)$ is considered as a multisubset of $\mathbb{F}_p$ which by a constant the best possible expected result. This implies $|F(A,A) \cap I| \gg |A||I|/p$, nevertheless this bound is possibly far from the average value $|F(A,A)||I|/p$.

Using the bound (1), we can provide a better result. We prove below that under the weaker hypothesis

$$|A||I|^2 \gg p^{5/2} \log^2 p,$$

the lower bound (4) remains valid: more precisely $\|F(A,A) \cap I\|$ is close to its expected value $|A|^2|I|/p$.

Denote

$$N := \Big|\{(x,y) \in A^2 : F(x,y) \in I\}\Big|.$$

Then

$$N = \frac{1}{p} \sum_{r \in \mathbb{F}_p} \sum_{(x,y) \in A^2} \sum_{t \in I} e_p\Big(r\big(f(x) + x^k g(y) - t\big)\Big).$$

Isolating the contribution from the term $r = 0$ we obtain

$$N \geq \frac{|I||A|^2}{p} - \frac{1}{p} \sum_{0<r<p} \Big|\sum_{t \in I} e_p(-rt)\Big| \Big|\sum_{(x,y) \in A^2} e_p\Big(\big(f(x) + x^k g(y)\big)\Big)\Big|.$$

Since $\sum_{t \in I} e_p(-rt)$ is a geometric summation, we have

$$\Big|\sum_{t \in I} e_p(-rt)\Big| \leq \frac{1}{|\sin(\pi r v/p)|},$$

thus

$$\sum_{0<r<p} \Big|\sum_{t \in I} e_p(-rt)\Big| \leq \sum_{0<r<p} \frac{1}{|\sin(\pi r v/p)|} = \sum_{0<r<p} \frac{1}{|\sin(\pi r/p)|} \leq \sum_{0<|r|<p/2} \frac{p}{2|r|} \leq p \log p.$$

Hence

$$N \geq \frac{|I||A|^2}{p} - (\log p) \cdot \max_{r \in \mathbb{F}_p \setminus \{0\}} T_r.$$

It follows by (3) that

$$N \geq \frac{|I||A|^2}{p} - O\big((\log p)(|A|^{3/2} p^{1/4} + |A| p^{1/2})\big),$$

where the implied constant depends on $F$. Finally $N$ is positive whenever

$$|A||I|^2 \gg p^{5/2}\log^2 p \text{ and } |A||I| \gg p^{3/2}\log p.$$

The latter condition being weaker than the former, we deduce the following result.

**Proposition 3.3.** *Let $F(x,y) \in \mathcal{H}$. Let $1/2 < \alpha < 1$ and set $\varrho_0(\alpha) = 5/4 - \alpha/2$. Then for any $\varrho > \varrho_0(\alpha)$, if $|I| \gg p^{\varrho}$ and $|A| \gg p^{\alpha}$, then*

$$\|F(A,A) \cap I\| = \big(1+o(1)\big)\frac{|A|^2|I|}{p}, \quad \text{as } p \to \infty.$$

*It implies that the function $F(x,y)$ is arithmetically well-distributed in order $(\alpha,\varrho)$.*

For an interval $I = \{a, a+d, a+2d, \dots, a+(k-1)d\}$ in $\mathbb{F}_p$ of size $k$, we have $I \supset J + J$, where $J = \overline{2}a + \{0, d, 2d, \dots, \lfloor (k-1)/2 \rfloor d\}$, where $\overline{x}$ denotes the multiplicative inverse of $x \in F$. We observe that $F(A,A) \cap I \neq \varnothing$ if $F(A,A) \cap (J+J) \neq \varnothing$, namely by using Fourier analysis

$$M := \sum_r T_r(\widehat{J}(r))^2 = \sum_{r\in\mathbb{F}_p} \sum_{a,b\in A} \sum_{x,y\in J} e_p\Big(r\big(F(a,b)-x-y\big)\Big) > 0,$$

where $\widehat{J}$ is the Fourier transform of the characteristic function of $J$. Clearly,

$$M \geq |A|^2|J|^2 - p\max_{r\neq 0}|T_r||J|.$$

From (1), it follows that $M > 0$ whenever $|A|^{1/2}|J| \gg p^{5/4}$. Since $|J| \gg |I|$, we infer the next result.

**Theorem 3.4.** *Under the notation of Proposition 3.3, for any $\varrho \geq \varrho_0(\alpha)$ and $p$ large enough, the function $F(x,y)$ is arithmetically well-distributed in order $(\alpha,\varrho)$.*

**Remark.** In the same way and by considering Weil's bound for trigonometric sums

$$\Big|\sum_{x\in\mathbb{F}_p} e_p\big(h(x)\big)\Big| \leq \big(\deg(h)-1\big)\sqrt{p}$$

which holds for any polynomial $h$, we could extend Theorem 3.4 to function $F(x,y) = f(x) + h(x)g(y)$ for non-constant polynomials $f, g$ and $h$.

### 3.3. Second meaning

A geometric interval $I$ is a subset of $\mathbb{F}_p \setminus \{0\}$ which can be written as $I = \{uv^k,\ k = 0, \dots, |I|-1\} \subseteq \mathbb{F}_p \setminus \{0\}$ for some $u, v \in \mathbb{F}_p \setminus \{0\}$.

**Definition.** Let $\alpha$ and $\varrho$ be two real numbers in $(0,1)$. We say that the map $F(x,y)$ is geometrically well-distributed (g.w.d.) in order $(\alpha,\varrho)$, if for every $A\subseteq\mathbb{F}_p\setminus\{0\}$ with $|A|\geq p^\alpha$, and for every geometric interval $I=\{uv^k,\ k=0,\dots,|I|-1\}\subseteq\mathbb{F}_p\setminus\{0\}$ with $|I|\gg p^\varrho$, we have $F(A,A)\cap I\neq\varnothing$ (or alternatively $\|F(A,A)\cap I\|\gg|A|^2|I|/p$).

We shall prove

**Theorem 3.5.** *Let $F(x,y)\in\mathcal{H}$. Let $1/2<\alpha<1$ and set $\varrho_0(\alpha)=5/4-\alpha/2$. Assume that $A$ is a subset of $\mathbb{F}_p\setminus\{0\}$ of size $p^\alpha$ and $I$ is a geometric interval of size $p^\varrho$. Then*

(i) *If $\varrho>\varrho_0(\alpha)$, one has $\|F(A,A)\cap I\|=\big(1+o(1)\big)|A|^2|I|/p$ as $p\to\infty$.*

(ii) *If $\varrho\geq\varrho_0(\alpha)$ and $p$ large enough, one has $\|F(A,A)\cap I\|\gg|A|^2|I|/p$, namely $F(x,y)$ is geometrically well-distributed in order $(\alpha,\varrho)$.*

P r o o f o f (i). Comparing to the proof of Proposition 3.3 we consider instead

$$E_\chi=\sum_{x,y\in A}\chi\big(f(x)+x^kg(y)\big)$$

where $\chi$ is any non-trivial multiplicative characters modulo $p$. By the triangle inequality

$$|E_\chi|\leq\sum_{x\in A}\Big|\sum_{y\in A}\chi\big(x^{-k}f(x)+g(y)\big)\Big|$$

Let $U$ (resp. $V$) be the set $u$ (resp. $v$) which can be written as $u=x^{-k}f(x)$ (resp. $v=g(x)$) with $x\in A$. We also denote $r(u)$ (resp. $s(v)$) the number of $x\in A$ such that $u=x^{-k}f(x)$ (resp. $v=g(x)$).

The summation on $x$ can be written and bounded by the Cauchy-Schwarz inequality as

$$\begin{aligned}|E_\chi|&\leq\sum_u r(u)\Big|\sum_{v\in V}s(v)\chi(u+v)\Big|\\&\leq\Big(\sum_{u\in U}r(u)^2\Big)^{1/2}\left(\sum_{v,v'\in V}s(v)s(v')\Big|\sum_{u\in U}\chi(u+v)\chi(u+v')\Big|\right)^{1/2}.\end{aligned}$$

We may observe here that both functions $r(u)$ and $s(v)$ are bounded by some constant depending only on the given map $F$. When $v\neq v'$, the sum on $u$ is bounded by $O(\sqrt{p})$ by Johnsen's Theorem (cf. [10]). Since $|U|,|V|\leq|A|$ we finally obtain for any $\chi\neq\chi_0$

$$|E_\chi|\ll|A|^{3/2}p^{1/4}+|A|p^{1/2},\tag{5}$$

where the implied constant depends only on the given function $F$. Now we deduce

$$\begin{aligned}\|F(A,A)\cap I\| &= \frac{1}{p}\sum_{\chi}\sum_{t\in I}\sum_{x,y\in A}\chi\big(f(x)+x^k g(y)\big)\overline{\chi(t)}\\ &= \frac{|A|^2|I|}{p-1} - O\big((\log p)(|A|^{3/2}p^{1/4}+|A|p^{1/2})\big),\end{aligned}$$

where we isolated the contribution of the principal character $\chi_0$ and used the bound

$$\sum_{\chi\neq\chi_0}\Big|\sum_{t\in I}\chi(t)\Big| \le p\log p \tag{6}$$

which can be obtained in a straightforward way by expliciting the characters $\chi$ as

$$\chi_q(t) = \exp\Big(\frac{2\pi i q\,\mathrm{ind}_\omega(t)}{p-1}\Big),\ q=0,\dots,p-2,$$

for some fixed primitive root $\omega$ modulo $p$ and where $t=\omega^{\mathrm{ind}_\omega(t)}$. Then letting $\ell=\mathrm{ind}_\omega(v)$, we get for each $q=1,\dots,p-2$,

$$\Big|\sum_{t\in I}\chi_q(t)\Big| = \Big|\sum_{0\le k\le |I|-1}\chi_q(uv^k)\Big| = \Big|\sum_{k=0}^{|I|-1}\exp\Big(\frac{2\pi i q k\ell}{p-1}\Big)\Big| \le \frac{1}{|\sin(\pi q\ell/(p-1))|}$$

and the desired result (6) follows. □

P r o o f o f (i i). The proof is the mutiplicative analogue of that of Theorem 3.4. For

$$I=\{uv^j,\ j=0,\dots,k-1\},$$

we write $I\supset uJ\cdot J$, where $J=\{v^j,\ j=0,\lfloor(k-1)/2\rfloor\}$. Clearly $\|F(A,A)\cap I\|\gg \|F(A,A)\cap(J+J)\|/|J|\gg |A|^2|J|/p\gg |A|^2|I|/p$ if

$$\sum_{\chi}E_\chi\overline{\chi(u)}\Big(\sum_{x\in J}\overline{\chi(x)}\Big)^2 - |A|^2|J|^2 \gg \max_{\chi\neq\chi_0}|E_\chi|\sum_{\chi}\Big|\sum_{x\in J}\chi(x)\Big|^2.$$

By Parseval and (5), we conclude. □

Similarly to the ending remark of the preceding subsection, we could extend Theorem 3.5 to functions $F(x,y)=f(x)+h(x)g(y)$ with non-constant polynomials $f,g,h$.

Both preceding results Theorems 3.4 and 3.5 on equidistribution concern functions $F(x,y)$ having the property that $F(x,y)-f(x)$ is a product $x^kg(y)$ with separate variables, and $F(x,y)x^{-k}=f(x)x^{-k}+g(y)$ is a sum, where the variables $x,y$ are also separated. This is not the case of the function $x^2y+xy^2$. Nevertheless it could be proved that it is well-distributed in similar order according to both meanings, even if it is not known that it is an expander (see details in [7]).

Under some natural restrictive condition, the same could be proved with map of the type $u(x)v(y)+w(x)t(y)$. We focus here on the map $x^2y+xy^2$.

**Proposition 3.6.** *Let $1/2<\alpha<1$ be a number. Then*

(i) *The function $f(x,y)=x^2y+xy^2$ is a.w.d and g.w.d. in order $(\alpha,\varrho)$ if $\varrho\geq 5/4-\alpha/2$.*

(ii) *The function $f(x,y)$ is a.w.d. in order in order $(\alpha,\varrho)$ if $\varrho\geq 11/8-3\alpha/4$.*

P r o o f. In view of the preceding proofs it is only needed to bound, in an efficient way, both characters sums

$$\sum_{x,y\in A} e_p\big(r(x^2y+xy^2)\big) \quad \text{and} \quad \sum_{x,y\in A}\chi\big((xy(x+y)\big)$$

when $r\neq 0$ and $\chi\neq\chi_0$.
For the first, we only consider the case $r=1$ and we have by Cauchy-Schwarz

$$\Big|\sum_{x,y\in A} e_p(x^2y+xy^2)\Big| \leq \sum_{x\in A}\Big|\sum_{y\in A} e_p(x^2y+xy^2)\Big|$$
$$\leq |A|^{1/2}\Big(\sum_{x\in\mathbb{F}_p}\sum_{y,y'\in A} e_p\Big((y-y')\big(x^2+(y+y')x\big)\Big)\Big)^{1/2}.$$

We denote by $\overline{x}$ the multiplicative inverse of $x\in\mathbb{F}_p\setminus\{0\}$. The inner summation can be inverted and bounded by

$$p|A|+\Big|\sum_{y\neq y'\in A} e_p\big(-\overline{2}^2(y-y')(y+y')^2\big)S(y-y',p)\Big|,$$

where $S(a,p)$ is the Gauss sum $\sum_{x\in\mathbb{F}_p} e_p(ax^2)=\sum_{z\in\mathbb{F}_p}\chi_L(z)e(az)$, where $\chi_L$ is the Legendre character, $a\neq 0$. It is well known that for odd prime numbers $p$

$$S(a,p)=\chi_L(a)\epsilon_p\sqrt{p}, \tag{7}$$

where $\epsilon_p=1$ or $i$ according to $p\equiv 1$ or $3\pmod 4$. Hence we get

$$\Big|\sum_{x,y\in A} e_p(x^2y+xy^2)\Big|\leq p^{1/2}|A|+p^{1/4}|A|^{3/2}.$$

We can do slightly sharper: for this we need to bound

$$Q:=\sum_{y\neq y'\in A}\chi_L(y-y')e_p\big(-\overline{2}^2(y-y')(y+y')^2\big).$$

By the triangle and the Cauchy-Schwarz inequalities we have

$$|Q|^2\leq |A|\Big(\sum_{y',y''\in A}\sum_{y\in\mathbb{F}_p}\chi_L(y-y')\chi_L(y-y'')e_p\Big(\overline{2}^2(y''-y')\big(y^2-(y'+y'')y\big)\Big)\Big),$$

hence

$$|Q|^2 \leq |A|\Big(p|A| + \sum_{y'\neq y''\in A}\Big|\sum_{y\in\mathbb{F}_p}\chi_L(y-y')\chi_L(y-y'')e_p\Big(\overline{2}^2(y''-y')\big(y-\overline{2}(y'+y'')\big)^2\Big)\Big|\Big).$$

Letting $z = y - \overline{2}(y'+y'')$, $z' = \overline{2}y'$ and $z'' = \overline{2}y''$ the inner sum can be written as

$$\sum_{z\in\mathbb{F}_p}\chi_L(z+z''-z')\chi_L(z+z'-z'')e_p\big(\overline{2}(z''-z')z^2\big).$$

We shall use the following lemma.

**Lemma 3.7.** *Let $a, b \in \mathbb{F}_p \setminus \{0\}$. One has*

$$\Big|\sum_{z\in\mathbb{F}_p}\chi_L(z^2-b)e_p(az^2)\Big| \leq 3\sqrt{p}.$$

P r o o f. Denote by $T$ the sum considered in the statement. Then

$$\begin{aligned} T &= \sum_{w\in\mathbb{F}_p}\big(\chi_L(w)+1\big)\chi_L(w-b)e_p(aw) \\ &= \sum_{w\in\mathbb{F}_p}\chi_L\big(w(w-b)\big)e_p(aw) + \sum_{w\in\mathbb{F}_p}\chi_L(w-b)e_p(aw). \end{aligned}$$

In view of (7) the last sum is

$$\sum_{v\in\mathbb{F}_p}\chi_L(v)e_p\big(a(v+b)\big) = e_p(ab)S(a,p) = e_p(ab)\chi_L(a)\epsilon_p\sqrt{p}.$$

Hence

$$T - e_p(ab)\chi_L(a)\epsilon_p\sqrt{p} \;=\; \sum_{w\in\mathbb{F}_p}\Big(\chi_L\big(w(w-b)\big)+1\Big)e_p(aw).$$

Since the expression $\chi_L(w(w-b))+1 = 2, 1$ or $0$ detects if $w(w-b)$ is a non zero square modulo $p$, zero or a non square modulo $p$ respectively, one has

$$T - e_p(ab)\chi_L(a)\epsilon_p\sqrt{p} \;=\; \sum_{\substack{w,t\in\mathbb{F}_p\\ w(w-b)=t^2}} e_p(aw).$$

Letting $u = 2\overline{b}(w-\overline{2}b+t)$ and $v = 2\overline{b}(w-\overline{2}b-t)$, one infers $w = \overline{2}^2b(u+v+2)$ and

$$T - e_p(ab)\chi_L(a)\epsilon_p\sqrt{p} = e_p(\overline{2}ab)\sum_{\substack{u,v\in\mathbb{F}_p\\ uv=1}} e_p\big(\overline{2}^2ab(u+v)\big)$$

yielding a Kloosterman sum that can be classically bounded by $2\sqrt{p}$ (see [18]). We conclude that $|T| \leq 3\sqrt{p}$. □

Returning to our problem we get $|Q|^2 \le p|A|^2 + 3|A|^3\sqrt{p}$ and finally

$$\Big|\sum_{x,y\in A} e_p(x^2y+xy^2)\Big| \le |A|^{1/2}\big(p|A|+p^{1/2}|Q|\big)^{1/2} \ll p^{1/2}|A|+p^{3/8}|A|^{5/4}$$

giving the statement (ii) in Proposition 3.6, arguing as in the proof of Theorem 3.4.

Concerning the multiplicative distribution, when $\chi \neq \chi_0$ we have

$$\begin{aligned}\Big|\sum_{x,y\in A}\chi\big(xy(x+y)\big)\Big| &\le \sum_{x\in A}\Big|\sum_{y\in A}\chi(y)\chi(x+y)\Big| \\ &\le |A|^{1/2}\Big(p|A| \ + \sum_{\substack{y,y'\in A\\ y\neq y'}}\sum_{x\in\mathbb{F}_p}\chi(x+y)\overline{\chi(x+y')}\Big)^{1/2}.\end{aligned}$$

By Johnsen's bound on the inner character sum, we finally get

$$\Big|\sum_{x,y\in A}\chi\big(xy(x+y)\big)\Big| \ll p^{1/2}|A|+p^{1/4}|A|^{3/2}.$$

The rest of the proof is clear by mimicking Theorem 3.5. □

## 4. Covering rational functions in $\mathbb{F}_p \setminus \{0\}$

One can expect that an expander $F(x,y)$ which blows up the size of its argument set, will cover many elements with respect with the size of $A$ and $B$. Indeed in [13] Shkredov showed that for the Bourgain's function $G(x,y)=x^2+xy$, $|G(A,B)| \ge (p-1)-\frac{40p^{5/2}}{|A||B|}$, thus if $|A||B| > p^{3/2+\varepsilon}$, $\varepsilon>0$, then $G(A,B)$ covers almost all $\mathbb{F}_p\setminus\{0\}$. This also shows that the equation $G(x,y)=z$, $(x,y,z)\in A\times B\times C$ has always a solution whenever $|A||B||C| \gg p^{5/2}$, namely both 3-variable covering functions $G(x,y)-z$ and $G(x,y)z$ are covering $\mathbb{F}_p$ as soon as the variables range in sufficiently big sets $A,B,C$.

In [12] Sárközy proved the following assertion. 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 at least a solution, provided $|A||B||C||D| > p^3$. This immediately implies that for the map $F(x,y,z,w)=x+y+zw$, one has $F(A,B,C,D)=\mathbb{F}_p$, for the indicated range of the sets $A,B,C,D$ (see also [14], [8]).

In [6] we proved the following statement.

**Theorem 4.1.** *There exist real numbers $0 < \delta, \delta' < 1$ such that for any $p$ and for any sets $A, B, C, D \subseteq \mathbb{F}_p$ with*

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

*there exist $a \in A, b \in B, c \in C, d \in D$ solving the equation*

$$a + b = F_{p,v}(c, d)$$

*and*

$$a + b = G_u(c, d),$$

*where $G_u(x, y) = x^{1+u}y + x^{2-u}h(y)$; $u \in \{0, 1\}, h(y) \in \mathbb{Z}[y]$ and $F_{p,v}(x, y) = x^{1+u}y + x^{2-u}g_p^y$, $g_p$ generates $\mathbb{F}_p^\times$ and $v \in \{0, 1\}$ is fixed.*

*Equivalently the maps $F_{p,v}(x, y) + z + w$ and $G_u(x, y) + z + w$ are covering polynomials on the indicated regions.*

The aim of this section is to show that some 'dilatations' of an expander polynomial also are covering rational functions on a given range.

More precisely

**Theorem 4.2.** *Let $F(x, y) = f(x) + x^k g(y)$ be the map defined in Theorem 3.1 and let $G(x, y, z, w) := F(x, y)(\alpha z + \beta w)^{-1}$, where $\alpha, \beta \in \mathbb{F}_p \setminus \{0\}$. Then if $|A||B||C| \gg p^{5/2}$, then $G(A, A, B, C)$ covers $\mathbb{F}_p \setminus \{0\}$.*

P r o o f. Changing $B$ and $C$ into $\alpha B$ and $-\beta C$ respectively we may assume that $\alpha = -\beta = 1$.

Let $h$ be any element of $\mathbb{F}_p \setminus \{0\}$. Denote by $N_G(h)$ the cardinality of the set

$$\Big\{(x, y, z, w) \in A \times A \times B \times C : \big(f(x) + x^k g(y)\big)(z - w)^{-1} = h\Big\}.$$

We again use Fourier analysis: we have

$$N_G(h) = \frac{1}{p} \sum_{r \in \mathbb{F}_p} \sum_{(x,y) \in A^2} \sum_{\substack{z \in B; w \in C \\ z \neq w}} e_p\Big(r\big(f(x) + x^k g(y) - h(z - w)\big)\Big). \tag{8}$$

Separating the contribution due to $r = 0$, we get

$$\begin{aligned} N_G(h) &\geq \frac{|A|^2|B||C|}{p} - \\ &\quad - \frac{1}{p} \sum_{r \in \mathbb{F}_p \setminus \{0\}} \Big| \sum_{\substack{z \in B; w \in C \\ z \neq w}} e_p\big(rh(z - w)\big)\Big| \cdot \Big| \sum_{(x,y) \in A^2} e_p\Big(r\big(f(x) + x^k g(y)\big)\Big)\Big| \\ &\geq \frac{|A|^2|B||C|}{p} - \Big(\max_{r \in \mathbb{F}_p \setminus \{0\}} |T_r|\Big) \times \frac{1}{p} \sum_{r \in \mathbb{F}_p} \Big| \sum_{\substack{z \in B; w \in C \\ z \neq w}} e_p\big(rh(z - w)\big)\Big|. \end{aligned}$$

In view of the bound (1) it remains to bound the sum on $r$. We have

$$\sum_{r\in\mathbb{F}_p}\Big|\sum_{\substack{z\in B;w\in C\\ z\neq w}} e_p\big(rh(z-w)\big)\Big| = \sum_{r\in\mathbb{F}_p}\Big|\sum_{z\in B;w\in C} e_p\big(rh(z-w)\big)\Big| + p|B\cap C|$$
$$\leq \Big(\sum_{r\in\mathbb{F}_p}|\hat{B}(rh)|^2\Big)^{1/2}\Big(\sum_{r\in\mathbb{F}_p}|\hat{C}(rh)|^2\Big)^{1/2} + p\min(|B|,|C|)$$
$$\leq 2p\sqrt{|B||C|}$$

by Cauchy-Schwarz inequality and Parseval identity. We thus infer from (1)

$$N_G(h) \geq \frac{|A|^2|B||C|}{p} - O(|A|^{3/2}p^{1/4}|B|^{1/2}|C|^{1/2}).$$

Hence the result. □

**Remark.** Shkredov conjectured in [13] that his method could provide a solution to the equation $z = F(x,y)$ for $(x,y,z)\in X\times Y\times Z$ whenever $|X||Y||Z| \gg p^{5/2}$. The above result, as the next one, gives a weak version of Shkredov's conjecture: we stress the fact that our results need an additional variable.

**Theorem 4.3.** *Let $F(x,y)$ be the map defined in Theorem 3.1 and let*

$$H(x,y,z,w) := F(x,y)zw.$$

*Then if $|A||B||C| \gg p^{5/2}$, then $H(A,A,B,C)$ covers $\mathbb{F}_p\setminus\{0\}$.*

P r o o f. The proof is similar to the preceding. For any $h\in\mathbb{F}_p\setminus\{0\}$, we denote $N_H(h)$ the number of quadruples $(x,y,z,w)\in A\times A\times B\times C$ such that $h = F(x,y)zw$. We have

$$N_H(h) = \frac{1}{p-1}\sum_{\chi}\sum_{(x,y)\in A^2}\chi\big(F(x,y)\big)\sum_{z\in B}\chi(z)\sum_{w\in C}\chi(w)\overline{\chi(h)},$$

where the sum is extended over all multiplicative characters $\chi$ of $\mathbb{F}_p\setminus\{0\}$. The number of pairs $(x,y)\in A^2$ such that $F(x,y)=0$ is a $O(|A|)$ hence

$$N_H(h) \geq \frac{(|A|^2 - O(|A|)|B||C|}{p-1}$$
$$-\frac{1}{p-1}\Big(\max_{\chi\neq\chi_0}\Big|\sum_{(x,y)\in A^2}\chi\big(F(x,y)\big)\Big|\Big)\sum_{\chi}\Big|\sum_{z\in B}\chi(z)\Big|\Big|\sum_{w\in C}\chi(w)\Big|.$$

By (5), Cauchy-Schwarz inequality and Parseval identity, we get

$$N_H(h) \geq \frac{(|A|^2 - O(|A|)|B||C|}{p-1} - O\big(|A|^{3/2}p^{1/4}|B|^{1/2}|C|^{1/2}\big),$$

which is positive whenever $|A||B||C| \gg p^{5/2}$, as asserted. □

We now consider the question of covering $\mathbb{F}_p \setminus \{0\}$ by a sufficiently large number of copies of the expander $F(x,y)$.

**Theorem 4.4.** *Let $F(x,y) = f(x) + x^k g(y)$ be the map defined in Theorem 3.1 and let $J(x,y,z,w,u,v) := F(x,y)F(z,w)F(u,v)$. Then if $|A| \gg p^{0.7}$, then $J(A,A,A,A,A,A)$ covers $\mathbb{F}_p \setminus \{0\}$.*

P r o o f. Let $h \in \mathbb{F}_p \setminus \{0\}$. The number $N_J(h)$ of 6-tuples $(x,y,z,w,u,v) \in A^6$ such that $h = F(x,y)F(z,w)F(u,v)$ is at least

$$N_J(h) \geq \frac{|A|^6}{p-1} - \frac{1}{p-1}\Big(\max_{\chi \neq \chi_0} |E_\chi|\Big) \sum_\chi |E_\chi|^2,$$

where $E_\chi$ has been defined in the proof of Theorem 3.5. We use (5) for bounding $\max_{\chi\neq\chi_0} |E_\chi|$. We now deal with the sum $\sum_\chi |E_\chi|^2$. A direct approach would lead to the bound $\sum_\chi |E_\chi|^2 = O(|A|^3)$ yielding the condition $|A| \gg p^{5/6}$. By a more thorough study we shall obtain a better result.

One first has

$$\frac{1}{p-1}\sum_\chi |E_\chi|^2 \leq \big|\big\{(x_1,x_2,y_1,y_2) \in A^4 \,:\, f(x_1) + x_1^k g(y_1) = f(x_2) + x_2^k g(y_2)\big\}\big|.$$

At this point we may use an incidence theorem given by the Bourgain-Katz-Tao bound (see [3] or [9] or [11] for an effective version). Under the assumption $|A| < p^{1-\epsilon}$ we shall obtain a positive number $\eta = \eta(\epsilon)$ such that there are at most $O(|A|^{3-\eta})$ quadruples $(x_1,x_2,y_1,y_2) \in A^4$ satisfying $f(x_1) + x_1^k g(y_1) = f(x_2) + x_2^k g(y_2)$. By [11], $\eta = 1/403 + o(1)$ is admissible when $|A| < \sqrt{p}$. For bigger $A$, namely $|A| = p^\delta > \sqrt{p}$, we may use Vinh's result implying that the choice $\eta = \frac{\min(\delta - 1/2, 1-\delta)}{\delta}$ is possible (cf. [17]): written in a different way the number of incidences is $O(|A|^4 p^{-1} + |A|^2 p^{1/2})$.

Here follows the appropriate application of the above quoted incidence results.

**Lemma 4.5.** *Let $u(x), v(x), w(x) \in \mathbb{F}_p[x]$ be non constant polynomials and let $A \subset \mathbb{F}_p$. We assume that the number of couples $(\alpha,\beta)$ such that $\gcd(u(x_2) - \alpha u(x_1), w(x_1) - w(x_2) - \beta u(x_1)) \neq 1$ is less than $M \geq 1$. Then the number $N'$ of quadruples $(x_1,x_2,y_1,y_2) \in A^4$ such that $u(x_1)v(y_1) - u(x_2)v(y_2) = w(x_1) - w(x_2)$ is $O(|A|^{3-\eta})$, where the constant implied in the $O$ depends only on the maximum $D$ of the degrees of the polynomials $u, v, w$ and on $M$.*

P r o o f. For each $Y \in \mathbb{F}_p$, denote by $|v^{-1}(Y)|$ the number of $y \in A$ such that $Y = v(y)$. Then clearly $|v^{-1}(Y)| \leq \deg(v) \leq D$. Let $\ell(x_1,x_2)$ be the line in ${\mathbb{F}_p}^2$ defined by the equation in variables $Y_1, Y_2$: $u(x_1)Y_1 - u(x_2)Y_2 = w(x_1) - w(x_2)$. We first investigate incidences with $u(x_1) = 0$. There are at most $\deg u$ such

elements $x_1 \in A$. For $u(x_2) = 0$ this gives less than $|A|^2$ points on each such line $\ell(x_1, x_2)$. For $u(x_2) \neq 0$, we then get only the points $(Y_1, -(w(x_1) - w(x_2))/u(x_2))$ on the line $\ell(x_1, x_2)$. Hence the number of incidences with $u(x_1) = 0$ is less than $(D^2 + D)|A|^2$. We denote by $\mathcal{L}$ the set of all lines $\ell(x_1, x_2)$ such that $u(x_1) \neq 0$. One thus has

$$N' \leq \sum_{Y_1, Y_2} |v^{-1}(Y_1)||v^{-1}(Y_2)| \sum_{\alpha,\beta} R(\alpha, \beta)\mathbb{1}_{Y_1 - \alpha Y_2 = \beta} + (D^2 + D)|A|^2,$$

where $R(\alpha, \beta)$ is the number of couples $(x_1, x_2) \in A^2$ such that $u(x_2) = \alpha u(x_1)$ and $w(x_1) - w(x_2) = \beta u(x_1)$ with $u(x_1) \neq 0$, and $\mathbb{1}_{\mathcal{C}} = 0$ or 1 according to the validity of the condition $\mathcal{C}$. The above equations define together the intersection of two curves in ${\mathbb{F}_p}^2$. In the case where the polynomials $P_\alpha(x_1, x_2) = u(x_2) - \alpha u(x_1)$ and $Q_\beta(x_1, x_2) = w(x_1) - w(x_2) - \beta u(x_1)$ are coprime then it is well known that the intersection of the corresponding curves has at most $\deg P_\alpha \times \deg Q_\beta \leq D^2$ pairs $(x_1, x_2)$ giving $R(\alpha, \beta) \leq D^2$. Now let $\alpha$, $\beta$ such that $P_\alpha$ and $Q_\beta$ are not coprime, we get at most $D|A|$ pairs $(x_1, x_2)$ such that $P_\alpha(x_1, x_2) = Q_\beta(x_1, x_2) = 0$ and at most $|A|$ incidences $(\alpha Y_2 + \beta, Y_2) \in \ell(x_1, x_2)$. By assumption there are at most $M$ such pairs $(\alpha, \beta)$, thus we infer

$$N' \leq D^4 \sum_{\ell \in \mathcal{L}} \sum_{(Y_1, Y_2) \in \ell \cap v(A)^2} 1 + (MD^3 + D^2 + D)|A|^2.$$

Since $|\mathcal{L}| \leq |A|^2$ and $|v(A)| \leq |A|$, we obtain the desired result by the Bourgain-Katz-Tao theorem. □

We now finish the proof of Theorem 4.4 keeping the notation for $P_\alpha$ and $Q_\beta$. We see that with the choice $u(x) = x^k$ and $w(x)$ not being on the form $\lambda x^k + \mu$, the hypotheses of Lemma 4.5 are satisfied. Indeed $x_2^k = \alpha x_1^k$ is possible only if $\alpha$ is $k$-th power. Fixing $K$ any algebraic closure of $\mathbb{F}_p$, there exists $\omega \in K$ such that $\omega^k = \alpha$ and consequently $P_\alpha(x_1, x_2) = \prod_{j=0}^{k-1}(x_2 - \zeta^j \omega x_1)$ where $\zeta$ is a primitive $k$-th root of the unity in $K \setminus \{0\}$. But $\gcd(P_\alpha, Q_\beta) \neq 1$ implies $Q_\beta(X, \zeta^j wX) = 0$ for some $j$, yielding the polynomial identity

$$w(\zeta^j \omega X) - w(X) = \beta X^k. \tag{9}$$

Write $w(X) = \sum_{i=0}^{d} w_i X^i$. Clearly we must have $\beta = (\alpha - 1)w_k$ by identifying the coefficients. Moreover, since $w(x)$ is not affinely dependent to $x^k$, there exists $i \neq k$ such that $w_i \neq 0$. Hence $\zeta^i \omega^i = 1$ by (9), and taking the $k$-th power, $\alpha^i = 1$. It follows that $\alpha$ is a root of unity in $K$ of degree less than than or equal to $d = \deg w$. We thus have proved that the number of pairs $(\alpha, \beta)$ for which $P_\alpha$ and $Q_\beta$ are not coprime is less than $d^2$.

We may thus apply Lemma 4.5 with $M = d^2$. We obtain

$$N_J(h) \geq \frac{|A|^6}{p} - O\left(|A|^{9/2-\eta}p^{1/4}\right),$$

which is positive whenever

$$|A|^{3/2+\eta} \gg p^{5/4}, \tag{10}$$

where for $|A| = p^\delta \geq p^{1/2}$, we have $\eta = \min(\delta - 1/2, 1-\delta)/\delta$. A sufficient condition for (10) is $\min(5\delta/2 - 1/2, \delta/2 + 1) \geq 5/4$, namely $\delta \geq 7/10$. This ends the proof of Theorem 4.4. □

Considering Theorem 4.2, we may ask a similar result of covering with the function $(z-w)F(x,y)$. We would need a good bound for

$$\sum_{\substack{x,y\in A\\ F(x,y)\neq 0}} e_p\big(rF(x,y)^{-1}\big), \qquad r \neq 0,$$

which is seemingly out of reach. Instead we shall prove the following:

**Theorem 4.6.** *Let $F(x,y)$ be the map defined in Theorem 3.1 and let*

$$K(x,y,z,w,u,v) := (z-w)\big(F(x,y) - F(u,v)\big).$$

*Then if $|A| \gg p^{2/3}$, then $K(A,A,A,A,A,A)$ covers $\mathbb{F}_p \setminus \{0\}$.*

P r o o f. We start by bounding the sum

$$S_r := \sum_{\substack{x,y,u,v\in A\\ F(x,y)\neq F(u,v)}} e_p\Big(r\big(F(x,y) - F(u,v)\big)^{-1}\Big), \qquad r \neq 0.$$

We have by orthogonality and using the notation (2)

$$\begin{aligned} S_r &= \sum_{x,y,u,v\in A} \frac{1}{p}\sum_{h=1}^{p}\sum_{t\neq 0} e_p\big(h(F(x,y) - F(u,v) - t)\big)e_p(rt^{-1}) \\ &= \frac{1}{p}\sum_{h=1}^{p}\Big(\sum_{t\neq 0} e_p(rt^{-1} - ht)\Big)|T_h|^2. \end{aligned}$$

Then

$$|S_r| \leq \frac{|A|^4}{p} + \frac{1}{p}\sum_{h\neq 0}\Big|\sum_{t\neq 0} e_p(rt^{-1} - ht)\Big||T_h|^2.$$

The inner sum is a Kloosterman sum that can be bounded by $2\sqrt{p}$ (cf.[18]). Moreover we have

$$\frac{1}{p}\sum_h |T_h|^2 = \big|\big\{(x_1,x_2,y_1,y_2)\in A^4 \,:\, f(x_1)+x_1^k g(y_1) = f(x_2)+x_2^k g(y_2)\big\}\big|$$
$$\ll \frac{|A|^4}{p} + |A|^2\sqrt{p}$$

as it was shown in the proof of Theorem 4.4. We deduce

$$|S_r| \ll \frac{|A|^4}{p} + \Big(\frac{|A|^4}{p} + |A|^2\sqrt{p}\Big)\sqrt{p} \ll \frac{|A|^4}{\sqrt{p}} + |A|^2 p.$$

Using the Parseval identity and the above bound, we obtain that the number of representations of $h$ under the form $h = (F(x,y)-F(u,v))(w-z)$, with $x,y,u,v,z,w\in A$, is at least

$$\frac{|A|^6}{p} - O\Big(\frac{|A|^4}{\sqrt{p}} + |A|^2 p\Big)|A|,$$

which is positive whenever $|A| \gg p^{2/3}$. □

**Acknowledgement.** This work is supported by OTKA grants K-81658, K-100291 and by 'ANR CAESAR' ANR-12-BS01-0011.

REFERENCES

[1] BARAK, B.—IMPAGLIAZZO, R.—WIGDERSON A.: *Extracting Randomness from Few Independent Sources*, in Proc. 45th FOCS. IEEE, 2004.

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

[3] Bourgain, J.—Katz, N.—Tao T. *A sum-product theorem in finite fields and application*, Geom. Funct. Anal. **14** (2004), 27–57.

[4] BRINGER, S.: *Equidistribution in certain multisets*, preprint.

[5] GELFOND, A.: *On prime numbers*, in: *Collexted Works of P.L. Chebychev*, **1**, Moscow-Leningrad, 1946, pp. 285–288, (In Russian)

[6] HEGYVÁRI, N.—HENNECART, F.: *Explicit construction of extractors and expanders*, Acta Arith. **140** (2009), 233–249.

[7] HEGYVÁRI, N.—HENNECART, F.: *Conditional expanding bounds for two-variable functions over prime fields*, European J. Combin. **34** (2013), 1365–1382.

[8] HEGYVÁRI, N.: *Some Remarks on Multilinear Exponential Sums with an Application*, J. Number Theory **132** (2012), 94–102.

[9] HELFGOTT, H.—RUDNEV, M.: *An explicit incidence theorem in* $\mathbb{F}_p$ , Mathematika **57** (2011), 135–145.

[10] JOHNSEN, J.: *On the distribution of powers in finite fields*, J. Reine Angew. Math. **251** (1971), 10–19.

[11] JONES, T. G. F.: *An improved incidence bound over fields of prime order*, arXiv:1110.4752v2.

[12] SÁRKÖZY, A.: *On sums and products of residues modulo p*, Acta Arith. **118** (2005), 403–409.

[13] SHKREDOV, I.D.: *On monochromatic solutions of some non linear equations in* $(\mathbb{Z}/p\mathbb{Z})^*$, Mathematical Notes **88** (2010), Issue 3–4, 603–611.

[14] SHPARLINSKI, I.: *On the solvability of bilinear equations in finite fields*, Glasgow Math. J. **50** (2008), 523–539.

[15] SHPARLINSKI, I.: *Additive combinatorics over finite fields: New results and applications*, in: *Proc. RICAM-Workshop on Finite Fields and Their Applications: Character Sums and Polynomials*, De Gruyter, 2013, pp.233–271.

[16] TAO T.: *Expanding Polynomials over finite fileds of large characteristic, and a regularity lemma for definable sets*, preprint (arXiv 1211.2894v2).

[17] VINH, L.: *Szemeredi-Trotter type theorem and sum-product estimate in finite fields*, European J. Combin. **32** (2011), 1177–1181.

[18] WEIL, A.: *On some exponential sums*, Proc. Natl. Acad. Sci. USA **34** (1948), 204–207.

Received March 25, 2014
Accepted July 30, 2014

**Norbert Hegyvári**
*ELTE TTK*
*Eötvös University*
*Institute of Mathematics*
*Pázmány st. 1/c*
*H-1117 Budapest*
*and*
*Alfréd Rényi Institute of Mathematics*
*Hungarian Academy of Science*
*H-1364 Budapest,*
*P.O.Box 127*
*HUNGARY*
*E-mail*: hegyvari@elte.hu

**François Hennecart**
*Université Jean-Monnet*
*Institut Camille Jordan*
*23, rue du Docteur Paul Michelon*
*42023 Saint-Etienne Cedex 02*
*FRANCE*
*E-mail*: francois.hennecart@univ-st-etienne.fr