ACTA ARITHMETICA
140.3 (2009)

Explicit constructions of extractors and expanders

by

Norbert Hegyvári (Budapest) and
François Hennecart (Saint-Étienne)

1. Introduction. The well-known Cauchy–Davenport theorem states that for any pair of sets A, B in $\mathbb{Z}_p$ such that $A + B \neq \mathbb{Z}_p$, we have $|A + B| \geq |A| + |B| - 1$, and this estimate is sharp: for arithmetic progressions A, B with common difference, $|A + B| = |A| + |B| - 1$. Now a natural question arises: what can we say about the image of a two-variable (or more generally multivariable) polynomial? One can ask which polynomial f blows up its domain, i.e. for any $A, B \subseteq \mathbb{Z}_p$ with $|A| \asymp |B|$ the set $f(A, B) := \{f(a, b) : a \in A,\, b \in B\}$ is ampler (in some uniform meaning) than $|A|$. As we remarked earlier, the polynomial $f(x, y) = x + y$ does not have this property.

Let us say that a polynomial $f(x, y)$ is an *expander* if $|f(A, B)|/|A|$ tends to infinity as p tends to infinity (a more precise definition will be given below).

According to the literature, very little is known about existence and construction of expanders; the only known explicit construction is due to J. Bourgain (see [3]) who proved that the polynomial $f(x, y) = x^2 + xy$ is an expander. More precisely, he proved that if $p^{\varepsilon} < |A| \asymp |B| < p^{1-\varepsilon}$ then $|f(A, B)|/|A| > p^{\gamma}$, where $\gamma = \gamma(\varepsilon)$ is a positive but inexplicit real number.

Our aim is to extend the class of known expanders and to give some effective estimates for $|f(A, B)|/|A|$. In particular, in Section 3 we exhibit an infinite family of expanders. The main tool is some incidence inequality that will also be used to construct explicit extractors with three variables. A function $f : \mathbb{Z}^3 \to \{-1, 1\}$ is said to be a 3-source *extractor* if under a certain condition on the size of A, B, C, the sum $\sum_{(a,b,c)\in A\times B\times C} f(a, b, c)$ is small compared to the number of its terms (see Section 5 for a precise definition and the details).

2010 *Mathematics Subject Classification*: 11L07, 11T06, 11B75.
Key words and phrases: expander, extractor, exponentially distributed polynomial.

DOI: 10.4064/aa140-3-2

Finally, in the last section we show that extractors are connected with some additive questions.

2. Incidence inequalities for points and hyperplanes. For any prime number p, we denote by $\mathbb{F}_p$ the field with p elements. The main tool used by Bourgain in [3] for exhibiting expanding maps and extractors is the following Szemerédi–Trotter type inequality:

Proposition 1 (Bourgain–Katz–Tao Theorem [4]). *Let $\mathcal{P}$ and $\mathcal{L}$ be respectively a set of points and a set of lines in $\mathbb{F}_p^2$ such that*

$$|\mathcal{P}|, |\mathcal{L}| < p^{\beta}$$

for some β, $0 < \beta < 2$. Then

$$|\{(P, L) \in \mathcal{P} \times \mathcal{L} : P \in L\}| \ll p^{(3/2-\gamma)\beta} \quad (\text{as } p \to \infty),$$

for some $\gamma > 0$ depending only on β.

In this statement, γ can be calculated in terms of β from the proof, but it would imply a cumbersome formula. We will need the following consequence:

Lemma 2. *Let $\mathcal{P}$ and $\mathcal{L}$ be respectively a set of points and a set of lines in $\mathbb{F}_p^2$ such that $|\mathcal{L}| < p^{\beta}$ for some β, $0 < \beta < 2$. Then*

$$|\{(P, L) \in \mathcal{P} \times \mathcal{L} : P \in L\}| \ll |\mathcal{P}|^{3/2-\gamma'} + p^{(3/2-\gamma')\beta} \quad (\text{as } p \to \infty), \tag{1}$$

for some $\gamma' > 0$ depending only on β.

Proof. We denote by $N(\mathcal{P}, \mathcal{L})$ the left-hand side of (1).

We may freely assume that in Proposition 1,

$$\gamma = \gamma(\beta) < (2 - \beta)/4. \tag{2}$$

If $|\mathcal{P}| < p^{2-(2-\beta)/3}$, then the result follows plainly from Proposition 1 with

$$\gamma' = \min(\gamma(\beta), \gamma(2 - (2 - \beta)/3)).$$

Otherwise, we use the obvious bound $N(\mathcal{P}, \mathcal{L}) \le |\mathcal{L}|p < p^{1+\beta}$ from which we deduce

$$N(\mathcal{P}, \mathcal{L}) < p^{(2-(2-\beta)/3)(3/2-\gamma)} \le |\mathcal{P}|^{3/2-\gamma}$$

by (2). Thus (1) holds with $\gamma' = \gamma$. ∎

In [9], Proposition 1 was generalized to an incidence inequality for points and hyperplanes in $\mathbb{F}_p^d$. It can be stated as follows:

Proposition 3 (L. A. Vinh [9]). *Let $d \ge 2$. Let $\mathcal{P}$ be a set of points in $\mathbb{F}_p^d$ and $\mathcal{H}$ be a set of hyperplanes in $\mathbb{F}_p^d$. Then*

$$|\{(P, H) \in \mathcal{P} \times \mathcal{H} : P \in H\}| \le \frac{|\mathcal{P}|\,|\mathcal{H}|}{p} + (1 + o(1))p^{(d-1)/2}(|\mathcal{P}|\,|\mathcal{H}|)^{1/2}.$$

From this, L. A. Vinh deduced in [9] that in Proposition 1, γ can be taken equal to $\min\{\beta-1; 2-\beta\}/4$ whenever $1<\beta<2$.

3. A family of expanding maps of two variables. For any prime number p, let $F_p : \mathbb{F}_p^k \to \mathbb{F}_p$ be an arbitrary function of k variables in $\mathbb{F}_p$. One says that the family of maps $F := (F_p)_p$, where p runs over the prime numbers, is an *expander* (in k variables) if for any α, $0<\alpha<1$, there exists $\epsilon = \epsilon(\alpha) > 0$ such that for any positive real numbers $L_1 \le L_2$, and a positive constant $c = c(F, L_1, L_2) > 0$ not depending on α, for any prime p and for any k-tuples $(A_i)_{1\le i\le k}$ of subsets of $\mathbb{F}_p$ satisfying $L_1 p^\alpha \le |A_i| \le L_2 p^\alpha$ $(1 \le i \le k)$, one has $|C_p| \ge cp^{\alpha+\epsilon}$ where

$$C_p = F_p(A_1, \dots, A_k) := \{F_p(a_1, \dots, a_k) : (a_1, \dots, a_k) \in A_1 \times \dots \times A_k\}.$$

If the maps F_p, p prime, are induced by some function $F : \mathbb{Z}^k \to \mathbb{Z}$, i.e. for any prime number p, we have

$$F_p(\pi_p(x_1), \dots, \pi_p(x_k)) = \pi_p(F(x_1, \dots, x_k)),$$

where π_p is the canonical morphism from $\mathbb{Z}$ onto $\mathbb{F}_p$, then we simply denote F_p by F. If such $(F_p)_p$ is an expander, then we will say that F induces or is an expander.

For example, any integral polynomial function F induces functions F_p also denoted by F. We will mainly concentrate on constructing expanders of this type.

In [3], Bourgain proved that $F(x,y) = x^2 + xy$ induces an expander and observed that more general maps with two variables can be considered. It is almost clear (see remark 1 in Section 6) that no map of the kind $f(x) + g(y) + c$ or $f(x)g(y) + c$ (where c is a constant) can be an expander. From this, one deduces that maps of the type $F(x,y) = f(x) + (uf(x)+v)g(y)$ where $u, v \in \mathbb{F}_p$ and f, g are integral polynomials, are not expanders. This is clear if $u = 0$, since in this case $F(x,y) = f(x) + vg(y)$. If $u \ne 0$, then $F(x,y) = (f(x)+vu^{-1})(1+ug(y)) - vu^{-1}$. In order to exhibit expanders of the type $f(x) + h(x)g(y)$, we thus have to assume that f and g are affinely independent, i.e., there is no $(u,v) \in \mathbb{Z}^2$ such that $f(x) = uh(x) + v$ or $h(x) = uf(x) + v$.

We will show the following:

Theorem 4. *Let $k \ge 1$ be an integer and f, g be polynomials with integer coefficients, and for any prime number p define the map F from $\mathbb{Z}^2$ onto $\mathbb{Z}$ by*

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

Assume that $f(x)$ and x^k are affinely independent. Then F induces an expander.

For p sufficiently large, the image $g(B)$ of any subset B of $\mathbb{F}_p$ has cardinality at least $|B|/\deg g$. It follows that we can restrict our attention to maps of the type $F(x,y) = f(x) + x^k y$. We let $d := \deg f$.

Let A and B be subsets of $\mathbb{F}_p$ with cardinality $|A| \asymp |B| \asymp p^\alpha$. For any $z \in \mathbb{F}_p$, we denote by $r(z)$ the number of couples $(x,y) \in A \times B$ such that $z = F(x,y)$, and by C the set of those z for which $r(z) > 0$. By the Cauchy–Schwarz inequality, we get

$$|A|^2|B|^2 = \Big(\sum_{z\in\mathbb{F}_p} r(z)\Big)^2 \leq |C|\Big(\sum_{z\in\mathbb{F}_p} r(z)^2\Big).$$

We now deal with the sum $\sum_{z\in\mathbb{F}_p} r(z)^2$ which is the number of quadruples $(x_1,x_2,y_1,y_2) \in A^2 \times B^2$ such that

$$f(x_1) + x_1^k y_1 = f(x_2) + x_2^k y_2. \tag{3}$$

For fixed $(x_1,x_2) \in A^2$ with $x_1 \neq 0$ or $x_2 \neq 0$, (3) can be viewed as the equation of a line ℓ_{x_1,x_2} whose points (y_1,y_2) are in $\mathbb{F}_p^2$. For (x_1,x_2) and (a,b) in A^2, the lines ℓ_{x_1,x_2} and $\ell_{a,b}$ coincide if and only if

$$\begin{cases} (x_1b)^k = (ax_2)^k, \\ b^k(f(x_2)-f(x_1)) = x_2^k(f(b)-f(a)), \end{cases}$$

or equivalently

$$\begin{cases} (x_1b)^k = (ax_2)^k, \\ (b^k-a^k)(f(x_2)-f(x_1)) = (x_2^k-x_1^k)(f(b)-f(a)). \end{cases} \tag{4}$$

At this point observe that by our assumption, there are only finitely many prime numbers p such that $f(x) = ux^k + v$ for some $(u,v) \in \mathbb{F}_p^2$, in which case the second equation in (4) holds trivially for any x_1 and x_2. We assume in the following that p is not such a prime number.

Let $(a,b) \in A^2$ be such that $a \neq 0$ or $b \neq 0$. Assume for instance that $b \neq 0$. By (4) we get $x_1 = \zeta a x_2/b$ for some kth root of unity ζ modulo p. Moreover, we obtain

$$b^k\bigg(f(x_2) - f\Big(\zeta\,\frac{ax_2}{b}\Big)\bigg) - x_2^k(f(b)-f(a)) = 0, \tag{5}$$

which is a polynomial equation in x_2. If we write $f(x) = \sum_{0\leq j\leq d} f_j x^j$ then

$$b^k\bigg(f(x) - f\Big(\zeta\,\frac{ax}{b}\Big)\bigg) = \sum_{1\leq j\leq d} b^k\bigg(1 - \frac{\zeta^j a^j}{b^j}\bigg) f_j x^j$$

is a polynomial which could be identically equal to $x^k(f(b)-f(a))$ only if the following two conditions are satisfied:

$$f(b) - f(a) = (b^k - a^k)f_k, \qquad f_j \neq 0 \;\Rightarrow\; b^j = \zeta^j a^j.$$

Since $f(x)$ and x^k are assumed to be affinely independent, we necessarily have $f_j \neq 0$ for some $0 < j \neq k$. If $b^j = \zeta^j a^j$ for ζ being a kth root of unity in $\mathbb{F}_p$, then $b = \eta a$ where η is some $(kd!)$th root of unity in $\mathbb{F}_p$. Let

$$X := \{(a,b) \in A^2 : b^{kd!} \neq a^{kd!}\}.$$

Since there are $kd!$ many $(kd!)$th roots of unity in $\mathbb{F}_p$, we have $|A^2 \setminus X| \leq kd!|A|$, hence $|X| \geq |A|^2/2$ for p large enough.

If $(a,b) \in X$, then (5) has at most $\max(k,d)$ solutions x_2, thus (4) has at most $k\max(k,d)$ solutions (x_1,x_2). We conclude that the number of distinct lines $\ell_{a,b}$ where (a,b) runs over A^2 is $c(k,f)|A|^2$ where $c(k,f)$ can be chosen equal to $(2k\max(k,d))^{-1}$, for p large enough. The set of all those pairwise distinct lines $\ell_{a,b}$ is denoted by $\mathcal{L}$; its cardinality satisfies $|A|^2 \ll |\mathcal{L}| \leq |A|^2$, as observed before. Let $\mathcal{P} = B^2$. Then putting $N := |A|^2 \asymp |B|^2$, by Proposition 1 we have

$$\{(p,\ell) \in \mathcal{P} \times \mathcal{L} : p \in \ell\} \ll N^{3/2-\delta}$$

for some $\delta > 0$. Hence the number of solutions of (4) is $O(N^{3/2-\delta}) = O(|A|^2|B|^{1-2\delta})$. Finally, $|C| \gg |B|^{1+2\delta}$, which is the desired conclusion.

4. Further results on expanders. When $\alpha > 1/2$, instead of Bourgain–Katz–Tao's incidence inequality, we can use Proposition 3. By the remark following Proposition 3, we can replace δ by $\min\{2\alpha-1; 2-2\alpha\}$ at the very end of our proof of Theorem 4. This gives

PROPOSITION 5. *Let F be as in Theorem 4 and $\alpha > 1/2$. For any pair (A,B) of subsets of $\mathbb{F}_p$ such that $|A| \asymp |B| \asymp p^\alpha$, we have*

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

The notion of expander which we discussed in the previous section is connected with the possibility of obtaining for a two-variable function F, inducing a sequence $(F_p)_p$, a nontrivial uniform lower bound for

$$\kappa_\alpha(F) = \inf_{0<L_1<L_2} \liminf_{p\to\infty} \min\left\{\frac{\ln|F_p(A,B)|}{\ln|A|} : A,B \subset \mathbb{F}_p \text{ and } L_1p^\alpha \leq |A|,|B| \leq L_2p^\alpha\right\}.$$

For F introduced in Theorem 4, we thus have

$$1 + \min\{2\alpha-1; 2-2\alpha\}/2 \leq \kappa_\alpha(F) \leq \min\{2; 1/\alpha\},$$

where the upper bound follows from the plain bounds $|F(A,B)| \leq |A|\,|B|$ and $|F(A,B)| \leq p$. To our knowledge, no explicit example of a function F such that $\kappa_\alpha(F) = \min\{2; 1/\alpha\}$ has been provided in the literature, even for a given real number α with $0 < \alpha < 1$. This question is certainly much more difficult than the initial question of providing an expander. This suggests the following definition:

Definition. Let $I \subset (0,1)$ be a nonempty interval. A family $F = (F_p)_p$ of two-variable functions is called

- a *strong expander according to* I if for any $\alpha \in I$, we have
$$\kappa_\alpha(F) = \min\{2; 1/\alpha\},$$
- a *complete expander according to* I if for any $\alpha \in I$, and any positive real numbers $L_1 \le L_2$, there exists a constant $c = c(F, L_1, L_2)$ such that for any prime number p and any pair (A, B) of subsets of $\mathbb{F}_p$ satisfying $L_1 p^\alpha \le |A|, |B| \le L_2 p^\alpha$, we have
$$|F_p(A, B)| \ge cp^{\min\{1;2\alpha\}}.$$

Complete expanders according to I are obviously strong expanders according to I. As indicated in [3], random mappings are strong expanders with a large probability, but no explicit example is known. Furthermore, functions F introduced in Theorem 4 could possibly be strong expanders, but we have not been able to prove or disprove this fact. Nevertheless, we can show that some of them are not complete expanders, including Bourgain's function $F(x, y) = x^2 + xy = x(x + y)$. Indeed, let A and B be the interval $[1, p^\alpha/2]$ in $\mathbb{Z}_p$. Then $A \cup (A + B) \subset [1, p^\alpha]$. If we assume $\alpha \le 1/2$, the following result, which is a direct consequence of a result by Erdős (see [5, 6]), implies that $F(A, B) = A \cdot (A + B)$ has cardinality at most $o(p^{2\alpha})$.

Lemma 6 (Erdős Lemma). *There exists a positive real number δ such that the number of different integers ab where $1 \le a, b \le n$ is $O(n^2/(\ln n)^\delta)$.*

A sharper result due to G. Tenenbaum [8] implies that δ can be taken equal to $1 - (1 + \ln\ln 2)/\ln 2$ in this statement.

In the same vein, we can extend Bourgain's result to more general functions:

Proposition 7. *Let $k \ge 2$ be an integer, $u \in \mathbb{Z}$ and $F(x, y) = x^{2k} + ux^k + x^k y = x^k(x^k + y + u)$. Then for any α with $0 < \alpha \le 1/2$, F is not a complete expander according to $\{\alpha\}$.*

Proof. Let L be a positive integer such that $L < \sqrt{p}/2$. The set of kth powers in $\mathbb{F}_p^*$ is a subgroup of $\mathbb{F}_p^*$ with index $l = \gcd(k, p-1) \le k$. Thus there exists $a \in \mathbb{F}_p^*$ such that $[1, L]$ contains at least L/l residue classes of the form ax^k, $x \in \mathbb{F}_p^*$. We let $A = \{x \in \mathbb{F}_p^* : ax^k \in [1, L]\}$, which has cardinality at least L since each kth power has l kth roots modulo p. We let $B = \{y \in \mathbb{F}_p : a(y + u) \in [1, L]\}$. We clearly have $|B| = L$. Moreover the elements of $F(A, B)$ are of the form $x^k(x^k + y + u)$ with $x \in A$ and

$y \in B$, thus of the form $a'^2x'y'$ where $x', y' \in [1, 2L]$ and $aa' = 1$ in $\mathbb{F}_p$. By the Erdős Lemma, we infer $|F(A,B)| = O(L^2/(\ln L)^\delta) = o(L^2)$. ∎

By using a deep bound by Weil on exponential sums with polynomials, we may slightly extend this result:

PROPOSITION 8. *Let $f(x)$ and $g(y)$ be nonconstant integral polynomials and $F(x,y) = f(x)(f(x) + g(y))$. Then F is not a complete expander according to $\{1/2\}$.*

We shall need the following result:

LEMMA 9. *Let $u \in \mathbb{F}_p$, L be a positive integer less than $p/2$, and $f(x)$ be any integral polynomial of degree $k \geq 1$ (as element of $\mathbb{F}_p[x]$). Then the number $N(I)$ of residues $x \in \mathbb{F}_p$ such that $f(x)$ lies in the interval $I = (u - L, u + L)$ of $\mathbb{F}_p$ is at least $L - (k-1)\sqrt{p}$.*

Proof. We will use the formalism of Fourier analysis. Recall the following notation and properties:

Let $\phi, \psi : \mathbb{F}_p \to \mathbb{C}$ and $x \in \mathbb{F}_p$.

- $\phi * \psi(x) := \sum_{y \in \mathbb{F}_p} \overline{\phi(y)}\, \psi(x+y)$;
- $\hat{\phi}(x) := \sum_{y \in \mathbb{F}_p} \phi(y) \mathrm{e}(yx/p)$, where $\mathrm{e}(t) := \exp(2i\pi t)$;
- $\widehat{\phi * \psi}(x) = \overline{\hat{\phi}(x)}\, \hat{\psi}(x)$;
- $\sum_{y \in \mathbb{F}_p} |\hat{\phi}(y)|^2 = p \sum_{y \in \mathbb{F}_p} |\phi(y)|^2$ (Parseval's identity).

Let J be the indicator function of the interval $[0, L)$ of $\mathbb{F}_p$ and let

$$T := \sum_{h \in \mathbb{F}_p} \widehat{J * J}(h) S_f(-h, p) \mathrm{e}(hu/p),$$

where the exponential sum

$$S_f(h, p) := \sum_{x \in \mathbb{F}_p} \mathrm{e}(hf(x)/p)$$

is known to satisfy the bound $|S_f(h,p)| \leq (k-1)\sqrt{p}$ whenever $h \neq 0$ in $\mathbb{F}_p$ and p is an odd prime number (see for instance [2]).

On the one hand, we have

$$\begin{aligned} T &= p\widehat{J * J}(0) + \sum_{h \in \mathbb{F}_p \setminus \{0\}} \widehat{J * J}(h) S_f(-h, p) \mathrm{e}(hu/p) \\ &\geq pL^2 - k\sqrt{p} \sum_{h \in \mathbb{F}_p \setminus \{0\}} |\widehat{J * J}(h)| \geq pL^2 - kLp^{3/2}, \end{aligned}$$

by the bound for Gaussian sums and Parseval's identity. Hence

$$T \geq pL(L - k\sqrt{p}). \tag{6}$$

On the other hand,

$$\begin{aligned} T &= \sum_{h\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)\mathrm{e}(h(y+u)/p)\sum_{x\in\mathbb{F}_p}\mathrm{e}(-hf(x)/p)\\ &= \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\sum_{z\in\mathbb{F}_p} J(z)J(y+z)\sum_{h\in\mathbb{F}_p}\mathrm{e}(h(y+u-f(x))/p)\\ &= p\sum_{x\in\mathbb{F}_p} d_L(f(x)-u), \end{aligned}$$

where $d_L(z)$ denotes the number of representations of z in $\mathbb{F}_p$ in the form $j-j'$, $0\le j,j'<L$. Since obviously $d_L(z)\le L$ for each $z\in\mathbb{F}_p$, we get

$$T\le pLN(I).$$

Combining this bound and (6), we deduce the lemma. ∎

Proof of Proposition 8. We choose p large enough so that both $f(x)$ and $g(y)$ are nonconstant polynomials modulo p. Let $L=k\sqrt{p}$, and define A (resp. B) to be the set of residue classes x (resp. y) such that $f(x)$ (resp. $g(y)$) lies in the interval $(0,2L)$. By the previous lemma, one has $|A|,|B|\ge\sqrt{p}$. Moreover, for any $(x,y)\in A\times B$, we have $f(x)$ and $f(x)+g(y)$ in the interval $(0,4L)$. By the Erdős Lemma, the number of residues modulo p which can be written as $F(x,y)$ with $(x,y)\in A\times B$ is at most $O(L^2/(\ln L)^\delta)=o(p)$, as p tends to infinity. ∎

5. A family of 3-source extractors with exponential distribution. Let us define the *entropy* of a k-source $f=(f_p)_p$, where $f_p:\mathbb{F}_p^k\to\{-1,1\}$, to be the infimum, denoted α_0, of $\alpha>0$ such that for any subsets A_j, $j=1,\dots,k$, of $\mathbb{F}_p$ with cardinality at least p^α we have

$$\sum_{\substack{a_j\in A_j\\ j=1,\dots,k}} f_p(a_1,\dots,a_k)=o\Big(\prod_{j=1}^k|A_j|\Big)\quad\text{as } p\to\infty.$$

When $\alpha_0<1$, f is called a k-source *extractor* (with entropy α_0).

The problem of finding k-source extractors can be reduced as follows. We are looking for functions $F_p:\mathbb{F}_p^k\to\mathbb{F}_p$ such that for any k-tuples $(A_1,\dots,A_k)$ of subsets of $\mathbb{F}_p$ with cardinality $\asymp p^\alpha$ and for any $r\in\mathbb{F}_p^\times$,

$$\Big|\sum_{\substack{a_j\in A_j\\ j=1,\dots,k}} \mathrm{e}_r(F_p(x_1,\dots,x_k))\Big|=O\Big(p^{-\gamma}\prod_{j=1}^k|A_j|\Big)\quad\text{as } p\to\infty,\tag{7}$$

for some $\gamma=\gamma(\alpha)$, where $\mathrm{e}_r(u):=\exp(ru/p)$. If (7) holds, Bourgain [3] has shown that

$$\sum_{\substack{a_j\in A_j\\ j=1,\dots,k}} f_p(a_1,\dots,a_k)=O\Big(p^{-\gamma'}\prod_{j=1}^{k}|A_j|\Big)\quad \text{as } p\to\infty, \tag{8}$$

for some $\gamma'>0$, where $f_p:=\operatorname{sgn}\sin(2\pi F_p/p)$. This gives a k-source extractor $f=(f_p)_p$. An extractor f such that (8) holds is said to have an *exponential distribution.*

In [3, Proposition 3.6], Bourgain proved that $F(x,y)=xy+x^2y^2$, by letting $F=F_p$ for any p, provides a 2-source extractor with exponential distribution and with entropy $1/2-\delta$ for some $\delta>0$. We will show that this result can be extended to give 3-source extractors with such entropy. It has to be mentioned that the explicit 3-source extractors with arbitrary positive entropy, given in [1], do not have exponential distribution. Here our goal is to exhibit 3-source extractors with exponential distribution.

THEOREM 10. *Let $F(x,y,z)=a(z)xy+b(z)x^2g(y)+h(y,z)\in\mathbb{Z}[x,y,z]$ where $a(z)$, $b(z)$ are any nonzero polynomial functions, $g(y)$ is any polynomial function of degree at least two, and $h(y,z)$ is an arbitrary polynomial function. Let $L_1\le L_2$ be positive real numbers, $\alpha\in(0,1)$ and A,B,C be subsets of $\mathbb{F}_p$ with $L_1p^\alpha\le|A|,|B|,|C|\le L_2p^\alpha$. For $r\in\mathbb{F}_p$, set*

$$S_r=\sum_{(x,y,z)\in A\times B\times C}\mathrm{e}_r(F(x,y,z)).$$

Then there exists $\gamma=\gamma(\alpha)>0$ such that

$$\max_{r\in\mathbb{F}_p\setminus\{0\}}|S_r|\ll p^{((22-\gamma/2)\alpha+1)/8},$$

where the implied constant depends only on F, L_1 and L_2.

Proof. The proof starts as in [3, Proposition 3.6]. For any $r\in\mathbb{F}_p\setminus\{0\}$, let

$$S_r=\sum_{(x,y,z)\in A\times B\times C}\mathrm{e}_r(F(x,y,z)).$$

The first transformations use the Cauchy–Schwarz inequality repeatedly to increase the number of variables and to relate S_r to the number of solutions of diophantine systems. We simply denote S_r by S. We denote by C_0 the subset of C formed by the elements $z\in C$ such that $a(z)b(z)=0$. We let $C':=C\setminus C_0$. Then $S=S_0+S'$ where in S_0 (resp. S') the summation over z is restricted to $z\in C_0$ (resp. $z\in C'$). Since the number of roots of the equation $a(z)b(z)=0$ is finite, we have $|S_0|\ll|A|\,|B|\ll p^{2\alpha}$. Moreover, we get

$$\begin{aligned}|S'| &\le \sum_{y,z}\Big|\sum_{x}\mathrm{e}_r\big(a(z)xy+b(z)x^2g(y)\big)\Big|\\ &\le \Big(\sum_{y,z}1\Big)^{1/2}\Big(\sum_{\substack{y,z\\x_1,x_2}}\mathrm{e}_r\big(a(z)(x_1-x_2)y+b(z)(x_1^2-x_2^2)g(y)\big)\Big)^{1/2},\end{aligned}$$

where the summation over z is restricted to $z\in C'$. Hence

$$\begin{aligned}|S'|^2 &\ll p^{2\alpha}\sum_{y,z}\Big|\sum_{x_1,x_2}\mathrm{e}_r\big(a(z)(x_1-x_2)y+b(z)(x_1^2-x_2^2)g(y)\big)\Big|\\ &\ll p^{2\alpha}\Big(\sum_{y,z}1\Big)^{1/2}\Big(\sum_{\substack{x_1,x_2\\x_3,x_4\\y,z}}\mathrm{e}_r\big(a(z)(x_1-x_2+x_3-x_4)y\\ &\qquad\qquad +b(z)(x_1^2-x_2^2+x_3^2-x_4^2)g(y)\big)\Big)^{1/2},\end{aligned}$$

so that

$$|S'|^4 \ll p^{6\alpha}\sum_{\substack{x_1,x_2\\x_3,x_4\\y,z}}\mathrm{e}_r\big(a(z)(x_1-x_2+x_3-x_4)y+b(z)(x_1^2-x_2^2+x_3^2-x_4^2)g(y)\big).$$

By a new application of the Cauchy–Schwarz inequality, we get

$$\begin{aligned}|S'|^8 &\ll p^{12\alpha}\Big(\sum_{\substack{x_1,x_2\\x_3,x_4\\z}}\Big|\sum_{y}\mathrm{e}_r\big(a(z)(x_1-x_2+x_3-x_4)y\\ &\qquad\qquad +b(z)(x_1^2-x_2^2+x_3^2-x_4^2)g(y)\big)\Big|\Big)^2\\ &\ll p^{17\alpha}\sum_{z}\sum_{\substack{x_1,x_2\\x_3,x_4\\y_1,y_2}}\mathrm{e}_r\big(a(z)(x_1-x_2+x_3-x_4)(y_1-y_2)\\ &\qquad\qquad +b(z)(x_1^2-x_2^2+x_3^2-x_4^2)(g(y_1)-g(y_2))\big)\\ &= p^{17\alpha}\sum_{z}\sum_{\underline{\xi},\underline{\eta}\in\mathbb{F}_p^2}\mu(\underline{\xi})\nu(\underline{\eta})\mathrm{e}_r(a(z)\xi_1\eta_1+b(z)\xi_2\eta_2)\end{aligned}$$

where $\mu(\underline{\xi})$ is the number of quadruples $(x_1,x_2,x_3,x_4)\in A^4$ such that

$$\begin{cases}\xi_1=x_1-x_2+x_3-x_4,\\ \xi_2=x_1^2-x_2^2+x_3^2-x_4^2,\end{cases}\tag{9}$$

and $\nu(\underline{\eta})$ is the number of couples $(y_1,y_2)\in B^2$ such that

$$\begin{cases}\eta_1=y_1-y_2,\\ \eta_2=g(y_1)-g(y_2).\end{cases}$$

Then clearly $\sum_{\underline{\eta}\in\mathbb{F}_p^2}\nu(\underline{\eta})^2$ can be expressed as the number of quadruples $(y_1,y_2,y_1',y_2')\in B^4$ such that

$$\begin{cases}y_1-y_2=y_1'-y_2',\\ g(y_1)-g(y_2)=g(y_1')-g(y_2').\end{cases}\tag{10}$$

If $y_1' = y_2'$ in this system then $y_1 = y_2$. Thus (10) has exactly $|B|^2$ solutions of the type (y_1, y_2, y_1', y_1'). If y_1' and y_2' are fixed with $t = y_1' - y_2' \neq 0$, then we can write $y_1 = y_2 + t$ and clearly $g(y_2 + t) - g(y_2) = g(y_1') - g(y_2')$ has at most $\deg g - 1$ solutions y_2 (since $\deg g \geq 2$). We thus have

$$\sum_{\underline{\eta} \in \mathbb{F}_p^2} \nu(\underline{\eta})^2 \ll p^{2\alpha}. \tag{11}$$

For any $\underline{\xi} = (\xi_1, \xi_2) \in \mathbb{F}_p^2$, we denote by $\mu_1(\underline{\xi})$ (resp. $\mu_2(\underline{\xi})$) the number of solutions $(x_1, x_2, x_3, x_4) \in A^4$ of (9) such that $x_1 = x_2$ (resp. $x_1 \neq x_2$). Then

$$\sum_{\underline{\xi} \in \mathbb{F}_p^2} \mu_1(\underline{\xi})^2 = |A|^2 N,$$

where N is the number of quadruples $(x_3, x_4, z_3, z_4) \in A^4$ such that

$$\begin{cases} x_3 - x_4 = z_3 - z_4, \\ x_3^2 - x_4^2 = z_3^2 - z_4^2. \end{cases}$$

By distinguishing solutions with $x_3 = x_4$ and solutions with $x_3 \neq x_4$, we plainly obtain $N \leq 2|A|^2$. Hence

$$\sum_{\underline{\xi} \in \mathbb{F}_p^2} \mu_1(\underline{\xi})^2 \ll p^{4\alpha}. \tag{12}$$

For any fixed $t \in A$, we denote by $\mu(\underline{\xi}, t)$ the number of solutions of (9) of the form $(x_1, x_2, t, x_4) \in A^4$ with $x_1 \neq x_2$. Eliminating x_4 by expressing it in terms of ξ_1 using the first equation, we see that $\mu(\underline{\xi}, t)$ is the number of couples $(x_1, x_2) \in A^2$ with $x_1 \neq x_2$ such that $\underline{\xi}$ lies on the curve

$$\xi_2' := \xi_2 + \xi_1^2 = 2(x_1 - x_2 + t)\xi_1 - (x_1 - x_2 + t)^2 + x_1^2 - x_2^2 + t^2. \tag{13}$$

Using the new variable ξ_2' instead of ξ_2, we find that each couple $(x_1, x_2) \in A^2$ with $x_1 \neq x_2$ defines a line ℓ_{x_1, w_2} in the plane $\mathbb{F}_p^2$ with equation

$$\xi_2' = 2(x_1 - x_2 + t)\xi_1 - (x_1 - x_2 + t)^2 + x_1^2 - x_2^2 + t^2. \tag{14}$$

It is clear that two couples $(x_1, x_2) \in A^2$ and $(x_1', x_2') \in A^2$ with $x_1 \neq x_2$ define the same line if and only if $x_1 - x_2 = x_1' - x_2'$ and $x_1^2 - x_2^2 = x_1'^2 - x_2'^2$, that is, $(x_1, x_2) = (x_1', x_2')$. It follows that all the lines ℓ_{x_1, x_2} with $x_1 \neq x_2$ are pairwise distinct and the number of these lines is equal to $|A|^2 - |A| \ll p^{2\alpha}$. We let $\mathcal{L} = \{\ell_{x_1, x_2} : (x_1, x_2) \in A^2,\ x_1 \neq x_2\}$. By applying Lemma 2, we get, for some $\gamma = \gamma(\alpha) > 0$,

$$|\{[(\xi_1, \xi_2'); \ell] \in C_k \times \mathcal{L} : (\xi_1, \xi_2') \in \ell\}| \ll |C_k|^{3/2 - \gamma} + p^{(3 - 2\gamma)\alpha},$$

where C_k is the set of couples $(\xi_1, \xi_2') \in \mathbb{F}_p^2$ such that the number of different couples $(x_1, x_2) \in A^2$ with $x_1 \neq x_2$ satisfying (14) with $\xi_1 - x_1 + x_2 - t \in A$ is at least k. Since there is a one-to-one correspondence between the couples

$(\xi_1,\xi_2')\in C_k$ and the couples $(\xi_1,\xi_2)\in\mathbb{F}_p^2$ such that $\mu(\underline{\xi},t)\ge k$, we plainly have $|C_k|\le p^{3\alpha}/k$. Furthermore, for fixed (ξ_1,ξ_2') in $\mathbb{F}_p^2$, each choice of $x_1\in A$ gives at most two different $x_2\in A$ such that (14) holds. Hence C_k is empty if $k>2|A|$. We let $c_k=|C_k|$. We obtain

$$c_k k\ll c_k^{3/2-\gamma}+p^{(3-2\gamma)\alpha},$$

giving either

$$c_k k\ll p^{(3-2\gamma)\alpha}\quad\text{or}\quad k\ll c_k^{1/2-\gamma}.$$

Since $c_k\ll p^{3\alpha}/k$, the last bound is available only if

$$k\le k(\alpha,\gamma):=cp^{(3-6\gamma)\alpha/(3-2\gamma)}\quad\text{for some constant } c>0.$$

We have

$$\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi},t)^2=\sum_{1\le k\le 2|A|}k^2(c_k-c_{k+1})=\sum_{1\le k\le 2|A|}(2k-1)c_k,$$

by partial summation. It follows that

$$\begin{aligned}\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi},t)^2&=\sum_{1\le k\le k(\alpha,\gamma)}(2k-1)c_k+\sum_{k(\alpha,\gamma)<k\le 2|A|}(2k-1)c_k\\&\le 2\sum_{1\le k\le k(\alpha,\gamma)}p^{3\alpha}+\sum_{k(\alpha,\gamma)<k\le 2|A|}p^{(3-2\gamma)\alpha}\\&\ll p^{12(1-\gamma)\alpha/(3-2\gamma)}+p^{(4-2\gamma)\alpha}\ll p^{(4-\gamma)\alpha}.\end{aligned}$$

By the Cauchy–Schwarz inequality, we get

$$\begin{aligned}\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu_2(\underline{\xi})^2&=\sum_{\underline{\xi}\in\mathbb{F}_p^2}\Big(\sum_{t\in A}\mu(\underline{\xi},t)\Big)^2\le|A|\sum_{t\in A}\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi},t)^2\\&\le|A|^2\sup_{t\in A}\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi},t)^2\ll p^{(6-\gamma)\alpha},\end{aligned}$$

which by (12) gives

$$\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi})^2\le 2\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu_1(\underline{\xi})^2+2\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu_2(\underline{\xi})^2\ll p^{(6-\gamma)\alpha}.\tag{15}$$

This yields a sharper bound for $\sum\mu(\underline{\xi})^2$ than could be expected in general, namely $O(p^{6\alpha})$.

Returning to the estimation of S', we obtain

$$\begin{aligned}|S'|^8&\ll p^{17\alpha}\sum_{z\in C'}\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi})\Big|\sum_{\underline{\eta}\in\mathbb{F}_p^2}\nu(\underline{\eta})\mathrm{e}_r(a(z)\xi_1\eta_1+b(z)\xi_2\eta_2)\Big|\\&\ll p^{17\alpha}\sum_{z\in C'}\Big(\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi})^2\Big)^{1/2}\Big(\sum_{\underline{\xi}\in\mathbb{F}_p^2}\Big|\sum_{\underline{\eta}\in\mathbb{F}_p^2}\nu(\underline{\eta})\mathrm{e}_r(a(z)\xi_1\eta_1+b(z)\xi_2\eta_2)\Big|^2\Big)^{1/2},\end{aligned}$$

which is

$$\ll p^{17\alpha}\sum_{z\in C'}\Big(\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi})^2\Big)^{1/2}$$
$$\times\Big(\sum_{\underline{\eta},\underline{\eta}'\in\mathbb{F}_p^2}\nu(\underline{\eta})\nu(\underline{\eta}')\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mathrm{e}_r\big(a(z)\xi_1(\eta_1-\eta_1')+b(z)\xi_2(\eta_2-\eta_2')\big)\Big)^{1/2}$$

by the Cauchy–Schwarz inequality. For $z\in C'$, the sum over $\underline{\xi}$ is p^2 if $\underline{\eta}=\underline{\eta}'$ and 0 otherwise. It follows that

$$|S'|^8\ll p^{17\alpha+1}|C'|\Big(\sum_{\underline{\xi}\in\mathbb{F}_p^2}\mu(\underline{\xi})^2\Big)^{1/2}\Big(\sum_{\underline{\eta}\in\mathbb{F}_p^2}\nu(\underline{\eta})^2\Big)^{1/2}.$$

By (11) and (15), this yields

$$|S'|^8\ll p^{(22-\gamma/2)\alpha+1},$$

hence

$$|S|\le|S_0|+|S'|\ll p^{((22-\gamma/2)\alpha+1)/8}.\ \blacksquare \tag{16}$$

We mention that in the statement of Theorem 10, $\gamma(\alpha)$ is a continuous function of α. As a corollary, we have

COROLLARY 11. *Let F be as in the theorem. Then the extractor defined by $\operatorname{sgn}\sin(2\pi F/p)$ has exponential distribution and entropy at most $1/2-\delta$, for some $\delta>0$.*

Proof. From Theorem 10, we obtain

$$\max_{r\in\mathbb{F}_p\smallsetminus\{0\}}|S_r|\ll p^{3\alpha-\epsilon(\alpha)},$$

where

$$\epsilon(\alpha)=\frac{\alpha}{8}\bigg(2+\frac{\gamma(\alpha)}{2}-\frac{1}{\alpha}\bigg). \tag{17}$$

Since $\gamma(1/2)>0$, we have $\epsilon(1/2)>0$, thus by continuity, there exists $\delta>0$ such that $\epsilon(\alpha)>0$ for $\alpha>1/2-\delta$.

The rest of the proof follows that in [3], namely we have

$$\sum_{(x,y,z)\in A\times B\times C}\operatorname{sgn}\sin(2\pi F(x,y,z)/p)=\sum_{r=1}^{p-1}c_rS_r+O(p^{3\alpha-1}),$$

where the coefficients c_r satisfy

$$\operatorname{sgn}\sin(2\pi t/p)=\sum_{r=1}^{p-1}c_r\exp(2i\pi t/p)+O(1/p),$$

and

$$\sum_{r=1}^{p-1} |c_r| = O(\ln p).$$

This gives

$$\sum_{(x,y,z)\in A\times B\times C} \operatorname{sgn}\sin(2\pi F(x,y,z)/p) = O((\ln p)p^{3-\epsilon}),$$

and the corollary follows. ■

6. Concluding remarks. 1. As indicated in Section 3, no function of the type $F(x,y) = f(x) + g(y)$ or any translate of it is an expander. Indeed, let I be an interval with length $\asymp Cp^{\alpha}$ $(0 < \alpha < 1, C > 0)$. By the averaging argument there are a and b in $\mathbb{F}_p$ such that

$$|\{a + I\} \cap \{f(x) : x \in \mathbb{F}_p\}| > C'p^{\alpha},$$
$$|\{b + I\} \cap \{g(y) : y \in \mathbb{F}_p\}| > C'p^{\alpha},$$

where C' depends only on C and the degree of f and g. Now let A be the inverse image of $\{a+I\} \cap \{f(x) : x \in \mathbb{F}_p\}$ and let B be the inverse image of $\{b + I\} \cap \{g(y) : y \in \mathbb{F}_p\}$. Then the set $F(A,B)$ of all elements of the form $F(x,y)$ for $(x,y) \in A \times B$ is contained in $a + b + 2I$, hence the cardinality of $F(A,B)$ is at most a constant times the cardinality of A and B.

A similar argument shows that no map of the kind $f(x)g(y) + c$ is an expander.

2. As cited after Corollary 11, the functions $f_p(x,y) = \operatorname{sgn}\sin F_p(x,y)$ give a 2-source extractor with entropy less than 1/2 if we let $F_p(x,y) = xy + x^2y^2$ or $F_p(x,y) = xy + g_p^{x+y}$, where g_p is any generator in $\mathbb{F}_p^{\times}$. From the proof one can easily infer that the functions

$$xy + x^2h(y), \quad xh(y) + x^2y, \quad xy + x^2g_p^y, \quad xg_p^y + x^2y \tag{18}$$

(where h is any nonconstant polynomial) also induce 2-source extractors with entropy less than 1/2 (see also remark 4 below).

3. It is worth mentioning that for points and lines in $\mathbb{F}_p^2$, the bound given by the effective version of the Szemerédi–Trotter theorem of [9] is weaker than the trivial one in the case where the number N of lines and points is less than p. For this reason, it seems that the former bound cannot provide an effective entropy less than 1/2 for a k-source extractor, in contrast to the Bourgain–Katz–Tao result which holds for $p^{\varepsilon} < N < p^{2-\varepsilon}$.

4. Extractors are related to additive questions in $\mathbb{F}_p$. In [7] Sárközy investigated the following problem: let $A, B, C, D \subseteq \mathbb{F}_p$ be nonempty sets. Then the equation

$$a + b = cd$$

is solvable in $a \in A$, $b \in B$, $c \in C$, $d \in D$ provided $|A|\,|B|\,|C|\,|D| > p^3$. This simple equation has many interesting consequences. One can ask the more general question about the solvability of

$$a + b = F(c,d) \tag{19}$$

where $F(x,y)$ is a two-variable polynomial with integer coefficients. Clearly the question is really interesting when we assume that $|C|, |D| < \sqrt{p}$.

Let us say that $F(x,y)$ is an *essential* polynomial if (under the condition $|C|, |D| < \sqrt{p}$) $|A|\,|B| > p^2$ implies the solvability of (19). So by Sárközy's result, $F(x,y) = xy$ is an essential polynomial. From the proofs of Propositions 3.6 and 3.7 of [3], it can be deduced that there exist $\delta, \epsilon > 0$ such that for any $r \in \mathbb{F}_p \setminus \{0\}$ and any $C, D \subset \mathbb{F}_p$ with $|C|, |D| > p^{1/2-\delta}$,

$$\Big|\sum_{c\in C,\, d\in D} \mathrm{e}_r(F_p(c,d))\Big| = O(|C|\,|D|p^{-\epsilon}), \tag{20}$$

where $F = (F_p)_p$ is any one of the following families of 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 nonconstant polynomial $h(y) \in \mathbb{Z}[y]$.
- $F_p(x,y) = x^{1+u}y + x^{2-u}g_p^y$ for any p where g_p generates $\mathbb{F}_p^\times$ and $u \in \{0,1\}$ is fixed.

This yields the following result:

Proposition 12. *Let $(F_p)_p$ be one of the two families of functions defined above. There exist real numbers $0 < \delta, \delta' < 1$ such that for any p and for any sets $A, B, C, D \subseteq \mathbb{F}_p$ satisfying 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

$$a + b = F_p(c,d). \tag{21}$$

Sketch of the proof. Let N be the number of solutions of (21). Then following Sárközy's argument and using the bound (20), we obtain

$$\left|N - \frac{|A|\,|B|\,|C|\,|D|}{p}\right| \ll |A|^{1/2}|B|^{1/2}|C|\,|D|p^{-\epsilon},$$

which gives the result for p large enough with $\delta' = \epsilon$. For $p \le p_0$, it suffices to reduce δ' in order to have also $p_0^{2-\delta'} \ge p_0^2 - 1$, and the result becomes trivial since $|A|\,|B| > p^{2-\delta'}$ implies either $A = \mathbb{F}_p$ or $B = \mathbb{F}_p$. ∎

5. Note that the range of our function $F(x,y,z) = a(z)xy + b(z)x^2g(y) + h(y,z)$ studied in Section 5 is well-spaced, i.e. the set $F(A,B,C)$ of elements of $\mathbb{F}_p$ of the form $F(x,y,z)$, where $(x,y,z) \in A \times B \times C$, intersects every not too long interval, provided the cardinalities of the sets are $\asymp p^\alpha$ with $\alpha > 1/2 - \delta$.

The bound we obtain for the exponential sum S in the proof of Theorem 10 yields the following result:

Corollary 13. *Let $\epsilon(\alpha)$ be given by* (17) *and δ as in Corollary* 11. *Let $L_1 \le L_2$ be arbitrary positive real numbers, $F(x,y,z) \in \mathbb{Z}[x,y,z]$ as in Theorem* 10 *and A, B, C be subsets of $\mathbb{F}_p$ with $L_1p^\alpha \le |A|, |B|, |C| \le L_2p^\alpha$ where $\alpha > 1/2 - \delta$. Then $F(A,B,C)$ intersects every interval $[u+1, u+L]$ in $\mathbb{F}_p$ provided $L \gg p^{1-\epsilon(\alpha)}$ where the implied constant depends only on F, L_1 and L_2.*

For completeness we include the proof.

Proof. Let $S(w)$ be the number of triples $(a,b,c) \in F(A,B,C)$ such that $w = F(a,b,c)$. Let $I = [1, L/2]$ and denote by $I(w)$ its indicator. Then $F(A,B,C) \cap [u+1, u+L]$ is not empty if and only if the real sum

$$T = \sum_w S(w-u) I * I(-w)$$

is not zero. Denote the Fourier transform of the indicators of S resp. I by S_r resp. I_r. By the Fourier inversion formula we have

$$\begin{aligned} T = \frac{1}{p}\sum_r S_r \overline{I_r^2} \mathrm{e}_r(-u) &\ge \frac{S_0 I_0^2}{p} - \frac{1}{p}\sum_{r\neq 0} |S_r|\,|I_r|^2 \\ &= \frac{1}{p}|A|\,|B|\,|C| I_0^2 - \frac{1}{p}\sum_{r\neq 0}|S_r|\,|I_r|^2. \end{aligned}$$

By the triangle inequality, the nontrivial upper bound for $|S_r|$ when $r \neq 0$, and by the Parseval formula, (16) and (17) we get

$$\left| T - \frac{1}{p}|A|\,|B|\,|C| I_0^2 \right| \le \frac{1}{p}\sum_{r\neq 0}|S_r|\,|I_r^2| \le \frac{1}{p}\max_{r\neq 0}|S_r| \sum_r |I_r^2| \ll p^{3\alpha-\epsilon(\alpha)} I_0.$$

Hence the set $F(A,B,C) \cap [u+1, u+L]$ is not empty if

$$\frac{1}{p}|A|\,|B|\,|C| I_0 \gg p^{3\alpha-\epsilon(\alpha)},$$

or equivalently if $L \gg p^{1-\epsilon(\alpha)}$, as asserted. ∎

Acknowledgements. Research of the first author was partially supported by "Balaton Program Project" and OTKA grants K 61908, K 67676.

References

[1] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov and A. Wigderson, *Simulating independence: new constructions of condensers, Ramsey graphs, dispersers, and extractors*, in: Proc. 37th Annual ACM Symposium on Theory of Computing, 2005, 1–10.

[2] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.

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

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

[5] P. Erdős, *Some remarks on number theory*, Riveon Lematematika 9 (1955), 45–48 (in Hebrew).

[6] —, *An asymptotic inequality in the theory of numbers*, Vestnik Leningrad. Univ. 15 (1960), no. 13, 41–49 (in Russian).

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

[8] G. Tenenbaum, *Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné*, Compos. Math. 51 (1984), 243–263.

[9] L. A. Vinh, *Szemerédi–Trotter type theorem and sum-product estimate in finite fields*, arXiv:0711.4427v1[CO].

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

LAMUSE
Université de Saint-Étienne
(PRES Université de Lyon)
23, rue Michelon
F-42023 Saint-Étienne, France
E-mail: francois.hennecart@univ-st-etienne.fr

Received on 17.11.2008
and in revised form on 21.4.2009 (5863)