SUM-PRODUCTS ESTIMATES WITH SEVERAL SETS AND APPLICATIONS

Antal Balog
Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Hungary
balog@renyi.hu

Kevin A. Broughan
Department of Mathematics, University of Waikato, Hamilton, New Zealand
kab@waikato.ac.nz

Igor E. Shparlinski
Department of Computing, Macquarie University, Sydney, Australia
igor.shparlinski@mq.edu.au

Received: 10/7/11, Accepted: 3/18/12, Published: 3/23/12

Abstract

We obtain several versions of the sum-product theorem with k-fold sums and product sets. We also give several applications of these estimates.

1. Introduction

Let $\mathbb{F}_p$ denote the finite field of p elements. For a set $\mathcal{A} \subseteq \mathbb{F}_p$ and a rational function $F(X_1, \ldots, X_m) \in \mathbb{F}_p(X_1, \ldots, X_m)$, which has no poles in $\mathcal{A}$, we define the set

$$F(\mathcal{A}, \ldots, \mathcal{A}) = \{F(a_1, \ldots, a_m) \ : \ a_1, \ldots, a_m \in \mathcal{A}\}.$$

In particular, for an integer k, $k\mathcal{A}$ and $\mathcal{A}^k$ denote k-fold sums and product sets, respectively.

The most interesting and well studied case in the classical sum-product problem where the goal is to show that at least one of sets $\mathcal{A}^2 = \mathcal{A} \cdot A$ and $2\mathcal{A} = \mathcal{A} + \mathcal{A}$ is of size substantially larger than $|\mathcal{A}|$. This direction, initiated by the pioneering work of Bourgain, Katz & Tao [6], has been developed in a various directions and has had several important applications, see [2, 4, 5, 13, 14, 18, 23, 24, 25] and references therein.

Here, motivated by some new applications, we consider the case of a k-fold sum and product sets $\mathcal{A}^k$ and $k\mathcal{A}$. We note that several results of these types for sets of integer and real numbers have been given by various authors, see [10] and references therein. For finite fields, there are also several results for multiple sum and product sets, see [10, 15, 16, 17], however this direction has not yet been systematically studied. Here we present several general results of this type. In particular, we use the method of Garaev [13], which in turn has its roots in the work of Elekes [11] on the sum-product problem over the reals, to show that for any integer $k \geq 2$ there is a constant $C > 0$ such that

$$|\mathcal{A}^k| \cdot |k\mathcal{A}| \geq C \min\left\{p|\mathcal{A}|, \frac{|\mathcal{A}|^{2k}}{p^{k-1}}\right\},$$

which with $k = 2$ recovers [13, Theorem 1].

We also give several new applications. For example, we improve one of the estimates of [1] on the number of solutions of exponential congruences

$$x^x \equiv a \pmod p, \qquad 1 \leq x \leq p-1. \tag{1}$$

We use the following notations. Throughout the paper, the implied constants in the symbols 'O', '$\ll$', '$\gg$' and '$\asymp$' may depend on the integer parameters k and ν and normally are for $p \to \infty$ through primes. Recall that the notations $U \ll V$ and $V \gg U$ are equivalent to $U = O(V)$. By $\mathbf{e}_p(u)$ we mean as usual $\exp(2\pi i u/p)$. If $\mathcal{A}$ is a finite set, $|\mathcal{A}|$ represents the number of elements of $\mathcal{A}$.

2. Estimates from Arithmetic Combinatorics

2.1. Sum-Product Estimates

We start with the following standard result on double exponential sums, see [4, Bound (1.4)].

Lemma 1. *Let p be prime and $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$. Then*

$$\max_{(n,p)=1} \left| \sum_{x\in\mathcal{A}} \sum_{y\in\mathcal{B}} e_p(nxy) \right| \leq \sqrt{p|\mathcal{A}||\mathcal{B}|}.$$

We now present the following simple modification of the result of Garaev [13].

Theorem 2. *For arbitrary sets $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_p$, with $0 \notin \mathcal{B}$, we have*

$$|\mathcal{A}\cdot\mathcal{B}| \cdot |\mathcal{A}+\mathcal{C}| \geq \frac{3}{8} \min\left\{p|\mathcal{A}|, \frac{|\mathcal{A}|^2|\mathcal{B}||\mathcal{C}|}{p}\right\}.$$

Proof. As in [13], we consider the solutions of the equation

$$s \cdot \frac{1}{b} + c = t, \qquad b \in \mathcal{B},\ c \in \mathcal{C},\ s \in \mathcal{S},\ t \in \mathcal{T}, \tag{2}$$

where $\mathcal{S} = \mathcal{A}\cdot\mathcal{B}$ and $\mathcal{T} = \mathcal{A}+\mathcal{C}$.

For any triplet $(a,b,c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$ there is a unique solution, namely $s = ab$, $t = a + c$. So (2) has at least $|\mathcal{A}||\mathcal{B}||\mathcal{C}|$ solutions. On the other hand, as in [13], using the bound for bilinear exponential sums given by Lemma 1 to estimate the total number of solutions to (2), one derives

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}| \leq \frac{|\mathcal{B}||\mathcal{C}||\mathcal{S}||\mathcal{T}|}{p} + \frac{1}{p}\sqrt{p|\mathcal{B}||\mathcal{S}|}\sqrt{p|\mathcal{C}|}\sqrt{p|\mathcal{T}|}, \tag{3}$$

which implies the result (in fact with the constant $(3-\sqrt{5})/2 \geq 3/8$). □

Corollary 3. *For an arbitrary subset $\mathcal{A} \subseteq \mathbb{F}_p^*$ and integer $k \geq 1$, we have*

$$|\mathcal{A}^k| \cdot |k\mathcal{A}| \geq \min\left\{cp|\mathcal{A}|,\ \frac{c^{k-1}|\mathcal{A}|^{2k}}{p^{k-1}}\right\},$$

where $c = 3/8$.

Proof. We prove the desired estimate by induction on k. For $k = 2$, it is essentially the results of [13] (and it also follows from Theorem 2 with $\mathcal{B} = \mathcal{C} = \mathcal{A}$).

Now, we assume that

$$|\mathcal{A}^{k-1}| \cdot |(k-1)\mathcal{A}| \geq \min\left\{cp|\mathcal{A}|,\ \frac{c^{k-2}|\mathcal{A}|^{2k-2}}{p^{k-2}}\right\}.$$

Then for $k \geq 3$ we use Theorem 2 with $\mathcal{B} = \mathcal{A}^{k-1}$ and $\mathcal{C} = (k-1)\mathcal{A}$, getting

$$\begin{aligned} |\mathcal{A}^k| \cdot |k\mathcal{A}| &\geq c\min\left\{p|\mathcal{A}|,\ \frac{|\mathcal{A}|^2|\mathcal{A}^{k-1}||(k-1)\mathcal{A}|}{p}\right\} \\ &\geq \min\left\{cp|\mathcal{A}|, c^2|\mathcal{A}|^3, \frac{c^{k-1}|\mathcal{A}|^{2k}}{p^{k-1}}\right\}. \end{aligned}$$

Since for $|\mathcal{A}| < (p/c)^{1/2}$ the result is trivial (as $c^{k-1}|\mathcal{A}|^{2k}/p^{k-1} \leq |\mathcal{A}|^2$) and for $|\mathcal{A}| \geq (p/c)^{1/2}$ we have $cp|\mathcal{A}| < c^2|\mathcal{A}|^3$, the result now follows. □

We also note that as in [26] one can use multiplicative character sums to estimate the number of solutions to (2). In particular we recall a result of Karatsuba [21] (see also [22, Chapter VIII, Problem 9]), (which in turn follows from the Weil bound and the Hölder inequality) asserting that for a nontrivial multiplicative character χ modulo p and arbitrary sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$ we have

$$\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} \chi(x-y) \ll |\mathcal{X}|^{1-1/2\nu}|\mathcal{Y}|p^{1/4\nu} + |\mathcal{X}|^{1-1/2\nu}|\mathcal{Y}|^{1/2}p^{1/2\nu}, \tag{4}$$

with any fixed integer $\nu \geq 1$. With this, instead of the bound (3) we derive

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}| \leq \frac{|\mathcal{B}||\mathcal{C}||\mathcal{S}||\mathcal{T}|}{p} + \frac{1}{p}\sqrt{p|\mathcal{B}|}\sqrt{p|\mathcal{S}|}\left(|\mathcal{T}|^{1-1/2\nu}|\mathcal{C}|p^{1/4\nu} + |\mathcal{T}|^{1-1/2\nu}|\mathcal{C}|^{1/2}p^{1/2\nu}|\right),$$

which leads to another version of Theorem 2 (that is stronger if $|\mathcal{C}|$ is small).

Our second approach depends on the following estimate of Bourgain & Garaev [4, Theorem 1.2].

Lemma 4. *For arbitrary subsets $\mathcal{X}, \mathcal{Y}, \mathcal{Z} \subseteq \mathbb{F}_p$, as $p \to \infty$,*

$$\left|\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}\sum_{z\in\mathcal{Z}} \mathbf{e}_p(xyz)\right| \le (|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|)^{13/16} p^{5/18+o(1)}.$$

We are now ready to prove the following estimate:

Theorem 5. *For arbitrary sets $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_p^*$, we have*

$$\max\{|\mathcal{A}\cdot\mathcal{B}\cdot\mathcal{C}|, |\mathcal{A}+\mathcal{D}|\} \gg \min\{\sqrt{p|\mathcal{A}|}, |\mathcal{A}|^{16/21}(|\mathcal{B}||\mathcal{C}|)^{1/7}|\mathcal{D}|^{8/21}p^{-40/189+o(1)}\}.$$

Proof. We use a modification of the argument of Theorem 2. For the sets $\mathcal{U} = \mathcal{A}\cdot\mathcal{B}\cdot\mathcal{C}$ and $\mathcal{V} = \mathcal{A}+\mathcal{D}$, we consider the the number J of solutions (b, c, d, u, v) to the equation

$$ub^{-1}c^{-1} + d = v, \quad b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D},\ u \in \mathcal{U},\ v \in \mathcal{V}.$$

Clearly for $a \in \mathcal{A},\ b \in \mathcal{B},\ c \in \mathcal{C},\ d \in \mathcal{D}$, the vector $(b, c, d, abc, a + d)$ is a solution. Thus

$$J \ge |\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}|. \tag{5}$$

On the other hand, we obviously have

$$J = \sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}}\sum_{d\in\mathcal{D}}\sum_{u\in\mathcal{U}}\sum_{v\in\mathcal{V}} \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p} \mathbf{e}_p\left(\lambda(ub^{-1}c^{-1} + d - v)\right).$$

Changing the order of summation, separating the term $|\mathcal{B}||\mathcal{C}||\mathcal{D}||\mathcal{U}||\mathcal{V}|/p$ corresponding to $\lambda = 0$, we obtain

$$J = \frac{|\mathcal{B}||\mathcal{C}||\mathcal{D}||\mathcal{U}||\mathcal{V}|}{p} + R, \tag{6}$$

where

$$|R| \le \frac{1}{p}\sum_{\lambda\in\mathbb{F}_p^*}\left|\sum_{u\in\mathcal{U}}\sum_{b\in\mathcal{B}}\sum_{c\in\mathcal{C}} \mathbf{e}_p\left(\lambda ub^{-1}c^{-1}\right)\right|\left|\sum_{d\in\mathcal{D}} \mathbf{e}_p(\lambda d)\right|\left|\sum_{v\in\mathcal{V}} \mathbf{e}_p(\lambda v)\right|.$$

By Lemma 4 we obtain

$$|R| \le (|\mathcal{B}||\mathcal{C}||\mathcal{U}|)^{13/16} p^{-13/18+o(1)} \sum_{\lambda=1}^{p-1}\left|\sum_{d\in\mathcal{D}} \mathbf{e}_p(\lambda d)\right|\left|\sum_{v\in\mathcal{V}} \mathbf{e}_p(\lambda v)\right|. \tag{7}$$

Applying Cauchy's inequality (and extending the summation over λ to $\mathbb{F}_p$) we derive

$$\left(\sum_{\lambda\in\mathbb{F}_p^*}\left|\sum_{d\in\mathcal{D}} \mathbf{e}_p(\lambda d)\right|\left|\sum_{v\in\mathcal{V}} \mathbf{e}_p(\lambda v)\right|\right)^2 \le \sum_{\lambda\in\mathbb{F}_p}\left|\sum_{d\in\mathcal{D}} \mathbf{e}_p(\lambda d)\right|^2 \sum_{\lambda\in\mathbb{F}_p}\left|\sum_{v\in\mathcal{V}} \mathbf{e}_p(\lambda v)\right|^2.$$

Clearly

$$\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{d\in\mathcal{D}}\mathbf{e}_p\left(\lambda d\right)\right|^2=\sum_{d_1,d_2\in\mathcal{D}}\sum_{\lambda\in\mathbb{F}_p}\mathbf{e}_p\left(\lambda(d_1-d_2)\right)=p|\mathcal{D}|$$

and similarly

$$\sum_{\lambda\in\mathbb{F}_p}\left|\sum_{v\in\mathcal{V}}\mathbf{e}_p\left(\lambda v\right)\right|^2=p|\mathcal{V}|.$$

Thus collecting the previous inequalities and recalling (7), we see from (6).

$$J=\frac{|\mathcal{B}||\mathcal{C}||\mathcal{D}||\mathcal{U}||\mathcal{V}|}{p}+O\left((|\mathcal{B}||\mathcal{C}||\mathcal{U}|)^{13/16}(|\mathcal{D}||\mathcal{V}|)^{1/2}p^{5/18+o(1)}\right). \qquad (8)$$

Thus denoting $M=\max\{|\mathcal{U}|,|\mathcal{V}|\}$ and comparing (5) with (8), we derive

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}||\mathcal{D}|\ll\frac{|\mathcal{B}||\mathcal{C}||\mathcal{D}|M^2}{p}+(|\mathcal{B}||\mathcal{C}|)^{13/16}|\mathcal{D}|^{1/2}M^{21/16}p^{5/18+o(1)}$$

and the result now follows. □

In particular, taking $\mathcal{A}=\mathcal{B}=\mathcal{C}=\mathcal{D}$ we see that Theorem 5 implies that for an arbitrary set $\mathcal{A}\subseteq\mathbb{F}_p^*$, we have

$$\max\{|\mathcal{A}^3|,\,|2\mathcal{A}|\}\gg\min\{\sqrt{p|\mathcal{A}|},|\mathcal{A}|^{10/7}p^{-40/189+o(1)}\}.$$

However this bound seems weaker that the one which one can derive using a combination of the bounds of Garaev [13]

$$\max\{|\mathcal{A}^3|,\,|2\mathcal{A}|\}\ge\max\{|\mathcal{A}^2|,\,|2\mathcal{A}|\}\gg\min\{\sqrt{p|\mathcal{A}|},|\mathcal{A}|^2p^{-1/2}\},$$

and Rudnev [24]

$$\max\{|\mathcal{A}^3|,\,|2\mathcal{A}|\}\ge\max\{|\mathcal{A}^2|,\,|2\mathcal{A}|\}\ge(\min\{|\mathcal{A}|,\sqrt{p}\})^{12/11+o(1)}. \qquad (9)$$

2.2. Sum Inversion Estimates

In Theorem 2 we can replace $\mathcal{A}$ by $\mathcal{A}^{-1}$ and $\mathcal{B}$ by $\mathcal{B}^{-1}$ to easily obtain an analogue of that result: For arbitrary sets $\mathcal{A},\mathcal{B},\mathcal{C}\subseteq\mathbb{F}_p^*$, we have

$$|\mathcal{A}\cdot\mathcal{B}|\cdot|\mathcal{A}^{-1}+\mathcal{C}|\ge\frac{3}{8}\min\left\{p|\mathcal{A}|,\,\frac{|\mathcal{A}|^2|\mathcal{B}||\mathcal{C}|}{p}\right\}.$$

Lemma 6. *For arbitrary sets $\mathcal{X},\mathcal{Y}\subseteq\mathbb{F}_p$, and a non-zero element $\lambda\in\mathbb{F}_p^*$,*

$$\left|\sum_{x\in\mathcal{X}}\sum_{\substack{y\in\mathcal{Y}\\ y\neq x}}\mathbf{e}_p\left(\lambda(x-y)^{-1}\right)\right|\le 2\sqrt{p|\mathcal{X}||\mathcal{Y}|}.$$

Theorem 7. *For arbitrary sets $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_p^*$, we have*

$$|\mathcal{A}+\mathcal{B}| \cdot |\mathcal{A}^{-1}+\mathcal{C}| \geq \frac{1}{6} \min\left\{p|\mathcal{A}|, \frac{|\mathcal{A}|^2|\mathcal{B}||\mathcal{C}|}{p}\right\}.$$

Proof. We now mimic the argument of Garaev [13] and consider the equation

$$c + (s-b)^{-1} = t, \quad (b, c, s, t) \in \mathcal{B} \times \mathcal{C} \times \mathcal{S} \times \mathcal{T}. \tag{10}$$

where $\mathcal{S} = \mathcal{A}+\mathcal{B}$ and $\mathcal{T} = \mathcal{A}^{-1}+\mathcal{C}$.

For any triplet $(a, b, c) \in \mathcal{A} \times \mathcal{B} \times \mathcal{C}$ there is a unique solution, namely $t = a^{-1}+c$, $s = a+b$. So (10) has at least $|\mathcal{A}||\mathcal{B}||\mathcal{C}|$ solutions. On the other hand, as in [13], using Lemma 6 to estimate the total number of solutions to (10), one derives

$$|\mathcal{A}||\mathcal{B}||\mathcal{C}| \leq \frac{|\mathcal{B}||\mathcal{C}||\mathcal{S}||\mathcal{T}|}{p} + \frac{2}{p}\sqrt{p|\mathcal{S}||\mathcal{B}|}\sqrt{p|\mathcal{C}|}\sqrt{p|\mathcal{T}|},$$

which implies the result (in fact with the constant $3-\sqrt{8} \geq 1/6$) □

Then as in Section 2.1 we obtain:

Corollary 8. *For an arbitrary set $\mathcal{A} \subseteq \mathbb{F}_p^*$, we have*

$$|k\mathcal{A}| \cdot |k\mathcal{A}^{-1}| \geq \min\left\{cp|\mathcal{A}|, \frac{c^{k-1}|\mathcal{A}|^{2k}}{p^{k-1}}\right\},$$

where $c = 1/6$.

Furthermore, taking $\mathcal{B} = \mathcal{A}^{-1}$ and $\mathcal{C} = \mathcal{A}$ in Theorem 7, we derive:

Corollary 9. *For an arbitrary set $\mathcal{A} \subseteq \mathbb{F}_p^*$, we have*

$$|\mathcal{A}+\mathcal{A}^{-1}| \geq 6^{-1/2} \min\left\{\sqrt{p|\mathcal{A}|}, \frac{|\mathcal{A}|^2}{\sqrt{p}}\right\}.$$

We also note that for smaller sets, Bourgain [3, Theorem 4.1] has shown that for any $\varepsilon > 0$ there exists $\delta > 0$ such for any set $\mathcal{A} \subseteq \mathbb{F}_p^*$ of cardinality $|\mathcal{A}| \leq p^{1-\varepsilon}$,

$$\max\left\{|\mathcal{A}+\mathcal{A}|, |\mathcal{A}^{-1}+\mathcal{A}^{-1}|\right\} \gg |\mathcal{A}|^{1+\delta}.$$

The dependence of δ on ε has not been made explicit in [3], however using a recent estimate of Helfgott & Rudnev [19, Theorem 2] or its improvement due to Jones [20] in the argument of [3] one can easily derive such a result.

3. Applications

3.1. Exponential Congruence

For a prime p and an integer $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$ we denote by $N(p; a)$ the number of solutions to the congruence (1).

By [1, Theorem 2] we have, uniformly for $t \mid p-1$,

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \operatorname{ord} a \mid t}} N(p;a) \le \max\{t, p^{1/2}t^{1/4}\}p^{o(1)}, \tag{11}$$

as $p \to \infty$, where $\operatorname{ord} a$ denotes the multiplicative order of $a \in \mathbb{F}_p^*$. Furthermore, for small values of t by [1, Theorem 4] we also have

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \operatorname{ord} a \mid t}} N(p;a) \le p^{1/3+o(1)}t^{2/3}, \tag{12}$$

as $p \to \infty$. We now give an estimate that improves (11) and (12) for $p^{1/4} \le t \le p^{2/3}$.

Theorem 10. *Uniformly over $t \mid p-1$, we have, as $p \to \infty$,*

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \operatorname{ord} a \mid t}} N(p;a) \le \max\{t, p^{1/2}\}p^{o(1)}.$$

Proof. We fix a primitive root $g \in \mathbb{F}_p^*$ and for $u \in \mathbb{F}_p^*$ (and so for any integer $u \not\equiv 0 \pmod p$) we use $\operatorname{ind} u$ for its discrete logarithm modulo p, that is, the unique residue class $v \pmod{p-1}$ with $g^v \equiv u \pmod p$.

As in the proof of [1, Theorem 2], for $d \mid (p-1)/t$, we denote by $\mathcal{Y}_d$ the set of integers y satisfying the congruence

$$\operatorname{ind}(dy) \equiv 0 \pmod{T_d}, \qquad 1 \le y \le D, \qquad \gcd(y, T_d) = 1,$$

where

$$T_d = \frac{p-1}{dt} \qquad \text{and} \qquad D = \frac{p-1}{d}.$$

Furthermore, let $\mathcal{W}_d$ be the set of residue classes represented by the elements of $\mathcal{Y}_d$ (that is, we embed $\mathcal{Y}_d$ in $\mathbb{F}_p$ in a canonical way). Then we have

$$\sum_{\substack{a \in \mathbb{Z}_p^* \\ \operatorname{ord} a \mid t}} N(p;a) = \sum_{d \mid (p-1)/t} |\mathcal{Y}_d| = \sum_{d \mid (p-1)/t} |\mathcal{W}_d|; \tag{13}$$

see [1, Equation (9)].

We note that for any integer $k \ge 1$ we have, $|k\mathcal{W}_d| \le kD$ and $|\mathcal{W}_d^k| \le dt$. (which are straight forward generalisations of [1, Equations (10) and (11)], respectively, that correspond to $k=2$). Applying Corollary 3, we see that for every fixed k

$$\min\left\{p|\mathcal{W}_d|, \frac{|\mathcal{A}|^{2k}}{p^{k-1}}\right\} \ll Ddt \le pt$$

or $|\mathcal{W}_d| \ll \max\{t, p^{1/2}\}t^{1/2k}$ (which substitutes [1, Equation (12)]). Since k is arbitrary, recalling (13), and the well-known bound $m^{o(1)}$ on the number of integer divisors of an integer $m \ge 1$, we derive the result. $\square$

3.2. Intersections of Almost Arithmetic and Geometric Progressions

We say that a set $\mathcal{I} \subseteq \mathbb{F}_p$ is an *almost arithmetic progression* if for every fixed integer $k \geq 1$ and real $\varepsilon > 0$ there is a constant $C_+(k, \varepsilon)$ such that

$$|k\mathcal{I}| \leq C_+(k, \varepsilon)|\mathcal{I}|p^{\varepsilon}.$$

We also say that a set $\mathcal{G} \subseteq \mathbb{F}_p$ is an *almost geometric progression* if for every fixed integer $k \geq 1$ and real $\varepsilon > 0$ there is a constant $C_\times(k, \varepsilon)$ such that

$$|\mathcal{G}^k| \leq C_\times(k, \varepsilon)|\mathcal{G}|p^{\varepsilon}.$$

Theorem 11. *For any almost arithmetic progression $\mathcal{I} \subseteq \mathbb{F}_p^*$ and almost geometric progression $\mathcal{G} \subseteq \mathbb{F}_p^*$ we have,*

$$|\mathcal{I} \cap \mathcal{G}| \leq \left(\frac{|\mathcal{I}||\mathcal{G}|}{p} + p^{1/2} \right) p^{o(1)}$$

as $p \to \infty$.

Proof. Let $\mathcal{A} = \mathcal{I} \cap \mathcal{G}$ then, for any fixed integer $k \geq 1$ we see that $|\mathcal{A}^k| \leq |\mathcal{G}|p^{o(1)}$ and $|k\mathcal{A}| \leq |\mathcal{I}|p^{o(1)}$. Applying Corollary 3, we derive

$$|\mathcal{G}||\mathcal{I}|p^{o(1)} \geq \min\left\{ cp|\mathcal{A}|, \frac{c^{k-1}|\mathcal{A}|^{2k}}{p^{k-1}} \right\},$$

where $c = 3/8$ or

$$|\mathcal{A}| \leq \left(\frac{|\mathcal{G}||\mathcal{I}|}{p} + p^{1/2}(|\mathcal{G}||\mathcal{I}|/p)^{1/2k} \right) p^{o(1)}.$$

Since k is arbitrary, the result now follows. □

We note that upper bounds for the number of residues modulo p of consecutive powers g^x with $x \in [K+1, K+M]$ in an interval of length M that belong to some other interval $[L+1, L+M]$ of length M are given by Cilleruelo & Garaev [9]. The estimates and methods of [9] improve those of [7]. However they do not seem to apply to almost arithmetic and geometric progressions (while the approach of [7] does and is actually used here). On the other hand, the bound (9) implies that for $M \leq p^{6/11}$ we have

$$|\mathcal{I} \cap \mathcal{G}| \leq M^{11/12+o(1)}.$$

Using Corollary 8 we also derive:

Theorem 12. *For any almost arithmetic progressions $\mathcal{I}, \mathcal{J} \subseteq \mathbb{F}_p^*$ we have,*

$$|\mathcal{I} \cap \mathcal{J}^{-1}| \leq \left(\frac{|\mathcal{I}||\mathcal{J}|}{p} + p^{1/2} \right) p^{o(1)}$$

as $p \to \infty$.

4. Comments

In relation to Corollary 8 it could be relevant to recall a well-known example given in [8], that shows there are infinitely many pairs $(p, \mathcal{A})$ of primes p and sets $\mathcal{A} \subseteq \mathbb{F}_p^*$ with

$$|\mathcal{A}| \sim p^{1/2+o(1)} \tag{14}$$

and such that for any fixed integer k,

$$\max\left\{|\mathcal{A}^k|, |k\mathcal{A}|\right\} \le p^{3/4+o(1)}. \tag{15}$$

Indeed, let $\mathcal{H}$ be a multiplicative subgroup of $\mathbb{F}_p^*$ of order $|\mathcal{H}| \sim p^{3/4+o(1)}$ (there are infinitely many primes for which such a subgroup exists, see [12]).

By the pigeon-hole principle, there exists an $s \in \mathbb{F}_p$ such that if we set

$$\mathcal{A} = \mathcal{H} \cap \{s, s+1, \ldots, s + \left\lfloor p^{3/4} \right\rfloor\}$$

we have

$$|\mathcal{A}| \sim \frac{|\mathcal{H}| p^{3/4}}{p} \sim p^{1/2+o(1)}.$$

It is now easy to see that (15) holds for any integer k. One can also obtain a similar example limiting the possible growth of $\max\{|k\mathcal{A}|, |k\mathcal{A}^{-1}|\}$ by considering the set $\mathcal{J} = \{j^{-1} \ : \ j = 1, \ldots, \left\lfloor p^{3/4} \right\rfloor\}$, and defining $\mathcal{A}$ as the most "popular" intersection (in $\mathbb{F}_p$) of $\mathcal{J}$ with one of the sets $\{s+1, \ldots, s + \left\lfloor p^{3/4} \right\rfloor\}$, $s \in \mathbb{F}_p$. Therefore we see that, for an infinite number of primes p, there is a set $\mathcal{A} \subseteq \mathbb{F}_p^*$ satisfying (14) and such that, for any fixed integer k, $\max\{|k\mathcal{A}|, |k\mathcal{A}^{-1}|\} \ll p^{3/4}$.

Acknowledgements Research of A. B. was supported in part by Hungarian National Science Foundation Grants K72731 and K81658 and that of I. S. was supported in part by Australia Research Council Grants DP0881473 and DP1092835.

References

[1] A. Balog, K. A. Broughan and I. E. Shparlinski, 'On the number of solutions of exponential congruences,' *Acta Arith.*, **148** (2011), 93–103.

[2] K. Bibak, 'Additive combinatorics with a view towards computer science and cryptography: An exposition,' *preprint*, 2011, (available from `http://arxiv.org/abs/1108.3790`).

[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 and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields,' *Math. Proc. Cambr. Phil. Soc.*, **146** (2008), 1–21.

[5] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, 'Estimates for the number of sums and products and for exponential sums in fields of prime order,' *J. Lond. Math. Soc.*, **73** (2006), 380–398.

[6] J. Bourgain, N. Katz and T. Tao, 'A sum product estimate in finite fields and applications,' *Geom. Funct. Analysis*, **14** (2004), 27–57.

[7] T. H. Chan and I. E. Shparlinski, 'On the concentration of points on modular hyperbolas and exponential curves,' *Acta Arith.*, **142** (2010), 59–66.

[8] M.-C. Chang, 'Some problems in combinatorial number theory,' *Integers*, **8** (2008), Article A1, 1–11.

[9] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications,' *Geom. and Func. Anal.*, **21** (2011), 892–904.

[10] E. Croot and D. Hart, 'h-fold sums from a set with few products,' *SIAM J. Discr. Math.*, **24** (2010), 505–519.

[11] G. Elekes, 'On the number of sums and products,' *Acta Arith.*, **81** (1997), 365–367.

[12] K. Ford, 'The distribution of integers with a divisor in a given interval,' *Annals Math.*, **168** (2008), 367–433.

[13] M. Z. Garaev, 'The sum-product estimate for large subsets of prime fields,' *Proc. Amer. Math. Soc.*, **136** (2008), 2735–2739.

[14] M. Z. Garaev, 'Sums and products of sets and estimates of rational trigonometric sums in fields of prime order,' *Uspekhi Mat. Nauk*, **65** (4) (2010), 5–66.

[15] A. Glibichuk, 'Sums of powers of subsets or arbitrary finite fields,' *Izv. Ross. Akad. Nauk Ser. Mat. (Transl. as Izvestiya. Mathematics)*, **75** (2) (2011), 3–36 (in Russian).

[16] A. Glibichuk and M. Rudnev, 'On additive properties of product sets in an arbitrary finite field,' *J. d'Analyse Math.*, **108** (2009), 159–170.

[17] D. Hart, A. Iosevich and J. Solymosi, 'Sums and products in finite fields via Kloosterman sums,' *Intern. Math. Res. Notices*, **2007** (2007), Article ID rnm007, 1–14.

[18] D. Hart, L. Li and C.-Y. Shen, 'Fourier analysis and expanding phenomena in finite fields,' *Preprint*, 2009 (available from `http://arxiv.org/abs/0909.5471`).

[19] H. A. Helfgott and M. Rudnev, 'An explicit incidence theorem in $\mathbb{F}_p$,' *Mathematika*, **57** (2011) 135–145.

[20] T. G. F. Jones, 'An improved incidence bound for fields of prime order,' *Preprint*, 2011 (available from `http://arxiv.org/abs/1110.4752v1`).

[21] A. A. Karatsuba, 'The distribution of values of Dirichlet characters on additive sequences,' *Doklady Acad. Sci. USSR*, **319** (1991), 543–545 (in Russian).

[22] A. A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, 1993.

[23] L. Li, 'Slightly improved sum-product estimates in fields of prime order,' *Acta Arith.*, **147** (2011), 153–160.

[24] M. Rudnev, 'An improved sum-product inequality in fields of prime order,' *preprint*, 2010 (available from `http://arxiv.org/abs/1011.2738`).

[25] C.-Y. Shen, 'An extension of Bourgain and Garaev's sum-product estimates,' *Acta Arith.*, **135** (2008), 351–256.

[26] I. E. Shparlinski, 'On the solvability of bilinear equations in finite fields,' *Glasgow Math. J.* **50** (2008), 523–529.