Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 2

A note on the set $A(A + A)$

Pierre-Yves Bienvenu, François Hennecart and Ilya Shkredov

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 2, 2019
dx.doi.org/10.2140/moscow.2019.8.179

A note on the set $A(A+A)$

Pierre-Yves Bienvenu, François Hennecart and Ilya Shkredov

Let p be a large enough prime number. When A is a subset of $\mathbb{F}_p \setminus \{0\}$ of cardinality $|A| > (p+1)/3$, then an application of the Cauchy–Davenport theorem gives $\mathbb{F}_p \setminus \{0\} \subset A(A+A)$. In this note, we improve on this and we show that $|A| \geq 0.3051p$ implies $A(A+A) \supseteq \mathbb{F}_p \setminus \{0\}$. In the opposite direction we show that there exists a set A such that $|A| > \left(\frac{1}{8}+o(1)\right)p$ and $\mathbb{F}_p \setminus \{0\} \not\subseteq A(A+A)$.

1. Introduction

The aim of this note is to study the size of the set $A(A+A) = \{a(b+c) : a, b, c \in A\}$ for a subset $A \subseteq \mathbb{F}_p \setminus \{0\}$. This sort of problem belongs to the realm of expanding polynomials and sum-product problems. In the literature, they are usually discussed in the sparse set regime; for instance, Roche-Newton et al. [2016] and Aksoy Yazici et al. [2017] proved that in the regime where $|A| \ll p^{2/3}$, one has $\min(|A+AA|, |A(A+A)|) \gg |A|^{3/2}$ (see also [Stevens and de Zeeuw 2017]). This implies in particular that as soon as $|A| \gg p^{2/3}$, both sets $A(A+A)$ and $A+AA$ occupy a positive proportion of $\mathbb{F}_p$.

Now we focus on the case where $A \subseteq \mathbb{F}_p$ occupies already a positive proportion of $\mathbb{F}_p$. Let $\alpha = |A|/p$, so we suppose that $\alpha > 0$ is bounded below by a positive constant, while p tends to infinity. We will see that in this case the set $A(A+A)$ contains all but a finite number of elements. Additionally, we prove that this finite number of elements may be strictly larger than 1, unless α is large enough.

Here are our main results.

Theorem 1.1. *Let $A \subseteq \mathbb{F}_p$ so that $|A| = \alpha p$ with $\alpha \geq 0.3051$. Then for any large enough prime p, we have $A(A+A) \supseteq \mathbb{F}_p \setminus \{0\}$.*

For smaller densities, we have the following result.

Theorem 1.2. *Let $A \subseteq \mathbb{F}_p \setminus \{0\}$ and $0 < \alpha < 1$ satisfy $|A| \geq \alpha p$. Then one has*

$$|A(A+A)| > p - 1 - \alpha^{-3}(1-\alpha)^2 + o(1).$$

We note that similar results were obtained [Hegyvári and Hennecart 2018] for the set $AA+A$. However, the constant 0.3051 is replaced by the larger $\frac{1}{3}$ in Theorem 1.1, and the term $\alpha^{-3}(1-\alpha)^2$ is replaced by the larger α^{-3}. Further, the slightly weaker bound $|A(A+A)| \geq p - \alpha^{-3}$ may be extracted from [Sárközy 2005].

In the opposite direction, we have the following result.

This work was performed within the framework of the Labex MILYON (ANR-10-LABX-0070) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).
MSC2010: 11B75.
Keywords: sum-product estimates, arithmetic combinatorics, finite fields.

Theorem 1.3. *There exists $A \subseteq \mathbb{F}_p \setminus \{0\}$ such that $|A| > \left(\frac{1}{8} + o(1)\right)p$ and $A(A+A) \subsetneq \mathbb{F}_p \setminus \{0\}$ for any large prime p. Additionally, for any $\epsilon > 0$ there exists a set of size $O(p^{3/4+\epsilon})$ such that $A(A+A)$ misses $\Omega(p^{1/4-\epsilon})$ elements.*

2. Proof of Theorem 1.1

In this section, we shall need the Cauchy–Davenport theorem, which we now state. See for instance [Nathanson 1996, Theorem 2.2] for a proof.

Lemma 2.1. *Let A and B be subsets of $\mathbb{F}_p$. Then $|A+B| \geq \min(|A|+|B|-1, p)$.*

In particular, if $|A|+|B| > p$, then $A+B = \mathbb{F}_p$, which is also obvious because A and $x-B$ cannot be disjoint for any x.

First, we note that if $\alpha > \frac{1}{2}$, then $|A+A| \geq |A| > p/2$ so that $A(A+A) = \mathbb{F}_p$. But as soon as $\alpha < \frac{1}{2}$, we can easily have $A(A+A) \subsetneq \mathbb{F}_p^*$, for instance by taking $A = \{1, \dots, \lfloor (p-1)/2 \rfloor\}$.

Here is another almost equally immediate corollary.

Corollary 2.2. *Let $A \subseteq \mathbb{F}_p \setminus \{0\}$ satisfy $|A| > (p+1)/3$. Then either $A(A+A) = \mathbb{F}_p$ or $\mathbb{F}_p \setminus \{0\}$.*

Proof. Let $B = (A+A) \setminus \{0\}$. Using Lemma 2.1, we have $|A+A| > (2p-1)/3$ so $|B| > (2p-4)/3$, whence $|A|+|B| > p-1$. We infer that for any $x \in \mathbb{F}_p \setminus \{0\}$ we have

$$xB^{-1} \cap A \neq \varnothing,$$

which yields $AB = \mathbb{F}_p \setminus \{0\}$. □

We now prove Theorem 1.1, which reveals that we can lower the density requirement from $\frac{1}{3}$ to 0.3051 while maintaining $A(A+A) \supset \mathbb{F}_p \setminus \{0\}$.

To start with, we recall the famous Freiman's $3k-4$ theorem for the integers, which gives precise structural information on a set which has quite small, but not necessarily minimal, doubling [Nathanson 1996, Theorem 1.16].

Proposition 2.3. *If $A \subset \mathbb{Z}$ satisfies $|A+A| \leq 3|A|-4$ then A is contained in an arithmetic progression of length at most $|A+A|-|A|+1$.*

An analogue of this proposition has been developed in $\mathbb{F}_p$, and it is known as the *Freiman 2.4-theorem*. A useful lemma in [Freiman 1962] (see also [Nathanson 1996, Theorem 2.9]) was derived in the proof thereof, and we will need it here. We also include an improvement due to Lev.

We first define the Fourier transform of a function $f : \mathbb{F}_p \to \mathbb{C}$ by

$$\hat{f}(t) = \sum_{x \in \mathbb{F}_p} f(x) e_p(tx)$$

for any $t \in \mathbb{F}_p$, where $e_p(x) = \exp(2i\pi x/p)$. The Parseval identity is

$$\sum_{x \in \mathbb{F}_p} f(x)\overline{g(x)} = \frac{1}{p} \sum_{h \in \mathbb{F}_p} \hat{f}(h)\overline{\hat{g}(h)}. \tag{1}$$

The characteristic function of a subset A of $\mathbb{F}_p$ is denoted by 1_A and for $r \in \mathbb{F}_p$ we let $rA = \{ra : a \in A\}$.

Lemma 2.4. *Let $A \subseteq \mathbb{F}_p$ with $|A| = \alpha p$ and $0 < \gamma < 1$ satisfy $|\hat{1}_A(r)| \geq \gamma|A|$ for some $r \in \mathbb{F}_p \setminus \{0\}$. Then there exists an interval modulo p of length at most $p/2$ that contains at least $\alpha_1 p$ elements of rA where α_1 can be freely chosen as*

(i) $\alpha_1 = (1+\gamma)\alpha/2$ (see [Freiman 1962]), *or*

(ii) $\alpha_1 = \alpha/2 + 1/(2\pi)\arcsin(\pi\gamma\alpha)$ (see [Lev 2005]).

There a few other basic results about Fourier transforms that we will need in the sequel.

Lemma 2.5. *Let P be an arithmetic progression in $\mathbb{F}_p$. Then*

$$\sum_{r\in\mathbb{F}_p} |\hat{1}_P(r)| \ll p\log p.$$

We now recall Weil's bound [1948] for Kloosterman sums.

Lemma 2.6. *For any $(a, b) \neq (0, 0)$, we have*

$$\left|\sum_{k\in\mathbb{F}_p\setminus\{0\}} e_p(ak + bk^{-1})\right| \leq 2\sqrt{p}.$$

We will also need a bound for so-called incomplete Kloosterman sums, whose proof follows easily from the last two lemmas.

Lemma 2.7. *Let $P \subseteq \mathbb{F}_p \setminus \{0\}$ be an arithmetic progression. Then for any $r \neq 0$ we have*

$$|\hat{1}_{P^{-1}}(r)| \ll \sqrt{p}\log p.$$

Now we start the proof of Theorem 1.1 itself. Let $\alpha \geq 0.3051$, let $A \subseteq \mathbb{F}_p \setminus \{0\}$ of size $|A| = \alpha p$ and set $B = (A + A) \setminus \{0\}$. We assume that there exists $x \in \mathbb{F}_p \setminus \{0\}$ such that $x \notin A(A + A)$. Then

$$xB^{-1} \cap A = \varnothing, \quad (xA^{-1} - A) \cap A = \varnothing. \tag{2}$$

It follows that $|A| + |B| \leq p - 1$, since otherwise $AB = \mathbb{F}_p \setminus \{0\}$. Hence $|A + A| \leq |B| + 1 \leq p - |A|$.

We define

$$r_1(y) = |\{(a, b) \in A \times A : y = xa^{-1} - b\}|,$$
$$r_2(y) = |\{(c, d) \in A \times A : c + d \neq 0 \text{ and } y = x(c + d)^{-1}\}|,$$

and $E_i = \sum_{y\in\mathbb{F}_p} r_i(y)^2$, $i = 1, 2$, the corresponding energies. Observe from (2) that

$$\sum_{\substack{y\in\mathbb{F}_p\\ r_1(y)+r_2(y)>0}} 1 \leq p - |A|.$$

By Cauchy–Schwarz we get

$$4|A|^4 = \left(\sum_{y\in\mathbb{F}_p} (r_1(y) + r_2(y))\right)^2 \leq (p - |A|) \times \sum_{y\in\mathbb{F}_p} (r_1(y) + r_2(y))^2. \tag{3}$$

Expanding the later inner sum gives

$$\sum_{y\in\mathbb{F}_p} (r_1(y) + r_2(y))^2 = E_1 + E_2 + 2\sum_{y\in\mathbb{F}_p} r_1(y)r_2(y).$$

Let

$$\gamma = \max_{h\neq 0} \frac{|\hat{1}_A(h)|}{|A|}.$$

We have by Parseval

$$pE_2 = \sum_h |\hat{1}_A(h)|^4 = |A|^4 + \sum_{h\neq 0} |\hat{1}_A(h)|^4 \le |A|^4 + \gamma^2 |A|^2 (p|A| - |A|^2)$$

and

$$\begin{aligned} pE_1 &= \sum_h |\hat{1}_{xA^{-1}}(h)|^2 |\hat{1}_A(h)|^2 = |A|^4 + \sum_{h\neq 0} |\hat{1}_{xA^{-1}}(h)|^2 |\hat{1}_A(h)|^2 \\ &\le |A|^4 + \gamma^2 |A|^2 (p|A| - |A|^2). \end{aligned}$$

Moreover

$$\begin{aligned} p \sum_{y\in\mathbb{F}_p} r_1(y) r_2(y) &= \sum_h \hat{1}_{xA^{-1}}(h) \hat{1}_A(-h) \hat{r}_2(h) \\ &\le |A|^4 + \max_{h\neq 0} |\hat{r}_2(h)| \sum_{h\neq 0} |\hat{1}_{xA^{-1}}(h)| \, |\hat{1}_A(h)| \\ &\le |A|^4 + \max_{h\neq 0} |\hat{r}_2(h)| (p|A| - |A|^2), \end{aligned}$$

by Parseval and Cauchy–Schwarz. For $h \neq 0$,

$$\hat{r}_2(h) = \sum_{\substack{c,d\in A \\ c+d\neq 0}} e_p(hx(c+d)^{-1}) = \frac{1}{p} \sum_r \sum_{z\neq 0} \sum_{c,d\in A} e_p(r(c+d-z)) e_p(hxz^{-1});$$

hence by the Parseval identity (1) and Lemma 2.6

$$|\hat{r}_2(h)| \le \frac{1}{p} \sum_r |\hat{1}_A(r)|^2 \left| \sum_{z\neq 0} e_p(hxz^{-1}) \right| \ll \sqrt{p}|A|;$$

similar arguments were used in [Moshchevitin 2007, Theorem 4]. We thus obtain from (3) and the above bounds

$$2\alpha \le (1-\alpha)(2\alpha + \gamma^2(1-\alpha) + o(1)).$$

This finally gives the lower bound

$$\gamma \ge \frac{\sqrt{2}\alpha}{1-\alpha} + o(1).$$

We are in position to apply Lemma 2.4(i). Let $A_1 \subset A$ be such that $|A_1| \ge (1+\gamma)|A|/2$ and rA_1 is included in an interval of length $p/2$ for some $r \neq 0$. This shows that A_1 is 2-Freiman isomorphic[1] to a subset A_1' of $\mathbb{Z}$. So we seek to apply Proposition 2.3 to A_1'. We get

$$\alpha_1 = \frac{|A_1|}{p} \ge f(\alpha) + o(1) := \frac{(1+(\sqrt{2}-1)\alpha)\alpha}{2(1-\alpha)} + o(1), \tag{4}$$

$$c_1 = \frac{|A_1 + A_1|}{|A_1|} \le \frac{|A+A|}{|A_1|} \le \frac{(1-\alpha)p}{\alpha_1 p} \le \frac{1-\alpha}{f(\alpha)} + o(1). \tag{5}$$

[1] That is, there exists a bijection $f : A_1 \to A_1'$ such that $a+b = c+d \iff f(a)+f(b) = f(c)+f(d)$ for all $a, b, c, d \in A_1$.

In order to have $c_1 < 3$, it is sufficient to have

$$\alpha > \frac{7-\sqrt{9+24\sqrt{2}}}{10-6\sqrt{2}} = 0.29513\dots,$$

which is satisfied since we have assumed $\alpha \geq 0.3051$. We thus obtain that A_1 (resp. A_1+A_1) is contained inside an arithmetic progression P_1 (resp. $Q_1 = P_1 + P_1$) of length $|P_1| = |A_1+A_1| - |A_1| + 1$ (resp. $2|P_1|-1$).

We define $B_1 = (A_1+A_1) \setminus \{0\}$ and $Q_1^* = Q_1 \setminus \{0\}$. We need to estimate

$$T = \frac{1}{p} \sum_{r \bmod p} \sum_{\substack{a\in P_1 \\ b\in Q_1^*}} e_p(r(a-b^{-1}x)) \geq \frac{|P_1||Q_1^*|}{p} - \frac{1}{p} \sum_{0<|r|<p/2} |\hat{1}_{P_1}(r)||\hat{1}_{Q_1^{*-1}}(rx)|,$$

which counts the solutions $(a,b) \in P_1 \times Q_1^*$ to the equation $a = b^{-1}x$.

Now $|\hat{1}_{P_1}(r)| \ll p/|r|$ by Lemma 2.5 and $|\hat{1}_{Q_1^{*-1}}(rx_0)| \ll \sqrt{p}\log p$ by Lemma 2.7 because Q_1^* is the union of at most two arithmetic progressions.

As a result, we have

$$T \geq \frac{|P_1||Q_1^*|}{p} + O(\sqrt{p}(\log p)^2).$$

The number of solutions to $a = b^{-1}x$ with $a \in P_1 \setminus A_1$ or $b \in Q_1^* \setminus B_1$ is at most $|P_1|-|A_1|+|Q_1^*|-|B_1|$. Since by assumption there is no solution to $a = b^{-1}x$ with $(a,b) \in A_1 \times B_1$ we get

$$T \leq |P_1| - |A_1| + |Q_1^*| - |B_1|$$

yielding

$$\frac{|P_1||Q_1^*|}{p} \leq |P_1| - |A_1| + |Q_1^*| - |B_1| + O(\sqrt{p}(\log p)^2).$$

This implies

$$\frac{(|B_1|-|A_1|)^2}{p} \leq |B_1| - 2|A_1| + O(\sqrt{p}(\log p)^2),$$

whence

$$\alpha_1(c_1-1)^2 \leq c_1 - 2 + o(1).$$

Because of (4), this gives

$$f(\alpha) \times (c_1-1)^2 - c_1 + 2 \leq o(1). \tag{6}$$

The left-hand side of this inequality defines a function of c_1 which is decreasing in the range $2 \leq c_1 \leq 1 + 1/(2f(\alpha))$, a contradiction. We check easily that $\alpha + f(\alpha) \geq \frac{1}{2}$ whenever $\alpha \geq 0.3$. Hence for such α

$$\frac{1-\alpha}{f(\alpha)} \leq 1 + \frac{1}{2f(\alpha)}.$$

We thus obtain from (5) and (6)

$$f(\alpha)\left(\frac{1-\alpha}{f(\alpha)} - 1\right)^2 - \frac{1-\alpha}{f(\alpha)} + 2 \leq o(1),$$

which reduces to

$$(1-\alpha-f(\alpha))^2-(1-\alpha-2f(\alpha))\le o(1).$$

In view of the definition of $f(\alpha)$ in (4), we get by expanding the above formula

$$(11-6\sqrt{2})\alpha^3-(22-6\sqrt{2})\alpha^2+17\alpha-4\le o(1),$$

giving $\alpha<0.305091+o(1)$, a contradiction for all p large enough. This concludes the proof of Theorem 1.1. □

Remark 2.8. Using instead the sharpest result (ii) of Lemma 2.4 leads to a slight improvement: if $|A|\ge 0.30065p$ then $\mathbb{F}_p\smallsetminus\{0\}\subseteq A(A+A)$ for any large p. The improvement is very small and uses nonalgebraic expressions, which is why we decided not to exploit it.

3. Proof of Theorem 1.2

We will now use multiplicative characters of $\mathbb{F}_p$. We denote by $\mathfrak{X}$ the set of all multiplicative characters modulo p and by χ_0 the trivial character. In this context Parseval's identity is the statement that

$$\frac{1}{p-1}\sum_{\chi\in\mathfrak{X}}\Bigg|\sum_{x\in\mathbb{F}_p\smallsetminus\{0\}}f(x)\chi(x)\Bigg|^2=\sum_{x\in\mathbb{F}_p\smallsetminus\{0\}}|f(x)|^2. \tag{7}$$

We state and prove a lemma which is a multiplicative analogue of a lemma of Vinogradov [1955], see also [Sárközy 2005, Lemma 7], according to which

$$\Bigg|\sum_{(x,y)\in A\times B}e_p(xy)\Bigg|\le\sqrt{p|A||B|}. \tag{8}$$

Lemma 3.1. *For any subsets A, B of $\mathbb{F}_p\smallsetminus\{0\}$ and any nontrivial character $\chi\in\mathfrak{X}$, we have*

$$\Bigg|\sum_{(y,z)\in A\times B}\chi(y+z)\Bigg|\le(|A||B|p)^{1/2}\left(1-\frac{|B|}{p}\right)^{1/2}.$$

We now prove Theorem 1.2. Let A be a subset of $\mathbb{F}_p\smallsetminus\{0\}$ and $\alpha=|A|/p$. We estimate the number of nonzero elements in $A(A+A)$ by estimating the number N of solutions to

$$x(y+z)=x'(y'+z')\ne 0,\quad x,y,z,x',y',z'\in A,$$

which we can rewrite as $x'x^{-1}(y+z)^{-1}(y'+z')=1$. This number is

$$\begin{aligned}N&=\frac{1}{p-1}\sum_{\chi\in\mathfrak{X}}\Bigg|\sum_{y,z\in A}\chi(z+y)\sum_{x\in A}\chi(x)\Bigg|^2\\&\le\frac{|A|^6}{p-1}+\max_{\chi\ne\chi_0}\Bigg|\sum_{y,z\in A}\chi(y+z)\Bigg|^2\times\frac{1}{p-1}\sum_{\chi\ne\chi_0}\Bigg|\sum_{x\in A}\chi(x)\Bigg|^2;\end{aligned}$$

hence by Lemma 3.1 and Parseval's identity (7)

$$\begin{aligned} N &\le \frac{|A|^6}{p-1} + p|A|^2(1-\alpha)\left(|A| - \frac{|A|^2}{p-1}\right) \\ &\le \frac{|A|^6}{p-1} + p|A|^3(1-\alpha)^2 \\ &\le \frac{|A|^6}{p-1}(1+p^2|A|^{-3}(1-\alpha)^2) \\ &\le \frac{|A|^6}{p-1}(1+p^{-1}\alpha^{-3}(1-\alpha)^2). \end{aligned}$$

We let $\rho(w) = |\{(x, y, z) \in A \times A \times A : w = x(y+z)\}|$ for $w \in \mathbb{F}_p$. Then

$$N = \sum_{w \in A(A+A)\setminus\{0\}} \rho(w)^2 \quad \text{and} \quad \sum_{w \in A(A+A)\setminus\{0\}} \rho(w) \ge |A|^6 - |A|^4.$$

Finally N is related to $|A(A+A)|$ by the Cauchy–Schwarz inequality as follows:

$$\begin{aligned} |A(A+A)| \ge |A(A+A)\setminus\{0\}| &\ge (|A|^6 - |A|^4)N^{-1} \\ &\ge (p-1)(1-\alpha^{-2}p^{-2})(1+p^{-1}\alpha^{-3}(1-\alpha)^2)^{-1} \\ &> p-1-\alpha^{-3}(1-\alpha)^2 + o(1). \end{aligned}$$

This concludes the proof of Theorem 1.2. □

4. Proof of Theorem 1.3

First we need a lemma.

Lemma 4.1. *Let $c < \frac{1}{2}$ and p be large enough. Let $P = \{1, \dots, \lceil cp \rceil\}$. Then the set $(P+P)^{-1}$ of the inverses (modulo p) of nonzero elements of $P+P$ has at most $2c^2 p + O(\sqrt{p}(\log p)^2)$ common elements with P; that is,*

$$|(P+P)^{-1} \cap P| \le 2c^2 p + O(\sqrt{p}(\log p)^2).$$

Proof. We note that $P + P = \{2, \dots, 2\lceil cp \rceil\} \subset \mathbb{F}_p \setminus \{0\}$.

Now we observe that

$$|P \cap (P+P)^{-1}| = \sum_{\substack{x \in P \\ y \in P+P \\ x = y^{-1}}} 1 = \frac{1}{p} \sum_{t \in \mathbb{F}_p} \sum_{\substack{x \in P \\ y \in P+P}} e_p(t(x - y^{-1})) = \frac{1}{p} \sum_{t \in \mathbb{F}_p} \sum_{x \in P} e_p(tx) \sum_{y \in P+P} e_p(-ty^{-1}).$$

Using Lemmas 2.5 and 2.7, we find that

$$\begin{aligned} |P \cap (P+P)^{-1}| &= \frac{|P||P+P|}{p} + \frac{1}{p} \sum_{t \in \mathbb{F}_p \setminus \{0\}} \hat{1}_P(t) \hat{1}_{(P+P)^{-1}}(-t) \\ &= 2c^2 p + O(\sqrt{p}(\log p)^2). \end{aligned}$$
□

Now we prove Theorem 1.3.

Let $c < \frac{1}{2}$ (to be determined later) and p be large enough. Let $P = \{1, \dots, \lceil cp \rceil\}$. Let $A = P \setminus (P+P)^{-1}$. It satisfies $A \cap (A+A)^{-1} = \varnothing$, i.e., $1 \neq A(A+A)$, and has cardinality at least $cp - 2c^2 p - O(\sqrt{p}(\log p)^2)$. To optimise, we take $c = \frac{1}{4}$, in which case $|A| \geq p/8 - O(\sqrt{p}(\log p)^2)$. For any $\epsilon > 0$, for p large enough, this is at least $\left(\frac{1}{8} - \epsilon\right)p$, whence the first part of the theorem.

For the second part, we note that Lemma 4.1 provides a bound for the cardinality $|P \cap x(P+P)^{-1}|$ for any x, so for any $k \leq p-1$ we can get a set a of size $cp - 2kc^2 p - O(k\sqrt{p}(\log p)^2)$ so that $A(A+A)$ misses 0 and k nonzero elements. The main term is optimised for $c = 1/(4k)$, where it is worth $p/(8k)$. Taking k of size $p^{1/4}(\log p)^{-3/2}$, the error term is significantly smaller than the main term (for large p), so we obtain a set A of size $\Omega(p^{3/4}(\log p)^{3/2})$ for which $A(A+A)$ misses at least $p^{1/4}(\log p)^{-3/2}$ elements. This is even a slightly stronger statement than claimed. □

5. Final remarks

5A. Let p be an odd prime, $a, b \in \mathbb{F}_p \setminus \{0\}$ and assume that $ba^{-1} = c^2$ is a square. Let $A \subset \mathbb{F}_p \setminus \{0\}$. Then $a \notin A(A+A)$ if and only if $b \notin cA(cA+cA) = c^2 A(A+A)$. Moreover $|cA| = |A|$.

We define

$$m_p = \max\{|A| : A \subseteq \mathbb{F}_p \setminus \{0\} \text{ and } A(A+A) \not\supseteq \mathbb{F}_p \setminus \{0\}\}.$$

From the above remark we have

$$m_p = \max\{|A| : A \subseteq \mathbb{F}_p \setminus \{0\} \text{ and } 1 \notin A(A+A) \text{ or } r \notin A(A+A)\},$$

where r is any fixed nonsquare residue modulo p. By Theorems 1.1 and 1.3 we have

$$3.277\ldots \leq \liminf_{p\to\infty} \frac{p}{m_p} \leq \limsup_{p\to\infty} \frac{p}{m_p} \leq 8.$$

5B. Let $p > 3$ be a prime number. The set I of residues modulo p in the interval $\{r \in \mathbb{F}_p : p/3 < r < 2p/3\}$ is sum-free (i.e., $a + b \neq c$ for any $a, b, c \in I$) and achieves the largest cardinality for those sets, namely $|I| = \lfloor (p+1)/3 \rfloor$, as it can be deduced from the Cauchy–Davenport theorem combined with the fact that $|I \cap (I+I)| = 0$.

Let

$$A = \{x \in I : x^{-1} \in I\}.$$

Then $A = A^{-1}$ and A is sum-free. It readily follows that $1 \notin A(A+A)$. Moreover, since I is an arithmetic progression, the events $x \in I$ and $x^{-1} \in I$ are independent, so we may observe that A has cardinality $\sim p/9$ as p tends to infinity (it can be formally proved using Fourier analysis). This raises the next question:

What is the largest size of a sum-free set $A \subset \mathbb{F}_p \setminus \{0\}$ such that $A = A^{-1}$?

From Theorem 1.1, we deduce the following statement.

Corollary 5.1. *Let $A \subset \mathbb{F}_p \setminus \{0\}$ be a sum-free set such that $A = A^{-1}$. Then $|A| < 0.3051p$ for any sufficiently large prime number p.*

This is related to the question of how large a sum-free multiplicative subgroup of $\mathbb{F}_p^*$ can be. Alon and Bourgain [2014] showed that it can be at least $\Omega(p^{1/3})$.

5C. Let $A \subset \mathbb{F}_p \setminus \{0\}$ with $\alpha = |A|/p \gg 1$, and let us set $A_s = A \cap (A+s)$. Let $0 < \epsilon < 1$ be defined by

$$E^+(A) = \sum_{s \in A-A} |A_s|^2 = (1-\epsilon)|A|^3,$$

and S be the subset of $A-A$ given by

$$S = \{s \in A-A : |A_s| > (1-\epsilon-p^{-1/3})|A|\}.$$

Then

$$E^+(A) \leq (1-\epsilon-p^{-1/3})|A| \sum_{s \notin S} |A_s| + |A|^2|S| = (1-\epsilon-p^{-1/3})|A|^3 + |A|^2|S|,$$

from which we deduce

$$|S| \geq |A| p^{-1/3}. \tag{9}$$

Assume that $A = A^{-1}$ and let N be the number of solutions to the equation

$$(a-s)(b-t) = 1, \quad (s,a,t,b) \in S \times A_s \times S \times A_t.$$

For fixed $s, t \in S$, we have

$$\begin{aligned} |(A-s) \cap (A_t-t)^{-1}| &= |A_s| + |A_t| - |(A-s) \cup (A_t-t)^{-1}| \\ &\geq 2(1-\epsilon-o(1))|A| - |A| = (1-2\epsilon-o(1))|A| \end{aligned}$$

since $A_s - s \subset A$ and $(A_t-t)^{-1} \subset A^{-1} = A$. This yields

$$N \geq (1-2\epsilon-o(1))|A|\,|S|^2. \tag{10}$$

On the other hand, defining $r(x) = |\{(a,s) \in A \times S : x(a-s) = 1\}|$, we have

$$N \leq \frac{1}{p} \sum_h \hat{1}_A(h)\hat{1}_S(-h)\hat{r}(-h) \leq \frac{|A|^2|S|^2}{p} + \max_{h \neq 0} |\hat{r}(h)| \times \frac{1}{p} \sum_h |\hat{1}_A(h)\hat{1}_S(h)|.$$

By adapting (8) we get $\max_{h \neq 0} |\hat{r}(h)| \leq \sqrt{p|A|\,|S|}$ and by Cauchy–Schwarz and Parseval we derive $N \leq |A|^2|S|^2/p + O(\sqrt{p}|A|\,|S|)$. Combined with (10), this gives

$$\alpha + O(\sqrt{p}|S|^{-1}) \geq 1 - 2\epsilon - o(1),$$

yielding by (9) that $\epsilon \geq (1-\alpha)/2 + o(1)$. Hence when $A = A^{-1}$,

$$E^+(A) \leq \frac{1+\alpha+o(1)}{2}|A|^3.$$

Together with Theorem 1.1, this implies the following result.

Proposition 5.2. *Let $A \subset \mathbb{F}_p^*$ be as in Corollary 5.1. Then for large enough p the additive energy satisfies*

$$E^+(A) \leq 0.6526|A|^3.$$

By considering similarly the multiplicative energy of A, it is possible to get the following sum-product upper bound for an arbitrary $A \subset \mathbb{F}_p$:

$$2E^+(A) + E^\times(A) \leq (2+\alpha+o(1))|A|^3.$$

References

[Aksoy Yazici et al. 2017] E. Aksoy Yazici, B. Murphy, M. Rudnev, and I. Shkredov, "Growth estimates in positive characteristic via collisions", *Int. Math. Res. Not.* **2017**:23 (2017), 7148–7189. MR Zbl

[Alon and Bourgain 2014] N. Alon and J. Bourgain, "Additive patterns in multiplicative subgroups", *Geom. Funct. Anal.* **24**:3 (2014), 721–739. MR Zbl

[Freiman 1962] G. A. Freiman, "Inverse problems of additive number theory, VII: The addition of finite sets, IV: The method of trigonometric sums", *Izv. Vysš. Učebn. Zaved. Matematika* **1962**:6 (1962), 131–144. MR

[Hegyvári and Hennecart 2018] N. Hegyvári and F. Hennecart, "A note on the size of the set $A^2 + A$", *Ramanujan J.* **46**:2 (2018), 357–372. MR Zbl

[Lev 2005] V. F. Lev, "Distribution of points on arcs", *Integers* **5**:2 (2005), art. id. A11. MR Zbl

[Moshchevitin 2007] N. G. Moshchevitin, "Sets of the form $\mathscr{A} + \mathscr{B}$ and finite continued fractions", *Mat. Sb.* **198**:4 (2007), 95–116. In Russian; translated in *Sb. Math* **198**:4 (2007), 537–557. MR Zbl

[Nathanson 1996] M. B. Nathanson, *Additive number theory*, Graduate Texts in Mathematics **165**, Springer, 1996. MR Zbl

[Roche-Newton et al. 2016] O. Roche-Newton, M. Rudnev, and I. D. Shkredov, "New sum-product type estimates over finite fields", *Adv. Math.* **293** (2016), 589–605. MR Zbl

[Sárközy 2005] A. Sárközy, "On sums and products of residues modulo p", *Acta Arith.* **118**:4 (2005), 403–409. MR Zbl

[Stevens and de Zeeuw 2017] S. Stevens and F. de Zeeuw, "An improved point-line incidence bound over arbitrary fields", *Bull. Lond. Math. Soc.* **49**:5 (2017), 842–858. MR Zbl

[Vinogradov 1955] I. M. Vinogradov, *An introduction to the theory of numbers*, Pergamon Press, London & New York, 1955. MR

[Weil 1948] A. Weil, "On some exponential sums", *Proc. Nat. Acad. Sci. U. S. A.* **34** (1948), 204–207. MR Zbl

Received 21 Nov 2018. Revised 14 Dec 2018.

PIERRE-YVES BIENVENU:

pbienvenu@math.univ-lyon1.fr
Université Lyon 1, CNRS, ICJ UMR 5208, Villeurbanne, France

FRANÇOIS HENNECART:

francois.hennecart@univ-st-etienne.fr
Université Jean-Monnet, CNRS, ICJ UMR 5208, Saint-Étienne, France

ILYA SHKREDOV:

ilya.shkredov@gmail.com
Steklov Mathematical Institute, Divison of Algebra and Number Theory, Moscow, Russia

and

IITP RAS, Moscow, Russia

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 2 2019