SUM-FREE SETS WHICH ARE CLOSED UNDER MULTIPLICATIVE INVERSES

KATHERINE BENJAMIN

ABSTRACT. Let A be a subset of a finite field $\mathbb{F}$. When $\mathbb{F}$ has prime order, we show that there is an absolute constant $c > 0$ such that, if A is both sum-free and equal to the set of its multiplicative inverses, then $|A| < (0.25 - c)|\mathbb{F}| + o(|\mathbb{F}|)$ as $|\mathbb{F}| \to \infty$. We contrast this with the result that such sets exist with size at least $0.25|\mathbb{F}| - o(|\mathbb{F}|)$ when $\mathbb{F}$ has characteristic 2.

1. INTRODUCTION

Let A be a subset of a finite field $\mathbb{F}$. We say A is *sum-free* if $A \cap (A + A) = \varnothing$, where

$$A + A := \{a + b : a, b \in A\}.$$

We say A is *closed under (multiplicative) inverses* if $0 \notin A$ and $A = A^{-1}$, where

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

In this paper, we study sets which are both sum-free and closed under inverses.

When $\mathbb{F}$ has prime order, a simple application of the Cauchy-Davenport inequality (see e.g. [7, Theorem 5.4]) shows that $|A| \leq (|\mathbb{F}| + 1)/3$ when A is sum-free. Lev showed in [6] that when $|A|$ is close to $|\mathbb{F}|/3$, A is similar in structure to an arithmetic progression, and therefore unlikely to be closed under inverses. So, we might expect $|A|$ to be smaller than $|\mathbb{F}|/3$ if A is also closed under inverses.

In this direction, Bienvenu et al. showed in [1, Corollary 5.1] that $|A| < 0.3051|\mathbb{F}| + o(|\mathbb{F}|)$ as $|\mathbb{F}| \to \infty$. We offer the following improvement on this:

Theorem 1.1. *There is an absolute constant $c > 0$ so that if $\mathbb{F}$ is a field of prime order and $A \subseteq \mathbb{F}^*$ is sum-free and closed under inverses then $|A| < (0.25 - c)|\mathbb{F}| + o(|\mathbb{F}|)$ as $|\mathbb{F}| \to \infty$.*

A careful inspection of the argument yields $c = 2.5 \times 10^{-8}$. This is in contrast to fields of characteristic 2, where we show:

Proposition 1.2. *If $\mathbb{F}$ is a field of characteristic 2 then there exists $A \subseteq \mathbb{F}^*$ which is both sum-free and closed under inverses, such that $|A| = 0.25|\mathbb{F}| + o(|\mathbb{F}|)$ as $|\mathbb{F}| \to \infty$.*

Write $\mu(\mathbb{F})$ for the density $|A|/|\mathbb{F}|$ of the largest $A \subseteq \mathbb{F}$ that is both sum-free and closed under inverses. Theorem 1.1 says that $\mu(\mathbb{F}_p) \leq 0.25 - c + o(1)$, whereas Proposition 1.2 says that $\mu(\mathbb{F}_{2^n}) \geq 0.25 - o(1)$. So we can deduce that:

Date: September 1, 2022.
2020 *Mathematics Subject Classification.* 11B75.
Key words and phrases. Sum-product estimates; sum-free sets; finite fields.

Corollary 1.3. *The limit* $\lim_{|\mathbb{F}|\to\infty} \mu(\mathbb{F})$ *does not exist.*

The rest of the paper is structured as follows. In Section 2 we recall some basic definitions of Fourier analysis, and establish some notation. In Section 3 we consider fields of prime order. We establish some Fourier analytic results and use them to prove Theorem 1.1. Then, in Section 4 we consider fields of even characteristic, and prove Proposition 1.2. In Section 5 we make some final remarks.

2. Notation and definitions from Fourier analysis

Let $\mathbb{F}$ be a finite field. We recall some basic definitions from Fourier analysis (see e.g. [7, Section 4] or [9, Section 1.1]).

If $X \subseteq \mathbb{F}$ is non-empty and $f\colon X \to \mathbb{C}$ is any function, we define the *mean*

$$\mathop{\mathbb{E}}_{x\in X}[f(x)] := \frac{1}{|X|}\sum_{x\in X} f(x).$$

We will also write

$$\mathbb{E}[f] = \mathop{\mathbb{E}}_{x}[f(x)] = \mathop{\mathbb{E}}_{x\in\mathbb{F}}[f(x)]$$

when it is unambiguous to do so. We denote by 1_X the indicator function

$$1_X(x) := \begin{cases} 1 & \text{if } x \in X, \\ 0 & \text{otherwise.} \end{cases}$$

We can view the set of functions $\mathbb{F} \to \mathbb{C}$ as a Hilbert space by equipping it with the inner product

$$\langle f, g\rangle := \mathbb{E}[f\overline{g}].$$

Write $e(\theta) = \exp(i\theta)$ for the exponential map $\mathbb{R} \to \mathbb{C}$. If $\mathbb{F}$ has prime order p then for each $r \in \mathbb{F}$ we can define the *character* $e_r\colon \mathbb{F} \to \mathbb{C}$ by $e_r(x) := e(2\pi rx/p)$.[1] The characters enjoy the following orthogonality property:

$$\langle e_r, e_s\rangle = \begin{cases} 1 & \text{if } r = s \\ 0 & \text{otherwise.} \end{cases}$$

This motivates the definition of the *Fourier coefficient of f at r* as

$$\widehat{f}(r) := \langle f, e_r\rangle.$$

Parseval's identity is then

$$\mathbb{E}[|f|^2] = \sum_{r\in\mathbb{F}} \left|\widehat{f}(r)\right|^2.$$

[1]We follow the notation of [7]. It is also common to write $e_p(x) = e(2\pi x/p)$.

3. Fields of prime order

The goal of this section is to prove Theorem 1.1. Let $\mathbb{F} = \mathbb{F}_p$ be a field of prime order $p > 2$. Let A be a subset of $\mathbb{F}^*$, not necessarily sum-free or closed under inverses, with density $\alpha = |A|/p$. We fix some $0 < \alpha_0 < 0.25$ and assume $\alpha \geq \alpha_0$, since otherwise Theorem 1.1 is immediate.

Order the elements $r_1, \ldots, r_{(p-1)/2}$ of the interval $\{1, \ldots, (p-1)/2\} \subseteq \mathbb{F}$ so that $\delta_1 \geq \cdots \geq \delta_{(p-1)/2}$, where $\left|\widehat{1_A}(r_i)\right| = \delta_i \alpha$. Note that

$$\mathbb{F}^* = \{r_1, \ldots, r_{(p-1)/2}\} \cup \{-r_1, \ldots, -r_{(p-1)/2}\}$$

and that $\widehat{1_A}(-r_i) = \overline{\widehat{1_A}(r_i)}$ for each i. We will also write $\theta_1 \in [0, 2\pi)$ for the argument of $\widehat{1_A}(r_1)$, so that $\widehat{1_A}(r_1) = (\delta_1\alpha)e(\theta_1)$ and $\widehat{1_A}(r_1) + \widehat{1_A}(-r_1) = 2\delta_1\alpha\cos\theta_1$.

3.1. **Properties of sum-free sets.** We begin by recalling a standard identity, which can be derived by considering the convolution $1_A * 1_A$ (see e.g. [7, p. 153]).

Proposition 3.1. *If A is sum-free then*

$$\alpha^3 + \sum_{r \neq 0} \left|\widehat{1_A}(r)\right|^2 \widehat{1_A}(r) = 0.$$

In fact, this sum is dominated by its largest terms.

Lemma 3.2. *Let k be a positive integer. For any p such that $k < (p-1)/2$, if $A \subseteq \mathbb{F}_p$ then*

$$\sum_{i > k} \delta_i^3 \to 0$$

as $k \to \infty$, uniformly in A provided $\alpha \geq \alpha_0$.

Proof. From Parseval's identity we know

$$\alpha^2 + 2\alpha^2 \sum_{i \geq 1} \delta_i^2 = \alpha,$$

whence, looking at the first k terms of the sum,

$$\delta_k^2 \leq \frac{1-\alpha}{2k\alpha}.$$

So

$$\sum_{i>k} \delta_i^3 \leq \delta_k \sum_{i>k} \delta_i^2 \leq k^{-1/2} \left(\frac{1-\alpha}{2\alpha}\right)^{3/2} \leq k^{-1/2} \left(\frac{1-\alpha_0}{2\alpha_0}\right)^{3/2} \to 0.$$

□

Corollary 3.3. *If A is sum-free then*

$$\sum_{i=1}^{k} \delta_i^3 \geq \delta_1^3 |\cos\theta_1| + \sum_{i=2}^{k} \delta_i^3 \geq \frac{1}{2} - o_{k\to\infty}(1),$$

where the error is uniform in A provided $\alpha \geq \alpha_0$.

Proof. The first inequality is immediate. For the second, we begin with Proposition 3.1 and make two applications of the triangle inequality.

$$\begin{aligned}
\alpha^3 &= \Big|\sum_{r\neq 0}\big|\widehat{1_A}(r)\big|^2\widehat{1_A}(r)\Big| \\
&= \Big|\sum_{i=1}^{(p-1)/2}\delta_i^2\alpha^2\left(\widehat{1_A}(r_i)+\widehat{1_A}(-r_i)\right)\Big| \\
&\leq \sum_{i=1}^{(p-1)/2}\delta_i^2\alpha^2\left|\widehat{1_A}(r_i)+\widehat{1_A}(-r_i)\right| \\
&\leq \delta_1^2\alpha^2|2\delta_1\alpha\cos\theta_1| + \sum_{i=2}^{(p-1)/2}\delta_i^2\alpha^2\left(\left|\widehat{1_A}(r_i)\right|+\left|\widehat{1_A}(-r_i)\right|\right) \\
&= 2\delta_1^3\alpha^3|\cos\theta_1| + \sum_{i=2}^{(p-1)/2}2\delta_i^3\alpha^3
\end{aligned}$$

Now divide through by $2\alpha^3$ and apply Lemma 3.2. □

Another corollary of Proposition 3.1 gives bounds on α in terms of the sizes of the largest two Fourier coefficients. The first, which considers only δ_1, is standard (*c.f.* [6, p. 226]). The second is stronger when δ_2 is small compared to δ_1.

Corollary 3.4. *If A is sum-free then*

$$\alpha \leq \frac{\delta_1}{1+\delta_1}.$$

Moreover, if $1+\delta_2+2\delta_1^2\delta_2-2\delta_1^3>0$ *then*

$$\alpha \leq \frac{\delta_2}{1+\delta_2+2\delta_1^2\delta_2-2\delta_1^3}.$$

Proof. We prove the second bound. The first is proved similarly. We begin with Proposition 3.1:

$$\begin{aligned}
\alpha^3 &= \Big|\sum_{r\neq 0}\big|\widehat{1_A}(r)\big|^2\widehat{1_A}(r)\Big| \\
&\leq 2\delta_1^3\alpha^3 + \Big|\sum_{r\neq 0,\pm r_1}\big|\widehat{1_A}(r)\big|^2\widehat{1_A}(r)\Big| \\
&\leq 2\delta_1^3\alpha^3 + \delta_2\alpha\sum_{r\neq 0,\pm r_1}\big|\widehat{1_A}(r)\big|^2 \\
&= 2\delta_1^3\alpha^3 + \delta_2\alpha\left(\alpha-\alpha^2-2\delta_1^2\alpha^2\right).
\end{aligned}$$

To get the final step here we use Parseval's identity. Now rearrange to find

$$\alpha\left(1+\delta_2+2\delta_1^2\delta_2-2\delta_1^3\right) \leq \delta_2$$

and apply the hypothesis. □

3.2. **Properties of sets which are closed under inverses.** To exploit the fact that $A = A^{-1}$ we will make use of the following result from [2, Proposition 1], which can be thought of as a version of Bessel's inequality for vectors which are 'almost orthogonal'.

Lemma 3.5. *Let H be a Hilbert space with inner product $\langle\, , \rangle$. Then for any $f, g_1, \ldots, g_M \in H$ we have the inequality*

$$\|f\|^2 \geq \sum_{i=1}^{M} \frac{|\langle f, g_i\rangle|^2}{\sum_{j=1}^{M} |\langle g_i, g_j\rangle|}.$$

We also recall Weil's estimate for Kloosterman sums [8, p. 207].

Lemma 3.6 (Weil's estimate)**.** *If p is prime and a, b are integers with $ab \neq 0$ then*

$$\Big|\sum_{x\in\mathbb{F}_p^*} e_a(x)e_b(x^{-1})\Big| \leq 2\sqrt{p}.$$

We arrive at a useful bound on the size of a set which is closed under inverses.

Proposition 3.7. *Suppose $A = A^{-1}$ and let $m \geq 0$. Suppose $s_1, \ldots, s_m$ are pairwise distinct elements of $\mathbb{F}_p^*$ with $\big|\widehat{1_A}(s_i)\big| = \lambda_i\alpha$. Then*

$$\alpha \leq \frac{1}{1 + 2\sum_{i=1}^{m} \lambda_i^2} + O\left(m/\sqrt{p}\right).$$

Moreover, if $k \geq 0$ then we have the bound

$$\alpha \leq \frac{1}{1 + 4\sum_{i=1}^{k} \delta_i^2} + O\left(k/\sqrt{p}\right).$$

Proof. Define $s_0 := 0$, and so $\lambda_0 = 1$. For each i define $\varphi_i := e_{s_i}$ and, if $i > 0$, $\psi_i(x) := \varphi_i(x^{-1})$, with the convention that $0^{-1} = 0$. We aim to apply Lemma 3.5 to 1_A and these 'almost orthogonal' functions. For $i \geq 0$ and $j > 0$ we have

$$|\langle\varphi_i, \psi_j\rangle| = \frac{1}{p}\Big|\sum_{x\in\mathbb{F}_p} e_{s_i}(x)\overline{e_{s_j}(x^{-1})}\Big| = \frac{1}{p}\Big|\sum_{x\in\mathbb{F}_p} e_{s_i}(x)e_{-s_j}(x^{-1})\Big| \leq \frac{1+2\sqrt{p}}{p}$$

by Weil's bound. Also, using the fact that the characters are orthonormal, we have

$$\langle\psi_i, \psi_j\rangle = \mathop{\mathbb{E}}_{x}\left[\varphi_i(x^{-1})\overline{\varphi_j(x^{-1})}\right] = \mathop{\mathbb{E}}_{x}\left[\varphi_i(x)\overline{\varphi_j(x)}\right] = \langle\varphi_i, \varphi_j\rangle = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Finally,

$$|\langle 1_A, \psi_i\rangle| = \frac{1}{p}\Big|\sum_{a\in A} \overline{\varphi_i(a^{-1})}\Big| = \frac{1}{p}\Big|\sum_{a\in A} \overline{\varphi_i(a)}\Big| = |\langle 1_A, \varphi_i\rangle| = \big|\widehat{1_A}(s_i)\big| = \lambda_i\alpha.$$

So, applying Lemma 3.5, we find

$$\begin{aligned}\alpha &\geq \sum_{i=0}^{m} \frac{\lambda_i^2 \alpha^2}{1 + m\left(1+2\sqrt{p}\right)/p} + \sum_{i=1}^{m} \frac{\lambda_i^2 \alpha^2}{1 + (m+1)\left(1+2\sqrt{p}\right)/p} \\ &\geq \alpha^2 \frac{1 + 2\sum_{i=1}^{m} \lambda_i^2}{1 + (m+1)\left(1+2\sqrt{p}\right)/p},\end{aligned}$$

from which the result follows.

For the moreover part, take $m = 2k$ and $s_i = r_i = -s_{m+1-i}$ for each $1 \leq i \leq k$. □

3.3. **Constructing large coefficients.** If $\left|\widehat{1_A}(r)\right| = \delta\alpha$ then an observation of Yudin recorded in [5, p. 258] yields the following bound on $\left|\widehat{1_A}(2r)\right|$:

$$\left|\widehat{1_A}(2r)\right| \geq \left(2\delta^2 - 1\right)\alpha. \tag{1}$$

We strengthen this in two ways. First we show that, given conditions on δ and the argument θ of $\widehat{1_A}(r)$, the coefficient $\widehat{1_A}(2r)$ lies in the right-half plane of $\mathbb{C}$. Second, we show that given some lower bound on α, we can obtain a slightly stronger lower bound on $\left|\widehat{1_A}(2r)\right|$. We shall prove (1) along the way.

Lemma 3.8. *Suppose $r \neq 0$ and $\widehat{1_A}(r) = (\delta\alpha)e(\theta)$. Then*

$$2\,\mathrm{Re}\,\widehat{1_A}(2r) = \widehat{1_A}(2r) + \widehat{1_A}(-2r) \geq 2\alpha\left(2\delta^2\cos^2\theta - 1\right).$$

Moreover, if $\alpha \geq \alpha_0 > 0$ then

$$\left|\widehat{1_A}(2r)\right| \geq \left(2\delta^2 - 1 + \varepsilon - o(1)\right)\alpha$$

as $p \to \infty$, where the error is uniform in A and $\varepsilon > 0$, which depends only on α_0, is given by

$$\varepsilon = \frac{2^9}{3^4 \times 5^5}{\alpha_0}^4.$$

Proof. For any $\omega \in S^1$, it can be seen that

$$\mathop{\mathbb{E}}_x\left[1_A(x)\left(\overline{\omega}e_r(x) + \omega e_{-r}(x)\right)^2\right] = 2\alpha + \omega^2\widehat{1_A}(2r) + \overline{\omega}^2\widehat{1_A}(-2r). \tag{2}$$

By applying Cauchy-Schwarz we can compute

$$\begin{aligned}\mathop{\mathbb{E}}_x\left[1_A(x)\right]\mathop{\mathbb{E}}_x\left[1_A(x)\left(\overline{\omega}e_r(x) + \omega e_{-r}(x)\right)^2\right] &\geq \mathop{\mathbb{E}}_x\left[1_A(x)\left(\overline{\omega}e_r(x) + \omega e_{-r}(x)\right)\right]^2 \\ &= \left(\omega\widehat{1_A}(r) + \overline{\omega}\widehat{1_A}(-r)\right)^2.\end{aligned}$$

Setting $\omega = 1$ and substituting in (2) then gives

$$\alpha\left(2\alpha + \widehat{1_A}(2r) + \widehat{1_A}(-2r)\right) \geq \left(\widehat{1_A}(r) + \widehat{1_A}(-r)\right)^2 = 4\delta^2\alpha^2\cos^2\theta,$$

from which the first inequality follows.

If instead we take $\omega = e(-\theta)$ then we find

$$\alpha \left(2\alpha + \omega^2\widehat{1_A}(2r) + \overline{\omega}^2\widehat{1_A}(-2r)\right) \geq \left(\left|\widehat{1_A}(r)\right| + \left|\widehat{1_A}(r)\right|\right)^2 = (2\delta\alpha)^2$$

which rearranges with the triangle inequality to give (1).

The Cauchy-Schwarz inequality $\mathbb{E}[XY]^2 \leq \mathbb{E}[X^2]\mathbb{E}[Y^2]$ is only close to equality when the random variables X and Y are close to proportional. However, $1_A(x)$ and

$$1_A(x) \cdot (\overline{\omega}e_r(x) + \omega e_{-r}(x)) = 1_A(x) \cdot 2\cos(2\pi rx/p + \theta)$$

are not approximately proportional, since A is not thin.

Concretely, set $\omega = e(-\theta)$ again. Using the fact that $\mathbb{E}[X^2] = \mathbb{E}[(X - \mathbb{E}[X])^2] + \mathbb{E}[X]^2$ for a random variable X, we can compute

$$\begin{aligned}
\mathop{\mathbb{E}}_{x\in\mathbb{F}_p}\left[1_A(x)(\overline{\omega}e_r(x) + \omega e_{-r}(x))^2\right] &= \alpha \mathop{\mathbb{E}}_{x\in A}\left[(\overline{\omega}e_r(x) + \omega e_{-r}(x))^2\right] \\
&= \alpha \mathop{\mathbb{E}}_{x\in A}\left[(\overline{\omega}e_r(x) + \omega e_{-r}(x) - 2\delta)^2\right] + 4\delta^2\alpha \\
&= \alpha \mathop{\mathbb{E}}_{x\in A}\left[(2\cos(2\pi rx/p + \theta) - 2\cos\varphi)^2\right] + 4\delta^2\alpha \\
&= 16\alpha \mathop{\mathbb{E}}_{x\in A}\left[\sin^2(t_1(x))\sin^2(t_2(x))\right] + 4\delta^2\alpha,
\end{aligned}$$

where $\varphi := \arccos(\delta) \in [0, \pi/2]$, $t_1(x) := \pi rx/p + \theta/2 + \varphi/2$ and $t_2(x) := \pi rx/p + \theta/2 - \varphi/2$.

We should be explicit about the fact that we are dealing with lifts $\tilde{y} \in \mathbb{Z}$ of the elements $y = rx \in \mathbb{F}_p$. We can make any choice of lift we like, so let us fix the lift so that $|\pi rx/p + \theta/2| \leq \pi/2$. It follows that

$$|t_i(x)| \leq \pi/2 + \varphi/2 \leq 3\pi/4$$

for $i = 1, 2$. Writing

$$m = \frac{2\sqrt{2}}{3\pi},$$

we therefore have that[2]

$$|\sin(t_i(x))| \geq m\,|t_i(x)|\,. \tag{3}$$

[2]This bound can be derived by considering the concavity of $\sin t$ in the region $0 \leq t \leq 3\pi/4$.

Now observe that, for any γ, $|t_1(x)| \leq \gamma$ for at most $1 + \frac{2\gamma}{\pi}p$ values of x. Similarly for t_2. We therefore have that $t_1(x)^2 t_2(x)^2 \leq \gamma^4$ for at most $2 + \frac{4\gamma}{\pi}p$ values of x. Thus

$$\begin{aligned}\mathop{\mathbb{E}}_{x\in A}\left[\sin^2(t_1(x))\sin^2(t_2(x))\right] &\geq m^4 \mathop{\mathbb{E}}_{x\in A}\left[t_1(x)^2 t_2(x)^2\right] \\ &\geq m^4\left(1 - \frac{4\gamma}{\alpha_0\pi} - \frac{2}{\alpha_0 p}\right)\gamma^4 \\ &= m^4\left(1 - \frac{4\gamma}{\alpha_0\pi}\right)\gamma^4 - o(1).\end{aligned}$$

Taking $\gamma = \frac{\pi}{5} \times \alpha_0$ makes $\left(1 - \frac{4\gamma}{\alpha_0\pi}\right)\gamma^4 = {\alpha_0}^4 \times \frac{\pi^4}{5^5}$.

Starting from (2) we can now compute

$$\begin{aligned}\omega^2\widehat{1_A}(2r) + \overline{\omega}^2\widehat{1_A}(-2r) &= \mathop{\mathbb{E}}_{x\in\mathbb{F}_p}\left[1_A(x)\left(\overline{\omega}e_r(x) + \omega e_{-r}(x)\right)^2\right] - 2\alpha \\ &\geq 16\alpha \mathop{\mathbb{E}}_{x\in A}\left[\sin^2\left(t_1(x)\right)\sin^2\left(t_2(x)\right)\right] + 4\delta^2\alpha - 2\alpha \\ &\geq 2\left(2\delta^2 - 1 + 8m^4\pi^4{\alpha_0}^4/5^5 - o(1)\right)\alpha,\end{aligned}$$

from which the triangle inequality gives the result with

$$\varepsilon = \frac{8m^4\pi^4}{5^5}{\alpha_0}^4 = \frac{2^9}{3^4 \times 5^5}{\alpha_0}^4.$$

□

Remarks. *If a lower bound on δ is assumed then ε can be made slightly larger, by strengthening the bound in* (3).

We also have as a corollary that

$$\left|\widehat{1_A}(r)\right| \leq \left(1 - \Omega\left({\alpha_0}^4\right) + o_{p\to\infty}(1)\right)\alpha$$

for any $r \neq 0$. A consequence of [5, Theorem 5], *is the stronger result that*

$$\left|\widehat{1_A}(r)\right| \leq \left(1 - \Omega\left({\alpha_0}^2\right) + o_{p\to\infty}(1)\right)\alpha$$

for any $r \neq 0$. This suggests that the factor of ${\alpha_0}^4$ in ε could be replaced with a factor of ${\alpha_0}^2$ with some more work.

3.4. **Proof of Theorem 1.1.** The proof of Theorem 1.1 is a case analysis on the values of $\widehat{1_A}(r_i)$. If δ_1 and δ_2 are both small, then Corollary 3.4 is strong enough. Otherwise, we use Proposition 3.7. The question then becomes: given that δ_1 is large, how small can $\sum_{i=1}^{k}\delta_i^2$ be under the constraints, such as Corollary 3.3, implied by the sum-free condition?

We will make use of the following fact for $x_1, \ldots, x_n \in [0,1]$, which is an instance of nesting of ℓ_p-norms:

$$\Big(\sum_{i=1}^{n} x_i^2\Big) \geq \Big(\sum_{i=1}^{n} x_i^3\Big)^{2/3}. \tag{4}$$

Proof of Theorem 1.1. We can assume that $\alpha \geq 0.24$, since otherwise we are done. We shall reason based on the value of δ_1. First, we make an observation common to several of the cases. If we can show that there is an $h > 0$ so that

$$\sum_{i=1}^{k} \delta_i^2 \geq 0.75 + h - o_{k\to\infty}(1),$$

where the error is uniform in A, then applying Proposition 3.7 will yield

$$\begin{aligned} \alpha &\leq \frac{1}{1 + 4 \times (0.75 + h - o_{k\to\infty}(1))} + O(k/\sqrt{p}) \\ &< 0.25 - c_h + o_{k\to\infty}(1) + O(k/\sqrt{p}) \end{aligned} \tag{†}$$

for some $c_h > 0$ depending only on h. Now, begin by choosing k large enough that the $o_{k\to\infty}(1)$ in (†) is less than $c_h/3$. Then, choose p large enough that the $O(k/\sqrt{p})$ in (†) is also less than $c_h/3$. Then $\alpha < 0.25 - c_h/3$ as required.

Case 1: $\delta_1 \leq 0.33$. Recall the first bound from Corollary 3.4:

$$\alpha \leq \frac{\delta_1}{1 + \delta_1}.$$

Note that as long as $\delta_1 < 1/3$, this is enough to bound $\alpha < 0.25$. In particular, here we have

$$\alpha \leq \frac{\delta_1}{1 + \delta_1} \leq \frac{0.33}{1.33} < 0.2482.$$

Case 2: $0.33 \leq \delta_1 \leq 0.45$. Now the first conclusion of Corollary 3.4 is not enough, but we can argue based on the value of δ_2. If δ_2 is small, then the second conclusion of Corollary 3.4 will suffice. Otherwise, we can force $\sum_{i=1}^{k} \delta_i^2$ to be large and apply (†). So, write $\delta_2 = a\delta_1$ where $a \in (0,1]$.

Case 2.1: $a \leq 0.7$. Apply the second conclusion of Corollary 3.4, noting that the hypothesis on δ_1 and δ_2 is met, to get

$$\alpha \leq \frac{a\delta_1}{1 + a\delta_1 + 2a\delta_1^3 - 2\delta_1^3} \leq \max_{x,y} \frac{xy}{1 + xy + 2x^3y - 2x^3},$$

where the maximum is taken over the range $0.33 \leq x \leq 0.45$, $0 \leq y \leq 0.7$.

This expression is increasing in y since $x^3 \leq 1/2$, so

$$\alpha \leq \max_x \frac{0.7x}{1 + 0.7x - 0.6x^3} \leq \max_x \frac{0.7x}{1 + 0.7x - 0.6 \times 0.45^3}.$$

The expression on the right hand side increases with x, so plugging in $x = 0.45$ gives $\alpha < 0.24994$.

Case 2.2: $a \geq 0.7$. Applying Corollary 3.3 gives

$$\sum_{i=3}^{k} \delta_i^3 \geq \frac{1}{2} - \delta_1^3 - \delta_2^3 - o_{k\to\infty}(1) = \frac{1}{2} - \left(1 + a^3\right) \delta_1^3 - o_{k\to\infty}(1)$$

whence, by (4),

$$\begin{aligned} \sum_{i=1}^{k} \delta_i^2 &\geq \left(1 + a^2\right) \delta_1^2 + \left(\frac{1}{2} - \left(1 + a^3\right) \delta_1^3\right)^{2/3} - o_{k\to\infty}(1) \\ &\geq \min_{x,y} \left(\left(1 + y^2\right) x^2 + \left(\frac{1}{2} - (1 + y^3)x^3\right)^{2/3} \right) - o_{k\to\infty}(1), \qquad (5) \end{aligned}$$

where the minimum is over the range $0.33 \leq x \leq 0.45$, $0.7 \leq y \leq 1$. One can check that the expression being minimised in (5) is increasing with y. Hence

$$\sum_{i=1}^{k} \delta_i^2 \geq \min_{x} \left(1.49x^2 + \left(0.5 - 1.343x^3\right)^{2/3} \right) - o_{k\to\infty}(1). \qquad (6)$$

This new expression increases with x (see Figure 1). So, we can compute

$$\sum_{i=1}^{k} \delta_i^2 \geq 1.49 \times 0.33^2 + \left(\frac{1}{2} - 1.343 \times 0.33^3\right)^{2/3} > 0.7510 - o_{k\to\infty}(1).$$

Case 3: $0.45 \leq \delta_1 \leq 0.7455$. Here δ_1 is quite large. Moreover, we have $\delta_1^3 < 1/2$, which will force δ_2 to also be quite large and allow us to use (†). In detail, Corollary 3.3 gives

$$\sum_{i=2}^{k} \delta_i^3 \geq \frac{1}{2} - \delta_1^3 - o_{k\to\infty}(1).$$

If k is large enough then the right hand side is positive. So from (4) we have

$$\begin{aligned} \sum_{i=1}^{k} \delta_i^2 &\geq \delta_1^2 + \left(\frac{1}{2} - \delta_1^3\right)^{2/3} - o_{k\to\infty}(1) \\ &\geq \min_{x} \left(x^2 + \left(\frac{1}{2} - x^3\right)^{2/3} \right) - o_{k\to\infty}(1), \qquad (7) \end{aligned}$$

where the minimum is taken over the range $0.45 \leq x \leq 0.7455$. This expression is smallest when $x = 0.7455$ (see Figure 1). So we have

$$\sum_{i=1}^{k} \delta_i^3 \geq 0.7455^2 + \left(\frac{1}{2} - 0.7455^3\right)^{2/3} - o_{k\to\infty}(1) > 0.7501 - o_{k\to\infty}(1).$$

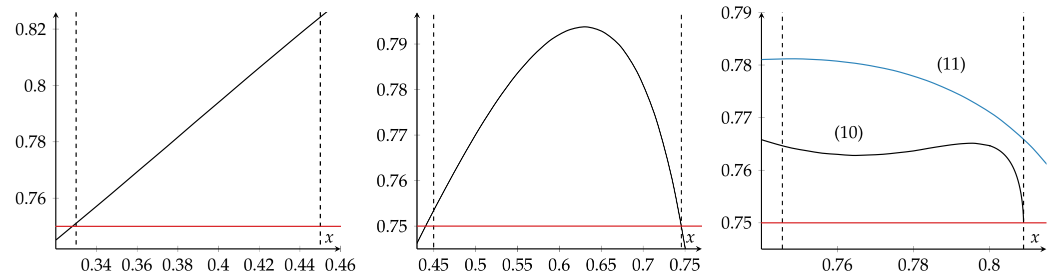

FIGURE 1. The function of x which is minimised to produce a lower bound on $\sum_{i=1}^{k}\delta_i^3$ in different cases, along with the region on which x is minimised in each case (dashed lines) and the constant 0.75 (red). *Left:* Case 2.2 given by (6). *Centre:* Case 3 given by (7). *Right:* Cases 4.1 given by (10) (black) and 4.2 given by (11) (blue).

Case 4: $0.7455 \leq \delta_1 \leq 0.809016$. If θ_1 is close to 0 or π then Lemma 3.8 will give us a large coefficient in the right half-plane. Otherwise, the contribution of r_1 to the sum in Corollary 3.3 is negligible. In either case, we end up being able to use (†).[3]

Assume $p > 3$ and let t be such that $2r_1 = \pm r_t$. Note that $t \neq 1$, as otherwise either $2r_1 = r_1$ or $3r_1 = 0$, which both imply $r_1 = 0$ since $p > 3$. If we write $\Delta(\delta,\theta) = 2\delta^2\cos^2\theta - 1$ for any δ,θ, then Lemma 3.8 says that

$$\operatorname{Re}\widehat{1_A}(r_t) \geq \Delta(\delta_1,\theta_1)\alpha.$$

We also know from (1) that $\delta_t \geq 2\delta_1^2 - 1$.

Case 4.1: $\Delta(\delta_1,\theta_1) > 0$. In this case, $\operatorname{Re}\widehat{1_A}(r_t) > 0$. From Proposition 3.1 and the triangle inequality we have

$$\delta_1^3|\cos\theta_1| + \sum_{i\neq 1,t}\delta_i^3 \geq \frac{1}{2} + \frac{\delta_t^2}{\alpha}\operatorname{Re}\widehat{1_A}(r_t) \geq \frac{1}{2} + \left(2\delta_1^2 - 1\right)^2\Delta(\delta_1,\theta_1).$$

By replacing θ_1 with $\pi - \theta_1$ if necessary, we can assume $\theta_1 \in [\pi/2, 3\pi/2]$. Then

$$\begin{aligned}\sum_{i\neq 1,t}\delta_i^3 &\geq \frac{1}{2} + \left(2\delta_1^2 - 1\right)^2\Delta(\delta_1,\theta_1) + \delta_1^3\cos\theta_1 \\ &\geq \min_t\left(\frac{1}{2} + \left(2\delta_1^2 - 1\right)^2\Delta(\delta_1,t) + \delta_1^3\cos t\right), \qquad (8)\end{aligned}$$

[3] The choice of boundary may seem odd here. The argument in this case gives $\alpha \leq 0.25 + o(1)$ exactly for $\delta_1 = \sqrt{(3+\sqrt{5})/8} \approx 0.809017$, so to get below that bound with this argument we consider a region slightly to the left of this critical point.

where the minimum is taken over the range $\pi/2 \leq t \leq 3\pi/2$. It can be checked that this minimum is attained when $t = \pi$. So

$$\sum_{i \neq 1,t} \delta_i^3 \geq \frac{1}{2} + \left(2\delta_1^2 - 1\right)^3 - \delta_1^3.$$

Then by Lemma 3.2, since we've fixed $\alpha \geq 0.24$, this becomes

$$\sum_{2 \leq i \leq k, i \neq t} \delta_i^3 \geq \frac{1}{2} + \left(2\delta_1^2 - 1\right)^3 - \delta_1^3 - o_{k\to\infty}(1). \tag{9}$$

We can lower bound $\frac{1}{2} + \left(2\delta_1^2 - 1\right)^3 - \delta_1^3 > 0.000001$ here. Therefore, by taking k large enough we can ensure that the right hand side of (9) is positive. It follows from (4) that

$$\begin{aligned}\sum_{i=1}^{k} \delta_i^2 &\geq \delta_1^2 + \left(2\delta_1^2 - 1\right)^2 + \left(\frac{1}{2} + \left(2\delta_1^2 - 1\right)^3 - \delta_1^3\right)^{2/3} - o_{k\to\infty}(1) \\ &\geq \min_x \left(x^2 + \left(2x^2 - 1\right)^2 + \left(\frac{1}{2} + \left(2x^2 - 1\right)^3 - x^3\right)^{2/3}\right) - o_{k\to\infty}(1), \qquad (10)\end{aligned}$$

where the minimum is taken in the range $0.7455 \leq x \leq 0.809016$. Now, it can be verified[4] that this attains its minimum when $x = 0.809016$ (see Figure 1), so we can calculate

$$\sum_{i=1}^{k} \delta_i^2 > 0.75001 - o_{k\to\infty}(1).$$

Case 4.2: $\Delta(\delta_1, \theta_1) \leq 0$. We shall apply Corollary 3.3, which says

$$\sum_{i=2}^{k} \delta_i^3 \geq \frac{1}{2} - \delta_1^3 |\cos\theta_1| - o_{k\to\infty}(1).$$

From the assumption that $\Delta(\delta_1, \theta_1) \leq 0$ we know that $\delta_1 |\cos\theta_1| \leq \sqrt{2}/2$. So

$$\sum_{i=2}^{k} \delta_i^3 \geq \frac{1}{2} - \frac{\sqrt{2}}{2}\delta_1^2 - o_{k\to\infty}(1).$$

Now, $1 - \delta_1^2\sqrt{2} \geq 1 - 0.809016^2 \times \sqrt{2} > 0$ here. So after taking k large enough the right hand side above is positive. Then applying (4) gives

$$\begin{aligned}\sum_{i=1}^{k} \delta_i^2 &\geq \delta_1^2 + \left(\frac{1}{2} - \frac{\sqrt{2}}{2}\delta_1^2\right)^{2/3} - o_{k\to\infty}(1) \\ &\geq \min_x \left(x^2 + \left(\frac{1}{2} - \frac{\sqrt{2}}{2}x^2\right)^{2/3}\right) - o_{k\to\infty}(1), \qquad (11)\end{aligned}$$

[4]Intuitively, this sum will be smallest when all of the mass is concentrated in δ_1 and δ_2, i.e when $\delta_1^3 - (2\delta_1^2 - 1)^3$ is close to $1/2$, which is when δ_1 is close to $\sqrt{(3+\sqrt{5})/8} \approx 0.809017$.

where the minimum is taken over the range $0.7455 \leq x \leq 0.809016$. This minimum is attained when $x = 0.809016$ (see Figure 1). So we can calculate

$$\sum_{i=1}^{k} \delta_i^2 > 0.7659 - o_{k\to\infty}(1).$$

Case 5: $\delta_1 \geq 0.809016$. Here, Lemma 3.8 will allow us to force $\delta_1^2 + \delta_2^2 > 0.750001$ and use Proposition 3.7. Note that we really do need the improvement over (1), as otherwise we get $\delta_1^2 + \delta_2^2 \geq 0.75$ when $\delta_1 = \left(\left(3+\sqrt{5}\right)/8\right)^{1/2}$. First, take p large enough that the error in Lemma 3.8 is less than 0.000001, given $\alpha_0 \geq 0.24$.

Then by Lemma 3.8 we know that $\delta_2 \geq 2\delta_1^2 - 1 + \varepsilon - 0.000001$ where

$$\varepsilon = \frac{2^9}{3^4 \times 5^5} \times 0.24^4 > 0.0000061,$$

which implies

$$\delta_1^2 + \delta_2^2 \geq \delta_1^2 + \left(2\delta_1^2 - 0.999994\right)^2 \geq \min_x \left(x^2 + \left(2x^2 - 0.999994\right)^2\right),$$

where the minimum is taken over the range $0.809016 \leq x \leq 1$. This is increasing since $x \geq 0.809016$ implies $2x^2 > 0.999994$, so

$$\delta_1^2 + \delta_2^2 \geq 0.809016^2 + \left(2 \times 0.809016^2 - 0.999994\right)^2 > 0.7500001.$$

Now applying Proposition 3.7 with $k = 2$ gives

$$\alpha \leq \frac{1}{1 + 4\left(\delta_1^2 + \delta_2^2\right)} + O\left(1/\sqrt{p}\right) \leq 0.249999975 + o(1).$$

□

4. Fields of characteristic 2

Now suppose that $\mathbb{F}$ is a field of order $q = 2^n$, and let A be a subset of $\mathbb{F}^*$. Define the *trace* $\mathrm{Tr} : \mathbb{F} \to \mathbb{F}_2$ by

$$\mathrm{Tr}(x) := \sum_{i=0}^{n-1} x^{2^i}.$$

Note that $\mathrm{Tr}(x) + \mathrm{Tr}(y) = \mathrm{Tr}(x+y)$. We shall make use of the following bound on Kloosterman sums over fields of characteristic 2 (see [3]).

Lemma 4.1. *If $a \in \mathbb{F}^*$ then*

$$\Big|\sum_{x\in\mathbb{F}^*} (-1)^{\mathrm{Tr}\left(x+ax^{-1}\right)}\Big| \leq 2\sqrt{q}.$$

Proof of Proposition 1.2. Let $\gamma\colon \mathbb{F} \to \mathbb{C}$ be the additive character on $\mathbb{F}$ given by

$$\gamma(x) = (-1)^{\mathrm{Tr}(x)}.$$

Define $X := \mathbb{F} \setminus \ker\gamma$ and, noting that $0 \notin X$ since $0 \in \ker\gamma$, $A := X \cap X^{-1}$. Then X is sum-free, and A is both sum-free and closed under inverses.

Note $1_X = \frac{1}{2}(1-\gamma)$. So, with the convention that $0^{-1} = 0$, we have

$$\begin{aligned}\alpha = \mathop{\mathbb{E}}_x \left[1_X(x)1_{X^{-1}}(x)\right] &= \mathop{\mathbb{E}}_x \left[1_X(x)1_X(x^{-1})\right] \\ &= \frac{1}{4}\mathop{\mathbb{E}}_x \left[(1-\gamma(x))(1-\gamma(x^{-1}))\right] \\ &= \frac{1}{4} + \frac{1}{4}\mathop{\mathbb{E}}_x \left[\gamma(x)\gamma(x^{-1})\right].\end{aligned}$$

Since $\mathrm{Tr}(x) + \mathrm{Tr}(x^{-1}) = \mathrm{Tr}(x + x^{-1})$, we have $\gamma(x)\gamma(x^{-1}) = \gamma(x + x^{-1})$. Then

$$\left|\mathop{\mathbb{E}}_x \left[\gamma(x)\gamma(x^{-1})\right]\right| = \left|\mathop{\mathbb{E}}_x \left[\gamma(x + x^{-1})\right]\right| \le \frac{2\sqrt{q}}{q} = o(1)$$

by Lemma 4.1, which gives our result. □

5. Final remarks

5.1. Write $\sigma(\mathbb{F})$ for the density $|A|/|\mathbb{F}|$ of the largest sum-free subset A of $\mathbb{F}$. This quantity was studied in the more general context of finite Abelian groups by Diananda and Yap in [4]. Recall from Section 1 that we define $\mu(\mathbb{F})$ to be the density of the largest subset of $\mathbb{F}$ which is both sum-free and closed under inverses.

When $\mathbb{F}$ has characteristic 2 it can be seen that $\sigma(\mathbb{F}) = 1/2$, as the set X in the proof of Proposition 1.2 demonstrates. Moreover, Proposition 1.2 itself shows $\mu(\mathbb{F}) \ge 1/4 - o(1)$.

When $\mathbb{F}$ has prime order $p > 2$, the interval $I = \{x \in \mathbb{F} : p/3 < x < 2p/3\}$ has density $1/3 + o(1)$, and this is the best possible for a sum-free set by the Cauchy-Davenport inequality. As described in [1, p. 8], the set $I \cap I^{-1}$ is then sum-free and closed under inverses, and has density $1/9 - o(1)$. So $\mu(\mathbb{F}) \ge 1/9 - o(1)$.

It is reasonable to suspect that the events 'A is sum-free' and 'A^{-1} is sum-free' are independent. So, we conjecture that the lower bounds above are in fact tight:

Conjecture 5.1. *Let $\mathbb{F}$ be a finite field. Then $\mu(\mathbb{F}) = \sigma(\mathbb{F})^2 + o(1)$ as $|\mathbb{F}| \to \infty$.*

5.2. For a set $A \subseteq \mathbb{F}^*$ we can use the quantity

$$I(A) := \frac{|A \cap A^{-1}|}{|A|}$$

to measure 'how much' A is closed under inverses. So we have studied sum-free sets A with $I(A) = 1$. When $\mathbb{F}$ has prime order p and A is sum-free with $I(A)$ large, we might still expect to do better than the bound of $|A| < (p+1)/3$ given by the

Cauchy-Davenport inequality. Indeed, since $A \cap A^{-1}$ is itself sum-free and closed under inverses we have

$$\alpha = |A|/p = \frac{|A \cap A^{-1}|}{I(A) \times p} \leq \frac{\mu(\mathbb{F})}{I(A)}.$$

So when $I(A) \geq 0.75$ we can use Theorem 1.1 to deduce

$$\alpha \leq \frac{\mu(\mathbb{F})}{0.75} \leq \frac{(0.25 - c) + o(1)}{0.75} \leq (1 - 4c)/3 + o(1).$$

Acknowlegements

This work was funded by a London Mathematical Society Undergraduate Research Bursary and the Mathematical Institute at the University of Oxford. I am immensely grateful to Tom Sanders for suggesting this topic of research and for his unwaveringly enthusiastic mentorship throughout the summer. His mathematical advice was invaluable, as were his many helpful comments on the drafts of this paper. I also gratefully acknowledge the anonymous reviewer for a very careful reading, and for their highly constructive comments and suggestions on an earlier draft.

References

[1] Pierre-Yves Bienvenu, François Hennecart, and Ilya Shkredov, *A note on the set $A(A + A)$*, Mosc. J. Comb. Number Theory, 8(2) (2019), pp. 179–188.

[2] Enrico Bombieri, *A note on the large sieve*, Acta Arithmetica, 18(1) (1971), pp. 401–404.

[3] Keith Conrad, *On Weil's proof of the bound for Kloosterman sums*, J. Number Theory, 97(2) (2002), pp. 439 – 446.

[4] Palahenedi Hewage Diananda and Hian Poh Yap, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad., 45(1) (1969), pp. 1–5.

[5] Vsevolod F. Lev, *Linear equations over $\mathbb{F}_p$ and moments of exponential sums*, Duke Math. J., 107(2) (2001), pp. 239–263.

[6] Vsevolod F. Lev, *Large sum-free sets in $\mathbb{Z}/p\mathbb{Z}$*, Israel J. Math., 154 (2006), pp. 221–233.

[7] Terence Tao and Van H. Vu, *Additive Combinatorics*, Cambridge University Press, 2006.

[8] André Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A., 34(5) (1948), pp. 204–207.

[9] Julia Wolf, *Finite field models in arithmetic combinatorics – ten years on*, Finite Fields and Their Applications, 32 (2015), pp. 233–274.

Mathematical Institute, University of Oxford, Woodstock Road, Oxford, United Kingdom.
Email address: katherine.benjamin@maths.ox.ac.uk