BOUNDS OF TRILINEAR AND TRINOMIAL EXPONENTIAL SUMS

SIMON MACOURT, GIORGIS PETRIDIS, ILYA D. SHKREDOV, AND IGOR E. SHPARLINSKI

Abstract. We prove, for a sufficiently small, subset \( A \) of a prime residue field an estimate on the number of solutions to the equation
\[
(a_1 - a_2)(a_3 - a_4) = (a_5 - a_6)(a_7 - a_8)
\]
with all variables in \( A \). We then derive new bounds on trilinear exponential sums and on the total number of residues equaling the product of two differences of elements of \( A \). We also prove a refined estimate on the number of collinear triples in a Cartesian product of multiplicative subgroups and derive stronger bounds for trilinear sums with all variables in multiplicative subgroups.

1. Introduction

Let \( p \) be a prime and let \( \mathbb{F}_p \) be the finite field of \( p \) elements. Now given three sets \( \mathcal{X}, \mathcal{Y}, \mathcal{Z} \subseteq \mathbb{F}_p \), and three sequences of complex weights \( \alpha = (\alpha_x)_{x \in \mathcal{X}}, \beta = (\beta_y)_{y \in \mathcal{Y}} \) and \( \gamma = (\gamma_z)_{z \in \mathcal{Z}} \) supported on \( \mathcal{X}, \mathcal{Y} \) and \( \mathcal{Z} \), respectively, we consider exponential sums
\[
S(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \alpha, \beta, \gamma) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sum_{z \in \mathcal{Z}} \alpha_x \beta_y \gamma_z \mathbf{e}_p(xy),
\]
where \( \mathbf{e}_p(z) = \exp(2\pi iz/p) \), the sets \( \mathcal{X}, \mathcal{Y}, \mathcal{Z} \subseteq \mathbb{F}_p \) are of cardinalities
\[
|\mathcal{X}| = X, \quad |\mathcal{Y}| = Y, \quad |\mathcal{Z}| = Z,
\]
and weights satisfy
\[
\max_{x \in \mathcal{X}} |\alpha_x| \leq 1, \quad \max_{y \in \mathcal{Y}} |\beta_y| \leq 1, \quad \max_{z \in \mathcal{Z}} |\gamma_z| \leq 1.
\]

We also define more general sums
\[
T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sum_{z \in \mathcal{Z}} \rho_{x,y} \sigma_{x,z} \tau_{y,z} \mathbf{e}_p(xy).
\]
with some weights $\rho = (\rho_{x,y})$, $\sigma = (\sigma_{x,z})$ and $\tau = (\tau_{y,z})$ satisfying
\begin{equation}
\max_{(x,y) \in X \times Y} |\rho_{x,y}| \leq 1, \quad \max_{(x,z) \in X \times Z} |\sigma_{x,z}| \leq 1, \quad \max_{(y,z) \in Y \times Z} |\tau_{y,z}| \leq 1.
\end{equation}

Investigation of the sums $S(X,Y,Z;\alpha,\beta,\gamma)$ has been initiated by Bourgain and Garaev [4] who have linked them to some problems of additive combinatorics and also have given nontrivial explicit bounds on these sums which go beyond the classical bilinear bound. Several more bounds on these sums, improving and complementing those of [4] can be found in [7,16,19].

The more general sums $T(X,Y,Z;\rho,\sigma,\tau)$ have been introduced and estimated in [16]. Several improvements of the results of [16] can be found in [9,19]. Furthermore, in the special case when the sets $X$, $Y$ and $Z$ are multiplicative subgroups on $\mathbb{F}_p^*$, bounds of these sums have found applications to new estimates of exponential sums with sparse polynomials [10,11].

We note that generally speaking the bound on bilinear sums does not apply to these sums. Instead, in [16] it was shown that they are related to the following combinatorial quantity. For any $A \subseteq \mathbb{F}_p$, of cardinality $A$, we define
\begin{equation}
D^X(A) = |\{(a_1 - a_2)(a_3 - a_4) = (a_5 - a_6)(a_7 - a_8) : a_1, \ldots, a_8 \in A\}|.
\end{equation}

It follows from [1] that $D^X(A) = O(A^{13/2})$ for $A \leq p^{2/3}$, see [16, Corollary 2.9]. It was shown in [16, Theorem 1.3] that under the conditions (1.2) and (1.5) we have
\begin{equation}
T(X,Y,Z;\rho,\sigma,\tau) = O\left(p^{1/8}X^{7/8}(YZ)^{29/32}\right),
\end{equation}
provided that $p^{2/3} \geq X \geq Y \geq Z$. In some ranges this bound has been improved in [9, Theorem 1.2] as
\begin{equation}
T(X,Y,Z;\rho,\sigma,\tau) = O\left(p^{3/16}X^{13/16}(YZ)^{7/8}\right),
\end{equation}
provided that $X \geq Y \geq Z$.

If $X \geq Y \geq Z$ and also $Y \leq p^{48/97}$ then (1.6) has been further improved in [19, Corollary 45] as
\begin{equation}
T(X,Y,Z;\rho,\sigma,\tau) = O\left(p^{1/8}X^{7/8}(YZ)^{29/32-1/3072}\right).
\end{equation}
This progress was based on the stronger bound $D^X(A) = O(A^{13/2-1/192})$ for $A \leq p^{48/97}$, see [19, Theorem 41].

Multilinear generalisations of the exponential sums in (1.1) and (1.4) have also been studied, see [2,7–9,16,19] and references therein. Although all the above works rely on ideas and results from additive
combinatorics and thus work the best in prime fields $\mathbb{F}_p$, extension to arbitrary finite fields can be found in [3, 5, 13, 15].

Here, as in all previous works, we improve the state-of-the-art on $D^k(A)$ for sufficiently small $A$, see Theorem 4.3 below, and then use some previously known estimates and obtain new concrete bounds on the exponential sums in (1.1) and (1.4), see Theorem 6.1 below. This progress is rooted at the eigenvalue method of Shkredov.

For the special case of multiplicative subgroups, we achieve further progress by an altogether different method: by improving existing bounds on the number of collinear triples of Cartesian products of multiplicative subgroups, see Theorems 5.2 and 6.2 below. Our results lead to small improvements on bounds on trinomial exponential sums, see [11] and Corollary 6.3.

We also bound from below the cardinality of the set
$$(A - A)(A - A) = \{(a_1 - a_2)(a_3 - a_4) : a_1 \ldots, a_4 \in A\},$$
see Theorem 6.4 below, improving [14, Theorem 27].

2. Notation

In what follows, it is convenient to introduce notation $A \preceq B$ and $B \succeq A$ as equivalents of $A \leq p^{o(1)}B$ as $p \to \infty$; and $A \asymp B$ as equivalent to $A \preceq B$ and $B \preceq A$.

We also recall that the notations $A = O(B)$, $A \ll B$ and $B \gg A$ are each equivalent to the statement that the inequality $A \leq cB$ holds with a constant $c > 0$ which is absolute throughout this paper.

3. Some combinatorial quantities

Given two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p$ we define

- $E^*(\mathcal{U}, \mathcal{V})$ where $* \in \{+, -, \times, /\}$ is one of the four arithmetic operations as the number of solutions to the equation
  $$u_1 * v_1 = u_2 * v_2, \quad u_1, u_2 \in \mathcal{U}, \; v_1, v_2 \in \mathcal{V};$$

- $E^*_k(\mathcal{U}, \mathcal{V})$ where $* \in \{+, -, \times, /\}$ as the number of solutions to the equation
  $$u_1 * v_1 = u_2 * v_2 = u_3 * v_3, \quad u_1, u_2, u_3 \in \mathcal{U}, \; v_1, v_2, v_3 \in \mathcal{V};$$

- $D^k(\mathcal{U}, \mathcal{V})$ as the number of solutions to the equation
  $$(u_1 - v_1)(u_2 - v_2) = (u_3 - v_3)(u_4 - v_4),$$
  $$u_i \in \mathcal{U}, \; v_i \in \mathcal{V}, \quad i = 1, 2, 3, 4;$$
\begin{itemize}
  \item $\tilde{D}^\times(\mathcal{U}, \mathcal{V})$ as the number of solutions to the equation
  \[(u_1 - u_2)(v_1 - v_2) = (u_3 - u_4)(v_3 - v_4) \neq 0,\]
  \[u_i \in \mathcal{U}, \ v_i \in \mathcal{V}, \ i = 1, 2, 3, 4;\]
  \item $\tilde{T}(\mathcal{U}, \mathcal{V})$ as the number of collinear triples in $\mathcal{U} \times \mathcal{V}$ with slopes in $\mathbb{F}_p^*$, that is, the number of solutions to the equation
  \[(u_1 - u_2)(v_1 - v_2) = (u_1 - u_3)(v_1 - v_3) \neq 0,\]
  \[u_i \in \mathcal{U}, \ v_i \in \mathcal{V}, \ i = 1, 2, 3;\]
  \item $N(\mathcal{U}, \mathcal{V}, \mathcal{W})$ as the number of solutions to
  \[u_1(v_1 - w_1) = u_2(v_2 - w_2), \quad u_1, u_2 \in \mathcal{U}, \ v_1, v_2 \in \mathcal{V}, \ w_1, w_2 \in \mathcal{W}.\]
\end{itemize}

In the case of equal sets $\mathcal{U} = \mathcal{V}$, we write

\[E^\times(\mathcal{U}, \mathcal{U}) = E^\times(\mathcal{U}) \text{ and } E^\times_3(\mathcal{U}, \mathcal{U}) = E^\times_3(\mathcal{U}).\]

Clearly

\[\tilde{D}^\times(\mathcal{U}) \leq D^\times(\mathcal{U}) \leq \tilde{D}^\times(\mathcal{U}) + 4|\mathcal{U}|^6.\]

Note that expressing $N(\mathcal{U}, \mathcal{V}, \mathcal{W})$ and $D^\times(\mathcal{U}, \mathcal{V})$ via multiplicative character sums, by the Cauchy inequality we immediately derive

\[(3.1) \quad N(\mathcal{U}, \mathcal{V}, \mathcal{W}) \leq \sqrt{E^\times(\mathcal{U}) D^\times(\mathcal{V}, \mathcal{W})}.\]

We also define these quantities with functions instead of sets. For example, for a function $F : \mathbb{F}_p \rightarrow \mathbb{R}$ and $* \in \{+, -, \times, /\}$ we define

\[E^\times_3(F) = \sum_{x_1, y_1, x_2, y_2, x_3, y_3 \in \mathbb{F}_p \atop x_1 y_1 = x_2 y_2 = x_3 y_3} F(x_1)F(y_1)F(x_2)F(y_2)F(x_3)F(y_3),\]

and also given a set $\mathcal{U} \subseteq \mathbb{F}_p$ we define

\[E^\times(F, \mathcal{U}) = \sum_{x_1, x_2 \in \mathbb{F}_p, \ u_1, v_2 \in \mathcal{U} \atop x_1 u_1 = x_2 v_2} F(x_1)F(x_2).\]

\section{A new bound on $D^\times(\mathcal{A})$}

We use results based on the eigenvalue method of Shkredov [19] to prove a new upper bound on $D^\times(\mathcal{A})$. Throughout the proof we use the convention that sets are written in curly script capital letters and their cardinality in roman script capital letters, for example, $|\mathcal{A}| = A$.

We start with a result which can be of independent interest.
**Lemma 4.1.** Let \( F : \mathbb{F}_p \to \mathbb{R} \) be a non-negative function and let \( K \geq 1 \) be an arbitrary parameter. Suppose that for \( * \in \{+, -, \times, \wedge \} \) and any set \( S \subseteq \mathbb{F}_p \) one has

\[
E^*(F, S) \leq KS^{3/2}.
\]

Then

\[
E^*(F) \leq (E_3^*)^{6/13} (F) K^{2/13} \|F\|^{12/13}_1,
\]

where

\[
\|F\|_1 = \sum_{x \in \mathbb{F}_p} F(x).
\]

**Proof.** By the Dirichlet principle, there exists some \( \Delta > 0 \) such that

\[
E^*(F) \approx \Delta^4 E^*(\mathcal{B}),
\]

where \( \mathcal{B} = \{x : \Delta < F(x) \leq 2\Delta\} \) is the dyadic level set of the function \( F \). Then

\[
B\Delta \leq \|F\|_1 \quad \text{and} \quad E_3^*(\mathcal{B}) \leq \Delta^{-6} E_3^*(F)
\]

and for any \( S \subseteq \mathbb{F}_p \), by our assumption one has

\[
\Delta^2 E^*(\mathcal{B}, S) \leq E^*(F, S) \leq KS^{3/2}.
\]

Applying [14, Theorem 34] (which holds for any type of energy) with

\[
D_1 = B^{-3} \Delta^{-6} E_3^*(F) \quad \text{and} \quad D_2 = \Delta^{-2} B^{-1} K,
\]

we obtain

\[
(E^*(\mathcal{B}))^{13} \leq D_1^6 D_2^2 B^{32} \leq \left( B^{-3} \Delta^{-6} E_3^*(F) \right)^6 \left( \Delta^{-2} B^{-1} K \right)^2 B^{32} = (E_3^*(F))^6 K^2 B^{12} \Delta^{-40} \leq (E_3^*(F))^6 K^2 \|F\|^{12}_1 \Delta^{-52}.
\]

In other words,

\[
(E^*(F))^{13} \sim (E^*(\mathcal{B}))^{13} \Delta^{52} \leq (E_3^*(F))^6 K^2 \|F\|^{12}_1
\]

as required. \(\square\)

In the proof of Theorem 4.3 below we apply Lemma 4.1 to the function

\[
r_{\mathcal{A} - \mathcal{A}}(x) = |\{(a, b) \in \mathcal{A} \times \mathcal{A} : a - b = x\}|
\]

and to multiplicative energy.
Lemma 4.2. Let $\mathcal{A} \subseteq \mathbb{F}_p$ be of cardinality $A \leq p^{2/3}$. Then

$$E'_3(r_{\mathcal{A} - \mathcal{A}}) \ll A^9 \log A,$$

and for any set $S \subseteq \mathbb{F}_p$ with $S \leq A^2$ one has

$$E'(r_{\mathcal{A} - \mathcal{A}}, S) \ll \frac{A^4 S^2}{p} + A^3 S^{3/2}.$$

Proof. For $a, b \in \mathbb{F}_p$ set

$$r_{(\mathcal{A} - a)/(\mathcal{A} - b)}(x) = \left\{ (c, d) \in \mathcal{A} \times \mathcal{A} : (c - a)/(d - b) = x \right\}.$$

From the definition of $E'_3(r_{\mathcal{A} - \mathcal{A}})$ collecting terms with the same value of $x_1/y_1 = x_2/y_2 = x_3/y_3 = z$ we have

$$E'_3(r_{\mathcal{A} - \mathcal{A}}) = \sum_{a \in \mathbb{F}_p} \sum_{x_1, x_2, x_3 \in \mathbb{F}_p} r_{\mathcal{A} - \mathcal{A}}(x_1) r_{\mathcal{A} - \mathcal{A}}(zx_1) r_{\mathcal{A} - \mathcal{A}}(x_2) r_{\mathcal{A} - \mathcal{A}}(zx_2)$$

$$r_{\mathcal{A} - \mathcal{A}}(x_3) r_{\mathcal{A} - \mathcal{A}}(zx_3)$$

$$= \sum_{a, b \in \mathcal{A}} \left( \sum_{x \in \mathbb{F}_p} r_{\mathcal{A} - \mathcal{A}}(x) r_{\mathcal{A} - \mathcal{A}}(xz) \right)^3.$$

We now observe that

$$\sum_{x \in \mathbb{F}_p} r_{\mathcal{A} - \mathcal{A}}(x) r_{\mathcal{A} - \mathcal{A}}(zx) = \left\{ (a, b, c, d) \in \mathcal{A} \times \mathcal{A} : (c - a)/(d - b) = z \right\}$$

$$= \sum_{a, b \in \mathcal{A}} r_{(\mathcal{A} - a)/(\mathcal{A} - b)}(z).$$

Using the Hölder inequality

$$E'_3(r_{\mathcal{A} - \mathcal{A}}) = \sum_{a, b \in \mathcal{A}} \left( \sum_{x \in \mathbb{F}_p} r_{(\mathcal{A} - a)/(\mathcal{A} - b)}(z) \right)^3$$

$$\leq A^4 \sum_{a, b \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_p} r_{(\mathcal{A} - a)/(\mathcal{A} - b)}(z).$$

Clearly

$$r_{(\mathcal{A} - a)/(\mathcal{A} - b)}(z)$$

$$= \left\{ (c_1, d_1, c_2, d_2, c_3, d_3) \in \mathcal{A}^6 : \frac{c_1 - a}{d_1 - b} = \frac{c_2 - a}{d_2 - b} = \frac{c_3 - a}{d_3 - b} = z \right\}.$$
Thus
\[ \sum_{z \in \mathbb{F}_p} r_{(A-a)/(A-b)}^3(z) = \left\{ (c_1, d_1, c_2, d_2, c_3, d_3) \in \mathcal{A}^6 : \frac{c_1 - a}{d_1 - b} = \frac{c_2 - a}{d_2 - b} = \frac{c_3 - a}{d_3 - b} \right\}. \]
Therefore we see that
\[ \sum_{a, b \in \mathbb{F}_p, z \in \mathbb{F}_p} r_{(A-a)/(A-b)}^3(z) = Q(A), \]
where
\[ Q(A) = \left\| (a_1, \ldots, a_8) \in \mathcal{A}^8 : \frac{a_1 - a_2}{b_1 - b_2} = \frac{a_1 - a_3}{b_1 - b_3} = \frac{a_1 - a_4}{b_1 - b_4} \right\| \]
is the number of ordered collinear quadruples
\[ ((a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)) \in (\mathcal{A} \times \mathcal{A})^4. \]
By [14, Theorem 11(2)] we have
\[ Q(A) \ll \frac{A^8}{p^2} + A^5 \log A \ll A^9 \log A \]
which together with (4.2) and (4.3) gives the first inequality.

To obtain the second inequality just apply the modern form of the incidence result of Rudnev [17], see, for example, [19, Theorem 10]. This completes the proof. \(\square\)

**Theorem 4.3.** Let \( \mathcal{A} \subseteq \mathbb{F}_p \) be of cardinality \( \mathcal{A} \leq p^{1/2} \). Then
\[ D^\times(\mathcal{A}) \leq A^{84/13}. \]

**Proof.** We begin by noting that
\[ D^\times(\mathcal{A}) = E^\times(r_{\mathcal{A}-\mathcal{A}}). \]
By the first inequality of Lemma 4.2 we have
\[ E^\times_3(r_{\mathcal{A}-\mathcal{A}}) \lesssim A^9 \]
while for all \( \mathcal{S} \) satisfying \( \mathcal{S} \leq A^2 \leq p \) the second inequality becomes
\[ E^\times(r_{\mathcal{A}-\mathcal{A}}, \mathcal{S}) \ll \frac{A^4 S^2}{p} + A^3 S^{3/2} \ll A^3 S^{3/2}. \]

By the remark after [14, Theorem 34], we only have to confirm (4.1) for sets \( \mathcal{S} \) of cardinality \( \mathcal{S} \ll A^4 / E^\times(A) \leq A^2 \), and so Lemma 4.2 gives \( K = A^3 \). Moreover
\[ \| r_{\mathcal{A}-\mathcal{A}} \|_1 = \sum_{x \in \mathbb{F}_p} r_{\mathcal{A}-\mathcal{A}}(x) = A^8. \]
Substituting all this in Lemma 4.1 with $F(x) = r_{A-A}(x)$ gives

$$D^\times(A) = E^\times(r_{A-A}) \lesssim A^{84/13},$$

which concludes the proof. □

5. A Refined Bound on $D^\times(\mathcal{G}, \mathcal{H})$ over Subgroups

Here we use $\tilde{T}(\mathcal{G}, \mathcal{H})$ to give stronger bounds on $D^\times(\mathcal{G}, \mathcal{H})$, where $\mathcal{G}$ and $\mathcal{H}$ are multiplicative subgroups.

First we recall the following result [12, Theorem 2].

Lemma 5.1. Let $\mathcal{G}$ and $\mathcal{H}$ be subgroups of $\mathbb{F}_p^*$ and let $\mathcal{M}_G$ and $\mathcal{M}_H$ be two complete sets of distinct coset representatives of $\mathcal{G}$ and $\mathcal{H}$ in $\mathbb{F}_p^*$. For an arbitrary set $\Theta \subseteq \mathcal{M}_G \times \mathcal{M}_H$ such that

$$|\Theta| \leq \min \left\{ |\mathcal{G}| |\mathcal{H}|, \frac{p^3}{|\mathcal{G}|^2 |\mathcal{H}|^2} \right\},$$

we have

$$\sum_{(u,v) \in \Theta} |\{ (x, y) \in \mathcal{G} \times \mathcal{H} : ux + vy = 1 \}| \ll (|\mathcal{G}| |\mathcal{H}| |\Theta|^2)^{1/3}.$$

Theorem 5.2. Let $\mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_p^*$ be subgroups with $|\mathcal{G}| = G, |\mathcal{H}| = H$ and $G \geq H$. Then

$$\tilde{T}(\mathcal{G}, \mathcal{H}) - \frac{G^3 H^3}{p} \ll \begin{cases} \frac{p^{1/2} G^{3/2} H^2}{G^{5/2} H^{5/2}} + H^2 G^2 \log G & \text{if } GH \geq p^{4/3}, \\
\frac{G^3 H \log G}{p^{1/2}} & \text{if } GH < p^{4/3}, \\
\frac{G^3 H^{3/2}}{p^{3/2}} & \text{if } GH \leq p. \end{cases}$$

Proof. The result for $GH \leq p$ is clear from [11, Lemma 2.6] once we eliminate the contribution from the zero solutions (see also [18]). Similarly for $GH \geq p^{4/3}$ from [9, Theorem 1.1]. We now prove for $p < GH < p^{4/3}$ by following the argument of [11].

We can think of $\mathcal{M}_G = \mathbb{F}_p^*/\mathcal{G}$ and similarly for $\mathcal{M}_H$. We now set

$$3 \leq \Delta = c \frac{G^{3/2} H^{3/2}}{p^{3/2}},$$

for a sufficiently small $c$ to be chosen later (it is better to think of $\Delta$ as a parameter to be chosen later), by [11, Corollaries 2.3 and 2.5] and
by observing that the contribution from lines with \( ab = 0 \) is at most \( O(G^2H^2) \) we have

\[
\tilde{T}(\mathcal{G}, \mathcal{H}) = \frac{G^3H^3}{p} \ll G^2H^2 + \Delta pG H
\]

(5.1)

Let

\[
W = \sum_{a,b \in \mathbb{F}_p^* \atop \ell_{a,b} \in \mathcal{G} \times \mathcal{H}} \left( \ell_{a,b} - \frac{G H}{p} \right)^2.
\]

We now let \( \tau > \Delta \) be another parameter and define

\[
\Theta_\tau = \{(\alpha, \beta) \in \mathcal{G} \times \mathcal{H} : |\{(x, y) \in \mathcal{G} \times \mathcal{H} : ux + vy = 1\}| \geq \tau\}.
\]

Hence,

\[
\Theta_\tau = \{(\alpha, \beta) \in \mathcal{G} \times \mathcal{H} : \ell_{a\beta^{-1}, \beta^{-1}} \geq \tau\}.
\]

By Lemma 5.1 we have

\[
|\Theta_\tau| \tau \ll (GH)^{1/3}|\Theta_\tau|^{2/3}
\]

provided \( G^2H^2|\Theta_\tau| \leq p^3 \) and \( |\Theta_\tau| \leq GH \). Clearly the second condition is satisfied since \( |\Theta_\tau| \leq |\mathcal{G}||\mathcal{H}| = (p - 1)^2/(GH) \leq GH \).

We now suppose that \( G^2H^2|\Theta_\tau| > p^3 \). We define

\[
Q_\tau = \{(\alpha, \beta) \in \mathbb{F}_p^* \times \mathbb{F}_p^* : \ell_{a\beta^{-1}, \beta^{-1}} \geq \tau\}.
\]

We can then think of \( \Theta_\tau \) as a union of cosets. We have the number of incidences between \( \mathcal{G} \times \mathcal{H} \) and lines \( \ell_{a\beta^{-1}, \beta^{-1}} \) with \( \alpha, \beta \in Q_\tau \) is at least

\[
|Q_\tau| \tau = GH|\Theta_\tau| \tau > p^3G^{-1}H^{-1}\tau \geq p^3G^{-1}H^{-1}\Delta.
\]

But from [20] we have the number of point–line incidences

\[
|Q_\tau| \tau \ll |Q_\tau|^{1/2}GH + |Q_\tau|,
\]

hence

\[
p^3G^{-1}H^{-1}\Delta < |Q_\tau| \tau \ll G^2H^2\tau^{-1} < G^2H^2\Delta^{-1}.
\]

It follows that for this inequality to hold we need \( \Delta^2 \ll G^3H^3/p^3 \). By choosing the constant \( c \) in the definition of \( \Delta \) small enough, we ensure this never happens.

We now let \( \tau_j = c^j\Delta \), for \( j = 0, 1, \ldots, J \) and \( J = \log(G^{1/2}H^{1/2}/\Delta) \).

We observe that the contributions from lines \( \ell_{a,b}, a, b \in F_p^* \) is in one to
one correspondence with those given by $\ell_{-a-1,\beta-1}$. Now from (5.2) we have

$$|Q_\tau| = GH|\Theta_\tau| \ll G^2 H^2 \tau^{-3}.$$ 

We also have $\tau_j \geq \tau_0 = \Delta \gg G^{3/2} H^{3/2} / p^{3/2} > GH / p$ for all $j$. It follows that the contribution to $W$ is bounded by

$$\sum_{j=0}^{J} |Q_{\tau_j}|^2 \ll \sum_{j=0}^{J} |Q_{\tau_j}|^3 \ll \sum_{j=0}^{J} G^2 H^2 \ll G^2 H^2 \log G.$$ 

Substituting into (5.1) we have the required result. □

In particular, we see from Theorem 5.2 that

$$\tilde{T}(G, \mathcal{H}) \ll \begin{cases} G^3 H^3 / p & \text{if } GH \geq p \log p, \\ G^2 H^2 \log G & \text{if } GH < p \log p. \end{cases}$$

Since $\tilde{T}(G, \mathcal{H}) \leq GH \tilde{D}^x(G, \mathcal{H})$, where $\tilde{D}^x(G, \mathcal{H})$ does not include the zero solutions of $D^x(G, \mathcal{H})$, we have the following.

**Corollary 5.3.** Let $G, \mathcal{H} \subseteq \mathbb{F}_p^*$ be subgroups of orders $G \geq H$. Then

$$\tilde{D}^x(G, \mathcal{H}) \ll \begin{cases} G^4 H^4 / p & \text{if } GH \geq p \log p, \\ G^3 H^3 \log G & \text{if } GH < p \log p. \end{cases}$$

We mention the above result is only new for $G$ and $H$ falling either side of $(p \log p)^{1/2}$; see the proof of [11, Lemma 3.5].

6. **Applications**

Let us record what Theorem 4.3 gives for the exponential sums mentioned in the Introduction.

**Theorem 6.1.** For any sets $\mathcal{X}, \mathcal{Y}, \mathcal{Z} \subseteq \mathbb{F}_p$ as in (1.2) and complex weights $\alpha, \beta$ and $\gamma$ as in (1.3) or $\rho, \sigma$ and $\tau$ as in (1.5), for the sums $S(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \alpha, \beta, \gamma)$ defined as in (1.1) or $T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)$ defined as in (1.4) we have

- For $Y \leq p^{1/2}$
  $$S(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \alpha, \beta, \gamma) \ll p^{1/4} X^{3/4} Y^{21/26} Z^{1/2} E^x(\mathcal{Z})^{1/8}.$$  
- For $Y, Z \leq p^{1/2}$
  $$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) \ll p^{1/8} X^{7/8} Y^{47/52} Z^{47/52} + X Y Z^{3/4}.$$
Proof. It is shown in the proof of [16, Theorem 1.1] that
\[ S(\mathcal{X}, \mathcal{Y}, Z; \alpha, \beta, \gamma) \ll p^{1/4} X^{3/4} Z^{1/2} N(Z, Y, Y)^{1/4}. \]
Hence, by (3.1) we have
\[ S(\mathcal{X}, \mathcal{Y}, Z; \alpha, \beta, \gamma) \ll p^{1/4} X^{3/4} D^\times(Y)^{1/8} Z^{1/2} E^\times(Z)^{1/8}. \]
Furthermore, it is shown in the proof of [16, Theorem 1.3] that
\[ T(\mathcal{X}, \mathcal{Y}, Z; \rho, \sigma, \tau) \ll p^{1/8} X^{7/8} Y^{1/2} D^\times(Y)^{1/16} Z^{1/2} D^\times(Z)^{1/16} + XYZ^{3/4}. \]
Using Theorem 4.3 proves both claims. \( \square \)

The bound on \( T(\mathcal{X}, \mathcal{Y}, Z; \rho, \sigma, \tau) \) improves (1.7) from [19]. Note that the range of non-triviality, that is the set of values of \( X, Y, Z \) for which 
\[ |T(\mathcal{X}, \mathcal{Y}, Z; \rho, \sigma, \tau)| \]
is smaller than \( XYZ \), obtained via the triangle-inequality, is \( X^{13} Y^{10} Z^{10} \gg p^{13} \). Taking \( \mathcal{X} = \mathcal{Y} = Z \) gives that when \( X \gg p^{13/33} \) the bound in Theorem 6.1 is non-trivial. The example where \( \mathcal{X} = \mathcal{Y} = Z = \{1, \ldots, X\} \) and all the weights equal 1, shows that \( X \gg p^{1/3} \) is necessary.

The bound on \( S(\mathcal{X}, \mathcal{Y}, Z; \alpha, \beta, \gamma) \) improves [16] under some conditions. For example, when \( \mathcal{X} = \mathcal{Y} = Z \), the bound
\[ S(\mathcal{X}, \mathcal{X}, \mathcal{X}; \alpha, \beta, \gamma) \ll p^{1/4} X^{19/8}, \]
has been given in [16], while Theorem 4.3 gives
\[ S(\mathcal{X}, \mathcal{X}, \mathcal{X}; \alpha, \beta, \gamma) \ll p^{1/4} X^{107/52} E^\times(\mathcal{X})^{1/8}, \]
which is better when \( E^\times(\mathcal{X}) \ll X^{33/13-\varepsilon} \) for some \( \varepsilon > 0 \). Note that \( 33/13 > 5/2 \) so this condition is not very restrictive as is known to be satisfied for many special sets. For example, see [18, Proposition 1], for shifted multiplicative subgroups of \( \mathbb{F}_p^* \).

Another interesting example is given by the set \( \mathcal{Z} = \{ z^{-1} + a : z \in \mathcal{I} \} \subset \mathbb{F}_p \) of shifted reciprocals modulo \( p \) of integers of an interval \( \mathcal{I} = [k + 1, k + Z] \) (embedded in \( \mathbb{F}_p \)) with some integers \( k \) and \( Z \geq 1 \). Clearly, the equation
\[ (u^{-1} + a) (v^{-1} + a) = (y^{-1} + a) (z^{-1} + a), \quad u, v, y, z \in \mathcal{I}, \]
has \( O(Z^2) \) solutions with
\[ (u^{-1} + a) (v^{-1} + a) = (y^{-1} + a) (z^{-1} + a) = 0 \text{ or } a^2, \quad u, v, y, z \in \mathcal{I}. \]
Otherwise we reduce it to \( O(Z^2) \) equations of the form
\[ (y^{-1} + a) (z^{-1} + a) = \lambda, \quad y, z \in \mathcal{I}, \]
with some fixed \( \lambda \in \mathbb{F}_p \setminus \{0, a^2\} \). One verifies that (6.1) is equivalent to
\[ (y + b)(z + b) = \mu, \quad y, z \in \mathcal{I} \setminus \{0\}, \]
with
\[ b = \frac{a}{a^2 - \lambda} \quad \text{and} \quad \mu = -\frac{\lambda}{(a^2 - \lambda)^2}, \]
which by a result of Cilleruelo and Garaev \cite[Equation (3)]{6}, has at most \( Z^{3/2} p^{-1/2+o(1)} + Z^{o(1)} \) solutions. Hence
\[ E^\times(\mathcal{Z}) \leq Z^{7/2} p^{-1/2+o(1)} + Z^{2+o(1)}. \]

**Theorem 6.2.** For subgroups \( \mathcal{F}, \mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_p \) with \( G \supseteq H \) and complex weights \( \rho, \sigma \) and \( \tau \) as in \((1.5)\), for the \( T(\mathcal{F}, \mathcal{G}, \mathcal{H}; \rho, \sigma, \tau) \) defined as in \((1.4)\) we have

- For \( GH \geq p \log p \),
  \[ T(\mathcal{F}, \mathcal{G}, \mathcal{H}; \rho, \sigma, \tau) \ll F^{7/8}GH + FGH^{3/4}. \]
- For \( GH < p \log p \),
  \[ T(\mathcal{F}, \mathcal{G}, \mathcal{H}; \rho, \sigma, \tau) \preceq p^{1/8} F^{7/8} G^{7/8} H^{7/8} + FGH^{3/4}. \]

**Proof.** Again, we recall that it is shown in \cite{16} that
\[ T(\mathcal{F}, \mathcal{G}, \mathcal{H}; \rho, \sigma, \tau) \ll p^{1/8} F^{7/8} G^{1/2} H^{1/2} \tilde{D}^\times(\mathcal{G}, \mathcal{H})^{1/8} + FGH^{3/4}. \]
Using Corollary 5.3 we prove the result. \( \square \)

The first bound of Theorem 6.2 is non-trivial when \( F \to \infty \) as \( p \to \infty \), while the second bound is non-trivial when \( FGH \geq p^{1+\varepsilon} \) for some fixed \( \varepsilon > 0 \). The first part of the theorem improves \cite[Lemma 3.5]{11} in the range \( H < p^{1/2} \), and \( GH \geq p \log p \) and leads to improved bounds on trinomial exponential sums in some ranges. The bound in \cite[Lemma 3.5]{11} in the range \( H < (p \log p)^{1/2} < G \leq F \) is
\[ T(\mathcal{F}, \mathcal{G}, \mathcal{H}; \rho, \sigma, \tau) \preceq p^{1/16} F^{7/8} GH^{7/8} \]
and
\[ \frac{F^{7/8} GH}{p^{1/16} F^{7/8} GH^{7/8}} = \left( \frac{H^2}{p} \right)^{1/16}. \]

As in \cite[Theorem 1.5]{11}, we can use Theorem 6.2 to estimate exponential sums
\[(6.2) \quad S_\chi(\Psi) = \sum_{x \in \mathbb{F}_p^*} \chi(x) e_p(\Psi(x)), \]
with trinomials
\[(6.3) \quad \Psi(X) = aX^k + bX^\ell + cX^m, \]
where \( \chi \) is an arbitrary multiplicative character of \( \mathbb{F}_p^* \).
Corollary 6.3. Let $\Psi(X)$ be a trinomial of the form (6.3) with $a, b, c \in \mathbb{F}_p^*$. Define
\[ d = \gcd(k, p - 1), \quad e = \gcd(\ell, p - 1), \quad f = \gcd(m, p - 1) \]
and
\[ g = \frac{d}{\gcd(d, f)}, \quad h = \frac{e}{\gcd(e, f)}. \]
Suppose $f \geq g \geq h$, then for sum (6.2) we have
\[ S_{\chi}(\Psi) \ll \begin{cases} \frac{p^{7/8} f^{1/8}}{g}, & \text{if } gh \geq p \log p, \\ p(f/gh)^{1/8} (\log p)^{1/8}, & \text{if } gh < p \log p. \end{cases} \]

Proof. As in the proof of [11, Theorem 1.5], adopting our new bound from Theorem 6.2, for $gh > p \log p$ we have
\[ S_{\chi}(\Psi) \ll p^{7/8} f^{1/8} + ph^{-1/4}. \]
The first term clearly dominates when $h^2 f > p$. Now,
\[ h^2 f \geq \frac{hf \log p}{g} > hp \log p \]
since $f \geq g$. Hence the first term dominates everywhere in this range.

For $gh < p \log p$ we have
\[ S_{\chi}(\Psi) \ll p(f/gh)^{1/8} (\log p)^{1/8} + ph^{-1/4}. \]
The first term clearly dominates when $fh \log^8 p > g$. Since $f \geq g$, the first term dominates everywhere in this range. This gives the required result. $\square$

In particular, Corollary 6.3 improves [11, Theorem 1.5] for $g \geq (p \log p)^{1/2} > h$.

Theorem 4.3 also improves the existing lower bound on $|(A - A)(A - A)|$ when $A \leq p^{1/2}$.

Theorem 6.4. For any set $A \subseteq \mathbb{F}_p$ of size $A \leq p^{1/2}$ we have
\[ |(A - A)(A - A)| \geq A^{20/13} \]

Proof. By an application of the Cauchy-Schwarz inequality we get
\[ |(A - A)(A - A)| \geq \frac{A^8}{D^*(A)} \geq A^{20/13}. \]
$\square$

This improves the exponent $68/45 - \varepsilon$ for all $\varepsilon > 0$ and $A \leq p^{9/16}$ give in [14, Theorem 27].
7. Acknowledgement

During the preparation of this work, S.M. was supported by the Australian Government Research Training Program Scholarship, G.P. by the NSF Award 1723016 (he also gratefully acknowledges the support from the RTG in Algebraic Geometry, Algebra, and Number Theory at the University of Georgia), I.D.S. by the of the Russian Government Grant N 075-15-2019-1926 and I.E.S. by Australian Research Council Grant DP170100786.

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev and I. D. Shkredov, ‘Growth estimates in positive characteristic via collisions’, Intern. Math. Res. Notices, 2017 (2017), 7148–7189.

[2] J. Bourgain, ‘Multilinear exponential sums in prime fields under optimal entropy condition on the sources’, Geom. and Funct. Anal., 18 (2009), 1477–1502.

[3] J. Bourgain, ‘On exponential sums in finite fields’, Bolyai Soc. Math. Stud., 21, János Bolyai Math. Soc., Budapest, 2010, 219–242.

[4] J. Bourgain and M. Z. Garaev, ‘On a variant of sum-product estimates and explicit exponential sum bounds in prime fields’, Math. Proc. Cambridge Phil. Soc., 146 (2009), 1–21.

[5] J. Bourgain and A. Glibichuk, ‘Exponential sum estimates over a subgroup in an arbitrary finite field’, J. d’Analyse Math., 115 (2011), 51–70.

[6] J. Cilleruelo and M. Z. Garaev, ‘Congruences involving product of intervals and sets with small multiplicative doubling modulo a prime and applications’, Math. Proc. Camb. Phil. Soc., 160 (2016), 477–494.

[7] M. Z. Garaev, ‘Sums and products of sets and estimates of rational trigonometric sums in fields of prime order’, Russian Math. Surveys, 65 (2010), 599–658 (Transl. from Uspekhi Mat. Nauk).

[8] B. Kerr and S. Macourt, ‘Multilinear exponential sums with a general class of weights’, Preprint, 2019 (available from http://arxiv.org/abs/1901.00975).

[9] S. Macourt, ‘Incidence results and bounds of trilinear and quadrilinear exponential sums’, SIAM J. Discrete Math., 32 (2018), 815–825.

[10] S. Macourt, ‘Bounds on exponential sums with quadrinomials’, J. Number Theory, 193 (2018), 118–127.

[11] S. Macourt, I. D. Shkredov and I. E. Shparlinski, ‘Multiplicative energy of shifted subgroups and bounds on exponential sums with trinomials in finite fields’, Canad. J. Math., 70 (2018), 1319–1338.

[12] D. A. Mit’kin, ‘Estimation of the total number of the rational points on a set of curves in a simple finite field’, Chebyshevskiy Sbornik, 4 (2003), n 94–102 (in Russian).

[13] A. Mohammadi, ‘Improved bounds on Gauss sums in arbitrary finite fields’, Intern. J. Number Theory, 15 (2019), 2027–2041.
[14] B. Murphy, G. Petridis, O. Roche–Newton, M. Rudnev, and I. D. Shkredov, ‘New results on sum-product type growth over fields’, *Mathematika*, **65** (2019), 588–642. 3, 5, 7, 13

[15] A. Ostafe, ‘Polynomial values in affine subspaces over finite fields’, *J. D’Analyse Math.*, **138** (2019), 49–81. 3

[16] G. Petridis and I. E. Shparlinski, ‘Bounds on trilinear and quadrilinear exponential sums’, *J. d’Analyse Math.*, **138** (2019), 613–641. 2, 11, 12

[17] M. Rudnev, ‘An improved sum-product inequality in fields of prime order’, Int. Math. Res. Not. (IMRN) no. 16, 3693–3705, 2012. 7

[18] I. D. Shkredov, ‘On tripling constant of multiplicative subgroups’, *Integers*, **16** (2016), #A75. 8, 11

[19] I. D. Shkredov, ‘On asymptotic formulae in some sum–product questions’, *Trans. Moscow Math. Soc.*, **79** (2018) 231–281. 2, 4, 7, 11

[20] S. Stevens and F. de Zeeuw, ‘An improved point-line incidence bound over arbitrary fields’, *Bull. London Math. Soc.*, **49** (2017) 842–858. 9

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: s.macourt@unsw.edu.au

Department of Mathematics, University of Georgia, Athens, GA 30602, USA

E-mail address: giorgis.petridis@gmail.com

Steklov Mathematical Institute of Russian Academy of Sciences, ul. Gubkina 8, Moscow, Russia, 119991, Institute for Information Transmission Problems of Russian Academy of Sciences, Bolshoy Karetny Per. 19, Moscow, Russia, 127994, and MIPT, Institutskii per. 9, Dolgoprudnii, Russia, 14170

E-mail address: ilya.shkredov@gmail.com

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au