Canad. J. Math. Vol. 70 (6), 2018 pp. 1319–1338
http://dx.doi.org/10.4153/CJM-2017-044-2

Multiplicative Energy of Shifted Subgroups and Bounds On Exponential Sums with Trinomials in Finite Fields

Simon Macourt, Ilya D. Shkredov, and Igor E. Shparlinski

Abstract. We prove a new bound on collinear triples in subgroups of prime finite fields and use it to give some new bounds on exponential sums with trinomials.

1 Introduction

1.1 Set Up

For a prime p, we use $\mathbb{F}_p$ to denote the finite field of p elements.

For a t-sparse polynomial

$$\Psi(X) = \sum_{i=1}^{t} a_i X^{k_i}$$

with some pairwise distinct positive integer exponents $k_1, \dots, k_t$, coefficients $a_1, \dots, a_t \in \mathbb{F}_p^*$, and a multiplicative character χ of $\mathbb{F}_p^*$, we define the sums

$$S_\chi(\Psi) = \sum_{x \in \mathbb{F}_p^*} \chi(x)\, \mathbf{e}_p(\Psi(x)),$$

where $\mathbf{e}_p(u) = \exp(2\pi i u/p)$ and χ is an arbitrary multiplicative character of $\mathbb{F}_p^*$. Certainly, the most interesting and well-studied special case is when $\chi = \chi_0$ is a principal character. However, most of our results extend to the general case without any loss of strength or complication of the argument, so this is how we present them.

The main challenge here is to estimate these sums better than by the Weil bound

$$|S_\chi(\Psi)| \le \max\{k_1, \dots, k_t\} p^{1/2}$$

(see [36, Appendix 5, Example 12]) by taking advantage of sparsity and of the arithmetic structure of the exponents $k_1, \dots, k_t$.

For monomials $\Psi(X) = aX^k$ (where we can always assume that $k \mid p-1$), the first bound of this type is due to Shparlinski [32], which has then been improved and extended in various directions by Bourgain, Glibichuk, and Konyagin [6], Bourgain [3], Heath-Brown and Konyagin [19], Konyagin [21], Shkredov [27], and Shteinikov [34].

Received by the editors June 19, 2017; revised October 3, 2017.
Published electronically December 20, 2017.
During the preparation of this work, author I. E. S. was supported by the Australian Research Council Grant DP170100786.
AMS subject classification: **11L07**, 11T23.
Keywords: exponential sum, sparse polynomial, trinomial.

Akulinichev [1] gives several bounds on binomials; see also [38]. Cochrane, Coffelt and Pinner, (see [8–13] and references therein) have given a series of other bounds on exponential sums with sparse polynomials, some of which we present in Section 1.2.

We also remark that exponential sums with sparse polynomials and a composite denominator have been studied in [4, 33].

Here we use a slightly different approach to improve some of the previous results. Our approach relies on reducing bounds of exponential sums with sparse polynomials to bounds of weighted multilinear exponential sums of the type considered in [25]. However, instead of applying the results of [25] directly, we first obtain a more precise variant for triple weighted sums over multiplicative subgroups of $\mathbb{F}_p^*$, which could be of independent interest; see Lemma 3.5.

This result rests on an extension of the bound on the number of collinear triples in multiplicative subgroups from [28, Proposition 1] to subgroups of any size; see Theorem 1.2. In turn, this gives a new bound on the multiplicative energy of arbitrary subgroups (see Corollary 4.1) and has several other applications; see Section 4.

Although here we concentrate on the case of trinomials

$$\Psi(X) = aX^k + bX^\ell + cX^m, \tag{1.1}$$

our method works, without any changes, for more general sums with polynomials of the shape

$$\Psi(X) = aX^k + F(X^\ell) + G(X^m)$$

with arbitrary polynomials $F, G \in \mathbb{F}_p[X]$ (uniformly in the degrees of F and G, which essentially means that they can be any functions defined on $\mathbb{F}_p$).

One can certainly use our approach for sums with quadrinomials by reducing it to quadrilinear sums and using our Lemma 3.3 in an appropriate place of the argument of the proof of [25, Theorem 1.4]. Furthermore, using results of [4, 5, 17], one can consider the case of arbitrary sparse polynomials.

The notation $A \ll B$ is equivalent to $|A| \le c|B|$ for some constant c, which throughout the paper may only depend on the number of monomials in the sparse polynomials under considerations.

1.2 Previous Results

We compare our results for trinomials (1.1) with the estimates of Cochrane, Coffelt, and Pinner [8, Equation (1.6)]

$$S_\chi(\Psi) \ll \Big(\frac{k\ell m}{\max\{k,\ell,m\}}\Big)^{1/4} p^{7/8}, \tag{1.2}$$

which is nontrivial for $\min\{k\ell, km, \ell m\} < p^{1/2}$, and of Cochrane and Pinner [10, Theorem 1.1]:

$$S_\chi(\Psi) \ll (k\ell m)^{1/9} p^{5/6}, \tag{1.3}$$

which is nontrivial for $k\ell m < p^{3/2}$.

We also recall the bound of Cochrane, Coffelt, and Pinner [9, Corollary 1.1]

$$S_\chi(\Psi) \ll D^{1/2} p^{7/8} + (k\ell m)^{1/4} p^{5/8}, \tag{1.4}$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

where $D = \gcd(k, \ell, m, p-1)$, which is nontrivial for $k\ell m < p^{3/2}$ and $D < p^{1/4}$.

1.3 New Results

The following quantity is one of our main objects of study.

Definition 1.1 (Collinear triples) For sets $\mathcal{U}_1, \mathcal{U}_2 \subseteq \mathbb{F}_p^*$ and elements $\lambda_1, \lambda_2 \in \mathbb{F}_p^*$, we define $\mathrm{T}_{\lambda_1,\lambda_2}(\mathcal{U}_1, \mathcal{U}_2)$ to be the number of solutions to

$$\frac{u_1 - \lambda_1 v_1}{u_1 - \lambda_1 w_1} = \frac{u_2 - \lambda_2 v_2}{u_2 - \lambda_2 w_2}, \qquad u_i, v_i, w_i \in \mathcal{U}_i, \ i = 1, 2. \tag{1.5}$$

We also set $\mathrm{T}(\mathcal{U}) = \mathrm{T}_{1,1}(\mathcal{U}, \mathcal{U})$.

As relation (2.1) shows, the triples (u_i, v_i, w_i), $i = 1, 2$ satisfying (1.5) define their collinear points. Recent results on the quantity $\mathrm{T}(\mathcal{U})$ for an arbitrary set $\mathcal{U}$ can be found in [24], where, in particular, the bound

$$\mathrm{T}(\mathcal{U}) = \frac{|\mathcal{U}|^6}{p} + O(p^{1/2}|\mathcal{U}|^{7/2})$$

is given. This bound was generalised in [22] as

$$\mathrm{T}_{\lambda_1,\lambda_2}(\mathcal{U}_1, \mathcal{U}_2) = \frac{|\mathcal{U}_1|^3|\mathcal{U}_2|^3}{p} + O\left(p^{1/2}|\mathcal{U}_1|^{3/2}|\mathcal{U}_2|^2 + |\mathcal{U}_1|^3|\mathcal{U}_2|\right), \tag{1.6}$$

provided that $|\mathcal{U}_1| \ge |\mathcal{U}_2|$.

Note that in (1.5), as well as in all similar expressions of this type, we consider only the values of the variables for which these expressions are defined (that is, $u_i \ne \lambda_i w_i$, $i = 1, 2$ in (1.5)). We begin by providing a new result on the number of collinear triples in subgroups. More generally, for a multiplicative subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$, we define $\mathrm{T}_\lambda(\mathcal{G}) = \mathrm{T}_{1,\lambda}(\mathcal{G})$, which is our main object of study.

Theorem 1.2 *Let $\mathcal{G}$ be a multiplicative subgroup of $\mathbb{F}_p^*$. Then for any $\lambda \in \mathbb{F}_p^*$, we have*

$$\mathrm{T}_\lambda(\mathcal{G}) - \frac{|\mathcal{G}|^6}{p} \ll \begin{cases} p^{1/2}|\mathcal{G}|^{7/2} & \text{if } |\mathcal{G}| \ge p^{2/3}, \\ |\mathcal{G}|^5 p^{-1/2} & \text{if } p^{2/3} > |\mathcal{G}| \ge p^{1/2}\log p, \\ |\mathcal{G}|^4 \log|\mathcal{H}| & \text{if } |\mathcal{G}| < p^{1/2}\log p. \end{cases}$$

Remark 1.3 Theorem 1.2 is new only for subgroups of intermediate size $p^{2/3} > |\mathcal{G}| > p^{1/2}$; otherwise, it is contained in [28, Proposition 1] (see also Lemma 2.6) or in the bound [22, (1.6)].

Remark 1.4 The method of proof of Theorem 1.2 also works without any changes for $\mathrm{T}_{\lambda,\mu}(\mathcal{G}, \mathcal{H})$ with two multiplicative subgroups, similarly to Lemma 2.6. However, for subgroups of significantly different sizes, the optimisation part becomes rather tedious.

We use Theorem 1.2 to obtain the following new bound on trinomial sums.

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

Theorem 1.5 *Let $\Psi(X)$ be a trinomial of the form (1.1) with $a, b, c \in \mathbb{F}_p^*$. Define*

$$d = \gcd(k, p-1), \qquad e = \gcd(\ell, p-1), \qquad f = \gcd(m, p-1),$$
$$g = \frac{d}{\gcd(d, f)}, \qquad h = \frac{e}{\gcd(e, f)}.$$

Suppose $f \ge g \ge h$; then

$$S_\chi(\Psi) \ll \begin{cases} p^{7/8} f^{1/8} & \text{if } h \ge (p \log p)^{1/2}, \\ p^{15/16} (f/h)^{1/8} (\log p)^{1/16} & \text{if } g \ge (p \log p)^{1/2} > h, \\ p (f/gh)^{1/8} (\log p)^{1/8} & \text{if } g < (p \log p)^{1/2}. \end{cases}$$

Note that the assumption $f \ge g \ge h$ of Theorem 1.5 does not present any additional restrictions on the class of polynomials to which it applies as the roles of k, ℓ, and m are fully symmetric: if $h > g$, say, one can simply interchange g and h in the bound.

We observe that the bound of Theorem 1.5 does not directly depend on the size of the exponents k, ℓ, and m but rather on various greatest common divisors. In particular, it is strongest for large d and e and small greatest common divisors f, $\gcd(d, f)$, and $\gcd(e, f)$. Furthermore, it may remain nontrivial even for polynomials of very large degrees, while the bounds (1.2), (1.3), and (1.4) all become trivial for trinomials of large degree. Thus, it is easy to give various families of parameters where Theorem 1.5 improves the bounds (1.2), (1.3), and (1.4) simultaneously. For example, we assume that $f > d > e$ are relatively prime positive integers with, say, $p^\delta < f < (de)^{1-\delta}$ for some fixed real $\delta > 0$. Then $g = d$ and $h = e$, and we also have $d < p^{1/2}$, $e < p^{1/3}$. Hence, the bound of Theorem 1.5 becomes

$$S_\chi(\Psi) \ll p(f/gh)^{1/8+o(1)} = p(f/de)^{1/8+o(1)},$$

which always gives a power saving against the trivial bound. On the other hand, choosing k, ℓ, and m as large multiples of d, e, and f, respectively, say, with $k, m, \ell \ge p^{1/2+\delta}$, we see that all bounds from Section 1.2, and of course the Weil bound, are trivial.

We also give further applications of Theorem 1.2 to some additive problems with multiplicative subgroups of $\mathbb{F}_p^*$ in Section 4. In particular, in Corollary 4.4 we consider a modular version of the Romanoff theorem and show that for almost all primes p, any residue class modulo p can be represented as a sum of a prime $\ell < p$ and three powers of any fixed integer $g \ge 2$. We recall that the classical result of Romanoff [26] asserts that for any fixed integer $g \ge 2$ a positive proportion of integers can be written in the form $\ell + g^k$, with some prime ℓ and nonnegative integer k. By a result of Crocker [14], there are infinitely many positive integers not of the form $\ell + 2^k + 2^m$. The case of three powers of 2 or any other base $g > 2$ is widely open.

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

2 Collinear Triples

2.1 Preliminaries

We require some previous results. We note that we use Lemma 2.1 only for $\mathcal{G} = \mathcal{H}$; however, we present it and some other results in full generality, as we believe they may result in several other applications, and this deserves to be better known.

The first one is a result of Mit'kin [23, Theorem 2] extending that of Heath-Brown and Konyagin [19, Lemma 5]; see also [21, 31] for further generalisations.

Lemma 2.1 *Let $\mathcal{G}$ and $\mathcal{H}$ be subgroups of $\mathbb{F}_p^*$ and let $\mathcal{M}_\mathcal{G}$ and $\mathcal{M}_\mathcal{H}$ be two complete sets of distinct coset representatives of $\mathcal{G}$ and $\mathcal{H}$ in $\mathbb{F}_p^*$. For an arbitrary set $\Theta \subseteq \mathcal{M}_\mathcal{G} \times \mathcal{M}_\mathcal{H}$ such that*

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

we have

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

Note that there is a natural bijection between $\mathcal{M}_\mathcal{G}$, $\mathcal{M}_\mathcal{H}$ and some subsets of the factor groups $\mathbb{F}_p^*/\mathcal{G}$ and $\mathbb{F}_p^*/\mathcal{H}$. So, one can think of Θ as a subset of $\mathbb{F}_p^*/\mathcal{G} \times \mathbb{F}_p^*/\mathcal{H}$.

Clearly, the trivial bound on the sum of Lemma 2.1 is

$$\sum_{(u,v)\in\Theta} \left|\left\{(x,y) \in \mathcal{G}\times\mathcal{H} : ux + vy = 1\right\}\right| \ll \min\{|\mathcal{G}|, |\mathcal{H}|\}|\Theta|.$$

Hence if, for example, $\mathcal{G} = \mathcal{H}$, then Lemma 2.1 always significantly improves this bound.

Given a line

$$\ell_{a,b} = \{(x,y) \in \mathbb{F}_p^2 : y = ax + b\}$$

for some pair $(a,b) \in \mathbb{F}_p^2$ and sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$, we let

$$\iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b}) = |\ell_{a,b} \cap (\mathcal{A}\times\mathcal{B})|.$$

The following elementary identities are well known and no doubt have appeared, implicitly and explicitly, in a number of works.

Lemma 2.2 *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ and $\lambda, \mu \in \mathbb{F}_p^*$. Then*

$$\sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b}) = \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b}) = p|\mathcal{A}||\mathcal{B}|,$$

$$\sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b}) = |\mathcal{A}|^2|\mathcal{B}|^2 - |\mathcal{A}||\mathcal{B}|^2 + p|\mathcal{A}||\mathcal{B}|.$$

Proof The first relation is obvious, as for every $(x,y,a) \in \mathcal{A}\times\mathcal{B}\times\mathbb{F}_p$, there is a unique $b = y - ax$ counted in that sum.

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

For the second sum, we write

$$\sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b}) = \sum_{(u,v,x,y)\in\mathcal{A}\times\mathcal{B}\times\mathcal{A}\times\mathcal{B}} \left|\{(a,b)\in\mathbb{F}_p^2 : v = au+b,\ y = \lambda ax + \mu b\}\right|.$$

We now note that the $|\mathcal{A}||\mathcal{B}|$ quadruples $(u,v,x,y)\in\mathcal{A}\times\mathcal{B}\times\mathcal{A}\times\mathcal{B}$ with

$$(u,v) = (\lambda\mu^{-1}x, \mu^{-1}y)$$

define exactly p pairs $(a,b) = (a, v-au) \in \mathbb{F}_p^2$ as above. Furthermore, the $|\mathcal{A}||\mathcal{B}|\,(|\mathcal{B}|-1)$ quadruples $(u,v,x,y)\in\mathcal{A}\times\mathcal{B}\times\mathcal{A}\times\mathcal{B}$ with $u = \lambda\mu^{-1}x$ but $v \ne \mu^{-1}y$ do not define any pairs (a,b) as above. The remaining

$$|\mathcal{A}|^2|\mathcal{B}|^2 - |\mathcal{A}||\mathcal{B}|\big(|\mathcal{B}|-1\big) - |\mathcal{A}||\mathcal{B}| = |\mathcal{A}|^2|\mathcal{B}|^2 - |\mathcal{A}||\mathcal{B}|^2$$

pairs (including the one with $u \ne \lambda\mu^{-1}x$ but $v = \mu^{-1}y$) define one pair $(a,b)\in\mathbb{F}_p^2$ each as above, which concludes the proof. ∎

Using Lemma 2.2 with $\lambda = \mu = 1$, we immediately derive the following result.

Corollary 2.3 *Let $\mathcal{A}\subseteq\mathbb{F}_p$. Then*

$$\sum_{(a,b)\in\mathbb{F}_p^2} \Big(\iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b}) - \frac{|\mathcal{A}||\mathcal{B}|}{p}\Big)^2 \le p|\mathcal{A}||\mathcal{B}|.$$

We now link the number of collinear triples $\mathrm{T}_{\lambda,\mu}(\mathcal{A},\mathcal{B})$ with the quantities $\iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})$.

Lemma 2.4 *Let $\mathcal{A},\mathcal{B}\subseteq\mathbb{F}_p$ and $\lambda,\mu\in\mathbb{F}_p^*$. Then*

$$\mathrm{T}_{\lambda,\mu}(\mathcal{A},\mathcal{B}) = \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b})^2 + O\big(|\mathcal{A}|^2|\mathcal{B}|^2\big).$$

Proof Transforming equation (1.5) into

$$\frac{u_1-\lambda v_1}{u_2-\mu v_2} = \frac{u_1-\lambda w_1}{u_2-\mu w_2}, \qquad u_1,v_1,w_1\in\mathcal{A}, u_2,v_2,w_2\in\mathcal{B},$$

we introduce an error of magnitude $O(|\mathcal{A}|^2|\mathcal{B}|^2)$ (coming from different pairs of variables which must be distinct). Then collecting, for every $a\in\mathbb{F}_p$, the solutions with

$$\frac{u_1-\lambda v_1}{u_2-\mu v_2} = \frac{u_1-\lambda w_1}{u_2-\mu w_2} = a,$$

we derive

$$u_1 - au_2 = \lambda v_1 - a\mu v_2 = \lambda w_1 - a\mu w_2.$$

We now denote this common value by b and observe that for any $(a,b)\in\mathbb{F}_p^2$, there are $\iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b})^2$ solutions to

$$u_1 - au_2 = \lambda v_1 - a\mu v_2 = \lambda w_1 - a\mu w_2 = b. \tag{2.1}$$

Summing over all pairs $(a,b)\in\mathbb{F}_p^2$, we obtain the result. ∎

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

Corollary 2.5 *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ and $\lambda, \mu \in \mathbb{F}_p^*$. Then*

$$\mathrm{T}_{\lambda,\mu}(\mathcal{A},\mathcal{B}) - \frac{|\mathcal{A}|^3|\mathcal{B}|^3}{p} = \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\Big(\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{|\mathcal{A}||\mathcal{B}|}{p}\Big)^2 + O(|\mathcal{A}|^2|\mathcal{B}|^2).$$

Proof Using the identity $X^2 = (X-Y)^2 + 2XY - Y^2$ with $X = \iota_{\mathcal{A},\mathcal{B}}\left(\ell_{\lambda a,\mu b}\right)$ and $Y = |\mathcal{A}||\mathcal{B}|/p$, we see that

$$\sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b})^2 = \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\Big(\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{|\mathcal{A}|^2}{p}\Big)^2 + R_1 - R_2, \tag{2.2}$$

where

$$R_1 = 2\frac{|\mathcal{A}||\mathcal{B}|}{p} \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b}),$$

$$R_2 = \frac{|\mathcal{A}|^2|\mathcal{B}|^2}{p^2} \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b}).$$

By Lemma 2.2, after simple calculations, we have

$$R_1 - R_2 = 2\big(|\mathcal{A}|^2|\mathcal{B}|^2 - |\mathcal{A}|^2|\mathcal{B}|^3/p\big) \ll |\mathcal{A}|^2|\mathcal{B}|^2.$$

Combining this with (2.2) yields

$$\sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}\left(\ell_{a,b}\right)\iota_{\mathcal{A},\mathcal{B}}\left(\ell_{\lambda a,\mu b}\right)^2 = \frac{|\mathcal{A}|^3|\mathcal{B}|^3}{p} + \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b})\Big(\iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b}) - \frac{|\mathcal{A}|^2}{p}\Big)^2 + O\big(|\mathcal{A}|^2|\mathcal{B}|^2\big).$$

Hence, using Lemma 2.4, we obtain the result. ∎

Given two sets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p$, we define $\mathrm{E}^{\times}(\mathcal{U},\mathcal{V})$ to be the *multiplicative energy* of $\mathcal{U}$ and $\mathcal{V}$, that is, the number of solutions to

$$u_1v_1 = u_2v_2, \qquad u_1,u_2 \in \mathcal{U},\ v_1,v_2 \in \mathcal{V}.$$

For $\mathcal{U} = \mathcal{V}$, we also write $\mathrm{E}^{\times}(\mathcal{U}) = \mathrm{E}^{\times}(\mathcal{U},\mathcal{U})$. It is easy to see that for any subgroup of $\mathcal{G},\mathcal{H} \subseteq \mathbb{F}_p^*$ and $\lambda,\mu \in \mathbb{F}_p^*$, we have

$$\begin{aligned}\mathrm{T}_{\lambda,\mu}(\mathcal{G},\mathcal{H}) &= \sum_{(g,h)\in\mathcal{G}\times\mathcal{H}} \mathrm{E}^{\times}(\mathcal{G}-\lambda g,\mathcal{H}-\mu h) + O\big(|\mathcal{G}|^3|\mathcal{H}|\big)\\ &= |\mathcal{G}||\mathcal{H}|\mathrm{E}^{\times}(\mathcal{G}-\lambda,\mathcal{H}-\mu) + O\big(|\mathcal{G}|^3|\mathcal{H}|\big),\end{aligned} \tag{2.3}$$

where the error term $O(|\mathcal{G}|^3|\mathcal{H}|)$ (which is obviously negative) accounts for zero values of the linear forms in the definition of $\mathrm{T}_{\lambda,\mu}(\mathcal{G},\mathcal{H})$.

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

Finally, we need the following bound for small subgroups, which is a slightly simplified form of [28, Proposition 1] combined with (2.3).

Lemma 2.6 *Let $\mathcal{G}$ be a subgroup of $\mathbb{F}_p^*$ with $|\mathcal{G}| \ge |\mathcal{H}|$ and $|\mathcal{G}||\mathcal{H}| < p$. Then*

$$\mathrm{T}_{\lambda,\mu}(\mathcal{G},\mathcal{H}) \ll |\mathcal{G}|^3|\mathcal{H}|\log|\mathcal{G}|.$$

2.2 Initial Reductions

The argument below follows [28, 29]. First, note that Lemma 2.6 implies the required result provided $|\mathcal{G}||\mathcal{H}| < p$, while the bound (1.6) implies it for $|\mathcal{G}| \ge p^{2/3}$.

So it remains to consider the case $p^{2/3} > |\mathcal{G}| > p^{1/2}$.

Let $\Delta \ge 3$ be a parameter to be chosen later. Using Corollaries 2.3 and 2.5, we obtain

$$\mathrm{T}_\lambda(\mathcal{G}) - \frac{|\mathcal{G}|^6}{p} \ll |\mathcal{G}|^4 + \Delta|\mathcal{G}|^2 p + W, \tag{2.4}$$

where

$$W = \sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ \iota_{\mathcal{G}}(\ell_{a,b})>\Delta}} \iota_{\mathcal{G}}(\ell_{a,b})\Big(\iota_{\mathcal{G}}(\ell_{a,\lambda b}) - \frac{|\mathcal{G}|^2}{p}\Big)^2.$$

Clearly, the contribution to W from lines with $ab = 0$ is at most $|\mathcal{G}|^4$, as in this case $\iota_{\mathcal{G}}(\ell_{a,b}) = 0$, unless $a \in \mathcal{G}$ or $b \in \mathcal{G}$, in which case $\iota_{\mathcal{G}}(\ell_{a,b}) = |\mathcal{G}|$. Therefore,

$$\sum_{\substack{(a,b)\in\mathbb{F}_p^2 \\ ab=0}} \iota_{\mathcal{G}}(\ell_{a,b})\Big(\iota_{\mathcal{G}}(\ell_{a,\lambda b}) - \frac{|\mathcal{G}|^2}{p}\Big)^2 = O\big(|\mathcal{G}|^4\big).$$

Thus,

$$W = W^* + O\big(|\mathcal{G}|^4\big), \tag{2.5}$$

where

$$W^* = \sum_{\substack{(a,b)\in(\mathbb{F}_p^*)^2 \\ \iota_{\mathcal{G}}(\ell_{a,b})>\Delta}} \iota_{\mathcal{G}}(\ell_{a,b})\Big(\iota_{\mathcal{G}}(\ell_{a,\lambda b}) - \frac{|\mathcal{G}|^2}{p}\Big)^2,$$

which is the sum we now consider.

Returning to (1.5), we see that the quantity $\mathrm{T}_\lambda(\mathcal{G})$, up to the error $O(|\mathcal{G}|^4)$ (which can be absorbed in the same error term that is already present in (2.4)), is equal to the number of solutions of the equation

$$(u_1 - v_1)(u_2 - \lambda w_2) = (u_1 - w_1)(u_2 - \lambda v_2) \ne 0,$$
$$u_i, v_i, w_i \in \mathcal{G}, \quad i = 1, 2.$$

2.3 Sets Θ_τ and $\mathcal{Q}_\tau$

As before, let $\mathcal{M}_{\mathcal{G}}$ be a set of distinct coset representatives of $\mathcal{G}$ in $\mathbb{F}_p^*$. Take another parameter $\tau \ge \Delta$ and put

$$\Theta_\tau = \big\{(\alpha,\beta) \in \mathcal{M}_{\mathcal{G}}^2 : \big|\big\{(x,y) \in \mathcal{G}^2 : \alpha x + \beta y = 1\big\}\big| \ge \tau\big\}.$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

In other words, Θ_τ is the set of $(\alpha, \beta) \in \mathcal{M}_{\mathcal{G}}^2$ for which the lines

$$\mathcal{L}_{\alpha,\beta} = \left\{ (x, y) \in \mathbb{F}_p^2 : \alpha x + \beta y = 1 \right\} = \ell_{-\alpha\beta^{-1},\beta^{-1}} \tag{2.6}$$

have the intersection with $\mathcal{G}^2$ of size at least $\iota_{\mathcal{G}}(\ell_{-\alpha\beta^{-1},\beta^{-1}}) \geq \tau$. In particular,

$$\Theta_\tau = \left\{ (\alpha, \beta) \in \mathcal{M}_{\mathcal{G}}^2 : \iota_{\mathcal{G}}(\mathcal{L}_{\alpha,\beta}) \geq \tau \right\}. \tag{2.7}$$

By Lemma 2.1, we have $|\Theta_\tau|\tau \ll (|\mathcal{G}||\Theta_\tau|)^{2/3}$ provided

$$|\mathcal{G}|^4|\Theta_\tau| < p^3, \tag{2.8}$$

$$|\Theta_\tau| \leq |\mathcal{G}|^2. \tag{2.9}$$

We also define the set

$$\mathcal{Q}_\tau = \left\{ (\alpha, \beta) \in (\mathbb{F}_p^*)^2 : \iota_{\mathcal{G}}(\mathcal{L}_{\alpha,\beta}) \geq \tau \right\}. \tag{2.10}$$

Comparing (2.7) and (2.10), we see that we can think of Θ_τ as of an union of cosets $\mathcal{Q}_\tau/\mathcal{G}$. Clearly, we have

$$|\mathcal{Q}_\tau| = |\mathcal{G}|^2|\Theta_\tau| \ll |\mathcal{G}|^4\tau^{-3} \tag{2.11}$$

provided conditions (2.8) and (2.9) are satisfied.

Condition (2.9) is trivial to verify. Indeed, since $|\mathcal{G}|^2 > p$, we have

$$|\Theta_\tau| \leq |\mathcal{M}_{\mathcal{G}}|^2 = (p-1)^2/|\mathcal{G}|^2 \leq |\mathcal{G}|^2,$$

and thus (2.9) holds.

We now show that condition (2.8) also holds for the choice

$$\Delta = c|\mathcal{G}|^3 p^{-3/2}, \tag{2.12}$$

with a sufficiently large constant c (recalling that $|\mathcal{G}| > p^{1/2}$ we see that the condition $\Delta \geq 3$ is satisfied).

Lemma 2.7 *For Δ given by (2.12), the bound (2.8) holds.*

Proof Suppose, to the contrary, that

$$|\Theta_\tau| > p^3|\mathcal{G}|^4. \tag{2.13}$$

Whence, the number of incidences between points of $\mathcal{P} = \mathcal{G}^2$ and the lines $\mathcal{L}_{\alpha,\beta}$ as above with $(\alpha, \beta) \in \mathcal{Q}_\tau$ is at least

$$|\mathcal{Q}_\tau|\tau = |\mathcal{G}|^2|\Theta_\tau|\tau > p^3|\mathcal{G}|^{-2}\Delta. \tag{2.14}$$

On the other hand, by a classical result that holds over any field (see, for example [7, Corollary 5.2] or [37, Exercise 8.2.1]), the number of incidences for any set of points $\mathcal{P}$ and a set of lines $\mathcal{Q}_\tau$ is at most $|\mathcal{Q}_\tau|^{1/2}|\mathcal{P}| + |\mathcal{Q}_\tau|$. Hence,

$$|\mathcal{Q}_\tau|\tau \leq |\mathcal{Q}_\tau|^{1/2}|\mathcal{P}| + |\mathcal{Q}_\tau|, \tag{2.15}$$

and we obtain

$$|\mathcal{Q}_\tau|\tau^2 \ll |\mathcal{P}|^2 = |\mathcal{G}|^4. \tag{2.16}$$

Combining (2.14) and (2.16), we derive

$$p^3|\mathcal{G}|^{-2}\Delta < |\mathcal{Q}_\tau|\tau \ll |\mathcal{G}|^4\tau^{-1} \leq |\mathcal{G}|^4\Delta^{-1}. \tag{2.17}$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

Recalling that $|\mathcal{G}| \ge p^{1/2}$, we see that for Δ given by (2.12) with a sufficiently large constant c, the inequalities (2.17) are impossible, which also shows that our assumption (2.13) is false, and this concludes the proof. ∎

2.4 Concluding the Proof of Theorem 1.2

We now define

$$\mathcal{R}_\tau = \left\{ (\alpha,\beta) \in (\mathbb{F}_p^*)^2 : \max\left\{ \iota_{\mathcal{G}}(\mathcal{L}_{\alpha,\beta}), \iota_{\mathcal{G}}(\mathcal{L}_{\alpha,\lambda\beta}) \right\} \ge \tau \right\}.$$

By Lemma 2.7, for the choice (2.12) of Δ, we have the desired condition (2.8) for any $\tau \ge \Delta$. Hence, the bound (2.11) also implies that

$$|\mathcal{R}_\tau| = |\mathcal{G}|^2 |\Theta_\tau| \ll |\mathcal{G}|^4 \tau^{-3}. \tag{2.18}$$

We see from (2.6) that there is a one-to-one correspondence between the lines $\ell_{a,b}$, $(a,b) \in \left(\mathbb{F}_p^*\right)^2$ and the lines $\mathcal{L}_{\alpha,\beta}$, $(\alpha,\beta) \in \left(\mathbb{F}_p^*\right)^2$. We now define

$$\tau_j = e^j \Delta, \qquad j = 0, 1, \ldots, J,$$

where $J = \lceil \log(|\mathcal{G}|/\Delta) \rceil$. Note that due to the choice of Δ and the condition $|\mathcal{G}| \ge p^{1/2}$, we have

$$\tau_j \ge \tau_0 = \Delta \gg |\mathcal{G}|^3 p^{-3/2} \ge |\mathcal{G}|^2/p, \qquad j = 0, 1, \ldots, J.$$

Then, recalling also the bound (2.18), we conclude that the contribution to W^* from the lines with $\tau_{j+1} \ge \iota_{\mathcal{G}}(\ell_{a,b}) > \tau_j$ is bounded by

$$|\mathcal{Q}_{\tau_j}| \tau_{j+1} \left(\tau_{j+1} + |\mathcal{G}|^2/p \right)^2 \ll |\mathcal{Q}_{\tau_j}| \tau_{j+1}^3 \ll |\mathcal{G}|^4. \tag{2.19}$$

Summing up (2.19) we obtain

$$W^* \ll J|\mathcal{G}|^4 \ll |\mathcal{G}|^4 \log|\mathcal{G}|.$$

Substituting this bound in (2.5) and combining it with (2.4), we obtain

$$\mathrm{T}_\lambda(\mathcal{G}) = \frac{|\mathcal{G}|^6}{p} + O\left(|\mathcal{G}|^5 p^{-1/2} + |\mathcal{G}|^4 \log|\mathcal{G}| \right)$$

in the range $p^{2/3} \ge |\mathcal{G}| \ge p^{1/2}$, which concludes the proof. ∎

Remark 2.8 In principle, a stronger version of the classical incidence bound that is used in (2.15) may lead to improvements of Theorem 1.2. However, the range where such improvements are known is far away from the range that appears in our applications; see [35].

3 Trinomial Sums

3.1 Preliminaries

We recall the following classical bound of bilinear sums, see, for example, [17, Lemma 4.1].

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

Lemma 3.1 *For any sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$ and any $\alpha = (\alpha_x)_{x\in\mathcal{X}}$, $\beta = (\beta_y)_{y\in\mathcal{Y}}$, with*

$$\max_{x\in\mathcal{X}} |\alpha_x| \le 1 \qquad \text{and} \qquad \max_{y\in\mathcal{Y}} |\beta_y| \le 1,$$

we have

$$\Big| \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \alpha_x \beta_y \, \mathbf{e}_p(xy) \Big| \le \sqrt{p|X||Y|}.$$

Definition 3.2 (Ratios of differences) For a set $\mathcal{U} \subseteq \mathbb{F}_p^*$, we define $D_\times(\mathcal{U})$ to be the number of solutions of

$$(u_1 - v_1)(u_2 - v_2) = (u_3 - v_3)(u_4 - v_4), \qquad u_i, v_i \in \mathcal{U}, \ i = 1, 2, 3, 4.$$

As before, we define $\mathrm{T}(\mathcal{U})$ to be the number of solutions to (1.5). We now recall the following bound from [25, Lemma 2.7].

Lemma 3.3 *For any set $\mathcal{U} \subseteq \mathbb{F}_p^*$ with $|\mathcal{U}| = U$, we have*

$$D_\times(\mathcal{U}) \ll U^2 \mathrm{T}(\mathcal{U}) + U^6.$$

Combining Lemma 3.3 with Theorem 1.2, we obtain

$$D_\times(\mathcal{G}) \ll \frac{|\mathcal{G}|^8}{p} + \begin{cases} p^{1/2}|\mathcal{G}|^{11/2} & \text{if } |\mathcal{G}| \ge p^{2/3}, \\ |\mathcal{G}|^7 p^{-1/2} & \text{if } p^{2/3} > |\mathcal{G}| \ge p^{1/2}\log p, \\ |\mathcal{G}|^6 \log|\mathcal{G}| & \text{if } |\mathcal{G}| < p^{1/2}\log p. \end{cases}$$

Since for $|\mathcal{G}| \ge (p\log p)^{1/2}$ the first term dominates, this simplifies as the following corollary.

Corollary 3.4 *For a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$, we have*

$$D_\times(\mathcal{G}) \ll \begin{cases} |\mathcal{G}|^8 p^{-1} & \text{if } |\mathcal{G}| \ge (p\log p)^{1/2}, \\ |\mathcal{G}|^6 \log|\mathcal{G}| & \text{if } |\mathcal{G}| < (p\log p)^{1/2}. \end{cases}$$

Substituting Corollary 3.4 into the proof of [25, Theorem 1.3], we obtain the following result for trilinear sums over subgroups, which improves its general bound.

Lemma 3.5 *For any multiplicative subgroups $\mathcal{F}, \mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_p^*$ of cardinalities F, G, H, respectively, with $F \ge G \ge H$ and weights $\rho = (\rho_{u,v})$, $\sigma = (\sigma_{u,w})$ and $\tau = (\tau_{v,w})$ with*

$$\max_{(u,v)\in\mathcal{F}\times\mathcal{G}} |\rho_{u,v}| \le 1, \qquad \max_{(u,w)\in\mathcal{F}\times\mathcal{H}} |\sigma_{u,w}| \le 1, \qquad \max_{(v,w)\in\mathcal{G}\times\mathcal{H}} |\tau_{v,w}| \le 1,$$

for the sum

$$T = \sum_{u\in\mathcal{F}} \sum_{v\in\mathcal{G}} \sum_{w\in\mathcal{H}} \rho_{u,v}\sigma_{u,w}\tau_{v,w} \, \mathbf{e}_p(auvw),$$

we have

$$T \ll \begin{cases} F^{7/8}GH & \text{if } H \ge (p\log p)^{1/2}, \\ p^{1/16}F^{7/8}GH^{7/8}(\log p)^{1/16} & \text{if } G \ge (p\log p)^{1/2} > H, \\ p^{1/8}F^{7/8}G^{7/8}H^{7/8}(\log p)^{1/8} & \text{if } G < (p\log p)^{1/2}, \end{cases}$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

uniformly over $a \in \mathbb{F}_p^*$.

Proof We see from [25, Equation (3.8)] that

$$T^8 \ll pF^7G^4H^4K + F^8G^8H^6,$$

where K is the number of solutions to the equation

$$(u_1 - u_2)(w_1 - w_2) = (u_3 - u_4)(w_3 - w_4) \neq 0,$$
$$(u_i, w_i) \in \mathcal{G} \times \mathcal{H}, \quad i = 1, 2, 3, 4.$$

As in the proof of [25, Theorem 1.3], expressing K via multiplicative character sums and using the Cauchy inequality, we obtain $K^2 \le D_\times(\mathcal{G})D_\times(\mathcal{H})$. Applying Corollary 3.4, instead of [25, Equation 3.9], we now obtain

$$K \ll \begin{cases} G^4H^4/p & \text{if } H \ge (p\log p)^{1/2}, \\ G^4H^3p^{-1/2}(\log p)^{1/2} & \text{if } G \ge (p\log p)^{1/2} > H, \\ (GH)^3 \log p & \text{if } G < (p\log p)^{1/2}. \end{cases}$$

We now deal with the three cases separately.

For $H \ge (p\log p)^{1/2}$, we have

$$T^8 \ll F^7G^8H^8 + F^8G^8H^6.$$

Since $F < p < H^2$, the first term dominates, and we obtain

$$T \ll F^{7/8}GH. \tag{3.1}$$

For $G \ge (p\log p)^{1/2} > H$, we have

$$T^8 \ll p^{1/2}F^7G^8H^7(\log p)^{1/2} + F^8G^8H^6$$

or

$$T \ll p^{1/16}F^{7/8}GH^{7/8}(\log p)^{1/16} + FGH^{3/4}. \tag{3.2}$$

The first term of (3.2) dominates for $p^{1/2} \ge F/H$.

We now note that by Lemma 3.1 and the trivial bound for the sum over $\mathcal{H}$, we also have

$$T \ll p^{1/2}F^{1/2}G^{1/2}H. \tag{3.3}$$

Furthermore, since for $F > p^{1/2}H$ and $G > p^{1/2}$, we have

$$p^{1/2}F^{1/2}G^{1/2}H = p^{1/16}F^{7/8}GH^{7/8}\Big(\frac{p^{7/2}H}{F^3G^4}\Big)^{1/8}$$
$$< p^{1/16}F^{7/8}GH^{7/8}\Big(\frac{p^3}{F^2G^4}\Big)^{1/8} < p^{1/16}F^{7/8}GH^{7/8},$$

we see that for $G \ge (p\log p)^{1/2} > H$ the bound (3.2) simplifies as

$$T \le p^{1/16}F^{7/8}GH^{7/8}(\log p)^{1/16}. \tag{3.4}$$

For $G < (p\log p)^{1/2}$, we have

$$T^8 \ll pF^7G^7H^7\log p + F^8G^8H^6$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

or

$$T \ll p^{1/8}F^{7/8}G^{7/8}H^{7/8}\,(\log p)^{1/8} + FGH^{3/4}. \tag{3.5}$$

The first term of (3.5) dominates for $pH \geq FG$. Otherwise, that is, for $pH < FG$, we have

$$\begin{aligned} p^{1/2}F^{1/2}G^{1/2}H &= p^{1/8}F^{7/8}G^{7/8}H^{7/8}\Big(\frac{p^3H}{F^3G^3}\Big)^{1/8} \\ &< p^{1/8}F^{7/8}G^{7/8}H^{7/8}\Big(\frac{1}{H^2}\Big)^{1/8} \leq p^{1/8}F^{7/8}G^{7/8}H^{7/8}. \end{aligned}$$

Thus, using (3.3) we see that the bound (3.5) simplifies as

$$T \leq p^{1/8}F^{7/8}G^{7/8}H^{7/8}\,(\log p)^{1/8}. \tag{3.6}$$

Combining (3.1), (3.4), and (3.6), we complete the proof. ∎

Clearly, the bound of Lemma 3.5 is nontrivial when F, G and H are all a little larger than $p^{1/3}$. More formally, for any $\varepsilon > 0$ there exists some $\delta > 0$ such that if $F \geq G \geq H \geq p^{1/3+\varepsilon}$, then the exponential sums of Lemma 3.5 are bounded by $O\left(FGHp^{-\delta}\right)$.

3.2 Proof of Theorem 1.5

Let $\mathcal{G}_d$ and $\mathcal{G}_e$ be the subgroups of $\mathbb{F}_p^*$ formed by the elements of orders dividing d and e, respectively.

We have

$$\begin{aligned} S_\chi(\Psi) &= \frac{1}{de}\sum_{y\in\mathcal{G}_d}\sum_{z\in\mathcal{G}_e}\sum_{x\in\mathbb{F}_p^*}\chi(xyz)\,\mathbf{e}_p\big(\Psi(xyz)\big) \\ &= \frac{1}{de}\sum_{x\in\mathbb{F}_p^*}\sum_{y\in\mathcal{G}_d}\sum_{z\in\mathcal{G}_e}\chi(x)\chi(y)\chi(z)\,\mathbf{e}_p\left(ax^kz^k + bx^\ell y^\ell + cx^m y^m z^m\right) \\ &= \frac{1}{de}\sum_{x\in\mathbb{F}_p^*}\sum_{z\in\mathcal{G}_e}\sum_{y\in\mathcal{G}_d}\rho_{x,y}\sigma_{x,z}\,\mathbf{e}_p(cx^m y^m z^m), \end{aligned}$$

where

$$\rho_{x,y} = \chi(x)\chi(y)\,\mathbf{e}_p(bx^\ell y^\ell) \qquad \text{and} \qquad \sigma_{x,z} = \chi(z)\,\mathbf{e}_p(ax^kz^k).$$

Clearly, the set $\mathcal{X} = \{x^m : x \in \mathbb{F}_p^*\}$ of nonzero m-th powers contains $(p-1)/f$ elements, each appearing with multiplicity f. Furthermore, direct examination shows that the sets $\mathcal{Y} = \{y^m : y \in \mathcal{G}_d\}$ and $\mathcal{Z} = \{z^m : z \in \mathcal{G}_e\}$ contain g and h elements with multiplicities $\gcd(d,f)$ and $\gcd(e,f)$, respectively. We recall that by our assumption

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

we have $f \ge g \ge h$, and we invoke Lemma 3.5, which gives us

$$\begin{aligned} S_\chi(\Psi) &\ll \frac{f \gcd(d,f)\gcd(e,f)}{de} \\ &\quad \times \begin{cases} (p/f)^{7/8} gh & \text{if } h \ge p^{1/2}\log p, \\ p^{1/16}(p/f)^{7/8} g h^{7/8} (\log p)^{1/16} & \text{if } g \ge (p\log p)^{1/2} > h, \\ p^{1/8}(p/f)^{7/8} g^{7/8} h^{7/8} (\log p)^{1/8} & \text{if } g < (p\log p)^{1/2}, \end{cases} \\ &= \begin{cases} p^{7/8} f^{1/8} & \text{if } h \ge (p\log p)^{1/2}, \\ p^{15/16} f^{1/8} h^{-1/8} (\log p)^{1/16} & \text{if } g \ge (p\log p)^{1/2} > g, \\ p f^{1/8} g^{-1/8} h^{-1/8} (\log p)^{1/8} & \text{if } g < (p\log p)^{1/2}. \end{cases} \end{aligned}$$

This concludes the proof. ∎

4 Further Applications

4.1 Additive Properties of Subgroups

As usual, given a rational function

$$R(X_1, \dots, X_m) \in \mathbb{F}_p(X_1, \dots, X_m),$$

and m sets $\mathcal{A}_1, \dots, \mathcal{A}_m \subseteq \mathbb{F}_p$, we define the set

$$R(\mathcal{A}_1, \dots, \mathcal{A}_m) = \left\{ R(a_1, \dots, a_m) : (a_1, \dots, a_m) \in (\mathcal{A}_1 \times \cdots \times \mathcal{A}_m) \setminus \mathcal{P}_R \right\},$$

where $\mathcal{P}_R$ is the set of poles of R.

We note that we have used $\mathcal{A}^m$ for the m-fold Cartesian product rather than for the m-fold product-set of a set $\mathcal{A}$ as the previous definition suggests. However, neither of these notations is used in this section.

For a scalar $\lambda \in \mathbb{F}_p$, we use the notation

$$\lambda\mathcal{A} = \{\lambda\} \cdot \mathcal{A} = \{\lambda a : a \in \mathcal{A}\}$$

for sets of multiples of $\mathcal{A} \subseteq \mathbb{F}_p$.

Applying the bound of Theorem 1.2 to cosets of $\mathcal{G}$, that is, to $T(\mathcal{G}, \lambda\mathcal{G})$, and using (2.3) we obtain the following corollary.

Corollary 4.1 *Let $\mathcal{G}$ be a multiplicative subgroup of $\mathbb{F}_p^*$. Then for any $\lambda \in \mathbb{F}_p^*$, we have*

$$\mathrm{E}^\times(\mathcal{G} + \lambda) - \frac{|\mathcal{G}|^4}{p} \ll \begin{cases} p^{1/2}|\mathcal{G}|^{3/2} & \text{if } |\mathcal{G}| \ge p^{2/3}, \\ |\mathcal{G}|^3 p^{-1/2} & \text{if } p^{2/3} > |\mathcal{G}| \ge p^{1/2}\log p, \\ |\mathcal{G}|^2 \log|\mathcal{G}| & \text{if } |\mathcal{G}| < p^{1/2}\log p. \end{cases}$$

Note that for $|\mathcal{G}|/\sqrt{p\log p} \to \infty$, Corollary 4.1 gives an asymptotic formula for $\mathrm{E}^\times(\mathcal{G} + \lambda)$; otherwise, we only have an upper bound.

Corollary 4.2 *For a multiplicative subgroup $\mathcal{G}$ of $\mathbb{F}_p^*$ and $\lambda, \mu \in \mathbb{F}_p^*$ we define the sets*

$$\mathcal{S}_1 = \mathcal{G} + \lambda\mathcal{G} + \mu\mathcal{G} \qquad \text{and} \qquad \mathcal{S}_2 = \left\{ \frac{u - \lambda}{v - \mu} : u, v \in \mathcal{G} \right\}.$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

We have:

- *if* $|\mathcal{G}| \ge p^{2/3}$, *then* $\mathbb{F}_p^* \subseteq \mathcal{S}_1$ *and* $\mathbb{F}_p^* \subseteq \mathcal{G}\mathcal{S}_2$;
- *if* $|\mathcal{G}| \le (p \log p)^{1/2}$, *then for* $i = 1, 2$,

$$|\mathcal{S}_i| \gg \frac{|\mathcal{G}|^2}{\log |\mathcal{G}|};$$

- *otherwise, for* $i = 1, 2$,

$$p - |\mathcal{S}_i| \ll \begin{cases} p^{5/2}|\mathcal{G}|^{-5/2} & \text{if } |\mathcal{G}| \ge p^{2/3}, \\ p^{3/2}|\mathcal{G}|^{-1} & \text{if } p^{2/3} > |\mathcal{G}| \ge p^{1/2} \log p, \\ p^2|\mathcal{G}|^{-2} \log p & \text{if } p^{1/2} \log p \ge |\mathcal{G}| > (p \log p)^{1/2}. \end{cases}$$

Proof We consider the set $\mathcal{S}_1$ first.

First we show that $\mathcal{S}_1 \supseteq \mathbb{F}_p^*$, provided $|\mathcal{S}_1| \ge p^{2/3}$. Clearly, the set $\mathcal{S}_1$ satisfies the property $\mathcal{S}_1\mathcal{G} = \mathcal{S}_1$, and hence if $\mathcal{S}_1 \supseteq \mathbb{F}_p^*$, then there is a nonzero ξ such that $\mathcal{S}_1 \cap \xi\mathcal{G} = \varnothing$. In other words, the equation

$$x + \lambda y + z\mu = \xi w, \qquad x, y, z, w \in \mathcal{G}$$

has no solutions. By the orthogonality property of exponential functions, this means that for the sum

$$\sigma = \sum_{a \in \mathbb{F}_p} \sum_{x \in \mathcal{G}} \mathbf{e}_p(ax) \sum_{y \in \mathcal{G}} \mathbf{e}_p(a\lambda y) \sum_{z \in \mathcal{G}} \mathbf{e}_p(a\mu z) \sum_{w \in \mathcal{G}} \mathbf{e}_p(-a\xi w),$$

we have $\sigma = 0$. Clearly, the contribution of σ corresponding to $a = 0$ equals $|\mathcal{G}|^4$. Using the well-known bound

$$\Big| \sum_{x \in \mathbb{F}_p} \mathbf{e}_p(bx^k) \Big| \le (k-1)p^{1/2}, \qquad b \in \mathbb{F}_p^*$$

(see, for example [19, Equation (1)]), combined with the identity

$$\sum_{z \in \mathcal{G}} \mathbf{e}_p(bz) = \frac{1}{k} \sum_{x \in \mathbb{F}_p^*} \mathbf{e}_p(bx^k),$$

where $k = (p-1)/|\mathcal{G}|$, we have

$$0 = \sigma \ge |\mathcal{G}|^4 - p \sum_{a \in \mathbb{F}_p^*} \Big| \sum_{x \in \mathcal{G}} \mathbf{e}_p(ax) \Big| \Big| \sum_{y \in \mathcal{G}} \mathbf{e}_p(a\lambda y) \Big|.$$

By the Cauchy inequality, we get

$$0 > |\mathcal{G}|^4 - p^2|\mathcal{G}| \ge 0,$$

and this is a contradiction, which gives the result for $|\mathcal{G}| \ge p^{2/3}$.

We now consider subgroups with $|\mathcal{G}| < p^{2/3}$. Clearly,

$$|\mathcal{S}_1| = |\mathcal{G} + \lambda\mathcal{G} + \mu\mathcal{G} + \lambda\mu| \ge |(\mathcal{G} + \lambda)(\mathcal{G} + \mu)|.$$

For $a \in \mathbb{F}_p^*$, we let $N(a)$ be the number of solutions to $(g+\lambda)(h+\mu) = a$ with $g, h \in \mathcal{G}$. Clearly,

$$\sum_{a \in \mathbb{F}_p} N(a) = |\mathcal{G}|^2.$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

Hence, by the Cauchy inequality, we have

$$|\mathcal{G}|^4 = \Big(\sum_{a\in\mathbb{F}_p} N(a)\Big)^2 \le |(\mathcal{G}+\lambda)(\mathcal{G}+\mu)| \sum_{a\in\mathbb{F}_p} N(a)^2 = |(\mathcal{G}+\lambda)(\mathcal{G}+\mu)|F,$$

where F is the number of solutions to

$$(g_1+\lambda)(h_1+\mu) = (g_2+\lambda)(h_2+\mu), \qquad g_1, g_2, h_1, h_2 \in \mathcal{G}.$$

There are obviously $O(|\mathcal{G}|^2)$ solutions when

$$(g_1+\lambda)(h_1+\mu) = (g_2+\lambda)(h_2+\mu) = 0.$$

For the other solutions we repeat the same argument as in the above. That is, for every $a \in \mathbb{F}_p$, we first collect together solutions with the same value

$$\frac{g_1+\lambda}{g_2+\lambda} = \frac{h_1+\mu}{h_2+\mu} = a.$$

After this, using the Cauchy inequality again, we obtain

$$F \le \sqrt{\mathrm{E}^\times(\mathcal{G}+\lambda)\mathrm{E}^\times(\mathcal{G}+\mu)} + O(|\mathcal{G}|^2).$$

Hence, putting the above inequalities together, we derive

$$|\mathcal{S}_1| \gg \frac{|\mathcal{G}|^4}{\sqrt{\mathrm{E}^\times(\mathcal{G}+\lambda)\mathrm{E}^\times(\mathcal{G}+\mu)} + O(|\mathcal{G}|^2)}.$$

Hence, using Corollary 4.1, we derive the result for $\mathcal{S}_1$. Indeed, let $\mathfrak{R}$ be the bound on $|\mathrm{E}^\times(\mathcal{G}+\lambda) - |\mathcal{G}|^4/p|$ given by Corollary 4.1. It is easy to see that for $\mathcal{G}$ to which the upper bound on $p - |\mathcal{S}_i|$ applies we have

$$\frac{|\mathcal{G}|^4}{p} \gg \mathfrak{R}.$$

Hence,

$$\begin{aligned}\mathrm{E}^\times(\mathcal{G}+\lambda)\mathrm{E}^\times(\mathcal{G}+\mu) &= \frac{|\mathcal{G}|^8}{p^2} + O\Big(\frac{|\mathcal{G}|^4}{p}\mathfrak{R} + \mathfrak{R}^2\Big)\\ &= \frac{|\mathcal{G}|^8}{p^2} + O\Big(\frac{|\mathcal{G}|^4}{p}\mathfrak{R}\Big) = \frac{|\mathcal{G}|^8}{p^2}\Big(1 + O\Big(\frac{p}{|\mathcal{G}|^4}\mathfrak{R}\Big)\Big),\end{aligned}$$

which, together with $\mathfrak{R} \gg |\mathcal{G}|^2$, implies

$$\begin{aligned}\sqrt{\mathrm{E}^\times(\mathcal{G}+\lambda)\mathrm{E}^\times(\mathcal{G}+\mu)} + O(|\mathcal{G}|^2) &= \frac{|\mathcal{G}|^4}{p}\Big(1 + O\Big(\frac{p}{|\mathcal{G}|^4}\mathfrak{R}\Big)\Big) + O(|\mathcal{G}|^2)\\ &= \frac{|\mathcal{G}|^4}{p}(1+\mathfrak{Q}),\end{aligned}$$

where

$$\mathfrak{Q} \ll \frac{p}{|\mathcal{G}|^4}\mathfrak{R}.$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

We note that by adjusting the implied constant in the upper bound on $p - |\mathcal{S}_1|$, we see that one can actually assume that $|\mathcal{G}| \ge C_0(p \log p)^{1/2}$ for some sufficiently large absolute constant C_0, so that $|\mathfrak{Q}| \le 1/2$. In this case

$$(1+\mathfrak{Q})^{-1} = 1 + O(\mathfrak{Q}) = 1 + O\Big(\frac{p}{|\mathcal{G}|^4}\mathfrak{R}\Big),$$

and the bound on $p - |\mathcal{S}_1|$ follows. For the lower bound on $|S_1|$, we simply remark that the error term $\mathfrak{R}$ dominates the main term $|\mathcal{G}|^4/p$ in Corollary 4.1, so in this case, we simply write

$$\sqrt{\mathrm{E}^{\times}(\mathcal{G}+\lambda)\mathrm{E}^{\times}(\mathcal{G}+\mu)} + O(|\mathcal{G}|^2) \ll \mathfrak{R},$$

and the bound follows.

Similar arguments also lead to the same bounds on $|\mathcal{S}_2|$. For example, consider the case $|\mathcal{G}| \ge p^{2/3}$ (where the statement about $\mathcal{S}_2$ is slightly different than that about $\mathcal{S}_1$). We denote

$$\mathcal{Q} = \mathcal{G}\mathcal{S}_2 = \frac{\lambda\mathcal{G} - \mathcal{G}}{\mu\mathcal{G} - \mathcal{G}}. \tag{4.1}$$

Using the orthogonality of exponential functions, for any $\xi \in \mathbb{F}_p^*$, we can write

$$\Big|\big\{\lambda u_1 - u_2 = \xi(\mu v_1 - v_2) : u_i, v_i \in \mathcal{G}, i = 1,2\big\}\Big| = \frac{|\mathcal{G}|^4}{p} + \frac{1}{p}\sum_{a\in\mathbb{F}_p^*}\sum_{u\in\mathcal{G}}\mathbf{e}_p(a\lambda u)\sum_{v\in\mathcal{G}}\mathbf{e}_p(v)\sum_{w\in\mathcal{G}}\mathbf{e}_p(a\xi\mu w)\sum_{z\in\mathcal{G}}\mathbf{e}_p(-a\xi z).$$

As before, we obtain

$$\Big|\Big|\big\{\lambda u_1 - u_2 = \xi(v_1 - v_2) : u_i, v_i \in \mathcal{G}, i = 1,2\big\}\Big| - \frac{|\mathcal{G}|^4}{p}\Big| < \sum_{a\in\mathbb{F}_p^*}\Big|\sum_{w\in\mathcal{G}}\mathbf{e}_p(a\xi w)\Big|^2 = p|\mathcal{G}| - |\mathcal{G}|^2.$$

Hence, for $|\mathcal{G}| > p^{2/3}$, we have

$$\Big|\big\{\lambda u_1 - u_2 = \xi(v_1 - v_2) : u_i, v_i \in \mathcal{G},\ i = 1,2\big\}\Big| > \frac{|\mathcal{G}|^4}{p} - p|\mathcal{G}| + |\mathcal{G}|^2 > |\mathcal{G}|^2.$$

Therefore, there is a solution with $v_1 \ne v_2$ that leads to a representation $\xi = (\lambda u_1 - u_2)/(v_1 - v_2)$ for every $\xi \in \mathbb{F}_p^*$.

Proofs of the other statements about $\mathcal{S}_2$ are the same as those about $\mathcal{S}_1$. ∎

In particular, Corollary 4.2 applies to $\mathcal{S}_1 = \mathcal{G} + \mathcal{G} + \mathcal{G}$ and $\mathcal{S}_1 = \mathcal{G} + \mathcal{G} - \mathcal{G}$. We note that for the set $\mathcal{Q}$ given by (4.1) we have $0 \in \frac{\lambda\mathcal{G}-\mathcal{G}}{\mu\mathcal{G}-\mathcal{G}}$ if and only if $\lambda \in \mathcal{G}$.

Remark 4.3 Let

$$\mathcal{Q} = \frac{\lambda\mathcal{G} - \mathcal{G}}{\mathcal{G} - \mathcal{G}} \quad \text{and} \quad \mathcal{R} = \frac{\lambda\mathcal{G} - 1}{\mathcal{G} - 1}.$$

Clearly,

$$\mathcal{R}\mathcal{G} = \mathcal{Q} \quad \text{and} \quad \mathcal{R} = 1 - \mathcal{R}.$$

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press

Hence, the set $\mathcal{Q}$ contains both $\mathcal{RG}$ and $(1-\mathcal{R})\mathcal{G}$, and hence $|\mathcal{Q}| \ge \max\{|\mathcal{RG}|, |(1-\mathcal{R})\mathcal{G}|\}$. Using [30, Theorem 18] and $|\mathcal{R}| \gg |\mathcal{G}|^2/\log|\mathcal{G}|$, one can show that there is an absolute constant $c > 0$ such that $|\mathcal{Q}| \gg |\mathcal{G}|^{2+c}$ for sufficiently small $\mathcal{G}$ (the condition $|\mathcal{Q}|^2|\mathcal{G}| \le p^2$ is enough). Thus, the lower bound for size of $\mathcal{Q}$, which follows from bounds on $|\mathcal{S}_2|$ in Corollary 4.2, can be improved for small subgroups.

We note that Corollary 4.2 also allows us to obtain the following version of the Romanoff theorem modulo almost all primes p.

Corollary 4.4 *For a fixed integer g with $|g| \ge 2$, and sufficiently large Q, for all but $o(Q/\log Q)$ primes $p \le Q$, every residue class modulo p can be represented as $\ell + g^k + g^m + g^n$ for a prime $\ell < p$ and positive integers $k, m, n \le p-1$.*

Proof We recall that by a special case of a result of Indlekofer and Timofeev [20, Corollary 6], given any positive $\alpha < 1$, for all but $o(Q/\log Q)$ primes $p \le Q$, the multiplicative order of g modulo p is at least $p^{1/2}\exp((\log p)^{\alpha})$. For each of these primes, we apply Corollary 4.2 to the set $\mathcal{S}_1 = \mathcal{G} + \mathcal{G} + \mathcal{G}$ with the group $\mathcal{G} \equiv \langle g \pmod p \rangle$ (only the first two inequalities are relevant) and use that for $|\mathcal{G}| \ge p^{2/3}$ we have $p^{5/2}|\mathcal{G}|^{-5/2} \le p^{3/2}|\mathcal{G}|^{-1}$. Hence, we obtain

$$p - |\mathcal{S}_1| \ll p^{3/2}|\mathcal{G}|^{-1} \ll p\exp\big(-(\log p)^{\alpha}\big) = o(p/\log p),$$

and by the prime number theorem, we conclude the proof. ∎

We remark that a classical result of Erdős and Murty [15] can also be used in the proof of Corollary 4.4; however, the bound of [20, Corollary 6] used in full strength allows us to get better estimates on the size of the exceptional set. Perhaps more recent results of Ford [16] can also be used to estimate the size of the exceptional set; however, we do not pursue this here.

4.2 Possible Application to Arbitrary Sets

Note that some auxiliary results established in the proofs of [18, Theorems 1 and 2] can be reformulated as bounds on the size of the set $(\mathcal{A}-\mathcal{A})(\mathcal{A}-\mathcal{A})$ for an arbitrary set $\mathcal{A} \subseteq \mathbb{F}_p$. We also refer to [2] for more recent results and references. Combined with the ideas of Balog [2], this may lead to further results on additive properties of the product sets of difference sets.

Acknowledgements The authors would like to thank Giorgis Petridis for his comments and suggestions and the referee for the very careful reading of the manuscript and numerous corrections.

References

[1] N. M. Akulinichev, *Estimates for rational trigonometric sums of a special type.* (Russian) Dokl. Akad. Nauk SSSR **161**(1965), 743–745.
[2] A. Balog, *Another sum-product estimate in finite fields.* Proc. Steklov Inst. Math. **280**(2013), Suppl. 2, S23–S29. http://dx.doi.org/10.1134/S0081543813030024

[3] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources.* Geom. and Funct. Anal. **18**(2009), 1477–1502. http://dx.doi.org/10.1007/s00039-008-0691-6
[4] ———, *Estimates of polynomial exponential sums.* Israel J. Math. **176**(2010), 221–240. http://dx.doi.org/10.1007/s11856-010-0027-8
[5] J. Bourgain and A. Glibichuk, *Exponential sum estimates over a subgroup in an arbitrary finite field.* J. Anal. Math. **115**(2011), 51–70. http://dx.doi.org/10.1007/s11854-011-0023-x
[6] 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. London Math. Soc. **73**(2006), 380–398. http://dx.doi.org/10.1112/S0024610706022721
[7] J. Bourgain, N. H. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications.* Geom. Funct. Anal. **14**(2004), 27–57. http://dx.doi.org/10.1007/s00039-004-0451-1
[8] T. T. Cochrane, J. Coffelt, and C. G. Pinner, *A further refinement of Mordell's bound on exponential sums.* Acta Arith. **116**(2005), 35–41. http://dx.doi.org/10.4064/aa116-1-4
[9] ———, *A system of simultaneous congruences arising from trinomial exponential sums.* J. Théor. Nombres Bordeaux **18**(2006), 59–72. http://dx.doi.org/10.5802/jtnb.533
[10] T. Cochrane and C. Pinner, *An improved Mordell type bound for exponential sums.* Proc. Amer. Math. Soc. **133**(2005), 313–320. http://dx.doi.org/10.1090/S0002-9939-04-07726-3
[11] ———, *Using Stepanov's method for exponential sums involving rational functions.* J. Number Theory **116**(2006), 270–292. http://dx.doi.org/10.1016/j.jnt.2005.04.001
[12] ———, *Bounds on fewnomial exponential sums over* $\mathbb{Z}_p$. Math. Proc. Cambridge Philos. Soc. **149**(2010), 217–227.
[13] ———, *Explicit bounds on monomial and binomial exponential sums.* Q. J. Math. **62**(2011), 323–349. http://dx.doi.org/10.1017/S0305004110000319
[14] R. Crocker, *On the sum of a prime and of two powers of two.* Pacific J. Math. **36**(1971), 103–107. http://dx.doi.org/10.2140/pjm.1971.36.103
[15] P. Erdős and R. Murty, *On the order of* $a \pmod p$. CRM Proc. Lecture Notes, American Mathematical Society, Providence, RI, 1999, pp. 87–97.
[16] K. Ford, *The distribution of integers with a divisor in a given interval.* Ann. of Math. **168**(2008), 367–433. http://dx.doi.org/10.4007/annals.2008.168.367
[17] M. Z. Garaev, *Sums and products of sets and estimates of rational trigonometric sums in fields of prime order.* Russian Math. Surveys **65**(2010), no. 4, 599–658. http://dx.doi.org/10.4213/rm9367
[18] A. Glibichuk, *Combinational properties of sets of residues modulo a prime and the Erdős-Graham problem.* Math. Notes **79**(2006), 356–365. http://dx.doi.org/10.4213/mzm2708
[19] D. R. Heath-Brown and S. V. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum.* Q. J. Math. **51**(2000), 221–235. http://dx.doi.org/10.1093/qjmath/51.2.221
[20] H.-K. Indlekofer and N. M. Timofeev, *Divisors of shifted primes.* Publ. Math. Debrecen **60**(2002), 307–345.
[21] S. V. Konyagin, *Bounds of exponential sums over subgroups and Gauss sums.* (Russian), Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications, Moscow Lomonosov State Univ., Moscow, 2002, pp. 86–114.
[22] S. Macourt, *Incidence results and bounds of trilinear and quadrilinear exponential sums.* arxiv:1707.08268
[23] D. A. Mit'kin, *Estimation of the total number of the rational points on a set of curves in a simple finite field.* (Russian) Chebyshevsky Sbornik **4**(2003), no.4, 94–102.
[24] B. Murphy, G. Petridis, O. Roche–Newton, M. Rudnev and I. D. Shkredov, *New results on sum–product type growth in positive characteristic.* arxiv:1702.01003
[25] G. Petridis and I. E. Shparlinski, *Bounds on trilinear and quadrilinear exponential sums.* J. d'Analyse Math., to appear.
[26] N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie.* Math. Ann. **109**(1934), 668–678. http://dx.doi.org/10.1007/BF01449161
[27] I. D. Shkredov, *On exponential sums over multiplicative subgroups of medium size.* Finite Fields Appl. **30**(2014), 72–87. http://dx.doi.org/10.1016/j.ffa.2014.06.002
[28] ———, *On tripling constant of multiplicative subgroups.* Integers **16**(2016), no. A75.
[29] ———, *Differences of subgroups in subgroups.* Integers, to appear.
[30] ———, *Some remarks on the asymmetric sum–product phenomenon.* Moscow J. Combin. and Number Theory, to appear.
[31] I. D. Shkredov and I. V. Vyugin, *On additive shifts of multiplicative subgroups.* (Russian) Mat. Sb. **203**(2012), 81–100.

[32] I. E. Shparlinski, *Estimates for Gaussian sums.* (Russian) Mat. Zametki **50**(1991), 122–130.
[33] I. E. Shparlinski, *On exponential sums with sparse polynomials and rational functions.* J. Number Theory **60**(1996), 233–244. http://dx.doi.org/10.1006/jnth.1996.0121
[34] Y. N. Shteinikov, *Estimates of trigonometric sums over subgroups and some of their applications.* (Russian) Mat. Zametki **98**(2015), 606–625. http://dx.doi.org/10.4213/mzm10629
[35] S. Stevens and F. de Zeeuw, *An improved point-line incidence bound over arbitrary fields.* Bull. London Math. Soc., to appear.
[36] A. Weil, *Basic number theory.* Die Grundlehren der Mathematischen Wissenschaften, 144, Springer-Verlag, New York-Berlin, 1974.
[37] T. Tao and V. Vu, *Additive combinatorics.* Cambridge Studies in Advanced Mathematics, 105, Cambridge University Press, Cambridge, 2006.
[38] H. B. Yu, *Estimates for complete exponential sums of special types.* Math. Proc. Cambridge Philos. Soc. **131**(2001), 321–326.

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
e-mail: s.macourt@unsw.edu.au

Steklov Mathematical Institute of Russian Academy of Sciences, ul. Gubkina 8, Moscow, Russia, 119991, and Institute for Information Transmission Problems of Russian Academy of Sciences, Bolshoy Karetny Per. 19, Moscow, Russia, 127994, and MIPT, Institutskii per. 9, Dolgoprudnii, Russia, 141701
e-mail: ilya.shkredov@gmail.com

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

https://doi.org/10.4153/CJM-2017-044-2 Published online by Cambridge University Press