EXPONENTIAL SUMS AND ADDITIVE COMBINATORICS

Simon Macourt

Supervisor: Professor Igor Shparlinski

School of Mathematics and Statistics
UNSW Sydney
Faculty of Science

March 2020

Submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

Thesis/Dissertation Sheet

Surname/Family Name	:	**Macourt**
Given Name/s	:	**Simon Thomas**
Abbreviation for degree as give in the University calendar	:	**PhD**
Faculty	:	**Faculty of Science**
School	:	**School of Mathematics and Statistics**
Thesis Title	:	**Exponential sums and additive combinatorics**

Abstract 350 words maximum: (PLEASE TYPE)

In this thesis we provide new results in additive combinatorics which in turn lead us to new bounds of certain exponential sums. We also use known bounds on exponential and character sums to give new results in additive combinatorics. Specifically we will see how bounds on some quantities from additive combinatorics appear naturally when trying to bound multilinear exponential sums. We then find applications to bounds of exponential sums of sparse polynomials. We also give new bounds for an analogue of the energy variant of the sum-product problem over arbitrary finite fields.

ORIGINALITY STATEMENT

'I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.'

Signed …….....

Date …….....

COPYRIGHT STATEMENT

Signed …….....

Date …….....

AUTHENTICITY STATEMENT

‘I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis.’

Signed …….....

Date …….....

INCLUSION OF PUBLICATIONS STATEMENT

UNSW is supportive of candidates publishing their research results during their candidature as detailed in the UNSW Thesis Examination Procedure.

Publications can be used in their thesis in lieu of a Chapter if:

- The candidate contributed greater than 50% of the content in the publication and is the "primary author", ie. the candidate was responsible primarily for the planning, execution and preparation of the work for publication
- The candidate has approval to include the publication in their thesis in lieu of a Chapter from their supervisor and Postgraduate Coordinator.
- The publication is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in the thesis

Please indicate whether this thesis contains published material or not:

☐ This thesis contains no publications, either published or submitted for publication
(if this box is checked, you may delete all the material on page 2)

☒ Some of the work described in this thesis has been published and it has been documented in the relevant Chapters with acknowledgement
(if this box is checked, you may delete all the material on page 2)

☐ This thesis has publications (either published or submitted for publication) incorporated into it in lieu of a chapter and the details are presented below

CANDIDATE'S DECLARATION

I declare that:

- I have complied with the UNSW Thesis Examination Procedure
- where I have used a publication in lieu of a Chapter, the listed publication(s) below meet(s) the requirements to be included in the thesis.

Candidate's Name	**Signature**	**Date (dd/mm/yy)**
Simon Macourt		26/03/20

Acknowledgements

Firstly, I am extremely grateful for the help and support of my supervisor. Igor has provided immense support throughout my candidature and encouraged me to grow and develop as a researcher. I am also very thankful for his many suggestions of problems and ideas, which almost always seemed to work.

I am also incredibly thankful for my wife Louisa who has supported me throughout this whole process. She has encouraged me to pursue my passions and given me much needed confidence when I have needed it.

I am thankful to my collaborators Bryce and Ilya, as well as Igor. Their suggestions, ideas and discussions have helped shape the research that appears in this thesis. I am also thankful to Giorgis Petridis for his suggestion, and reading, of the project on collinear triples and multilinear exponential sums.

I am also thankful to Gerry Myerson. He was my supervisor for my Masters of Research and his support, encouragement and guidance helped me to get to where I am today. I am also grateful for his suggestion of Igor Shparlinski as a supervisor for my PhD.

Finally, I am thankful for the UNSW School of Mathematics and Statistics for their support throughout this PhD, as well as the many friends and connections I have been able to make in this school.

Abstract

In this thesis we provide new results in additive combinatorics which in turn lead us to new bounds of certain exponential sums. We also use known bounds on exponential and character sums to give new results in additive combinatorics. Specifically we will see how bounds on some quantities from additive combinatorics appear naturally when trying to bound multilinear exponential sums. We then find applications to bounds of exponential sums of sparse polynomials. We also give new bounds for an analogue of the energy variant of the sum-product problem over arbitrary finite fields.

Contents

1 Introduction **1**
1.1 Background and Notation 1
1.2 Overview of Thesis 2
1.2.1 Collinear Triples 2
1.2.2 A Low Energy Decomposition 3
1.2.3 Multilinear Exponential Sums 5
1.2.4 Multinomial Exponential Sums 6

2 Collinear Triples **9**
2.1 Introduction 9
2.1.1 Set Up 9
2.1.2 New Results 10
2.1.3 Previous Results 10
2.2 Collinear Triples Over Subsets 11
2.2.1 Preliminaries 11
2.2.2 Proof of Theorem 2.1.1 15
2.2.3 Consequences 16
2.3 Collinear Triples Over Subgroups 18
2.3.1 Preliminaries 18
2.3.2 Initial Reductions 19
2.3.3 Sets Θ_τ and $\mathcal{Q}_\tau$ 19
2.3.4 Concluding the Proof of Theorem 2.1.2 21
2.3.5 Consequences 22
2.4 Open Problems 23

3 A Low Energy Decomposition of Subsets of Finite Fields **25**
3.1 Introduction 25
3.1.1 Set Up 25
3.1.2 Notation 26
3.1.3 Main Results 26
3.2 Energy Bounds 27
3.2.1 Preliminary Results 27

3.2.2 Proof of Theorem 3.1.1 . . . 37
3.2.3 Proofs of Theorems 3.1.2 and 3.1.3 . . . 38
3.3 Open Problems . . . 38

4 Multilinear Exponential Sums **41**
4.1 Trilinear and Quadrilinear Exponential Sums . . . 41
4.1.1 Set Up . . . 41
4.1.2 New Results . . . 42
4.1.3 Previous Results . . . 42
4.1.4 Preliminaries . . . 43
4.1.5 Proof of Theorem 4.1.1 . . . 45
4.1.6 Proof of Theorem 4.1.2 . . . 46
4.2 Higher Dimensional Multilinear Exponential Sums . . . 48
4.2.1 Set Up . . . 48
4.2.2 Main Results . . . 49
4.2.3 Reduction Mean Values . . . 50
4.2.4 Estimates for $D_k^{\times}(\mathcal{A})$ . . . 56
4.2.5 Proof of Theorem 4.2.1 . . . 63
4.2.6 Proof of Theorem 4.2.2 . . . 65
4.3 Open Problems . . . 66

5 Multinomial Exponential Sums **67**
5.1 Introduction . . . 67
5.1.1 Set Up . . . 67
5.1.2 Previous Results . . . 68
5.1.3 Main Results . . . 69
5.2 Trinomial and Quadrinomial Exponential Sums . . . 72
5.2.1 Preliminaries . . . 72
5.2.2 Bounds On Trilinear and Quadrilinear Exponential Sums Over Subgroups . . . 73
5.2.3 Proof of Theorem 5.1.1 . . . 77
5.2.4 Proof of Theorem 5.1.2 . . . 78
5.3 Multinomial Exponential Sums . . . 79
5.3.1 Preliminaries . . . 79
5.3.2 Proof of Theorem 5.1.6 . . . 80
5.4 Open Problems . . . 80

References **83**

1 Introduction

1.1 Background and Notation

This thesis is based on a collection of papers related to bounds of exponential sums and results in additive combinatorics. For the entirety of this thesis we use the notation

$$\mathbf{e}_p(x) = \exp(2\pi i x/p)$$

where p will always be a large prime number. We also use $\mathbb{F}_p$ to denote the finite field of p elements. We consider the exponential sum, over some arbitrary subset $\mathcal{X} \subseteq \mathbb{F}_p$,

$$\sum_{x \in \mathcal{X}} \mathbf{e}_p(f(x))$$

for some suitably chosen function f. The challenge in studying such sums is to be able to provide upper bounds. Trivially, one has

$$\left| \sum_{x \in \mathcal{X}} \mathbf{e}_p(f(x)) \right| \leqslant |\mathcal{X}|,$$

and for many functions and sets we are unable to say much more.

The field of additive combinatorics gives methods of providing upper bounds on certain exponential sums, as we will see in Chapter 4. Similarly, bounds on exponential and character sums also lead to estimates in additive combinatorics, as we will see in Chapter 3.

Finally, we frequently use the notation

$$A \ll B \qquad \text{and} \qquad A = O(B)$$

which both are equivalent to $|A| \leqslant c|B|$ for some absolute constant c. We also use

$$A \ll_k B \qquad \text{and} \qquad A = O_k(B)$$

when c depends on some other parameter k.

1.2 Overview of Thesis

Although this thesis is built on a collection of articles, we present them in a restructured format so as to keep related ideas together in chapters. The relevant articles are:

- [22] which appears in Chapters 2 and 4,
- [24] which appears in Chapters 2 and 5,
- [23] which appears in Chapter 3,
- [18] which appears in Chapters 4 and 5,
- [21] which appears in Chapter 5.

At the end of each chapter there will also be a section on open problems and other possible directions. Here we provide a short overview of each chapter.

1.2.1 Collinear Triples

Bounds on the number of collinear triples are of particular importance when finding bounds on certain types of exponential sums (as we will see in Chapters 4 and 5) as well as being a tool for giving bounds on sum and product sets. We define the number of collinear triples, $T(\mathcal{A}, \mathcal{B})$, to be the number of solutions of

$$(a_1 - a_2)(b_1 - b_2) = (a_1 - a_3)(b_1 - b_3), \quad a_i \in \mathcal{A}, b_i \in \mathcal{B}, i = 1, 2, 3. \tag{1.2.1}$$

In Chapter 2, we consider a more general form of this equation for further applications in Chapters 4 and 5.

Transforming our expression (1.2.1), we can see that $T(\mathcal{A},\mathcal{B})$ can be considered to be the number of solutions of

$$b_1 - ca_1 = b_2 - ca_2 = b_3 - ca_3$$

with the $a_i \in \mathcal{A}$, $b_i \in \mathcal{B}$ and $c \in \mathbb{F}_p$, if we include an added error term of $O(|\mathcal{A}||\mathcal{B}|^3 + |\mathcal{A}|^2|\mathcal{B}|^2)$, which comes from counting relevant zero solutions to (1.2.1). It is here that we see collinear triples namesake more clearly. In this chapter, we adapt existing techniques to give new bounds on the number of collinear triples, which are stronger when $\mathcal{A} \neq \mathcal{B}$. Previous results on this asymmetric case have been given using the Cauchy-Schwartz inequality by first finding bounds on $T(\mathcal{A},\mathcal{A})$. Although this is usually just stated, we prove the following using multiplicative characters. If we consider $T^*(\mathcal{A},\mathcal{B})$ to be the non-zero solutions to (1.2.1), χ a multiplicative character and Ω the set of all multiplicative characters over $\mathbb{F}_p$, we have

$$\begin{aligned} T^*(\mathcal{A},\mathcal{B}) &= \sum_{\substack{a_i\in\mathcal{A}\\ i=1,2,3}} \sum_{\substack{b_i\in\mathcal{B}\\ i=1,2,3}} \frac{1}{p-1}\sum_{\chi\in\Omega}\chi(a_1-a_2)\chi(b_1-b_2)\overline{\chi}(a_1-a_3)\overline{\chi}(b_1-b_3) \\ &= \frac{1}{p-1}\sum_{\chi\in\Omega}\sum_{a_1\in\mathcal{A}}\left|\sum_{a_2\in\mathcal{A}}\chi(a_1-a_2)\right|^2\sum_{b_1\in\mathcal{B}}\left|\sum_{b_2\in\mathcal{B}}\chi(b_1-b_2)\right|^2. \end{aligned}$$

We now square both sides and apply the Cauchy-Schwartz inequality to obtain

$$\begin{aligned} T^*(\mathcal{A},\mathcal{B})^2 &\leqslant \frac{1}{p-1}\sum_{\chi\in\Omega}\left|\sum_{a_1\in\mathcal{A}}\left|\sum_{a_2\in\mathcal{A}}\chi(a_1-a_2)\right|^2\right|^2 \frac{1}{p-1}\sum_{\chi\in\Omega}\left|\sum_{b_1\in\mathcal{B}}\left|\sum_{b_2\in\mathcal{B}}\chi(b_1-b_2)\right|^2\right|^2 \\ &= T^*(\mathcal{A},\mathcal{A})T^*(\mathcal{B},\mathcal{B}). \end{aligned}$$

Instead, considering $T(\mathcal{A},\mathcal{B})$ directly leads to our improvements on previous results. Such improvements become stronger when the size of $\mathcal{A}$ and $\mathcal{B}$ are significantly different.

In this chapter we also provide some stronger bounds on the number of collinear triples where our sets $\mathcal{A}$ and $\mathcal{B}$ are subgroups. Finally, as previously mentioned, in this chapter we give a more general form of $T(\mathcal{A},\mathcal{B})$ then what has been considered previously. We instead consider our collinear triples over two parameters λ and μ. This leads us to new bounds on multiplicative energy of shifted subgroups.

1.2.2 A Low Energy Decomposition

Additive and multiplicative energy have seen much study in recent years, as we will see in Chapter 3. Of particular importance is their relationship to sum and product

sets. We define the additive energy

$$E^+(\mathcal{A},\mathcal{B}) = |\{(a_1,a_2,b_1,b_2) \in \mathcal{A}^2 \times \mathcal{B}^2 : a_1+b_1 = a_2+b_2\}|.$$

Similarly, we define the multiplicative energy

$$E^\times(\mathcal{A},\mathcal{B}) = |\{(a_1,a_2,b_1,b_2) \in \mathcal{A}^2 \times \mathcal{B}^2 : a_1b_1 = a_2b_2\}|.$$

Here, we are most interested in the cases $\mathcal{A} = \mathcal{B}$ and thus define $E^+(\mathcal{A},\mathcal{A}) = E^+(\mathcal{A})$ and $E^\times(\mathcal{A},\mathcal{B}) = E^\times(\mathcal{A})$. We also define the sum and product sets respectively as

$$\mathcal{A}+\mathcal{B} = \{a+b : a \in \mathcal{A}, b \in \mathcal{B}\}$$
$$\mathcal{A}\cdot\mathcal{B} = \{ab : a \in \mathcal{A}, b \in \mathcal{B}\}.$$

If we define $r^+_{\mathcal{A}}(x)$ to be the number of solutions of $a_1+a_2 = x$ for $a_1,a_2 \in \mathcal{A}$ it is clear

$$\sum_{x\in\mathcal{A}+\mathcal{A}} r^+_{\mathcal{A}}(x) = |\mathcal{A}|^2 \qquad \text{and} \qquad \sum_{x\in\mathcal{A}+\mathcal{A}} (r^+_{\mathcal{A}}(x))^2 = E^+(\mathcal{A}).$$

Using the Cauchy-Schwartz inequality and squaring we have

$$|\mathcal{A}+\mathcal{A}|E^+(\mathcal{A}) \geqslant |\mathcal{A}|^4.$$

It follows that strong upper bounds on additive energy correspond to strong lower bounds on the size of the sum set. Similarly, for product sets. This is of particular importance as Erdős and Szemerédi [15] showed over finite sets of real numbers that

$$\max(\mathcal{A}+\mathcal{A}, \mathcal{A}\cdot\mathcal{A}) \geqslant |\mathcal{A}|^{1+\epsilon}$$

for some small $\epsilon > 0$. However, they also conjectured that we can take ϵ arbitrarily close to 1 when $\mathcal{A}$ is a finite subset over the reals.

In a similar way, one may hope to find an analogue of this result for energy, that is we may hope that either the additive or multiplicative energy always has to be small (of size $|\mathcal{A}|^2$). Such hope is, of course, in vain as we can take $\mathcal{A}$ to be a union of a geometric series and an arithmetic series each of size $|\mathcal{A}|/2$ to ensure both energies are maximal. However, in this style, Balog and Wooley [2] showed that we can find a decomposition of disjoint subsets $\mathcal{B} \sqcup \mathcal{C} = \mathcal{A}$ such that

$$\max(E^+(\mathcal{B}), E^\times(\mathcal{C})) \ll |\mathcal{A}|^{3-\delta}.$$

Their bound is given both over the reals and finite fields $\mathbb{F}_p$ (with different choices of δ). The ideas of their proof rely on certain incidence results.

One then might like to revisit the energy variant of the sum-product problem and suggest that we can always find a decomposition such that

$$\max(E^+(\mathcal{B}), E^\times(\mathcal{C})) \ll |\mathcal{A}|^2.$$

Balog and Wooley [2] also considered this in their paper and were able to construct a set $\mathcal{A}$ for which any subset $\mathcal{A}'$ satisfying $|\mathcal{A}'| = \alpha|\mathcal{A}|$ gives

$$E^+(\mathcal{A}'), E^\times(\mathcal{A}') \gg \alpha|\mathcal{A}|^{7/3}.$$

In Chapter 3 we consider a slightly different problem. We prove an extension of results of Roche-Newton, Shparlinski and Winterhof [31] which shows

$$\max(E^+(\mathcal{B}), E^+(f(\mathcal{C}))) \ll |\mathcal{A}|^{3-\delta} \tag{1.2.2}$$

over $\mathbb{F}_q$, where q is a prime power, f is a suitably chosen function and $\mathcal{A}$ is of sufficient size. Our bounds, similarly to [31], rely on bounds on certain character sums. Our extensions will show that we can replace E^+ with $E^\times$ in either or both terms in (1.2.2), as long as we suitably change our restriction on our function f.

1.2.3 Multilinear Exponential Sums

Multilinear exponential sums are those of the form

$$T(\mathcal{X}_1, \dots, \mathcal{X}_n) = \sum_{x_1 \in \mathcal{X}_1} \dots \sum_{x_n \in \mathcal{X}_n} \mathbf{e}_p(ax_1 \dots x_n)$$

for $\mathcal{X}_i \subseteq \mathbb{F}_p$ for each $i = 1, \dots, n$ and any $a \in \mathbb{F}_p^*$. The first results in this direction are due to Vinogradov who provided the following bound on bilinear exponential sums (for example, see [5, Equation 1.4]). Here we also provide a simple proof.

Lemma 1.2.1. *Let $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$, and α_x, β_y be complex weights such that*

$$\sum_{x \in \mathcal{X}} |\alpha_x|^2 = A \qquad \sum_{y \in \mathcal{Y}} |\beta_y|^2 = B.$$

Then

$$\left| \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \alpha_x \beta_y \, \mathbf{e}_p(axy) \right| \leqslant (pAB)^{1/2}$$

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

Proof. By the Cauchy-Schwartz inequality we have

$$\left|\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}\alpha_x\beta_y\,\mathbf{e}_p(axy)\right|^2 \leqslant A\sum_{x\in\mathcal{X}}\left|\sum_{y\in\mathcal{Y}}\beta_y\,\mathbf{e}_p(axy)\right|^2.$$

We now extend the outer sum over all $\mathbb{F}_p$ to obtain

$$\begin{aligned}\left|\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}\alpha_x\beta_y\,\mathbf{e}_p(axy)\right|^2 &\leqslant A\sum_{x\in\mathbb{F}_p}\left|\sum_{y\in\mathcal{Y}}\beta_y\,\mathbf{e}_p(axy)\right|^2\\ &= A\sum_{x\in\mathbb{F}_p}\sum_{y_1,y_2\in\mathcal{Y}}\beta_{y_1}\overline{\beta_{y_2}}\,\mathbf{e}_p(ax(y_1-y_2))\\ &= A\sum_{\substack{y_1,y_2\in\mathcal{Y}\\ y_1=y_2}}\beta_{y_1}\overline{\beta_{y_2}}\sum_{x\in\mathbb{F}_p}\mathbf{e}_p(ax(y_1-y_2))\\ &= Ap\sum_{y\in\mathcal{Y}}|\beta_y|^2\\ &= pAB.\end{aligned}$$

This completes the proof. □

The focus of this chapter is to consider multilinear exponential sums of the form

$$T(\mathcal{X}_1,\ldots,\mathcal{X}_n)=\sum_{x_1\in\mathcal{X}_1}\ldots\sum_{x_n\in\mathcal{X}_n}\omega_1(\mathbf{x})\ldots\omega_n(\mathbf{x})\,\mathbf{e}_p(ax_1\ldots x_n) \tag{1.2.3}$$

where $a\in\mathbb{F}_p^*$ and the ω_i's are $n-1$ dimensional complex weights, that is, complex numbers of modulus $|\omega_i|\leqslant 1$ depending on all but the i-th coordinate of $\mathbf{x}$. Our results are an extension of [30] and use similar techniques, however some improvements are made in certain regions on trilinear and quadrilinear exponential sums due to estimates on collinear triples from Chapter 2. We have also been able to extend these results to general multilinear sums beyond $n=4$. This extension is certainly non-trivial, and is due to some recent results in additive combinatorics.

An overview of similar types of sums will also be mentioned in this chapter as we analyse the differences between the respective bounds.

1.2.4 Multinomial Exponential Sums

We define a t-sparse polynomial

$$\Psi_t(X)=\sum_{i=1}^{t}a_iX^{k_i}$$

with pairwise distinct, non-zero, integer exponents $k_1, \ldots, k_t$ with corresponding coefficients $a_1, \ldots, a_t \in \mathbb{F}_p^*$. We consider the multinomial exponential sum

$$S_{\mathcal{X}}(\Psi_t) = \sum_{x \in \mathbb{F}_p^*} \chi(x)\, \mathbf{e}_p(\Psi_t(x)). \tag{1.2.4}$$

The bounds on such sums that appear in Chapter 5 come as a result of bounds on weighted multilinear sums from Chapter 4. By extending the sum over t multiplicative subgroups of $\mathbb{F}_p^*$ we are able to express our multinomial sum as a weighted multilinear sum. It is worth mentioning that in this chapter we find stronger results on multilinear exponential sums than those in Chapter 4 for when our arbitrary sets are, instead, multiplicative groups.

The methods used to give our bounds provide interesting results as our bounds do not depend directly on the size of the powers of our polynomials, but rather they depend on the size of some greatest common divisors of our powers. This is in contrast to the well-known Weil bound, which gives

$$|S_{\mathcal{X}}(\Psi_t)| \leqslant \max\{k_1, \ldots, k_t\} p^{1/2}.$$

2

Collinear Triples

2.1 Introduction

2.1.1 Set Up

We define the line

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

for any $(a, b) \in \mathbb{F}_p^2$. We let $\mathcal{A}$, $\mathcal{B} \subseteq \mathbb{F}_p$, with $|\mathcal{A}| = A$, $|\mathcal{B}| = B$ and $A \leqslant B$. We also define the number of incidences of any line with $\mathcal{A} \times \mathcal{B}$ to be

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

Furthermore, for $\lambda, \mu \in \mathbb{F}_p^*$, we define the number of collinear triples $T_{\lambda,\mu}(\mathcal{A}, \mathcal{B})$ to be the number of solutions to

$$(a_1 - \lambda a_2)(b_1 - \mu b_2) = (a_1 - \lambda a_3)(b_1 - \mu b_3), \quad a_i \in \mathcal{A}, b_i \in \mathcal{B}, i = 1, 2, 3.$$

We define $T_{1,1}(\mathcal{A}, \mathcal{B}) = T(\mathcal{A}, \mathcal{B})$ and for $\mathcal{A} = \mathcal{B}$ we define $T(\mathcal{A}, \mathcal{A}) = T(\mathcal{A})$.

2.1.2 New Results

Our main result of this chapter is the following theorem on the number of collinear triples.

Theorem 2.1.1. *Let $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ with $|\mathcal{A}| = A \leqslant |\mathcal{B}| = B$ and $\lambda, \mu \in \mathbb{F}_p^*$. Then*

$$T_{\lambda,\mu}(\mathcal{A}, \mathcal{B}) - \frac{A^3B^3}{p} \ll p^{1/2}A^2B^{3/2} + AB^3.$$

Our bound is dependent on a result of Murphy et al. [27] on the number of point-line incidences, which is given in the following section.

We also provide 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 2.1.2. *Let $\mathcal{G}$ be a multiplicative subgroup of $\mathbb{F}_p^*$. Then for any $\lambda \in \mathbb{F}_p^*$, we have*

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

Remark 2.1.3. *Theorem 2.1.2 is new only for subgroups of intermediate size, where $p^{2/3} > |\mathcal{G}| > p^{1/2}$, otherwise it is contained in [35, Proposition 1], see also Lemma 2.3.2 below, or in the bound of Theorem 2.1.1.*

Remark 2.1.4. *The method of proof of Theorem 2.1.2 also works without any changes for $\mathrm{T}_{\lambda,\mu}(\mathcal{G}, \mathcal{H})$ with two multiplicative subgroups, similarly to Lemma 2.3.2. However, for subgroups of significantly different sizes the optimisation part becomes rather tedious.*

2.1.3 Previous Results

Recent results on $T(\mathcal{A}, \mathcal{B})$ have been given by using the Cauchy-Schwartz inequality on bounds for $T(\mathcal{A})$. For this reason previous bounds for $T(\mathcal{A}, \mathcal{B})$ are symmetric. We compare our result with that of Aksoy Yazici, Murphy, Rudnev and Shkredov [1, Proposition 5]

$$T(\mathcal{A}) \ll \frac{A^6}{p} + A^{9/2}$$

hence, by the Cauchy-Schwartz inequality,

$$T(\mathcal{A}, \mathcal{B}) \ll \left(\frac{A^3}{p^{1/2}} + A^{9/4}\right)\left(\frac{B^3}{p^{1/2}} + B^{9/4}\right) + AB^3.$$

We see that for $A = B$ the bound in Theorem 2.1.1 is stronger for $p^{1/2} < A < p^{2/3}$ and of the same strength for $A \geqslant p^{2/3}$. More generally, our new bound is stronger when $AB^3 > p^2$. We also compare our result to that of Murphy, Petridis, Roche-Newton, Rudnev and Shkredov [27, Theorem 10],

$$T(\mathcal{A}) \ll \frac{A^6}{p} + A^{7/2}p^{1/2},$$

hence, by the Cauchy-Schwartz inequality,

$$T(\mathcal{A},\mathcal{B}) \ll \left(\frac{A^3}{p^{1/2}} + A^{7/4}p^{1/4}\right)\left(\frac{B^3}{p^{1/2}} + B^{7/4}p^{1/4}\right) + AB^3.$$

We see that our bound is equal to the above result for $A = B$, and stronger otherwise.

We also mention the trivial bound for $A \leqslant B$

$$T(\mathcal{A},\mathcal{B}) \leqslant A^3B^2.$$

It is clear that this comes from taking all possible choice for a_1, a_2, a_3, b_1, b_2 and then there is at most one choice for b_3. It follows that our bound from Theorem 2.1.1 is non-trivial as long as $A^2B > p$. It is also clear that there is an obvious trivial lower bound coming from the zero solutions. Hence

$$T(\mathcal{A},\mathcal{B}) \geqslant AB^3.$$

2.2 Collinear Triples Over Subsets

2.2.1 Preliminaries

In this section we use $\ell = \ell_{c,d}$ to indicate lines of the form $y = cx + d$. We also use the notation

$$\sum_{\ell} = \sum_{c\in\mathbb{F}_p}\sum_{d\in\mathbb{F}_p},$$

to indicate that we are summing over all lines of the form $\ell_{c,d}$.

We mention the following results.

Lemma 2.2.1. *Let $\mathcal{A},\mathcal{B} \in \mathbb{F}_p$ with $|\mathcal{A}| = A, |\mathcal{B}| = B$ and $\lambda,\mu \in \mathbb{F}_p^*$. Then*

$$\sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) = \sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) = pAB$$

and

$$\sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\lambda b}) = A^2B^2 - AB^2 + pAB.$$

Proof. The first result is clear since for each choice of $(x, y, u) \in \mathcal{A} \times \mathcal{B} \times \mathbb{F}_p$ there is a unique choice of $v \in \mathbb{F}_p$ that satisfies $y = ux + v$. The second result we have

$$\sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\lambda b}) = \sum_{(a_1,a_2,b_1,b_2)\in\mathcal{A}^2\times\mathcal{B}^2} |\{(c,d) \in \mathbb{F}_p^2 : b_1 = ca_1 + d, b_2 = \lambda c a_2 + \mu d\}|.$$

Now, we can see there are AB quadruples $(a_1, a_2, b_1, b_2) \in \mathcal{A}^2 \times \mathcal{B}^2$ which are given by $(a_1, b_1) = (\lambda\mu^{-1}a_2, \mu^{-1}b_2)$ which define p pairs $(c, d) = (c, b_1 - ca_1)$. There are $AB(B-1)$ quadruples with $b_1 \neq \mu^{-1}b_2$ and $a_1 = \lambda\mu^{-1}a_2$ which do not define any pairs (c, d), as they are parallel. The remaining

$$A^2B^2 - AB(B-1) - AB = A^2B^2 - AB^2$$

quadruples define one pair (c, d) each, as they are the non-parallel lines. □

We immediately have the following corollary.

Corollary 2.2.2. *Let $\mathcal{A}, \mathcal{B} \in \mathbb{F}_p$ with $|\mathcal{A}| = A, |\mathcal{B}| = B$ and $\lambda, \mu \in \mathbb{F}_p^*$. Then*

$$\sum_{\ell} \left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p} \right)^2 \leqslant pAB.$$

We need an analogue of [27, Lemma 9]. First we recall [27, Theorem 7], which is dependent on incident results of Stevens and de Zeeuw [41].

Lemma 2.2.3. *Let $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ with $|\mathcal{A}| = A \leqslant |\mathcal{B}| = B$ and let L be a collection of lines in $\mathbb{F}_p^2$. Assume that $A|L| \leqslant p^2$. Then the number of incidences $I(P, L)$ between the point set $P = \mathcal{A} \times \mathcal{B}$ and L is bounded by*

$$I(P, L) \ll A^{3/4}B^{1/2}|L|^{3/4} + |P| + |L|.$$

We define $L_{N_{\lambda,\mu}}$ to be the collection of lines that are incident to between N and $2N$ points, that is

$$L_{N_{\lambda,\mu}} = \{\ell_{\lambda a,\mu b} \in L : N < \iota_{A\times B}(\ell_{\lambda a,\mu b}) \leqslant 2N\}$$

for $\lambda, \mu \in \mathbb{F}_p^*$, and L the collection of all lines in $\mathbb{F}_p^2$. We then have the following lemma.

Lemma 2.2.4. *Let $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ with $|\mathcal{A}| = A \leqslant |\mathcal{B}| = B$, $\lambda, \mu \in \mathbb{F}_p^*$ and furthermore let $2AB/p \leqslant N \leqslant A$ be an integer greater than 1. Then*

$$|L_{N_{\lambda,\mu}}| \ll \min\left(\frac{pAB}{N^2}, \frac{A^3B^2}{N^4} \right).$$

Proof. Since $\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) \geqslant N$ for $\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) \in L_{N_{\lambda,\mu}}$ and $AB/p \leqslant N/2$, we have

$$\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - AB/p \geqslant N - N/2 = N/2.$$

Therefore, using Corollary 2.2.2,

$$\begin{aligned}\frac{N^2}{4}|L_{N_{\lambda,\mu}}| &\leqslant \sum_{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})\in L_{N_{\lambda,\mu}}} (\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - AB/p)^2 \\ &\leqslant \sum_{l}(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - AB/p)^2 \\ &\leqslant pAB.\end{aligned} \tag{2.2.1}$$

Now suppose $2AB/p \leqslant N < 2AB^{1/2}/p^{1/2}$. From (2.2.1)

$$|L_{N_{\lambda,\mu}}| \ll \frac{pAB}{N^2} < \frac{pAB}{N^2} \times \frac{4A^2B}{N^2p} = \frac{4A^3B^2}{N^4}.$$

We now suppose $N \geqslant 2AB^{1/2}/p^{1/2} \geqslant 2AB/p$. By (2.2.1) $L_{N_{\lambda,\mu}} \leqslant 4pAB/N^2 \leqslant p^2/A$. We can now apply Lemma 2.2.3 to obtain

$$N|L_{N_{\lambda,\mu}}| \ll A^{3/4}B^{1/2}|L_{N_{\lambda,\mu}}|^{3/4} + AB + |L_{N_{\lambda,\mu}}|.$$

We now observe when each term dominates, omitting the last term as it gives $N \ll 1$, to get

$$|L_{N_{\lambda,\mu}}| \ll \frac{A^3B^2}{N^4} + \frac{AB}{N}.$$

We now recall $N \leqslant A$, hence

$$|L_{N_{\lambda,\mu}}| \ll \frac{A^3B^2}{N^4}.$$

This completes the proof. □

We now need the following lemma.

Lemma 2.2.5. *For $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ with $|\mathcal{A}| = A < |\mathcal{B}| = B$ and $\lambda, \mu \in \mathbb{F}_p^*$,*

$$\sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p}\right)^2 \ll p^{1/2}A^2B^{3/2}.$$

Proof. We begin by splitting our sum over a parameter $\Delta \geqslant 2AB/p$ which will be chosen later. We also observe that $\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) \leqslant A$. We then find a bound on

$$\sum_{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\leqslant\Delta} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p}\right)^2$$
$$+ \sum_{\substack{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta \\ \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})\leqslant\Delta}} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p}\right)^2$$
$$+ \sum_{\substack{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta \\ \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})>\Delta}} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p}\right)^2 = I + II + III.$$

By Corollary 2.2.2 it is clear that $I \leqslant \Delta pAB$. By Lemma 2.2.1 we also have

$$II \leqslant \sum_{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\left(\Delta - \frac{AB}{p}\right)^2$$
$$\leqslant \left(\Delta - \frac{AB}{p}\right)^2 pAB.$$

From Lemma 2.2.1, and using the identity $X^2 = (X-Y)^2 + 2XY - Y^2$, we have

$$\sum_{\substack{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta \\ \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})>\Delta}} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})^2$$
$$\geqslant \sum_{\substack{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta \\ \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})>\Delta}} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p}\right)^2$$
$$+ \frac{3A^2B^2}{p^2} \sum_{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})$$
$$\geqslant \sum_{\substack{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta \\ \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})>\Delta}} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p}\right)^2 = III.$$

We can now use a dyadic decomposition and Lemma 2.2.4 to obtain

$$\sum_{\substack{\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})>\Delta \\ \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})>\Delta}} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})^2 \ll \sum_{k\geqslant 0}(2^k\Delta)^3|L_{2^k\Delta}|$$
$$\ll \sum_{k\geqslant 0}(2^k\Delta)^3\frac{A^3B^2}{(\Delta 2^k)^4}$$
$$\ll \frac{A^3B^2}{\Delta}.$$

Therefore,

$$\sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p} \right)^2 \ll \Delta pAB + II + \frac{A^3B^2}{\Delta}.$$

We choose $\Delta = 2AB^{1/2}/p^{1/2} \geqslant 2AB/p$ to get

$$\begin{aligned} II &\ll \frac{A^2B}{p} \left(1 - \frac{B^{1/2}}{p^{1/2}} \right) p^{3/2}B^{1/2} \\ &\ll p^{1/2}A^2B^{3/2} \end{aligned}$$

and

$$\sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p} \right)^2 \ll p^{1/2}A^2B^{3/2}.$$

This completes the proof. □

2.2.2 Proof of Theorem 2.1.1

We can transform $T_{\lambda,\mu}(\mathcal{A},\mathcal{B})$ to be the number of solutions of

$$\frac{b_1 - \mu b_2}{a_1 - \lambda a_3} = \frac{b_1 - \mu b_3}{a_1 - \lambda a_2},$$

by adding an error term of $O(AB^3 + A^2B^2)$ coming from the trivial cases where $a_1 = \lambda a_2 = \lambda a_3$, or $a_1 = \lambda a_3$ and $b_1 = \mu b_2$, or $a_1 = \lambda a_2$ and $b_1 = \mu b_3$. Then collecting our solutions for each $c \in \mathbb{F}_p$,

$$\frac{b_1 - \mu b_2}{a_1 - \lambda a_3} = \frac{b_1 - \mu b_3}{a_1 - \lambda a_2} = c$$

and rearranging and relabelling, we obtain

$$b_1 - ca_1 = \mu b_2 - \lambda c a_2 = \mu b_3 - \lambda c a_3.$$

Therefore,

$$T_{\lambda,\mu}(\mathcal{A},\mathcal{B}) = \sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})^2 + O(AB^3 + A^2B^2). \tag{2.2.2}$$

We use the result $X^2 = (X-Y)^2 + 2XY - Y^2$ with $X = \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})$ and $Y = AB/p$ and see

$$\begin{aligned} &\sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})^2 \\ &\qquad = \sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{AB}{p} \right)^2 \\ &\qquad\quad + \frac{2AB}{p} \sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{A^2B^2}{p^2} \sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}). \end{aligned} \tag{2.2.3}$$

We now apply Lemma 2.2.1 to obtain,

$$\begin{aligned}&\sum_{\ell}\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})^2\\&\quad=\sum_{\ell}\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})\left(\iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})-\frac{AB}{p}\right)^2+\frac{A^3B^3-2A^3B^2}{p}+2A^2B^2.\end{aligned}\tag{2.2.4}$$

Combining (2.2.2), (2.2.3) and Lemma 2.2.5 we complete the proof.

2.2.3 Consequences

We give some results that come as a consequence of Theorem 2.1.1, these are necessary for our proofs of Theorem 4.1.1 and Theorem 4.1.2.

We define $D_{\lambda,\mu}(\mathcal{A},\mathcal{B})$ to be the number of solutions to

$$(a_1-\lambda a_2)(b_1-\mu b_2)=(a_3-\lambda a_4)(b_3-\mu b_4)\tag{2.2.5}$$

for $(a_i,b_i)\in\mathcal{A}\times\mathcal{B}$, $i=1,2,3,4$, and $\lambda,\mu\in\mathbb{F}_p^*$. We define $T^*_{\lambda,\mu}(\mathcal{A},\mathcal{B})$ to be the number of solutions of

$$(a_1-\lambda a_2)(b_1-\mu b_2)=(a_1-\lambda a_3)(b_1-\mu b_3)\neq 0$$

and, similarly, $D^*_{\lambda,\mu}(\mathcal{A},\mathcal{B})$ to be the number of solutions of

$$(a_1-\lambda a_2)(b_1-\mu b_2)=(a_3-\lambda a_4)(b_3-\mu b_4)\neq 0.$$

We also define $D^*_{1,1}(\mathcal{A},\mathcal{B})=D^*(\mathcal{A},\mathcal{B})$, $D_{1,1}(\mathcal{A},\mathcal{B})=D(\mathcal{A},\mathcal{B})$ and similarly define $T^*_{1,1}(\mathcal{A},\mathcal{B})=T^*(\mathcal{A},\mathcal{B})$.

Lemma 2.2.6. *Let $\mathcal{A},\mathcal{B}\subset\mathbb{F}_p$ with $|\mathcal{A}|=A\leqslant|\mathcal{B}|=B$ and $\lambda,\mu\in\mathbb{F}_p^*$. Then*

$$D^*_{\lambda,\mu}(\mathcal{A},\mathcal{B})\ll p^{1/2}A^3B^{5/2}+\frac{A^4B^4}{p}.$$

Proof. We rearrange $D^*_{\lambda,\mu}(\mathcal{A},\mathcal{B})$ so it is the number of solutions of

$$\frac{b_1-\mu b_2}{a_3-\lambda a_4}=\frac{b_3-\mu b_4}{a_1-\lambda a_2}\neq 0.$$

We define $J(\xi)$ to be the number of quadruples $(a_1,a,b_1,b)\in\mathcal{A}^2\times\mathcal{B}^2$ with

$$\frac{b-\mu b_1}{a-\lambda a_1}=\xi.\tag{2.2.6}$$

We also let $J_{a,b}(\xi)$ be the number of pairs $(a_1, b-!) \in \mathcal{A} \times \mathcal{B}$ for which (2.2.6) holds. Then by the Cauchy-Schwartz inequality, we have

$$\begin{aligned} D^*_{\lambda,\mu}(\mathcal{A},\mathcal{B}) &= \sum_{\xi\in\mathbb{F}_p^*} J(\xi)^2 = \sum_{\xi\in\mathbb{F}_p^*} \left(\sum_{(a,b)\in\mathcal{A}\times\mathcal{B}} J_{a,b}(\xi) \right)^2 \\ &\leqslant AB \sum_{\xi\in\mathbb{F}_p^*} \sum_{(a,b)\in\mathcal{A}\times\mathcal{B}} J_{a,b}(\xi)^2 \\ &= AB \sum_{(a,b)\in\mathcal{A}\times\mathcal{B}} \sum_{\xi\in\mathbb{F}_p^*} J_{a,b}(\xi)^2. \end{aligned}$$

Now

$$\sum_{\xi\in\mathbb{F}_p^*} J_{a,b}(\xi)^2 = |\{(a_1,a_2,b_1,b_2) \in \mathcal{A}^2 \times \mathcal{B}^2 : \frac{b-\mu b_1}{a-\lambda a_1} = \frac{b-\mu b_2}{a-\lambda a_2} \neq 0\}|,$$

hence

$$\begin{aligned} D^*_{\lambda,\mu}(\mathcal{A},\mathcal{B}) &\leqslant ABT^*_{\lambda,\mu}(\mathcal{A},\mathcal{B}) \\ &\leqslant AB \sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b}) \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{\lambda a,\mu b})^2 \\ &\ll p^{1/2}A^3B^{5/2} + \frac{A^4B^4}{p}. \end{aligned}$$

by (2.2.4) and Lemma 2.2.5. This concludes the proof. □

The number of solutions for when (2.2.5) is equal to 0 is $O(A^2B^4 + A^3B^3 + A^4B^2)$ and we therefore get the following simple corollary.

Corollary 2.2.7. *Let $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_p$ with $|\mathcal{A}| = A \leqslant |\mathcal{B}| = B$ and $\lambda, \mu \in \mathbb{F}_p^*$. Then*

$$D_{\lambda,\mu}(\mathcal{A},\mathcal{B}) \ll p^{1/2}A^3B^{5/2} + \frac{A^4B^4}{p} + A^2B^4.$$

We compare the bound of Lemma 2.2.6 to that of Petridis and Shparlinski [30, Corollary 2.9],

$$D^*(\mathcal{A},\mathcal{A}) \ll \frac{A^8}{p} + A^{13/2}.$$

It is clear for the case $A = B$ that our bound is stronger for $A > p^{1/2}$. For $A < B$, by the Cauchy-Schwartz inequality, [30, Corollary 2.9] gives

$$D^*(\mathcal{A},\mathcal{B}) \ll \frac{A^4B^4}{p} + \frac{A^{13/4}B^4}{p^{1/2}} + A^{13/4}B^{13/4}.$$

Again our bound gives stronger results for $A^{1/2}B^{3/2} > p$.

2.3 Collinear Triples Over Subgroups

2.3.1 Preliminaries

We require some previous results. We note that we use Lemma 2.3.1 only for $\mathcal{G} = \mathcal{H}$, however we present it and also some other results in full generality as we believe they may find several other applications and this deserves to be known better.

The first one is a result of Mit'kin [25, Theorem 2] extending that of Heath-Brown and Konyagin [17, Lemma 5], see also [19, 38] for further generalisations.

Lemma 2.3.1. *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 $\mathcal{H}$ respectively in $\mathbb{F}_p^*$. For an arbitrary set $\Theta \subseteq \mathcal{M}_\mathcal{G} \times \mathcal{M}_\mathcal{H}$ such that*

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

we have

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

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 2.3.1 is

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

Hence if, for example, $\mathcal{G} = \mathcal{H}$, then Lemma 2.3.1 always significantly improves this bound.

We recall from (2.2.2) and (2.2.3)

$$\mathrm{T}_{\lambda,\mu}(\mathcal{A},\mathcal{B}) - \frac{|\mathcal{A}|^3|\mathcal{B}|^3}{p} \tag{2.3.1}$$

$$= \sum_{(a,b)\in\mathbb{F}_p^2} \iota_{\mathcal{A},\mathcal{B}}(\ell_{a,b}) \left(\iota_{\mathcal{A},\mathcal{B}}(\ell_{\lambda a,\mu b}) - \frac{|\mathcal{A}||\mathcal{B}|}{p}\right)^2 + O(|\mathcal{A}|^2|\mathcal{B}|^2 + |\mathcal{A}|\mathcal{B}|^3). \tag{2.3.2}$$

Finally, we need the following bound for small subgroups, which is a slightly simplified form of [35, Proposition 1] combined with (2.3.19).

Lemma 2.3.2. *Let $\mathcal{G}$ be a subgroup of $\mathbb{F}_p^*$ with $|\mathcal{G}| \geqslant |\mathcal{H}|$ and $|\mathcal{G}||\mathcal{H}| < p$. Then*

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

2.3.2 Initial Reductions

The argument below follows [35, 36].

First of all, note that Lemma 2.3.2 implies the required result provided $|\mathcal{G}||\mathcal{H}| < p$ while Theorem 2.1.1 implies it for $|\mathcal{G}| \geqslant p^{2/3}$.

So it remains to consider the case

$$p^{2/3} > |\mathcal{G}| > p^{1/2}.$$

Let $\Delta \geqslant 3$ be a parameter to be chosen later. Using Corollary 2.2.2 and (2.3.1), we obtain

$$\mathrm{T}_\lambda(\mathcal{G}) - \frac{|\mathcal{G}|^6}{p} \ll |\mathcal{G}|^4 + \Delta|\mathcal{G}|^2 p + W\,, \tag{2.3.3}$$

where

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

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

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

Thus

$$W = W^* + O\left(|\mathcal{G}|^4\right) \tag{2.3.4}$$

where

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

which is the sum we now consider.

2.3.3 Sets Θ_τ and $\mathcal{Q}_\tau$

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

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

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

$$\mathcal{L}_{\alpha,\beta} = \{(x, y) \in \mathbb{F}_p^2 \ : \ \alpha x + \beta y = 1\} = \ell_{-\alpha\beta^{-1},\beta^{-1}} \tag{2.3.5}$$

have the intersection with $\mathcal{G}^2$ of size

$$\iota_{\mathcal{G}}\left(\ell_{-\alpha\beta^{-1},\beta^{-1}}\right) \geqslant \tau.$$

In particular,

$$\Theta_\tau = \{(\alpha, \beta) \in \mathcal{M}_{\mathcal{G}}^2 \ : \ \iota_{\mathcal{G}}\left(\mathcal{L}_{\alpha,\beta}\right) \geqslant \tau\}. \tag{2.3.6}$$

By Lemma 2.3.1, we have $|\Theta_\tau|\tau \ll (|\mathcal{G}||\Theta_\tau|)^{2/3}$ provided

$$|\mathcal{G}|^4|\Theta_\tau| < p^3 \tag{2.3.7}$$

and

$$|\Theta_\tau| \leqslant |\mathcal{G}|^2. \tag{2.3.8}$$

We also define the set

$$\mathcal{Q}_\tau = \{(\alpha, \beta) \in \left(\mathbb{F}_p^*\right)^2 \ : \ \iota_{\mathcal{G}}\left(\mathcal{L}_{\alpha,\beta}\right) \geqslant \tau\}. \tag{2.3.9}$$

Comparing (2.3.6) and (2.3.9), we see that we can think of Θ_τ as a union of cosets $\mathcal{Q}_\tau/\mathcal{G}$. Clearly, we have

$$|\mathcal{Q}_\tau| = |\mathcal{G}|^2|\Theta_\tau| \ll |\mathcal{G}|^4\tau^{-3} \tag{2.3.10}$$

provided the conditions (2.3.7) and (2.3.8) are satisfied.

The condition (2.3.8) is trivial to verify. Indeed, since $|\mathcal{G}|^2 > p$, we have

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

and thus (2.3.8) holds.

We now show that the condition (2.3.7) also holds for the following choice

$$\Delta = c|\mathcal{G}|^3 p^{-3/2}, \tag{2.3.11}$$

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

Lemma 2.3.3. *For Δ given by* (2.3.11) *the bound* (2.3.7) *holds.*

Proof. Suppose, to the contrary, that

$$|\Theta_\tau| > p^3/|\mathcal{G}|^4 . \tag{2.3.12}$$

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

$$|\mathcal{Q}_\tau|\tau = |\mathcal{G}|^2|\Theta_\tau|\tau > p^3|\mathcal{G}|^{-2}\Delta . \tag{2.3.13}$$

On the other hand, by a classical result which holds over any field (see, for example [8, Corollary 5.2] or [42, 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

$$|\mathcal{Q}_\tau|\tau \leqslant |\mathcal{Q}_\tau|^{1/2}|\mathcal{P}| + |\mathcal{Q}_\tau| \tag{2.3.14}$$

and we obtain

$$|\mathcal{Q}_\tau|\tau^2 \ll |\mathcal{P}|^2 = |\mathcal{G}|^4. \tag{2.3.15}$$

Combining (2.3.13) and (2.3.15), we derive

$$p^3|\mathcal{G}|^{-2}\Delta < |\mathcal{Q}_\tau|\tau \ll |\mathcal{G}|^4\tau^{-1} \leqslant |\mathcal{G}|^4\Delta^{-1}. \tag{2.3.16}$$

Recalling that $|\mathcal{G}| \geqslant p^{1/2}$, we see that for Δ given by (2.3.11) with a sufficiently large constant c the inequalities (2.3.16) are impossible, which also shows that our assumption (2.3.12) is false and this concludes the proof. □

2.3.4 Concluding the Proof of Theorem 2.1.2

We now define

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

By Lemma 2.3.3, for the choice (2.3.11) of Δ we have the desired condition (2.3.7) for any $\tau \geqslant \Delta$. Hence, the bound (2.3.10) also implies that

$$|\mathcal{R}_\tau| = |\mathcal{G}|^2|\Theta_\tau| \ll |\mathcal{G}|^4\tau^{-3}. \tag{2.3.17}$$

We see from (2.3.5) 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

$$J = \left\lceil \log(|\mathcal{G}|/\Delta) \right\rceil .$$

Note that due to the choice of Δ and the condition $|\mathcal{G}| \geqslant p^{1/2}$ we have

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

Then, recalling also the bound (2.3.17), we conclude that the contribution to W^* from the lines with $\tau_{j+1} \geqslant \iota_{\mathcal{G}}(\ell_{a,b}) > \tau_j$ is bounded by

$$\left|\mathcal{R}_{\tau_j}\right| \tau_{j+1} \left(\tau_{j+1} + |\mathcal{G}|^2/p\right)^2 \ll \left|\mathcal{R}_{\tau_j}\right| \tau_{j+1}^3 \ll |\mathcal{G}|^4. \tag{2.3.18}$$

Summing up (2.3.18) we obtain

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

Substituting this bound in (2.3.4) and combining it with (2.3.3), 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 $p^{2/3} \geqslant |\mathcal{G}| \geqslant p^{1/2}$, which concludes the proof.

Remark 2.3.4. *In principle, a stronger version of the classical incidence bound which is used* (2.3.14) *may lead to improvements of Theorem 2.1.2. However, the range where such improvements are known is far away from the range which appears in our applications, see [41].*

2.3.5 Consequences

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

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

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

$$\begin{aligned} \mathrm{T}_{\lambda,\mu}(\mathcal{G}, \mathcal{H}) &= \sum_{(g,h) \in \mathcal{G} \times \mathcal{H}} \mathrm{E}^\times(\mathcal{G} - \lambda g, \mathcal{H} - \mu h) + O(|\mathcal{G}|^3 |\mathcal{H}|). \\ &= |\mathcal{G}||\mathcal{H}| \mathrm{E}^\times(\mathcal{G} - \lambda, \mathcal{H} - \mu) + O(|\mathcal{G}|^3 |\mathcal{H}|), \end{aligned} \tag{2.3.19}$$

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 $\mathrm{T}_{\lambda,\mu}(\mathcal{G}, \mathcal{H})$. It follows that bounds on the number of collinear triples over multiplicative subgroups leads us to new bounds of multiplicative energy over shifted subgroups.

2.4 Open Problems

A natural extension of considering the number of collinear triples is to instead consider the number of collinear quadruples. One can consider this as the fourth moment

$$Q(\mathcal{A},\mathcal{B}) = \sum_{\ell} \iota_{\mathcal{A}\times\mathcal{B}}(\ell_{a,b})^4.$$

Similarly, one can reformulate this, similarly to what we have done to collinear triples, to be the number of solutions to

$$\frac{a_2-a_1}{a_3-a_1} = \frac{b_2-b_1}{b_3-b_1} \qquad \text{and} \qquad \frac{a_4-a_1}{a_2-a_1} = \frac{b_4-b_1}{b_2-b_1}$$

where $a_i \in \mathcal{A}$ and $b_i \in \mathcal{B}$. One can look at [27, 29] for recent bounds on collinear quadruples $Q(\mathcal{A},\mathcal{A}) = Q(\mathcal{A})$. Here we ask the same question as we have for $T(\mathcal{A},\mathcal{B})$ of whether we can give new bounds for $Q(\mathcal{A},\mathcal{B})$ where $\mathcal{A}$ and $\mathcal{B}$ are sets of different sizes. Furthermore, we can also consider the generalisation $Q_{\lambda,\mu}(\mathcal{A},\mathcal{B})$ in a equivalent way to $T_{\lambda,\mu}(\mathcal{A},\mathcal{B})$.

3

A Low Energy Decomposition of Subsets of Finite Fields

3.1 Introduction

3.1.1 Set Up

Let $\mathbb{F}_q$ denote the finite field of q elements of characteristic p.

Given two sets $\mathcal{U}, \mathcal{V} \subset \mathbb{F}_q$ we define their sum and product sets as

$$\mathcal{U} + \mathcal{V} = \{u + v : u \in \mathcal{U}, v \in \mathcal{V}\} \quad \text{and} \quad \mathcal{U} \cdot \mathcal{V} = \{uv : u \in \mathcal{U}, v \in \mathcal{V}\}.$$

We define the additive and multiplicative energy of a set as follows

$$E^+(\mathcal{U}) = \#\{(u_1, u_2, u_3, u_4) \in \mathcal{U}^4 : u_1 + u_2 = u_3 + u_4\}$$
$$E^\times(\mathcal{U}) = \#\{(u_1, u_2, u_3, u_4) \in \mathcal{U}^4 : u_1 u_2 = u_3 u_4\}.$$

We mention the interesting sum-product problem which suggests that at least one of the sets $\mathcal{U} + \mathcal{U}$ and $\mathcal{U} \cdot \mathcal{U}$ must be large. This problem has been studied extensively in recent years, coming initially from work of Bourgain, Katz and Tao [8]. There is a natural relation to the sum-product problem to bounds on additive and

multiplicative energy. For example, by applying the Cauchy-Schwarz inequality one can see that

$$E^{\times}(\mathcal{U}) \geqslant \frac{|\mathcal{U}|^4}{|\mathcal{U}\cdot\mathcal{U}|},$$

and similarly

$$E^{+}(\mathcal{U}) \geqslant \frac{|\mathcal{U}|^4}{|\mathcal{U}+\mathcal{U}|}.$$

It follows that strong upper bounds on energy results correspond to strong lower bounds on the relevant sum-product estimate and vice-versa.

Balog and Wooley [2] proved that in finite fields the set $\mathcal{U}$ can be decomposed into a disjoint union of subsets $\mathcal{V}$ and $\mathcal{W}$ such that $E^{+}(\mathcal{V})$ and $E^{\times}(\mathcal{W})$ are both small. These results have been improved on by Konyagin and Shkredov [20] and Rudnev, Shkredov and Stevens [33].

Our main results are an extension of [31], which themselves are a generalisation of the Balog-Wooley decomposition [2, Theorem 1.3].

3.1.2 Notation

For $a \in \mathbb{F}_q$ and a rational function $f \in \mathbb{F}_q(X)$ we use $r^{+}_{\mathcal{U},\mathcal{V}}(f,a)$ to denote the number of solutions to $f(u)+f(v)=a$, $(u,v)\in\mathcal{U}\times\mathcal{V}$. Similarly, we use $r^{\times}_{\mathcal{U},\mathcal{V}}(f,a)$ to denote the number of solutions to $f(u)f(v)=a$. If $\mathcal{U}=\mathcal{V}$ we write $r^{+}_{\mathcal{U}}(f,a)$ and if $f(X)=X$ we write $r^{+}_{\mathcal{U},\mathcal{V}}(a)$.

For this chapter we use the convention that capital letters in italics, such as $\mathcal{U}$, will be used to represent sets. Corresponding capital letters in Roman will denote their cardinalities, such as $U=|\mathcal{U}|$. We also use $\mathcal{X}$ and Ψ to denote the sets of multiplicative and additive characters respectively, with $\mathcal{X}^*$ indicating all non-principal characters, and we will use the lower case χ and ψ to represent their respective characters.

3.1.3 Main Results

Here we extend the result of [31, Theorem 1.1] to multiplicative energy and a hybrid of additive and multiplicative energies.

Theorem 3.1.1. *For any set $\mathcal{A} \subset \mathbb{F}_q^*$ and any rational function $f \in \mathbb{F}_q(X)$ of degree k which is not of the form $f(X) = rg(X)^d X^\lambda$ where $d|q-1$ and $d \geqslant 2$, there exist disjoint sets $\mathcal{S}, \mathcal{T} \subset \mathcal{A}$ such that $\mathcal{A} = \mathcal{S} \cup \mathcal{T}$ and*

$$\max\{E^\times(\mathcal{S}), E^\times(f(\mathcal{T}))\} \ll_k \frac{A^3}{M(A)}$$

where

$$M(\mathcal{A}) = \min\left\{\frac{q^{1/2}}{A^{1/2}(\log A)^{11/4}}, \frac{A^{4/5}}{q^{2/5}(\log A)^{31/10}}\right\}.$$

Theorem 3.1.2. *For any set $\mathcal{A} \subset \mathbb{F}_q^*$ and any rational function $f \in \mathbb{F}_q(X)$ of degree k which is not of the form $f(X) = g(X)^p - g(X) + \lambda X + \mu$, there exist disjoint sets $\mathcal{S}, \mathcal{T} \subset \mathcal{A}$ such that $\mathcal{A} = \mathcal{S} \cup \mathcal{T}$ and*

$$\max\{E^\times(\mathcal{S}), E^+(f(\mathcal{T}))\} \ll_k \frac{A^3}{M(A)}.$$

Theorem 3.1.3. *For any set $\mathcal{A} \subset \mathbb{F}_q^*$ and any rational function $f \in \mathbb{F}_q(X)$ of degree k which is not of the form $f(X) = rg(X)^d X^\lambda$ where $d|q-1$ and $d \geqslant 2$, there exist disjoint sets $\mathcal{S}, \mathcal{T} \subset \mathcal{A}$ such that $\mathcal{A} = \mathcal{S} \cup \mathcal{T}$ and*

$$\max\{E^+(\mathcal{S}), E^\times(f(\mathcal{T}))\} \ll_k \frac{A^3}{M(A)}.$$

It is simple to check that the above results are all non-trivial for $A > q^{1/2+\epsilon}$, for any fixed $\epsilon > 0$.

We also present the previous result of [31, Theorem 1.1]. It has the same conditions as Theorem 3.1.2 and gives the bound

$$\max\{E^+(\mathcal{S}), E^+(f(\mathcal{T}))\} \ll_k \frac{A^3}{M(A)}.$$

We mention that it was our hope that these results would lead to further applications in bounds of character sums, as in [31]. However, at this stage we were unable to provide such applications due to the restrictions placed on the exceptional functions. Despite this, we still hope that such applications will be possible.

3.2 Energy Bounds

3.2.1 Preliminary Results

We give a series of lemmas, the proofs of which follow those of [31] with multiplicative characters replacing additive characters and other equivalent substitutions.

Lemma 3.2.1. *Let $(\chi, \psi) \in \mathcal{X}^* \times \Psi$ and χ with order d and sets $\mathcal{U}, \mathcal{V} \subset \mathbb{F}_q^*$. For any rational function $f \in \mathbb{F}_q(X)$ of degree k, such that for any integers r and λ f is not of the form $f(X) = rg(X)^d X^\lambda$ if ψ is trivial, we have*

$$\sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \chi(f(uv))\psi(uv) \ll_k \sqrt{UVq}.$$

Proof. Let

$$\Sigma = \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \chi(f(uv))\psi(uv).$$

Then,

$$\begin{aligned}\Sigma &= \sum_{x \in \mathbb{F}_q} \psi(x)\chi(f(x)) \frac{1}{d} \sum_{\substack{\tau \in \mathcal{X}^* \\ \text{ord } \tau | d}} \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \tau(uvx^{-1}) \\ &= \frac{1}{d} \sum_{\substack{\tau \in \mathcal{X}^* \\ \text{ord } \tau | d}} \sum_{x \in \mathbb{F}_q} \psi(x)\chi(f(x))\tau(x^{-1}) \sum_{u \in \mathcal{U}} \tau(u) \sum_{v \in \mathcal{V}} \tau(v).\end{aligned}$$

By the Weil bound we have

$$\Sigma \ll_k \frac{q^{1/2}}{d} \sum_{\substack{\tau \in \mathcal{X}^* \\ \text{ord } \tau | d}} \left| \sum_{u \in \mathcal{U}} \tau(u) \right| \left| \sum_{v \in \mathcal{V}} \tau(v) \right|.$$

Using the Cauchy-Schwarz inequality we obtain

$$\begin{aligned}&\sum_{\substack{\tau \in \mathcal{X}^* \\ \text{ord } \tau | d}} \left| \sum_{u \in \mathcal{U}} \tau(u) \right| \left| \sum_{v \in \mathcal{V}} \tau(v) \right| \\ &\qquad \leqslant \left(\sum_{\substack{\tau \in \mathcal{X}^* \\ \text{ord } \tau | d}} \left| \sum_{u \in \mathcal{U}} \tau(u) \right|^2 \right)^{1/2} \left(\sum_{\substack{\tau \in \mathcal{X}^* \\ \text{ord } \tau | d}} \left| \sum_{v \in \mathcal{V}} \tau(v) \right|^2 \right)^{1/2} \\ &\qquad \leqslant (d^2 UV)^{1/2}.\end{aligned}$$

□

Lemma 3.2.2. *Suppose $\mathcal{U}, \mathcal{V}, \mathcal{Y}, \mathcal{Z} \subset \mathbb{F}_q^*$. For any rational function $f \in \mathbb{F}_q(X)$ of degree k which is not of the form $f(X) = rg(X)^d X^\lambda$ where $d | q-1$ and $d \geqslant 2$, the number of solutions J to the equation*

$$f(uv) = yz \qquad (u, v, y, z) \in \mathcal{U} \times \mathcal{V} \times \mathcal{Y} \times \mathcal{Z}$$

satisfies the bound

$$J \leqslant \frac{UVYZ}{q-1} + O_k((UVYZq)^{1/2}).$$

Proof. Using the approximate orthogonality of multiplicative characters, we have

$$J \leqslant \sum_{(u,v,y,z)\in\mathcal{U}\times\mathcal{V}\times\mathcal{Y}\times\mathcal{Z}} \frac{1}{q-1}\sum_{\chi\in\mathcal{X}^*}\chi(f(uv)(yz)^{-1}).$$

Re-arranging and separating the contribution from the trivial character

$$J-\frac{UVYZ}{q-1} \leqslant \frac{1}{q-1}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{(u,v)\in\mathcal{U}\times\mathcal{V}}\chi(f(uv))\right|\left|\sum_{y\in\mathcal{Y}}\chi(y^{-1})\right|\left|\sum_{z\in\mathcal{Z}}\chi(z^{-1})\right|.$$

Now by Lemma 3.2.1 with the trivial additive character, we have

$$\begin{aligned} J-\frac{UVYZ}{q-1} &\ll_k \frac{\sqrt{UVq}}{q-1}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{y\in\mathcal{Y}}\chi(y^{-1})\right|\left|\sum_{z\in\mathcal{Z}}\chi(z^{-1})\right| \\ &\ll_k \frac{\sqrt{UV}}{q^{1/2}}\cdot(q^2YZ)^{1/2}. \end{aligned}$$

This completes the proof. □

Lemma 3.2.3. *Let $\mathcal{A},\mathcal{S},\mathcal{U}\subset\mathbb{F}_q^*$. Let $u>0$ be such that $r^{\times}_{\mathcal{S},\mathcal{A}^{-1}}(x)\geqslant u$ for all $x\in\mathcal{U}$. Let k be a fixed positive integer and suppose also that*

$$\tau \geqslant 2\frac{kASU}{uq}.$$

Then, for any rational function $f\in\mathbb{F}_q(X)$ of degree k which is not of the form $f(X)=rg(X)^dX^{\lambda}$ where $d|p-1$ and $d\geqslant 2$, we have

$$\#\{x\in\mathbb{F}_q : r^{\times}_{\mathcal{U}}(f,x)\geqslant\tau\} \ll_k \frac{AUSq}{u^2\tau^2}.$$

Proof. Our proof follows [31, Lemma 2.3] where here we replace $r_{\mathcal{U}}(f,x)$ with $r^{\times}_{\mathcal{U}}(f,x)$. Define

$$\mathcal{R}=\{x\in\mathbb{F}_q : r^{\times}_{\mathcal{U}}(f,x)\geqslant\tau\}.$$

Clearly,

$$\tau R \leqslant \sum_{x\in\mathcal{R}} r^{\times}_{\mathcal{U}}(f,x) = \{(x,y,z)\in\mathcal{R}\times\mathcal{U}\times\mathcal{U} : x=f(y)f(z)\}.$$

Now $r^{\times}_{\mathcal{S},\mathcal{A}^{-1}}(z)\geqslant u$ for $z\in\mathcal{U}$, hence

$$\begin{aligned} &\#\{(x,y,z)\in\mathcal{R}\times\mathcal{U}\times\mathcal{U} : x=f(y)f(z)\} \\ &\qquad\leqslant u^{-1}\#\{(v,w,x,y)\in\mathcal{S}\times\mathcal{A}\times\mathcal{R}\times\mathcal{U} : x=f(y)f(vw^{-1})\}. \end{aligned}$$

Therefore, we have

$$\begin{aligned}\tau uR &\leqslant \#\{(v,w,x,y) \in \mathcal{S}\times\mathcal{A}\times\mathcal{R}\times\mathcal{U} : x = f(y)f(vw^{-1})\}\\ &\leqslant k\cdot\#\{(v,w,x,z) \in \mathcal{S}\times\mathcal{A}\times\mathcal{R}\times f(\mathcal{U}) : x = zf(vw^{-1})\}.\end{aligned}$$

We then apply Lemma 3.2.2 to obtain

$$\tau uR \leqslant \frac{kARSU}{q} + O_k((ARSUq)^{1/2}).$$

The assumed lower bound on τ implies

$$\tau uR \ll_k (ARSUq)^{1/2}.$$

This concludes the proof. □

Lemma 3.2.4. *Let $\mathcal{A}_1,\dots,\mathcal{A}_n \subset \mathbb{F}_q^*$. Then*

$$E^\times\left(\bigcup_{i=1}^n \mathcal{A}_i\right) \leqslant \left(\sum_{i=1}^n E^\times(\mathcal{A}_i)^{1/4}\right)^4.$$

Proof. We assume the sets $\mathcal{A}_1,\dots,\mathcal{A}_n$ are disjoint. Then using the Cauchy-Schwarz inequality twice we have,

$$\begin{aligned}E^\times\left(\bigcup_{i=1}^n \mathcal{A}_i\right) &= \sum_{i,j,k,\ell=1}^n \sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_i,\mathcal{A}_j}(x) r^\times_{\mathcal{A}_k,\mathcal{A}_\ell}(x)\\ &\leqslant \sum_{i,j,k,\ell=1}^n \left(\sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_i,\mathcal{A}_j}(x)^2\right)^{1/2}\left(\sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_k,\mathcal{A}_\ell}(x)^2\right)^{1/2}\\ &= \left(\sum_{i,j=1}^n \left(\sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_i,\mathcal{A}_j}(x)^2\right)^{1/2}\right)^2\\ &= \left(\sum_{i,j=1}^n \left(\sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_i,\mathcal{A}_i^{-1}}(x) r^\times_{\mathcal{A}_j,\mathcal{A}_j^{-1}}(x)\right)^{1/2}\right)^2\\ &\leqslant \left(\sum_{i,j=1}^n \left(\sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_i,\mathcal{A}_i^{-1}}(x)^2\right)^{1/4}\left(\sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_j,\mathcal{A}_j^{-1}}(x)^2\right)^{1/4}\right)^2\\ &= \left(\sum_{i=1}^n \left(\sum_{x\in\mathbb{F}_q} r^\times_{\mathcal{A}_i,\mathcal{A}_i^{-1}}(x)^2\right)^{1/4}\right)^4 = \left(\sum_{i=1}^n E^\times(\mathcal{A}_i)^{1/4}\right)^4.\end{aligned}$$

This concludes the proof. □

Lemma 3.2.5. *Let $\mathcal{A} \subset \mathbb{F}_q$. Then for any rational function $f \in \mathbb{F}_q(X)$ of degree k which is not of the form $f(X) = rg(X)^d X^\lambda$ where $d|p-1$ and $d \geqslant 2$, there exists $\mathcal{U} \subset \mathcal{A}$ of cardinality U such that*

$$U \gg \frac{E^\times(\mathcal{A})^{1/2}}{A^{1/2}(\log A)^{7/4}}$$

and

$$E^\times(f(\mathcal{U})) \ll_k \frac{AU^6q^{-1}(\log A)^{11/2} + AU^3q(\log A)^6}{E^\times(\mathcal{A})}.$$

Proof. Clearly,

$$E^\times(\mathcal{A}) = \sum_{x \in \mathcal{A}\cdot\mathcal{A}} r^\times_{\mathcal{A}}(x)^2.$$

We dyadically decompose this sum and define the set

$$\mathcal{S}^\times = \{x \in \mathcal{A}\cdot\mathcal{A} : \rho \leqslant r^\times_{\mathcal{A}}(x) < 2\rho\}$$

with some integer $1 \leqslant \rho \leqslant A$ where ρ is a power of 2, and such that

$$\rho^2 S \gg \frac{E^\times(\mathcal{A})}{\log A}, \tag{3.2.1}$$

where $|\mathcal{S}^\times| = S$. Consider

$$\mathcal{P} = \{(a,b) \in \mathcal{A}\times\mathcal{A} : ab \in \mathcal{S}^\times\}.$$

Now we have

$$\rho S \leqslant P < 2\rho S. \tag{3.2.2}$$

We then make another dyadic decomposition of $\mathcal{S}$ to find a large subset supported on vertical lines. That is, we define

$$\mathcal{A}_x = \{y : (x,y) \in \mathcal{P}\}.$$

Therefore, for some s there exists a dyadic set

$$\mathcal{V} = \{x \in \mathcal{A} : s \leqslant \mathcal{A}_x < 2s\}$$

such that

$$Vs \gg \frac{P}{\log A} \gg \frac{\rho S}{\log A}. \tag{3.2.3}$$

We now separate into two cases. First, suppose

$$V \geqslant \frac{s}{(\log A)^{1/2}}.$$

Then for any $x \in \mathcal{V}$, there exist

$$y_1, y_2, \dots, y_s \in \mathcal{A}_x \subset \mathcal{A}$$

such that $(x, y_i) \in \mathcal{P}$ for all $1 \leqslant i \leqslant s$. Therefore

$$xy_1, xy_2, \dots, xy_s \in \mathcal{S}^{\times}.$$

It follows that $r^{\times}_{\mathcal{S}^{\times},\mathcal{A}^{-1}}(x) \geqslant s$ for every $x \in \mathcal{V}$ and in this case we define

$$\mathcal{U} = \mathcal{V} \qquad \text{and} \qquad u = s. \tag{3.2.4}$$

Now suppose

$$V < \frac{s}{(\log A)^{1/2}}.$$

We now consider the point set

$$\mathcal{Q} = \{(x, y) \in \mathcal{P} : x \in \mathcal{V}\}.$$

As before, for any $x \in \mathcal{V}$ there exist at least s values of $y \in \mathcal{A}_x \subset \mathcal{A}$ with $(x, y) \in \mathcal{P}$. Hence $Q \geqslant Vs$.

For any $y \in \mathbb{F}_q$ we define

$$\mathcal{B}_y = \{x : (x, y) \in \mathcal{Q}\}.$$

Clearly,

$$\sum_{y \in \mathcal{A}} B_y = Q.$$

Therefore, for some t there exists a dyadic set

$$\mathcal{W} = \{y \in \mathcal{A} : t \leqslant B_y < 2t\}$$

such that

$$Wt \gg \frac{Q}{\log A} \geqslant \frac{Vs}{\log A}. \tag{3.2.5}$$

Now since $\mathcal{Q} \subset \mathcal{V} \times \mathcal{A}$ we also have $t \leqslant V$. From (3.2.5) and our assumption on s we have

$$WV \geqslant Wt \gg \frac{Vs}{\log A} > \frac{V^2}{(\log A)^{1/2}},$$

hence

$$W \gg \frac{V}{(\log A)^{1/2}} \geqslant \frac{t}{(\log A)^{1/2}}. \tag{3.2.6}$$

Now, by (3.2.5) and (3.2.3)

$$Wt \gg \frac{Vs}{\log A} \gg \frac{\rho S}{(\log A)^2}. \tag{3.2.7}$$

Now, let $y \in \mathcal{W}$. Then there exist $x_1, \dots, x_t \in \mathcal{A}$ such that $(x_i, y) \in \mathcal{P}$ for all $1 \leqslant i \leqslant t$. Therefore,

$$x_1 y, \dots, x_t y \in \mathcal{S}.$$

Then $r^{\times}_{\mathcal{S},\mathcal{A}^{-1}}(y) \geqslant t$ for every $y \in \mathcal{W}$.

We then take

$$\mathcal{U} = \mathcal{W} \qquad \text{and} \qquad u = t. \tag{3.2.8}$$

It is clear for both (3.2.4) and (3.2.8) we have $\mathcal{U} \subset \mathcal{A}$,

$$U \gg \frac{u}{(\log A)^{1/2}} \tag{3.2.9}$$

and

$$uU \gg \frac{\rho S}{(\log A)^2} \tag{3.2.10}$$

where $r^{\times}_{\mathcal{S},\mathcal{A}^{-1}}(x) \geqslant u$ for all $x \in \mathcal{U}$. Multiplying (3.2.9) and (3.2.10) and using (3.2.1) we obtain

$$U^2 \gg \frac{\rho S}{(\log A)^{5/2}} \gg \frac{E^{\times}(\mathcal{A})}{A(\log A)^{7/2}}. \tag{3.2.11}$$

We now need a bound on $E^{\times}(f(\mathcal{U}))$. We have

$$E^{\times}(f(\mathcal{U})) = \sum_{x \in \mathbb{F}_q} r^{\times}_{f(\mathcal{U})}(x)^2 \leqslant \sum_{x \in \mathbb{F}_q} r^{\times}_{\mathcal{U}}(f, x)^2. \tag{3.2.12}$$

We define the set

$$\mathcal{R}_0 = \left\{ x \in \mathbb{F}_q : r^{\times}_{\mathcal{U}}(f, x) \leqslant 2\frac{kASU}{uq} \right\}$$

and for $J = \lceil \log A / \log 2 \rceil$, we define the sets

$$\mathcal{R}_j = \left\{ x \in \mathbb{F}_q : 2^j \frac{kASU}{uq} < r_{\mathcal{U}}^{\times}(f,x) \leqslant 2^{j+1} \frac{AkSU}{uq} \right\}, \ j = 1, \dots, J.$$

Since,

$$\sum_{x \in \mathbb{F}_q} r_{\mathcal{U}}^{\times}(f,x) = U^2$$

we have

$$\sum_{x \in \mathcal{R}_0} r_{\mathcal{U}}^{\times}(f,x)^2 \leqslant 2\frac{kASU}{uq} \sum_{x \in \mathbb{F}_q} r_{\mathcal{U}}^{\times}(f,x) \ll \frac{kASU^3}{uq}. \tag{3.2.13}$$

For $i = 1, \dots, J$, we apply Lemma 3.2.3 with

$$\tau = 2^j \frac{AkSU}{uq}$$

to obtain

$$\sum_{x \in \mathcal{R}_j} r_{\mathcal{U}}^{\times}(f,x)^2 \leqslant (2\tau)^2 R_j \ll_k \frac{ASUq}{u^2}. \tag{3.2.14}$$

Combining (3.2.13) and (3.2.14) we get

$$E^{\times}(f(\mathcal{U})) \ll_k \frac{ASU^3}{uq} + \frac{ASUq}{u^2} \log A. \tag{3.2.15}$$

Now, multiplying (3.2.10) with (3.2.11) and applying (3.2.1), we obtain

$$uU^3 \gg \frac{\rho^2 S^2}{(\log A)^{9/2}} \gg \frac{SE^{\times}(\mathcal{A})}{(\log A)^{11/2}}$$

which gives

$$\frac{S}{u} \ll \frac{U^3 (\log A)^{11/2}}{E^{\times}(\mathcal{A})}. \tag{3.2.16}$$

Also, squaring (3.2.10) and applying (3.2.1)

$$u^2U^2 \gg \frac{\rho^2 S^2}{(\log A)^4} \gg \frac{SE^{\times}(\mathcal{A})}{(\log A)^5}$$

which gives

$$\frac{S}{u^2} \ll \frac{U^2 (\log A)^5}{E^{\times}(\mathcal{A})}. \tag{3.2.17}$$

Applying (3.2.16) and (3.2.17) into the first and second terms of (3.2.15) respectively we obtain

$$E^{\times}(f(\mathcal{U})) \ll_k \frac{AU^6 q^{-1} (\log A)^{11/2} + AU^3 q (\log A)^6}{E^{\times}(\mathcal{A})}.$$

This concludes the proof. □

Corollary 3.2.6. *Let $\mathcal{A} \subset \mathbb{F}_q$. Then for any rational function $f \in \mathbb{F}_q(X)$ of degree k which is not of the form $f(X) = g(X)^p - g(X) + \lambda X + \mu$, there exists $\mathcal{U} \subset \mathcal{A}$ of cardinality U such that*

$$U \gg \frac{E^\times(\mathcal{A})^{1/2}}{A^{1/2}(\log A)^{7/4}}$$

and

$$E^+(f(\mathcal{U})) \ll_k \frac{AU^6q^{-1}(\log A)^{11/2} + AU^3q(\log A)^6}{E^\times(\mathcal{A})}.$$

Proof. We follow the proof of Lemma 3.2.5, however we replace $E^\times$ with E^+ in (3.2.12), and then use analogous results following from [31, Equation 2.12]. Explicitly, we have

$$E^+(f(\mathcal{U})) = \sum_{x\in\mathbb{F}_q} r^+_{f(\mathcal{U})}(x)^2 \leqslant \sum_{x\in\mathbb{F}_q} r^+_{\mathcal{U}}(f,x)^2. \tag{3.2.18}$$

We define the set

$$\mathcal{R}^+_0 = \left\{x \in \mathbb{F}_q : r^+_{\mathcal{U}}(f,x) \leqslant 2\frac{kASU}{uq}\right\}$$

and for $J = \lceil \log A/\log 2\rceil$, we define the sets

$$\mathcal{R}^+_j = \left\{x \in \mathbb{F}_q : 2^j\frac{kASU}{uq} < r^+_{\mathcal{U}}(f,x) \leqslant 2^{j+1}\frac{AkSU}{uq}\right\},\ j = 1,\dots,J.$$

Since,

$$\sum_{x\in\mathbb{F}_q} r^+_{\mathcal{U}}(f,x) = U^2$$

we have

$$\sum_{x\in\mathcal{R}^+_0} r^+_{\mathcal{U}}(f,x)^2 \leqslant 2\frac{kASU}{uq}\sum_{x\in\mathbb{F}_q} r^+_{\mathcal{U}}(f,x) \ll \frac{kASU^3}{uq}. \tag{3.2.19}$$

For $i = 1,\dots,J$, we apply [31, Lemma 2.3] (which is the additive version of our Lemma 3.2.3) with

$$\tau = 2^j\frac{AkSU}{uq}$$

to obtain

$$\sum_{x\in\mathcal{R}^+_j} r^+_{\mathcal{U}}(f,x)^2 \leqslant (2\tau)^2R^+_j \ll_k \frac{ASUq}{u^2}. \tag{3.2.20}$$

Combining (3.2.19) and (3.2.20) we get

$$E^+(f(\mathcal{U})) \ll_k \frac{ASU^3}{uq} + \frac{ASUq}{u^2}\log A. \tag{3.2.21}$$

Applying (3.2.16) and (3.2.17) into the first and second terms of (3.2.21) respectively we obtain

$$E^+(f(\mathcal{U})) \ll_k \frac{AU^6q^{-1}(\log A)^{11/2} + AU^3q(\log A)^6}{E^\times(\mathcal{A})}.$$

This concludes the proof as the first result is given in Lemma 3.2.5. □

Corollary 3.2.7. *Let $\mathcal{A} \subset \mathbb{F}_q$. Then for any rational function $f \in \mathbb{F}_q(X)$ of degree k which is not of the form $f(X) = rg(x)^d x^\lambda$ where $d|p-1$ and $d \geqslant 2$, there exists $\mathcal{U} \subset \mathcal{A}$ of cardinality U such that*

$$U \gg \frac{E^+(\mathcal{A})^{1/2}}{A^{1/2}(\log A)^{7/4}}$$

and

$$E^\times(f(\mathcal{U})) \ll_k \frac{AU^6q^{-1}(\log A)^{11/2} + AU^3q(\log A)^6}{E^+(\mathcal{A})}.$$

Proof. We follow the proof of [31, Lemma 2.5], however we replace E^+ with $E^\times$ in equation there (2.12) and the proceed as in our Lemma 3.2.5. Explicitly, from [31, Equation (2.11)]

$$U^2 \gg \frac{E^+(\mathcal{A})}{A(\log A)^{7/2}} \tag{3.2.22}$$

and from (3.2.15)

$$E^\times(f(\mathcal{U})) \ll_k \frac{ASU^3}{uq} + \frac{ASUq}{u^2}\log A.$$

Again from [31], we have

$$\frac{S}{u} \ll \frac{U^3(\log A)^{11/2}}{E^+(\mathcal{A})} \tag{3.2.23}$$

and

$$\frac{S}{u^2} \ll \frac{U^2(\log A)^5}{E^+(\mathcal{A})}. \tag{3.2.24}$$

Substituting into (3.2.15) we obtain

$$E^\times(f(\mathcal{U})) \ll_k \frac{AU^6q^{-1}(\log A)^{11/2} + AU^3q(\log A)^6}{E^+(\mathcal{A})}.$$

This concludes the proof. □

3.2.2 Proof of Theorem 3.1.1

Proof. Our strategy is to construct nested sequences of subsets

$$\varnothing = \mathcal{U}_1 \subset \cdots \subset \mathcal{U}_m$$

and

$$\mathcal{V}_m \subset \cdots \subset \mathcal{V}_1 = \mathcal{A}$$

where the disjoint union $\mathcal{U}_i \sqcup \mathcal{V}_i = \mathcal{A}$. We suppose $E^{\times}(\mathcal{V}_i) > A^3/M(\mathcal{A})$ for some i. By Lemma 3.2.5 there exists $\mathcal{W}_i \subset \mathcal{V}_i$ such that

$$W_i \gg \frac{E^{\times}(\mathcal{V}_i)^{1/2}}{V_i^{1/2}(\log V_i)^{7/4}} \gg \frac{A}{M(\mathcal{A})^{1/2}(\log A)^{7/4}}$$

and

$$\begin{aligned} E^{\times}(f(\mathcal{W}_i)) &\ll_k \frac{V_i W_i^6 q^{-1}(\log V_i)^{11/2} + V_i W_i^3 q(\log V_i)^6}{E^{\times}(\mathcal{V}_i)} \\ &\ll_k \frac{M(\mathcal{A})}{A^3}\left(\frac{V_i W_i^6 (\log A)^{11/2}}{q} + V_i W_i^3 q(\log A)^6\right). \end{aligned} \tag{3.2.25}$$

It is clear that we have

$$V_i \ll W_i M(\mathcal{A})^{1/2}(\log A)^{7/4}. \tag{3.2.26}$$

We now define $\mathcal{V}_{i+1} = \mathcal{V}_i \backslash \mathcal{W}_i$. Hence, $\mathcal{U}_{i+1} = \mathcal{U}_i \sqcup \mathcal{W}_i$. Iterating, we have

$$\mathcal{U}_{i+1} = \bigsqcup_{j=1}^{i} \mathcal{W}_i.$$

We note that we have a uniform lower bound on $\mathcal{W}_i$ and so V_i is strictly decreasing. Hence, we can reach the desired result

$$V_m \leqslant A^3/M(\mathcal{A}),$$

at which point we terminate the sequence.

Now, by Lemma 3.2.4, (3.2.25) and (3.2.26)

$$\begin{aligned} E^{\times}(f(\mathcal{U}_m))^{1/4} &= \left(E^{\times}\left(\bigcup_{i=1}^{m-1} f(\mathcal{W}_i)\right)\right)^{1/4} \leqslant \sum_{i=1}^{n} E^{\times}(f(\mathcal{W}_i))^{1/4} \\ &\ll_k \sum_{i=1}^{m-1}\left(\frac{M(\mathcal{A})}{A^3}\left(\frac{V_i W_i^6(\log A)^{11/2}}{q} + V_i W_i^3 q(\log A)^6\right)\right)^{1/4} \\ &\ll_k \sum_{i=1}^{m-1}\left(\frac{M(\mathcal{A})}{A^3}\left(\frac{V_i W_i^6(\log A)^{11/2}}{q} + M(\mathcal{A})^{1/2} W_i^4 q(\log A)^{31/4}\right)\right)^{1/4}. \end{aligned}$$

Clearly, $A \geqslant V_i \geqslant W_i$, hence $V_i W_i^6 \leqslant A^3 W_i^4$ so

$$E^{\times}(f(\mathcal{U}_m))^{1/4} \ll_k \left(\frac{M(\mathcal{A})(\log A)^{11/2}}{q} + \frac{M(\mathcal{A})^{3/2} q(\log A)^{31/4}}{A^3}\right)^{1/4} \sum_{i=1}^{m-1} W_i.$$

Since the $\mathcal{W}_i$ are disjoint we have

$$\sum_{i=1}^{m-1} W_i \leqslant A.$$

Hence,

$$E^{\times}(f(\mathcal{U}_m)) \ll_k \frac{A^4 M(\mathcal{A})(\log A)^{11/2}}{q} + A M(\mathcal{A})^{3/2} q(\log(A))^{31/4}. \tag{3.2.27}$$

We now choose $M(\mathcal{A})$ as in the statement of Theorem 3.1.1 to balance (3.2.27) and

$$E^{\times}(\mathcal{V}_m) \leqslant \frac{A^3}{M(\mathcal{A})}.$$

This completes the proof. □

3.2.3 Proofs of Theorems 3.1.2 and 3.1.3

Proof. The proofs follow that of Theorem 3.1.1 but Corollary 3.2.6 and Corollary 3.2.7 are used in place of Lemma 3.2.5 respectively. □

3.3 Open Problems

As mentioned in the beginning of this chapter, the hope in finding our bounds was to be able to give applications to certain types of character sums. For example, the authors in [31] are able to give some bounds on certain types of additive and multiplicative character sums, mixed character sums and incomplete bilinear sums

of Kloosterman sums. Unfortunately we have been unable to provide similar applications for natural choices of character sums, so here we leave the challenge for the reader to find some applications to some interesting sums.

We also leave the question of whether we can consider a slightly more general problem of

$$\max\{E^*(S), E^*(f(T), g(T))$$

where $* = \{+, \times\}$, and f and g are suitably chosen functions. This was raised in [31] and we extend it by taking any choice of additive or multiplicative energy. [31] also leaves a question on bivariate polynomials which we encourage the reader to consider.

4

Multilinear Exponential Sums

4.1 Trilinear and Quadrilinear Exponential Sums

4.1.1 Set Up

We define the weighted trilinear exponential sums over sets $\mathcal{X}, \mathcal{Y}, \mathcal{Z} \subset \mathbb{F}_p$

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sum_{z \in \mathcal{Z}} \rho_{x,y} \sigma_{x,z} \tau_{y,z} \, \mathbf{e}_p(axyz),$$

where $a \in \mathbb{F}_p^*$ and $\rho_{x,y}, \sigma_{x,z}, \tau_{y,z}$ are 2-dimensional weights that are bounded by 1.

Similarly, we define the weighted quadrilinear exponential sums over sets $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z} \subset \mathbb{F}_p$

$$\begin{aligned} &T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau) \\ &\qquad = \sum_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sum_{z \in \mathcal{Z}} \vartheta_{w,x,y} \rho_{w,x,z} \sigma_{w,y,z} \tau_{x,y,z} \, \mathbf{e}_p(awxyz), \end{aligned}$$

where $a \in \mathbb{F}_p^*$ and $\vartheta_{w,x,y}, \rho_{w,x,z}, \sigma_{w,y,z}, \tau_{x,y,z}$ are 3-dimensional weights that are bounded by 1.

4.1.2 New Results

Using Lemma 2.2.6, which comes as a consequence of Theorem 2.1.1, we provide the following new bounds on trilinear and quadrilinear exponential sums.

Theorem 4.1.1. *Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z} \subset \mathbb{F}_p$ with $|\mathcal{X}| = X$, $|\mathcal{Y}| = Y$, $|\mathcal{Z}| = Z$, and $X \geqslant Y \geqslant Z$. Then,*

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) \ll p^{3/16} X^{13/16} Y^{7/8} Z^{7/8}.$$

We compare the above the result with previous bounds in the following section. As an example, in the special case where $X = Y = Z$ the bound from Theorem 4.1.1 is stronger than previous results for $p^{1/2} < X < p^{5/9}$.

Theorem 4.1.2. *Let $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z} \subset \mathbb{F}_p^*$ with $|\mathcal{W}| = W, |\mathcal{X}| = X, |\mathcal{Y}| = Y$, $|\mathcal{Z}| = Z$ and $W \geqslant X \geqslant Y \geqslant Z$. Then,*

$$T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau) \ll p^{3/32} W^{29/32} X^{15/16} Y^{15/16} Z^{31/32} + p^{1/32} W^{29/32} X Y^{15/16} Z + W X^{15/16} Y Z^{31/32} + p^{-1/16} W X Y Z + W X Y^{7/8} Z.$$

Again, we give an example of when our bound is non-trivial by considering the special case $W = X = Y = Z$ and note that the bound from Theorem 4.1.2 is stronger than existing bounds for $p^{1/2} < W < p^{3/4}$.

In the proof we also compare it to the classical bilinear bound in the case of one-dimensional weights. In this context it also is non-trivial for $p^{1/2} < W < p^{13/24}$.

4.1.3 Previous Results

Trilinear sums have been estimated by Bourgain and Garaev [5]. Variations and improvements have been made since, see [3, 4, 6, 16, 28]. More recently Petridis and Shparlinski [30] have given new bounds on weighted trilinear and quadrilinear exponential sums. We compare our bound on trilinear sums to [30, Theorem 1.3]

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) \ll p^{1/8} X^{7/8} Y^{29/32} Z^{29/32} + X Y Z^{3/4}.$$

We see that our new bound, Theorem 4.1.1, improves that of Petridis and Shparlinski [30] for $XY^{1/2}Z^{1/2} \geqslant p$. Our bound from Theorem 4.1.1 is stronger than that of the triangle inequality

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) \ll XYZ$$

for $XY^{2/3}Z^{2/3} > p$. Similarly, it is also stronger than the classical bound on bilinear sums (with one-dimensional weights), from Lemma 4.1.3,

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) \ll p^{1/2}X^{1/2}Y^{1/2}Z$$

for $XY^{6/5}Z^{-2/5} \leqslant p$. Letting $X = Y = Z$ we see that under these conditions Theorem 4.1.1 is stronger than previous bounds for $p^{1/2} < X < p^{5/9}$. We give another example for when our bound is non-trivial. Setting $X = p^{2/3}, Y = Z = p^{2/5}$ we obtain from Theorem 4.1.1

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) \ll p^{343/240} = XYZp^{-3/80}.$$

One can easily compare this with results from previous bounds and see that our new bound is stronger. We also mention that our bound is strongest for X much larger than Y. We finally mention the bound on unweighted trilinear sums due to Garaev [16]. We note that when our bound is stronger than that of Shparlinski and Petridis [30], it also outperforms that of Garaev [16].

Similarly, we also compare our results on quadrilinear exponential sums to [30, Theorem 1.4]

$$T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau) \ll p^{1/16}W^{15/16}(XY)^{61/64}Z^{31/32} + WXY^{7/8}Z, \tag{4.1.1}$$

as well as that coming from the classical bound on bilinear sums (for one-dimensional weights),

$$T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau) \ll p^{1/2}W^{1/2}X^{1/2}YZ. \tag{4.1.2}$$

For $W = X = Y = Z$ Theorem, 4.1.2 is stronger than the classical bound and (4.1.1) for all $p^{1/2} < W < p^{13/24}$, in this range it is also stronger than the bound of Petridis and Shparlinski [30]. We give another example for when our bound is non-trivial. Setting $W = p^{2/3}, X = Y = Z = p^{3/8}$ we obtain from Theorem 4.1.2

$$T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau) \ll p^{1355/768} = WXYZp^{-7/256}.$$

We also mention that our bound is strongest for W much larger than X.

4.1.4 Preliminaries

We recall the classical bound for bilinear exponential sums, see [5, Equation 1.4] or [16, Lemma 4.1].

Lemma 4.1.3. *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*

$$\sum_{x\in\mathcal{X}} |\alpha_x|^2 = A \qquad \text{and} \qquad \sum_{y\in\mathcal{Y}} |\beta_y|^2 = B,$$

we have

$$\left|\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} \alpha_x\beta_y \,\mathbf{e}_p(xy)\right| \leqslant \sqrt{pAB}.$$

We define $N(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ to be the number of solutions to

$$x_1(y_1 - z_1) = x_2(y_2 - z_2)$$

with $x_1, x_2 \in \mathcal{X}$, $y_1, y_2 \in \mathcal{Y}$ and $z_1, z_2 \in \mathcal{Z}$. We now recall [30, Corollary 2.4].

Lemma 4.1.4. *Let $\mathcal{X}, \mathcal{Y}, \mathcal{Z} \subset \mathbb{F}_p^*$ with $|\mathcal{X}| = X$, $|\mathcal{Y}| = Y$, $|\mathcal{Z}| = Z$. Then*

$$N(\mathcal{X}, \mathcal{Y}, \mathcal{Z}) \ll \frac{X^2Y^2Z^2}{p} + X^{3/2}Y^{3/2}Z^{3/2} + MXYZ$$

where $M = \max(X, Y, Z)$.

We also recall [30, Lemma 2.10].

Lemma 4.1.5. *Let $n \geqslant 2$. For any additive character ϕ of $\mathbb{F}_q$, sets $\mathcal{X}_i \subseteq \mathbb{F}_q$ with $|\mathcal{X}_i| = X_i$ and weights $w_i = (w_i(\mathbf{x}))_{\mathbf{x}\in\mathbb{F}_q^n}$ such that $w_i(\mathbf{x})$ does not depend on the ith coordinate of $\mathbf{x} = (x_1, \dots, x_n)$,*

$$\max_{\mathbf{x}\in\mathbb{F}_q^n} |w_i(\mathbf{x})| \leqslant 1$$

for $i = 1, \dots, n$, and

$$T_\phi(\mathcal{X}_1, \dots, \mathcal{X}_n; w_1, \dots, w_n) = \sum_{x_1\in\mathcal{X}_1} \dots \sum_{x_n\in\mathcal{X}_n} \omega_1(\mathbf{x}) \dots \omega_n(\mathbf{x})\phi(x_1 \dots x_n),$$

we have

$$\begin{aligned}|T_\phi(\mathcal{X}_1, \dots, \mathcal{X}_n; w_1, \dots, w_n)|^{2^{n-1}} \\ \leqslant X_1^{2^{n-1}-1}(X_2 \dots X_n)^{2^{n-1}-2} \sum_{x_2,y_2\in\mathcal{X}_2} \dots \sum_{x_n,y_n\in\mathcal{X}_n} \\ \left|\sum_{x_1\in\mathcal{X}_1} \phi(x_1(x_2 - y_2) \dots (x_n - y_n))\right|.\end{aligned}$$

4.1.5 Proof of Theorem 4.1.1

Our proof follows [30, Theorem 1.3] but we use Lemma 2.2.6 to give a new bound on trilinear exponential sums.

By Lemma 4.1.5 we have

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)^4 \leqslant X^2Y^3Z^2 \sum_{x_1,x_2 \in \mathcal{X}} \sum_{z_1,z_2 \in \mathcal{Z}} \left| \sum_{y \in \mathcal{Y}} \mathbf{e}_p(y(x_1 - x_2)(z_1 - z_2)) \right|.$$

Now the number of quadruples which satisfy $(x_1 - x_2)(z_1 - z_2) = 0$ is at most $O(X^2Z)$, in which case the inner sum is equal to Y. Hence,

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)^4 \ll X^2Y^3Z^2 \sum_{\substack{x_1,x_2 \in \mathcal{X} \\ x_1 \neq x_2}} \sum_{\substack{z_1,z_2 \in \mathcal{Z} \\ z_1 \neq z_2}} \left| \sum_{y \in \mathcal{Y}} \mathbf{e}_p(y(x_1 - x_2)(z_1 - z_2)) \right| + X^4Y^4Z^3.$$

We now collect the quadruples $(x_1, x_2, z_1, z_2) \in \mathcal{X}^2 \times \mathcal{Z}^2$ with the value of the product $(x_1 - x_2)(z_1 - z_2) = \lambda \in \mathbb{F}_p^*$. And we let $J(\lambda)$ be the number of such quadruples for each λ. Hence,

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)^4 \ll X^2Y^3Z^2 \sum_{\lambda \in \mathbb{F}_p^*} \left| \sum_{y \in \mathcal{Y}} J(\lambda)\, \mathbf{e}_p(y\lambda) \right| + X^4Y^4Z^3.$$

Applying the Cauchy-Schwartz inequality we obtain

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)^8 \ll X^4Y^6Z^4K \sum_{\lambda \in \mathbb{F}_p} \left| \sum_{y \in \mathcal{Y}} \mathbf{e}_p(y\lambda) \right|^2 + X^8Y^8Z^6$$

where

$$K = \sum_{\lambda \in \mathbb{F}_p^*} J(\lambda)^2.$$

It is clear that

$$\sum_{\lambda \in \mathbb{F}_p} \left| \sum_{y \in \mathcal{Y}} \mathbf{e}_p(y\lambda) \right|^2 = pY.$$

Therefore,

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)^8 \ll pX^4Y^7Z^4K + X^8Y^8Z^6.$$

Now K is simply $D^*(\mathcal{X}, \mathcal{Z})$, hence by Lemma 2.2.6

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)^8 \ll p^{3/2}X^{13/2}Y^7Z^7 + X^8Y^7Z^8 + X^8Y^8Z^6. \tag{4.1.3}$$

We now compare our result with the classical bound on bilinear sums, Lemma 4.1.3, combined with the triangle inequality to obtain

$$\begin{aligned} |T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau)|^2 &\leqslant XY \sum_{z_1, z_2 \in \mathcal{Z}} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \sigma_{x,z_1}\overline{\sigma_{x,z_2}}\tau_{y,z_1}\overline{\tau_{y,z_2}}\, \mathbf{e}_p(axy(z_1 - z_2)) \\ &\leqslant p^{1/4}X^{3/4}Y^{3/4}Z, \end{aligned} \tag{4.1.4}$$

where we have taken the bilinear bounds over x and y. For our bound to be stronger than the inequality in (4.1.4) we need

$$p^{3/16}X^{13/16}Y^{7/8}Z^{7/8} \leqslant p^{1/2}X^{3/2}Y^{3/2}Z^2,$$

or equivalently

$$X^{1/16}Y^{1/8}Z^{-1/8} \leqslant p^{1/16}.$$

Now for $XY^2Z^{-2} \leqslant p$ we have

$$XYZ^{3/4} \leqslant p^{3/16}X^{13/16}Y^{5/8}Z^{9/8} \leqslant p^{3/16}X^{13/16}Y^{7/8}Z^{7/8}.$$

Hence our first term dominates our final term over the non-trivial region. Furthermore, when our bound is trivial, i.e. for $XY^2Z^{-2} \geqslant p$,

$$T(\mathcal{X}, \mathcal{Y}, \mathcal{Z}; \rho, \sigma, \tau) \ll p^{1/4}X^{3/4}Y^{3/4}Z \ll p^{3/16}X^{13/16}Y^{7/8}Z^{7/8} + XY^{7/8}Z.$$

This concludes the proof.

4.1.6 Proof of Theorem 4.1.2

We use Lemma 2.2.6 in the proof of [30, Theorem 1.4] to give a new bound on weighted quadrilinear exponential sums. As in the proof of [30, Theorem 1.4], after permuting the variables, we have

$$\begin{aligned} &T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau)^8 \\ &\quad \ll (WXY)^6Z^7 \sum_{\mu \in \mathbb{F}_p^*} \sum_{\lambda \in \mathbb{F}_p} J(\mu)\eta_\mu I(\lambda)\, \mathbf{e}_p(\lambda\mu) + (WXZ)^8Y^7, \end{aligned} \tag{4.1.5}$$

where $I(\lambda)$ is the number of triples $(x_1, x_2, z) \in \mathcal{X}^2 \times \mathcal{Z}$ with $z(w_1 - w_2) = \lambda$, $J(\mu)$ is the number of quadruples $(w_1, w_2, y_1, y_2) \in \mathcal{W}^2 \times \mathcal{Y}^2$ with $(w_1 - w_2)(y_1 - y_2) = \mu$ and η_μ is a complex number with $|\eta_\mu| = 1$. It is clear that

$$\sum_{\mu \in \mathbb{F}_p^*} J(\mu)^2 = D^*(\mathcal{W}, \mathcal{Y}) \ll p^{1/2}W^{5/2}Y^3 + \frac{W^4Y^4}{p}.$$

We now use Lemma 4.1.4 to obtain

$$\sum_{\lambda\in\mathbb{F}_p} I(\lambda)^2 \ll \frac{Z^2X^4}{p} + Z^{3/2}X^3 + ZX^3 \ll \frac{X^4Z^2}{p} + X^3Z^{3/2}.$$

We now apply the classical bound for bilinear sums, Lemma 4.1.3, to (4.1.5) and obtain

$$\begin{aligned} &T(\mathcal{W},\mathcal{X},\mathcal{Y},\mathcal{Z};\vartheta,\rho,\sigma,\tau)^8 \\ &\quad\ll (WXY)^6Z^7\left(p^{1/4}W^{5/4}Y^{3/2} + \frac{W^2Y^2}{p^{1/2}}\right)\left(p^{1/2}X^{3/2}Z^{3/4} + X^2Z\right) \\ &\qquad\qquad + (WXZ)^8Y^7. \end{aligned}$$

This concludes the proof.

We also compare the above bound with the classical bound on bilinear sums on 1 dimensional weights combined with the triangle inequality

$$T(\mathcal{W},\mathcal{X},\mathcal{Y},\mathcal{Z};\alpha,\beta,\gamma,\delta)^8 \ll p^4W^4X^4Y^8Z^8$$

coming from Lemma 4.1.3, where $\alpha = \alpha(w)$ is bounded by 1, and similarly for β,γ and δ. For our bound to be non-trivial in this setting we need

$$p^{3/4}W^{29/4}X^{15/2}Y^{15/2}Z^{31/4} \leqslant p^4W^4X^4Y^8Z^8.$$

That is,

$$W^{13/4}X^{7/2}Y^{-1/2}Z^{-1/4} \leqslant p^{13/4},$$

therefore, since $Z \leqslant Y \leqslant X$,

$$WX^{11/13} \leqslant p.$$

Now for $WX^{11/13} \leqslant p$,

$$X^2Z \leqslant p^{13/48}X^{3/2}Z \leqslant p^{13/32}X^{3/2}Z^{3/4} < p^{1/2}X^{3/2}Z^{3/4}.$$

Similarly,

$$\frac{W^2Y^2}{p^{1/2}} \leqslant \frac{p^{3/4}W^{5/4}Y^2}{X^{33/52}p^{1/2}} \leqslant p^{1/4}W^{5/4}Y^{71/52} \leqslant p^{1/4}W^{5/4}Y^{3/2}.$$

Finally,

$$\begin{aligned} (WXZ)^8Y^7 \leqslant p^{3/4}W^{29/4}X^{383/52}Y^7Z^8 &\leqslant p^{3/4}W^{29/4}X^{15/2}Y^7Z^8 \\ &\leqslant p^{3/4}W^{29/4}X^{15/2}Y^{15/2}Z^{31/4}. \end{aligned}$$

Hence, for $WX^{11/13} \leqslant p$, after taking 8th roots

$$T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau) \ll p^{3/32} W^{29/32} X^{15/16} Y^{15/16} Z^{31/32}.$$

However, for $WX^{11/13} > p$, then our bound is trivial and

$$\begin{aligned} T(\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}; \vartheta, \rho, \sigma, \tau) &\ll p^{1/2} W^{1/2} X^{1/2} Y Z \\ &\ll p^{3/32} W^{29/32} X^{15/16} Y^{15/16} Z^{31/32}. \end{aligned}$$

4.2 Higher Dimensional Multilinear Exponential Sums

4.2.1 Set Up

Given subsets $\mathcal{X}_1, \ldots, \mathcal{X}_n \subseteq \mathbb{F}_p^*$ and sequences of complex numbers $\omega_1(\mathbf{x}), \ldots, \omega_n(\mathbf{x})$, we define the weighted multilinear exponential sum over n variables by

$$S(\mathcal{X}_1, \ldots, \mathcal{X}_n; \omega_1, \ldots, \omega_n) = \sum_{x_1 \in \mathcal{X}_1} \ldots \sum_{x_n \in \mathcal{X}_n} \omega_1(\mathbf{x}) \ldots \omega_n(\mathbf{x}) \, \mathbf{e}_p(x_1 \ldots x_n), \qquad (4.2.1)$$

where the ω_i are $n-1$ dimensional weights that depend on all but the ith variable. Assuming each $|\omega_i(\mathbf{x})| \leqslant 1$, we are interested in obtaining upper bounds of the form

$$|S(\mathcal{X}_1, \ldots, \mathcal{X}_n; \omega_1, \ldots, \omega_n)| \leqslant X_1 \ldots X_n p^{-\delta},$$

where $|\mathcal{X}_i| = X_i$. For values of $n \geqslant 3$ progress has been made through additive combinatorics with the first results due to Bourgain, Glibichuck and Konyagin [7] under some restrictions on the sets, weights and number of variables occuring in (4.2.1) although their result was general enough to obtain new estimates for sums over small subgroups. Bourgain [3] extended the results of [7] and obtained an optimal result with respect to the size of $X_1 \ldots X_n$. In particular, Bourgain showed that for all $\varepsilon > 0$ there exists a $\delta > 0$ such that

$$\sum_{x_1 \in \mathcal{X}_1} \ldots \sum_{x_n \in \mathcal{X}_n} e_p(x_1 \ldots x_n) \ll X_1 \ldots X_n p^{-\delta},$$

provided

$$X_i > p^{\varepsilon}, \quad X_1 \ldots X_n \geqslant p^{1+\varepsilon},$$

and we note that Bourgain gives the dependence of δ on ε. Recently, Shkredov [37] has made significant quantitative improvements to the results of Bourgain by exploiting a direct connection with geometric incidence estimates of Rudnev [32]. Of

particular relevance are the results of Petridis and Shparlinski [30] and Macourt [22], which have been presented in the previous section, for recent estimates of three and four dimensional multilinear sums and Shkredov [34] for the sharpest current results for exponential sums over subgroups of medium size. We mention that a direct application of the methods from [30, 22] is unable to give bounds for multilinear sums beyond four dimensional sums. However, in this section we are able to break through this barrier and apply related techniques to give new non-trivial results for multilinear sums beyond four variables.

Given a set $\mathcal{A} \subseteq \mathbb{F}_p$ and an integer k we let $D_k^{\times}(\mathcal{A})$ count the number of solutions to the equation

$$(a_1 - a_2)(a_3 - a_4)\dots(a_{2k-1} - a_{2k}) = (b_1 - b_2)(b_3 - b_4)\dots(b_{2k-1} - b_{2k}),$$

for $a_i, b_i \in \mathcal{A}$. The quantity $D_k(\mathcal{A})$ plays an important role in our arguments and we obtain some new estimates for $D_k(\mathcal{A})$, one of which improves the error term in a result of Shkredov [37, Theorem 32] for sets of cardinality $|\mathcal{A}| \geqslant p^{1/2}$. We then apply our estimates to obtain some new bounds for sums of the form (4.2.1) which are motivated by applications to exponential sums with sparse polynomials in the next chapter.
For the entirety of this section we let $|\mathcal{X}_i| = X_i$, and similarly for other sets $|\mathcal{Y}| = Y$.

4.2.2 Main Results

In what follows we keep notation as in (4.2.1).

Theorem 4.2.1. *Let $n \geqslant 4$, $\mathcal{X}_i \subset \mathbb{F}_p^*$ subsets satisfying*

$$|\mathcal{X}_i| = X_i, \quad X_1 \geqslant X_2 \geqslant \dots \geqslant X_n,$$

and

$$X_1 X_n^{1/2} \leqslant p.$$

Then we have

$$S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)$$
$$\ll_n X_1 \dots X_n \left(\frac{1}{X_1^{1/2}} + \dots + \frac{1}{X_n^{1/2^n}} + p^{\frac{1}{2^n}} X_1^{-\frac{1}{2^n}} X_n^{-\frac{1}{2^{n+1}}} \prod_{i=2}^{n-1} B_n(\mathcal{X}_i) \right)$$

where

$$B_n(\mathcal{X}) = \begin{cases} p^{\frac{1}{2^{2n-3}(n-2)}} X^{-\frac{2^{n-2}+1}{2^{2n-3}(n-2)}+o(1)}, & \text{if } p^{\frac{1}{2}+\frac{1}{2^{n-1}+2}} \geqslant X \geqslant p^{\frac{217}{433}}, \\ X^{-\frac{2^{n-2}-1+2c_1}{2^{2n-3}(n-2)}+o(1)}, & \text{if } p^{\frac{217}{433}} > X \geqslant p^{\frac{48}{97}}, \\ X^{-\frac{2^{n-2}-1+2c_2}{2^{2n-3}(n-2)}+o(1)}, & \text{if } X < p^{\frac{48}{97}}, \end{cases}$$

and $c_1 = \frac{1}{434}$ *and* $c_2 = \frac{1}{192}$.

Here the $X^{o(1)}$ represents a power of $\log X$ and is used multiple times in the remainder of this chapter to simplify the presentation of logarithmic terms. We give an example of when Theorem 4.2.1 is nontrivial. Suppose $n = 6$ and $X_1 = X_2 = \cdots = X_6 \leqslant p^{\frac{48}{97}}$. Then we have

$$S(\mathcal{X}_1, \ldots, \mathcal{X}_6; \omega_1, \ldots, \omega_6) \ll p^{\frac{1}{64}} X_1^{\frac{3110399}{524288}+o(1)}.$$

One can see that this is stronger than the trivial bound

$$S(\mathcal{X}_1, \ldots, \mathcal{X}_6; \omega_1, \ldots, \omega_6) \ll X_1^6$$

for $X_1 > p^{8/27}$. In the case of sets of cardinality a little larger than $p^{1/2}$ we can obtain sharper estimates.

Theorem 4.2.2. *Let* $\mathcal{X}_i \subset \mathbb{F}_p$ *satisfy* $|\mathcal{X}_i| = X_i$, $X_1 \geqslant X_2 \geqslant \cdots \geqslant X_n$

$$|\mathcal{X}_i| \geqslant p^{1/2+1/(2^{n+1}-6)}. \tag{4.2.2}$$

Then we have

$$|S(\mathcal{X}_1, \ldots, \mathcal{X}_n; \omega_1, \ldots, \omega_n)| \ll_n X_1 \ldots X_n \left(\frac{1}{X_1^{1/2}} + \cdots + \frac{1}{X_n^{1/2^n}} + p^{o(1)} \left(\frac{p^{1/2}}{(X_1 \ldots X_n)^{1/n}} \right)^{1/2^n} \right).$$

4.2.3 Reduction Mean Values

The following result is a variant of [30, Lemma 2.10] which is more suitable for applications to exponential sums when the variables may run through sets of differing cardinalities.

Lemma 4.2.3. *Let $n \geqslant 2$. Suppose $S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)$ is defined as in (4.2.1). Then*

$$|S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^{2^{n-1}} \ll (X_1 \dots X_n)^{2^{n-1}} \left(\frac{1}{X_n^{2^{n-2}}} + \dots + \frac{1}{X_2} \right) + X_1^{2^{n-1}-1} (X_2 \dots X_n)^{2^{n-1}-2} \sum_{\substack{x_2, y_2 \in \mathcal{X}_2 \\ x_2 \neq y_2}} \dots \sum_{\substack{x_n, y_n \in \mathcal{X}_n \\ x_n \neq y_n}} \times \left| \sum_{x_1 \in \mathcal{X}_1} \mathbf{e}_p(x_1(x_2 - y_2) \dots (x_n - y_n)) \right|.$$

Proof. We proceed by induction on n and first consider the case $n = 2$. Our sums take the form

$$S(\mathcal{X}_1, \mathcal{X}_2, \omega_1, \omega_2) = \sum_{x_1 \in \mathcal{X}_1} \sum_{x_2 \in \mathcal{X}_2} \omega_1(x_2) \omega_2(x_1) e_p(x_1 x_2),$$

and hence by the Cauchy-Schwarz inequality

$$|S(\mathcal{X}_1, \mathcal{X}_2, \omega_1, \omega_2)|^2 \leqslant X_1 \sum_{x_1 \in \mathcal{X}_1} \left| \sum_{x_2 \in \mathcal{X}_2} e_p(x_1 x_2) \right|^2.$$

Expanding the square, interchanging summation and isolating the diagonal contribution, we get

$$|S(\mathcal{X}_1, \mathcal{X}_2, \omega_1, \omega_2)|^2 \leqslant X_1^2 X_2 + X_1 \sum_{\substack{x_2, y_2 \in \mathcal{X}_2 \\ x_2 \neq y_2}} \left| \sum_{x_1 \in \mathcal{X}_1} e_p(x_1(x_2 - y_2)) \right|.$$

Suppose the statement of Lemma 4.2.3 is true for some integer $n-1 \geqslant 2$ and consider the sums $S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)$. By the Cauchy-Schwarz inequality

$$|S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^2 \leqslant X_1 \dots X_{n-1} \sum_{\substack{x_i \in \mathcal{X}_i \\ 1 \leqslant i \leqslant n-1}} \left| \sum_{x_n \in \mathcal{X}_n} \omega_1(\mathbf{x}) \dots \omega_{n-1}(\mathbf{x}) e_p(x_1 \dots x_n) \right|^2,$$

which after expanding the square, interchanging summation and isolating the diagonal contribution results in

$$|S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^2 \leqslant \frac{(X_1 \dots X_n)^2}{X_n} + X_1 \dots X_{n-1} \sum_{\substack{x_n, y_n \in \mathcal{X}_n \\ x_n \neq y_n}} S(x_n, y_n),$$

where

$$S(x_n, y_n) = \left| \sum_{\substack{x_i \in \mathcal{X}_i \\ 1 \leqslant i \leqslant n-1}} \omega_1'(\mathbf{x}', x_n, y_n) \dots \omega_{n-1}'(\mathbf{x}', x_n, y_n) e_p(x_1 \dots x_{n-1}(x_n - y_n)) \right|,$$

and

$$\mathbf{x}' = (x_1, \dots, x_{n-1}), \quad \omega_j(\mathbf{x}', x_n, y_n) = \omega_j(\mathbf{x}', x_n)\overline{\omega}_j(\mathbf{x}', y_n).$$

By Hölder's inequality

$$\begin{aligned} |S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^{2^{n-1}} &\ll \frac{(X_1 \dots X_n)^{2^{n-1}}}{X_n^{2^{n-2}}} \\ &+ (X_1 \dots X_{n-1})^{2^{n-2}} X_n^{2^{n-1}-2} \sum_{\substack{x_n, y_n \in \mathcal{X}_n \\ x_n \neq y_n}} S(x_n, y_n)^{2^{n-2}}. \end{aligned}$$

We next fix some pair $x_n \neq y_n$ and apply our induction hypothesis to the sum $S(x_n, y_n)$. This gives

$$\begin{aligned} S(x_n, y_n)^{2^{n-2}} &\leqslant (X_1 \dots X_{n-1})^{2^{n-2}} \left(\frac{1}{X_{n-1}^{2^{n-3}}} + \dots + \frac{1}{X_2} \right) \\ &+ X_1^{2^{n-2}-1} (X_2 \dots X_{n-1})^{2^{n-2}-2} \\ &\sum_{\substack{x_i, y_i \in \mathcal{X}_i \\ x_i \neq y_i \\ 2 \leqslant i \leqslant n-1}} \left| \sum_{x_1 \in \mathcal{X}_1} e_p(x_1(x_2 - y_2) \dots (x_{n-1} - y_{n-1})(x_n - y_n)) \right|, \end{aligned}$$

which combined with the above implies

$$\begin{aligned} |S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^{2^{n-1}} &\leqslant (X_1 \dots X_n)^{2^{n-1}} \left(\frac{1}{X_n^{2^{n-2}}} + \dots + \frac{1}{X_2} \right) \\ &+ X_1^{2^{n-1}-1} (X_2 \dots X_n)^{2^{n-1}-2} \\ &\times \sum_{\substack{x_i, y_i \in \mathcal{X}_i \\ x_i \neq y_i \\ 2 \leqslant i \leqslant n-1}} \left| \sum_{x_1 \in \mathcal{X}_1} e_p(x_1(x_2 - y_2) \dots (x_{n-1} - y_{n-1})(x_n - y_n)) \right|, \end{aligned}$$

and completes the proof. □

We mention that the above proof is independent of the sizes of the X_i, and as such the lemma is left without such restrictions.

For any set $\mathcal{A} \subset \mathbb{F}_p$ we define

$$\begin{aligned} &D_k^{\times}(\mathcal{A}) \\ &= |\{(a_1 - a_2)\dots(a_{2k-1} - a_{2k}) = (b_1 - b_2)\dots(b_{2k-1} - b_{2k}) : a_i, b_i \in \mathcal{A}\}|, \end{aligned}$$

and extend the notation when variables run through different sets by defining $D_k^{\times}(\mathcal{X}_1, \dots, \mathcal{X}_k)$ to be the number of solutions to

$$(w_1 - x_1)\dots(w_k - x_k) = (y_1 - z_1)\dots(y_k - z_k),$$

for $w_i, x_i, y_i, z_i \in \mathcal{X}_i$. Finally, we use the notation $D_k^{\times,*}$ for the above cases where we exclude the solutions when the equation is 0 and define

$$\widetilde{D}_k^{\times,*}(\mathcal{X}_1, \dots, \mathcal{X}_k) = D_k^{\times,*}(\mathcal{X}_1, \dots, \mathcal{X}_k) - \frac{\left(\prod_{i=1}^k X_i(X_i - 1)\right)^2}{p-1}.$$

We note that $\widetilde{D}_k^{\times,*}$ is the error in approximation of $D_k^{\times,*}$ by the expected main term.

Lemma 4.2.4. *Let $\mathcal{X}_1, \dots, \mathcal{X}_k \subset \mathbb{F}_p$. Then*

$$D_k^{\times,*}(\mathcal{X}_1, \dots, \mathcal{X}_k) \leqslant (D_k^{\times,*}(\mathcal{X}_1)\dots D_k^{\times,*}(\mathcal{X}_k))^{1/k}.$$

Proof. We let $K = D_k^{\times,*}(\mathcal{X}_1, \dots, \mathcal{X}_k)$ and express K in terms of multiplicative characters

$$\begin{aligned} K = \sum_{w_1,x_1,y_1,z_1 \in \mathcal{X}_1} \dots \sum_{w_k,x_k,y_k,z_k \in \mathcal{X}_k} \\ \frac{1}{p-1} \sum_{\chi \in \Omega} \chi(w_1 - x_1)\dots(w_k - x_k)\overline{\chi}(y_1 - z_1)\dots(y_k - z_k) \end{aligned}$$

where Ω is the set of all distinct characters. Clearly,

$$K = \frac{1}{p-1} \sum_{\chi \in \Omega} \left| \sum_{w_1,x_1 \in \mathcal{X}_1} \chi(w_1 - x_1) \right|^2 \dots \left| \sum_{w_k,x_k \in \mathcal{X}_k} \chi(w_k - x_k) \right|^2.$$

Using Holder's inequality, we obtain

$$\begin{aligned} K^k &\leqslant \frac{1}{(p-1)^k} \sum_{\chi \in \Omega} \left| \sum_{w_1,x_1 \in \mathcal{X}_1} \chi(w_1 - x_1) \right|^{2k} \dots \sum_{\chi \in \Omega} \left| \sum_{w_k,x_k \in \mathcal{X}_k} \chi(w_k - x_k) \right|^{2k} \\ &= D_k^{\times,*}(\mathcal{X}_1)\dots D_k^{\times,*}(\mathcal{X}_k). \end{aligned}$$

□

The proof of the following is similar to that of Lemma 4.2.4 with summation only over non-principal characters.

Lemma 4.2.5. *Let $\mathcal{X}_1, \dots, \mathcal{X}_k \subset \mathbb{F}_p$. Then*

$$\widetilde{D}_k^{\times,*}(\mathcal{X}_1, \dots, \mathcal{X}_k) \leqslant (\widetilde{D}_k^{\times,*}(\mathcal{X}_1) \dots \widetilde{D}_k^{\times,*}(\mathcal{X}_k))^{1/k}.$$

Using Lemma 4.2.3, Lemma 4.2.4 and Lemma 4.2.5 we give two general results relating estimates for $S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)$ to the quantities $D_k^{\times}(\mathcal{A})$ and $\widetilde{D}_k^{\times}(\mathcal{A})$.

Lemma 4.2.6. *Let $n \geqslant 2$. Suppose $S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)$ is defined as in* (4.2.1) *and that*

$$X_1 \geqslant X_2 \cdots \geqslant X_n.$$

Then

$$|S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^{2^n} \ll (X_1 \dots X_n)^{2^n} \left(\frac{1}{X_1^{2^{n-1}}} + \cdots + \frac{1}{X_{n-1}^2} \right) + pX_n^{2^n-1}(X_1 \dots X_{n-1})^{2^n-4}(D_{n-1}^{\times,*}(\mathcal{X}_1) \dots D_{n-1}^{\times,*}(\mathcal{X}_{n-1}))^{1/(n-1)}.$$

Proof. Writing

$$S = \sum_{\substack{x_1, y_1 \in \mathcal{X}_1 \\ x_1 \neq y_1}} \dots \sum_{\substack{x_{n-1}, y_{n-1} \in \mathcal{X}_{n-1} \\ x_{n-1} \neq y_{n-1}}} \left| \sum_{x_n \in \mathcal{X}_n} \mathbf{e}_p(x_n(x_1 - y_1) \dots (x_{n-1} - y_{n-1})) \right|,$$

by Lemma 4.2.3 it is sufficient to show that

$$S^2 \leqslant pX_n(D_{n-1}^{\times,*}(\mathcal{X}_1) \dots D_{n-1}^{\times,*}(\mathcal{X}_{n-1}))^{1/(n-1)}.$$

Let $I(\lambda)$ count the number of solutions to the equation

$$\lambda = (x_1 - y_1) \dots (x_{n-1} - y_{n-1}), \quad x_i, y_i \in \mathcal{X}_i, \quad x_i \neq y_i,$$

so that

$$S = \sum_{\lambda} I(\lambda) \left| \sum_{x_n \in \mathcal{X}_n} e_p(\lambda x_1) \right|,$$

and hence by Lemma 4.1.3

$$S^2 \leqslant \left(\sum_{\lambda} I(\lambda)^2 \right) pX_n,$$

and the result follows from Lemma 4.2.4 since

$$\sum_{\lambda} I(\lambda)^2 = D_{n-1}^{\times}(\mathcal{X}_1, \dots, \mathcal{X}_{n-1}).$$

□

Our next estimate does better in applications over Lemma 4.2.6 when our sets $\mathcal{X}_1, \dots, \mathcal{X}_n$ have large cardinalities.

Lemma 4.2.7. *Let $n \geqslant 2$. Suppose $S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)$ is defined as in (4.2.1). Then we have*

$$|S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^{2^n} \ll (X_1 \dots X_n)^{2^n} \left(\frac{1}{X_1^{2^{n-1}}} + \dots + \frac{1}{X_n} \right) + p^{1/2} (X_1 \dots X_n)^{2^n - 2} (\widetilde{D}_n^{\times,*}(\mathcal{X}_1) \dots \widetilde{D}_n^{\times,*}(\mathcal{X}_n))^{1/2n}.$$

Proof. Writing

$$S = \sum_{\substack{x_2, y_2 \in \mathcal{X}_2 \\ x_2 \neq y_2}} \dots \sum_{\substack{x_n, y_n \in \mathcal{X}_n \\ x_n \neq y_n}} \left| \sum_{x_1 \in \mathcal{X}_1} \mathbf{e}_p(x_1(x_2 - y_2) \dots (x_n - y_n)) \right|,$$

by Lemma 4.2.3 it is sufficient to show that

$$S^2 \leqslant \frac{(X_1 \dots X_n)^4}{X_1^2} + (X_2 \dots X_n)^2 p^{1/2} (\widetilde{D}_n^{\times,*}(\mathcal{X}_1) \dots \widetilde{D}_n^{\times,*}(\mathcal{X}_n))^{1/2n}.$$

Applying the Cauchy-Schwarz inequality, interchanging summation and isolating the diagonal contribution gives

$$S^2 \leqslant X_1 (X_2 \dots X_n)^4 + (X_2 \dots X_n)^2 \left| \sum_{\lambda=1}^{p-1} I(\lambda) e_p(\lambda) \right|, \tag{4.2.3}$$

where $I(\lambda)$ counts the number of solutions to the equation

$$(x_1 - y_1) \dots (x_n - y_n) = \lambda, \quad x_i, y_i \in \mathcal{X}_i, \quad x_i \neq y_i.$$

Let

$$\Delta = \frac{X_1(X_1 - 1) \dots X_n(X_n - 1)}{p - 1},$$

and write

$$\sum_{\lambda=1}^{p-1} I(\lambda) e_p(\lambda) = \Delta \sum_{\lambda=1}^{p-1} e_p(\lambda) + \sum_{\lambda=1}^{p-1} (I(\lambda) - \Delta) e_p(\lambda).$$

We have

$$\left| \sum_{\lambda=1}^{p-1} I(\lambda) e_p(\lambda) \right| \ll \frac{(X_1 \dots X_n)^2}{p} + \sum_{\lambda=1}^{p-1} |I(\lambda) - \Delta|. \tag{4.2.4}$$

With notation as in Lemma 4.2.5, by the Cauchy-Schwarz inequality

$$\sum_{\lambda=1}^{p-1}|I(\lambda)-\Delta| \leqslant p^{1/2}\left(\sum_{\lambda=1}^{p-1}|I(\lambda)-\Delta|^2\right)^{1/2} = p^{1/2}\widetilde{D}_n^{\times,*}(\mathcal{X}_1,\dots,\mathcal{X}_n)^{1/2},$$

and hence

$$\sum_{\lambda=1}^{p-1}|I(\lambda)-\Delta| \leqslant p^{1/2}(\widetilde{D}_n^{\times,*}(\mathcal{X}_1)\dots\widetilde{D}_n^{\times,*}(\mathcal{X}_n))^{1/2n}.$$

Combining the above with (4.2.3) and (4.2.4) gives

$$\begin{aligned} S^2 &\leqslant \frac{(X_1\dots X_n)^4}{X_1^3}+\frac{(X_1\dots X_n)^4}{p} \\ &\qquad +(X_2\dots X_n)^2p^{1/2}(\widetilde{D}_n^{\times,*}(\mathcal{X}_1)\dots\widetilde{D}_n^{\times,*}(\mathcal{X}_n))^{1/2n} \\ &\ll \frac{(X_1\dots X_n)^4}{X_1^3}+(X_2\dots X_n)^2p^{1/2}(\widetilde{D}_n^{\times,*}(\mathcal{X}_1)\dots\widetilde{D}_n^{\times,*}(\mathcal{X}_n))^{1/2n}, \end{aligned}$$

and completes the proof. □

4.2.4 Estimates for $D_k^{\times}(\mathcal{A})$

In this section we give estimates for $D_k^{\times}(\mathcal{A})$ which will be combined with results from Section 4.2.3 to obtain estimates for multilinear sums. We first recall the following result [37, Theorem 32].

Lemma 4.2.8. *Suppose $\mathcal{A}\subset\mathbb{F}_p$ is a set and $|\mathcal{A}|=A$. For all $k\geqslant 2$*

$$D_k^{\times}(\mathcal{A})-\frac{A^{4k}}{p} \ll_k (\log A)^4A^{4k-2-2^{-k+2}}E^+(\mathcal{A})^{1/2^{k-1}}.$$

We then have the following lemma [37, Theorem 41].

Lemma 4.2.9. *Let $\mathcal{A}\subset\mathbb{F}_p$ be a set, $A\leqslant p^{2846/4991}$. Then for any $c<\frac{1}{434}$ one has*

$$D_2^{\times}(\mathcal{A}) \ll A^{13/2-c}.$$

Furthermore, if $A\leqslant p^{48/97}$, then for any $c_1<\frac{1}{192}$ one has

$$D_2^{\times}(\mathcal{A}) \ll A^{13/2-c_1}.$$

We first notice that from the proof of [37, Theorem 32] we have

$$D_k^{\times}(\mathcal{A})-\frac{A^{4k}}{p} \ll_k (\log A)^2A^{2k+1}\left(D_{k-1}^{\times}(A)-\frac{A^{4(k-1)}}{p}\right)^{1/2}. \tag{4.2.5}$$

Using $E^+(\mathcal{A})\leqslant A^3$, combined with Lemma 4.2.9 and (4.2.5) we have the following corollary.

Corollary 4.2.10. *Suppose $\mathcal{A} \subset \mathbb{F}_p$ is a set and $|\mathcal{A}| = A$. For all $k \geqslant 2$*

$$D_k^{\times}(\mathcal{A}) - \frac{A^{4k}}{p} \ll_k (\log A)^4 A^{4k-2+2^{-k+1}}.$$

Similarly if $A \leqslant p^{2846/4991}$, for any $c < \frac{1}{434}$ we have

$$D_k^{\times}(\mathcal{A}) - \frac{A^{4k}}{p} \ll_k (\log A)^4 A^{4k-2+2^{-k+1}-c2^{-k+2}}$$

and if $A \leqslant p^{48/97}$, for any $c_1 < \frac{1}{192}$ we have

$$D_k^{\times}(\mathcal{A}) - \frac{A^{4k}}{p} \ll_k (\log A)^4 A^{4k-2+2^{-k+1}-c_1 2^{-k+2}}.$$

It is clear that we can use the above to give other estimates on $D_k^{\times}$ using previous estimates on $D_2^{\times}$. We recall the following result [22, Lemma 2.6], which is given from Murphy et. al [27] result on collinear triples.

Lemma 4.2.11. *Let $\mathcal{A} \subset \mathbb{F}_p$. Then*

$$D_2^{\times}(\mathcal{A}) - \frac{A^8}{p} \ll p^{1/2} A^{11/2}.$$

Again, we have the following corollary.

Corollary 4.2.12. *Let $\mathcal{A} \subset \mathbb{F}_p$. Then*

$$D_k^{\times}(\mathcal{A}) - \frac{A^{4k}}{p} \ll_k p^{2^{1-k}} (\log A)^4 A^{4k-2-2^{-k+1}}.$$

We next prepare to give an estimate for $D_k^{\times}(\mathcal{A})$ which improves on the above results for sets of cardinality a little larger than $p^{1/2}$. As in Shkredov [37], our main tool is Rudnev's point plane incidence bound [32].

Lemma 4.2.13. *Let p be an odd prime, $\mathcal{P} \subset \mathbb{F}_p^3$ a set of points and Π a collection of planes in $\mathbb{F}_p^3$. Suppose $|\mathcal{P}| \leqslant |\Pi|$ and that k is the maximum number of collinear points in $\mathcal{P}$. Then the number of point-planes incidences satisfies*

$$\mathcal{I}(\mathcal{P}, \Pi) \leqslant \frac{|\mathcal{P}||\Pi|}{p} + |\mathcal{P}|^{1/2}|\Pi| + k|\mathcal{P}|.$$

Lemma 4.2.14. *For a prime number p and a subset $\mathcal{A} \subseteq \mathbb{F}_p$ with $|\mathcal{A}| = A$ we have*

$$D_2^{\times}(\mathcal{A}) = \frac{A^8}{p} + O\left(A^6(\log A)^2 + p^{1/2}A^4 E_+(\mathcal{A})^{1/2}(\log A)^2\right) + O\left(pA^4(\log A)^2\right).$$

Proof. We have

$$D_2^{\times}(\mathcal{A}) = \sum_{\substack{a_i \in \mathcal{A} \\ (a_1-a_2)(a_3-a_4)=(a_5-a_6)(a_7-a_8) \\ a_5 \neq a_6}} 1 + O(A^6).$$

Let $I(x)$ denote the indicator function of the multiset

$$\{a - a' \ : \ a, a' \in \mathcal{A}\},$$

and let $\widehat{I}$ denote the Fourier transform of I. We note that the Fourier coefficients satisfy

$$\widehat{I}(x) = \left| \sum_{a \in \mathcal{A}} e_p(ax) \right|^2. \tag{4.2.6}$$

We have

$$\begin{aligned} D_2^{\times}(A) &= \sum_{\substack{a_i \in \mathcal{A} \\ a_5 \neq a_6}} I\left(\frac{(a_1-a_2)(a_3-a_4)}{(a_5-a_6)} \right) + O(A^6) \\ &= \frac{A^8}{p} + O(A^6) + W, \end{aligned} \tag{4.2.7}$$

where

$$W = \frac{1}{p} \sum_{y=1}^{p-1} \widehat{I}(y) \sum_{\substack{a_i \in \mathcal{A} \\ a_5 \neq a_6}} e_p(-y(a_1-a_2)(a_3-a_4)(a_5-a_6)^{-1}).$$

We have

$$\begin{aligned} W &\leqslant \frac{1}{p} \sum_{y=1}^{p-1} \sum_{z=1}^{p} \widehat{I}(y)\widehat{I}(z) \sum_{\substack{a_i \in \mathcal{A} \\ (a_1-a_2)y=(a_3-a_4)z \\ a_3 \neq a_4}} 1 \\ &= \frac{A^5}{p} \sum_{y=1}^{p-1} \widehat{I}(y) + \frac{1}{p} \sum_{y=1}^{p-1} \sum_{z=1}^{p-1} \widehat{I}(y)\widehat{I}(z) \sum_{\substack{a_i \in \mathcal{A} \\ (a_1-a_2)y=(a_3-a_4)z}} 1, \end{aligned}$$

where we have removed the condition $a_3 \neq a_4$ in the last display since by (4.2.6) the Fourier coefficients are nonnegative. The above implies

$$W \leqslant W_0 + O(A^6), \tag{4.2.8}$$

where

$$W_0 = \frac{1}{p} \sum_{y=1}^{p-1} \sum_{z=1}^{p-1} \widehat{I}(y)\widehat{I}(z) \sum_{\substack{a_i \in \mathcal{A} \\ (a_1-a_2)y=(a_3-a_4)z}} 1.$$

For integer $i \geqslant 1$ we define the sets

$$J(i) = \{1 \leqslant z \leqslant p \ : \ 2^{i-1} - 1 \leqslant \widehat{I}(z) < 2^i - 1\}, \tag{4.2.9}$$

so that

$$W_0 \ll \frac{1}{p} \sum_{1 \leqslant i,j \ll \log A} 2^{i+j} W(i,j), \tag{4.2.10}$$

where

$$W(i,j) = \sum_{\substack{a_i \in \mathcal{A}, y \in J(i), z \in J(j) \\ (a_1 - a_2)y = (a_3 - a_4)z}} 1.$$

Fix some pair (i,j) and consider $W(i,j)$. If $|J(i)| \leqslant |J(j)|$, then we consider the set of points

$$\mathcal{P} = \{(a_1 y, y, a_3) \ : \ y \in J(i), \ a_1, a_3 \in \mathcal{A}\},$$

and the collection of planes

$$\Pi = \{x_1 - a_2 x_2 - z x_3 + a_4 z = 0 \ : \ z \in J(j), \quad a_2, a_4 \in \mathcal{A}\}.$$

We see that $W(i,j)$ is bounded by the number of point-plane incidences between $\mathcal{P}$ and Π

$$W(i,j) \leqslant \mathcal{I}(\mathcal{P}, \Pi).$$

Since the maximum number of collinear points in $\mathcal{P}$ is $\max\{A, |J(i)|\}$ an application of Lemma 4.2.13 gives

$$\begin{aligned} W(i,j) \ll \frac{A^4 |J(i)||J(j)|}{p} + A^3 |J(i)|^{1/2} |J(j)| \\ + A^2 |J(i)| \max\{A, |J(i)|\}. \end{aligned} \tag{4.2.11}$$

In a similar fashion, if $|J(j)| \leqslant |J(i)|$ then

$$\begin{aligned} W(i,j) \ll \frac{A^4 |J(i)||J(j)|}{p} + A^3 |J(j)|^{1/2} |J(i)| \\ + A^2 |J(j)| \max\{A, |J(j)|\}. \end{aligned} \tag{4.2.12}$$

This implies that

$$\begin{aligned} W(i,j) &\ll \frac{A^4 |J(i)||J(j)|}{p} + A^3 |J(i)|^{1/2} |J(j)| + A^3 |J(j)|^{1/2} |J(i)| \\ &\quad + A^2 \min\{|J(i)|^2, |J(j)|^2\} \\ &\ll \frac{A^4 |J(i)||J(j)|}{p} + A^3 |J(i)|^{1/2} |J(j)| + A^3 |J(j)|^{1/2} |J(i)| \\ &\quad + A^2 |J(i)||J(j)|, \end{aligned}$$

and hence substituting the above into (4.2.10) we get

$$W_0 \ll \frac{A^4}{p^2}\left(\sum_{1\leqslant i\ll \log A} 2^i|J(i)|\right)^2 + \frac{A^3}{p}\left(\sum_{1\leqslant i\ll \log A} 2^i|J(i)|^{1/2}\right)\left(\sum_{1\leqslant i\ll \log A} 2^i|J(i)|\right) + \frac{A^2}{p}\left(\sum_{1\leqslant i\ll \log A} 2^i|J(i)|\right)^2.$$

Recalling (4.2.6) and (4.2.9), we have

$$\sum_{1\leqslant i\ll \log A} 2^i|J(i)| \ll p + \sum_{2\leqslant i\ll \log A} 2^i|J(i)| \ll p + \log A \sum_{y=1}^{p} |\sum_{a\in\mathcal{A}} e_p(ya)|^2 = pA\log A,$$

and

$$\left(\sum_{1\leqslant i\ll \log A} 2^i|J(i)|^{1/2}\right)^2 \ll p + \log A \sum_{2\leqslant i\ll \log A} 2^{2i}|J(i)| \ll p + (\log A)^2 \sum_{y=1}^{p}\left|\sum_{a\in\mathcal{A}} e_p(ya)\right|^4,$$

so that

$$\sum_{1\leqslant i\ll \log A} 2^i|J(i)|^{1/2} \ll p^{1/2}E_+(\mathcal{A})^{1/2}\log A.$$

This implies

$$W \ll A^6(\log A)^2 + p^{1/2}A^4E_+(\mathcal{A})^{1/2}(\log A)^2 + pA^4,$$

and hence by (4.2.7) and (4.2.8)

$$D_2^{\times}(A) = \frac{A^8}{p} + O\left(A^6(\log A)^2\right) + O\left(p^{1/2}A^4E_+(\mathcal{A})^{1/2}(\log A)^2\right) + O(pA^4(\log A)^2),$$

which completes the proof. □

We next establish a recurrence type inequality similar to [37, Theorem 32].

Lemma 4.2.15. *For a prime number p and a subset $\mathcal{A} \subseteq \mathbb{F}_p$ with $|\mathcal{A}| = A$ we have*

$$D_k^{\times}(\mathcal{A}) = \frac{A^{4k}}{p} + O_k\left(\left(A^{4k-2} + pA^{4k-4} + p^{1/2}A^{2k}D_{k-1}^{\times}(\mathcal{A})^{1/2}\right)\log^2 A\right).$$

Proof. Let $D_k'(\mathcal{A})$ count the number of solutions to the equation

$$(a_{1,1} - a_{1,2})\dots(a_{k,1} - a_{k,2}) = (a_{k+1,1} - a_{k+1,2})\dots(a_{2k,1} - a_{2k,2}),$$

with variables $a_{1,1}, \dots, a_{2k,2} \in \mathcal{A}$ satisfying

$$a_{1,1} \neq a_{1,2}, \quad a_{k+1,1} \neq a_{k+1,2},$$

so that

$$D_k^{\times}(\mathcal{A}) = D_k'(\mathcal{A}) + O(A^{4k-2}). \tag{4.2.13}$$

Let $I(y)$ denote the indicator function of the multiset

$$\{(a_{2,1} - a_{2,2})\dots(a_{k,1} - a_{k,2}) \ : a_{2,1}, \dots, a_{k,2} \in \mathcal{A}\},$$

and let $\widehat{I}(y)$ denote the Fourier transform of I. We have

$$\begin{aligned} D_k'(\mathcal{A}) &= \sum_{\substack{a_{j,1},a_{j,2}\in\mathcal{A}\\ a_{1,1}\neq a_{1,2}\\ a_{k+1,1}\neq a_{k+1,2}}} I((a_{k+1,1} - a_{k+1,2})\dots(a_{2k,1} - a_{2k,2})(a_{1,1} - a_{1,2})^{-1}) \\ &= \frac{1}{p}\sum_{y=1}^{p-1}\widehat{I}(y) \\ &\quad \sum_{\substack{a_{j,1},a_{j,2}\in\mathcal{A}\\ a_{1,1}\neq a_{1,2}\\ a_{k+1,1}\neq a_{k+1,2}}} e_p\left(-y(a_{k+1,1} - a_{k+1,2})\dots(a_{2k,1} - a_{2k,2})(a_{1,1} - a_{1,2})^{-1}\right) \\ &= \frac{1}{p}\sum_{z=1}^{p}\sum_{y=1}^{p-1}\widehat{I}(y)\widehat{I}(-z) \sum_{\substack{a_{i,j}\in\mathcal{A}\\ y(a_{1,1}-a_{1,2})=z(a_{2,1}-a_{2,2})\\ a_{j,1}\neq a_{j,2},\ j=1,2}} 1, \end{aligned}$$

which implies that

$$D_k'(\mathcal{A}) = \frac{A^{4k}}{p} + W_0 + O(A^{4k-2}), \tag{4.2.14}$$

where

$$W_0 = \frac{1}{p}\sum_{z=1}^{p-1}\sum_{y=1}^{p-1}\widehat{I}(y)\widehat{I}(-z) \sum_{\substack{a_{i,j}\in\mathcal{A}\\ y(a_{1,1}-a_{1,2})=z(a_{2,1}-a_{2,2})\\ a_{j,1}\neq a_{j,2},\ j=1,2}} 1.$$

For integer $i \geqslant 1$ we define

$$J(i) = \{y \in \mathbb{F}_p^* \ : \ 2^{i-1} - 1 \leqslant |\widehat{I}(y)| \leqslant 2^i - 1\},$$

so that

$$W_0 \ll \frac{1}{p} \sum_{i,j \ll \log A^{2k}} 2^{i+j} W(i,j), \tag{4.2.15}$$

where

$$W(i,j) = \sum_{\substack{a_{i,j} \in \mathcal{A}, \\ y \in J(i), z \in J(j) \\ y(a_{1,1}-a_{1,2}) = z(a_{2,1}-a_{2,2}) \\ a_{j,1} \neq a_{j,2}, \ j=1,2}} 1.$$

Using Lemma 4.2.13 as in the proof of Lemma 4.2.14, we see that

$$\begin{aligned} W(i,j) \ll \frac{A^4|J(i)||J(j)|}{p} + A^3|J(i)|^{1/2}|J(j)| + A^3|J(j)|^{1/2}|J(i)| \\ + A^2|J(i)||J(j)|. \end{aligned} \tag{4.2.16}$$

We have

$$\begin{aligned} &\sum_{i \ll \log A} 2^i |J(i)| \\ &\quad \ll p + \sum_{y=1}^{p-1} \left| \sum_{\substack{a_{i,1}, a_{i,2} \in \mathcal{A} \\ 1 \leqslant i \leqslant k-1}} e_p(y(a_{1,1}-a_{1,2}) \dots (a_{k-1,1}-a_{k-1,2})) \right| \\ &\quad \leqslant p + \sum_{\substack{a_{i,1}, a_{i,2} \in \mathcal{A} \\ 2 \leqslant i \leqslant k-1}} \sum_{y=1}^{p-1} \left| \sum_{a \in A} e_p(y(a_{2,1}-a_{2,2}) \dots (a_{k-1,1}-a_{k-1,2})a) \right|^2 \\ &\quad \ll pA^{2k-3}, \end{aligned}$$

and

$$\begin{aligned} &\sum_{i \ll \log A} 2^i |J(i)|^{1/2} \ll p^{1/2} \\ &+ \left(\log A \sum_{y=1}^{p-1} \left| \sum_{\substack{a_{i,1}, a_{i,2} \in \mathcal{A} \\ 1 \leqslant i \leqslant k-1}} e_p(y(a_{1,1}-a_{1,2}) \dots (a_{k-1,1}-a_{k-1,2})) \right|^2 \right)^{1/2}, \end{aligned}$$

so that

$$\sum_{i \ll \log A} 2^i |J(i)|^{1/2} \ll_k (\log A)^{1/2} p^{1/2} D_{k-1}^{\times}(\mathcal{A})^{1/2}.$$

Combining the above with (4.2.15) and (4.2.16) we see that

$$W_0 \ll_k \left(A^{4k-2} + pA^{4k-4} + p^{1/2}A^{2k}D_{k-1}^{\times}(\mathcal{A})^{1/2}\right)\log^2 A,$$

and hence by (4.2.13) and (4.2.14)

$$D_k^{\times}(A) = \frac{A^{4k}}{p} + O_k\left(\left(A^{4k-2} + pA^{4k-4} + p^{1/2}A^{2k}D_{k-1}^{\times}(\mathcal{A})^{1/2}\right)\log^2 A\right),$$

which completes the proof. □

Combining Lemma 4.2.14 and Lemma 4.2.15 with an induction argument gives the following Corollary.

Corollary 4.2.16. *For a prime number p and a subset $\mathcal{A} \subseteq \mathbb{F}_p$ with $|\mathcal{A}| = A \geqslant p^{1/2}$ we have*

$$D_k^{\times}(\mathcal{A}) = \frac{A^{4k}}{p} + O_k\left(\left(A^{4k-2} + p^{1-2^{-(k-1)}}A^{4k-4}E_+(\mathcal{A})^{2^{-(k-1)}}\right)\log^4 A\right).$$

Using the trivial bound $E_+(\mathcal{A}) \leqslant A^3$ in Corollary 4.2.16 gives the following sharp asymptotic formula for $D_k^{\times}(\mathcal{A})$ for sets of cardinality a little larger than $p^{1/2}$.

Corollary 4.2.17. *For any $k \geqslant 3$ and $A \geqslant p^{1/2+1/(2^{k+1}-6)}$ we have*

$$D_k^{\times}(\mathcal{A}) = \frac{A^{4k}}{p} + O_k\left(A^{4k-2}\log^4 A\right).$$

4.2.5 Proof of Theorem 4.2.1

We define $N(\mathcal{X}, \mathcal{Y}, \mathcal{Z})$ to be the number of solutions to

$$x_1(y_1 - z_1) = x_2(y_2 - z_2)$$

with $x_1, x_2 \in \mathcal{X}, y_1, y_2 \in \mathcal{Y}$ and $z_1, z_2 \in \mathcal{Z}$.

Let

$$S = S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n).$$

By Lemma 4.2.3, after permuting the variables, we have

$$\begin{aligned}|S|^{2^{n-1}} \ll (X_1 \dots X_n)^{2^{n-1}} &\left(\frac{1}{X_{n-1}} + \dots + \frac{1}{X_1^{2^{n-2}}}\right) \\ &+ (X_1 \dots X_{n-1})^{2^{n-1}-2} X_n^{2^{n-1}-1} \sum_{\substack{x_1, y_1 \in \mathcal{X}_1 \\ x_1 \neq y_1}} \dots \sum_{\substack{x_{n-1}, y_{n-1} \in \mathcal{X}_{n-1} \\ x_{n-1} \neq y_{n-1}}} \\ &\left| \sum_{x_n \in \mathcal{X}_n} \mathbf{e}_p(x_n(x_1 - y_1) \dots (x_{n-1} - y_{n-1})) \right|.\end{aligned}$$

We now collect together $(x_2 - y_2) \dots (x_{n-1} - y_{n-1}) = \lambda$ and denote the number of solutions to this equation to be $J(\lambda)$. Similarly we collect $x_1(x_n - y_n) = \mu$ and we denote the number of solutions to this equation to be $I(\mu)$. Hence,

$$\begin{aligned}|S|^{2^{n-1}} &\ll_n (X_1 \dots X_n)^{2^{n-1}} \left(\frac{1}{X_{n-1}} + \dots + \frac{1}{X_1^{2^{n-2}}}\right) \\ &\quad + (X_1 \dots X_{n-1})^{2^{n-1}-2} X_n^{2^{n-1}-1} \sum_{\lambda \in \mathbb{F}_p^*} J(\lambda) \left| \sum_{\mu \in \mathbb{F}_p} I(\mu)\, \mathbf{e}_p(\lambda\mu) \right| \\ &= (X_1 \dots X_n)^{2^{n-1}} \left(\frac{1}{X_{n-1}} + \dots + \frac{1}{X_1^{2^{n-2}}}\right) \\ &\quad + (X_1 \dots X_{n-1})^{2^{n-1}-2} X_n^{2^{n-1}-1} \sum_{\lambda \in \mathbb{F}_p^*} \sum_{\mu \in \mathbb{F}_p} J(\lambda) \eta_\lambda I(\mu)\, \mathbf{e}_p(\lambda\mu)\end{aligned}$$

for some complex weight η_λ with $|\eta_\lambda| = 1$. Now, by Lemma 4.1.4 with $X = Y = X_1, Z = X_n$ we have

$$\sum_{\mu \in \mathbb{F}_p} I(\mu)^2 = N(\mathcal{X}_n, \mathcal{X}_1, \mathcal{X}_1) \ll X_1^3 X_n^{3/2}.$$

Similarly,

$$\sum_{\lambda \in \mathbb{F}_p^*} J(\lambda)^2 = D_{n-2}^{\times,*}(\mathcal{X}_2, \dots, \mathcal{X}_{n-1}).$$

By Lemma 4.2.4 we have

$$\sum_{\lambda \in \mathbb{F}_p^*} J(\lambda)^2 \leqslant \left(D_{n-2}^{\times,*}(\mathcal{X}_2) \dots D_{n-2}^{\times,*}(\mathcal{X}_{n-1})\right)^{\frac{1}{n-2}}. \tag{4.2.17}$$

Then applying the bound on bilinear exponential sums, Lemma 4.1.3, we have

$$|S|^{2^{n-1}} \ll_n (X_1 \dots X_n)^{2^{n-1}} \left(\frac{1}{X_{n-1}} + \dots + \frac{1}{X_1^{2^{n-2}}} \right) + (X_1 \dots X_{n-1})^{2^{n-1}-2} X_n^{2^{n-1}-1} p^{1/2} \left(\sum_{\lambda \in \mathbb{F}_p^*} J(\lambda)^2 \sum_{\mu \in \mathbb{F}_p} I(\mu)^2 \right)^{1/2}$$

Finally, we apply Corollary 4.2.10 and 4.2.12 to (4.2.17) to best optimise over each set, and define

$$B_n(\mathcal{X}) = \begin{cases} p^{\frac{1}{2^{2n-3}(n-2)}} X^{-\frac{2^{n-2}+1}{2^{2n-3}(n-2)}+o(1)}, & \text{if } p^{\frac{1}{2}+\frac{1}{2^{n-1}+2}} \geqslant X \geqslant p^{\frac{217}{433}}, \\ X^{-\frac{2^{n-2}-1+2c_1}{2^{2n-3}(n-2)}+o(1)}, & \text{if } p^{\frac{217}{433}} > X \geqslant p^{\frac{48}{97}}, \\ X^{-\frac{2^{n-2}-1+2c_2}{2^{2n-3}(n-2)}+o(1)}, & \text{if } X < p^{\frac{48}{97}}, \end{cases}$$

where $c_1 = \frac{1}{434}$ and $c_2 = \frac{1}{192}$. Finally, we obtain

$$|S|^{2^{n-1}} \ll_n (X_1 \dots X_n)^{2^{n-1}} \left(\frac{1}{X_{n-1}} + \dots + \frac{1}{X_1^{2^{n-2}}} \right) + (X_1 \dots X_n)^{2^{n-1}} p^{1/2} X_1^{-1/2} X_n^{-1/4} \left(\prod_{i=2}^{n-1} B_n(\mathcal{X}_i)^{2^{n-1}} \right).$$

This completes the proof.

4.2.6 Proof of Theorem 4.2.2

We note that the conditions (4.2.2) and Corollary 4.2.17 imply that

$$\widetilde{D}_n^{\times,*}(\mathcal{X}_i) \ll (\log p)^4 X_i^{4n-2},$$

and hence by Lemma 4.2.7

$$|S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n)|^{2^n} \ll (X_1 \dots X_n)^{2^n} \left(\frac{1}{X_1^{2^{n-1}}} + \dots + \frac{1}{X_n} \right) + (\log p)^4 p^{1/2} (X_1 \dots X_n)^{2^n - 1/n},$$

from which the desired result follows.

4.3 Open Problems

One could consider arbitrary finite field analogues of the sums

$$S(\mathcal{X}_1, \dots, \mathcal{X}_n; \omega_1, \dots, \omega_n) = \sum_{x_1 \in \mathcal{X}_1} \dots \sum_{x_n \in \mathcal{X}_n} \omega_1(\mathbf{x}) \dots \omega_n(\mathbf{x}) \, \mathbf{e}_q(x_1 \dots x_n),$$

where $\mathcal{X}_i \subseteq \mathbb{F}_q$ where $q = p^k$. We mention that recent progress has been made in the field of additive combinatorics over arbitrary finite fields. Moreover, [26] has provided new bounds on point-line incidences over $\mathbb{F}_q$, which was central to our results on trilinear and quadrilinear exponential sums over $\mathbb{F}_p$. We present [26, Theorem 2] as a lemma below.

Lemma 4.3.1. *Let $\mathcal{A} \subset \mathbb{F}_q$ and let $\mathcal{L}$ be a set of lines in $\mathbb{F}_q$. Suppose that*

$$|\mathcal{A} \cap (c\mathbb{G} + d)| \ll \max\{|\mathbb{G}|^{1/2}, |\mathcal{A}|^{51/52}\},$$

for all proper subfields $\mathbb{G} \subset \mathbb{F}_q$ and all elements $c, d \in \mathbb{F}_q$. Then

$$\begin{aligned} T(\mathcal{A}) &\ll |\mathcal{A}|^{5-1/104} + q^{-1/95}|\mathcal{A}|^{5+1/95} \\ I(\mathcal{A} \times \mathcal{A}) &\ll (|\mathcal{A}|^{173/104} + q^{-1/285}|\mathcal{A}|^{476/285})|\mathcal{L}|^{2/3} + |\mathcal{L}| \\ L(\mathcal{A} \times \mathcal{A}) &\gg \min\{|\mathcal{A}|^{2+1/52}, q^{2/95}|\mathcal{A}|^{2-2/95}\} \end{aligned}$$

where $T(\mathcal{A})$ is the number of collinear triples, $I(\mathcal{A} \times \mathcal{A})$ is the number of point-line incidences and $L(\mathcal{A} \times \mathcal{A})$ is the number of distinct lines determined by pairs of points of $\mathcal{A} \times \mathcal{A}$.

We also mention that our bounds in this section can easily be adapted to multilinear exponential sums with one-dimensional weights, or no weights using bounds in this chapter. However, we do not consider these as our motivation was to give applications to multinomial exponential sums, as we will see in the next chapter.

Finally, as part of our exploration of the term $D_k^{\times}(\mathcal{A})$ we considered the number of solutions of sums of products. That is, we let $D_k^{+}(\mathcal{A})$ be the number of solutions to

$$a_1b_1 + a_2b_2 + \dots + a_kb_k = c_1d_1 + c_2d_2 + \dots + c_kd_k.$$

Our hope was that we could apply similar techniques to Lemma 4.2.14 and Lemma 4.2.15. However, we were unable to reduce the problem to one where we could apply the bound of Rudnev [32] on point-plane incidences.

5

Multinomial Exponential Sums

5.1 Introduction

5.1.1 Set Up

For a t-sparse polynomial

$$\Psi(X) = \sum_{i=1}^{t} a_i X^{k_i} \tag{5.1.1}$$

with some pairwise distinct non-zero integer exponents $k_1, \ldots, k_t$ and coefficients $a_1, \ldots, a_t \in \mathbb{F}_p^*$, 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 χ is an arbitrary multiplicative character of $\mathbb{F}_p^*$. The challenge for such sums is to provide a bound that is stronger than the Weil bound

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

see [43, Appendix 5, Example 12], by taking advantage of the arithmetic structure of the exponents. The case of exponential sums of monomials has seen much study

with Shparlinski [39] providing the first such bound. Further improvements have been made by various other authors, see [7, 3, 17, 19, 34, 40]. We also mention that Cochrane, Coffelt and Pinner, as well as others, have given several bounds on exponential sums with sparse polynomials, see [9, 10, 11, 12, 13, 14] and references therein, some of which we outline in Section 5.1.2.

First we provide some new bounds on trinomial and quadrinomial exponential sums. We thus define

$$\Psi_3(X) = aX^k + bX^\ell + cX^m \tag{5.1.2}$$

$$\Psi_4(X) = aX^k + bX^\ell + cX^m + dX^n. \tag{5.1.3}$$

We mention that all our results extend naturally to more general sums with polynomials of the shape

$$\Psi(X) = aX^k + f(X^\ell) + g(X^m) + h(X^n)$$

for polynomials $f, g, h \in \mathbb{F}_p[X]$.

5.1.2 Previous Results

We compare our results for trinomials and quadrinomials to those of Cochrane, Coffelt and Pinner [9, Theorem 1.1]

$$S_\chi(\Psi) \ll \left(\frac{k\ell mn}{\max(k,\ell,m,n)}\right)^{1/9} p^{8/9} \tag{5.1.4}$$

which is non-trivial for

$$\frac{k\ell mn}{\max(k,\ell,m,n)} < p,$$

and of Cochrane and Pinner [11, Theorem 1.1]

$$S_\chi(\Psi) \ll (k\ell mn)^{1/16} p^{7/8} \tag{5.1.5}$$

which is non-trivial for $k\ell mn < p^2$. Our new results in Theorem 5.1.1 and Theorem 5.1.2 are independent of the size of the exponents but instead depend on various greatest common divisors. We also mention a similar result of Cochrane and Pinner

[13, Theorem 1.1] which for Laurent polynomials g, g_2, g_3, g_4 where $g(x)$ contains a monomial aX^{k_1}, $k_1 \neq 0$, $p \nmid a$, and

$$\Psi(X) = g(X) + g_2(X^{k_2}) + \cdots + g_r(X^{k_r})$$

we have

$$S_\chi(\Psi) \leqslant p \sum_{i=0}^{r-2} \left(\frac{\gcd(k_{r-i}, k_1, p-1)}{\gcd(k_{r-i}, p-1)} \right)^{\frac{1}{2^{i+1}}} + D^{\frac{1}{2^{r-1}}} p^{1-\frac{1}{2^r}} \tag{5.1.6}$$

where

$$D = \begin{cases} \deg(g) - 1, & \text{if } g(X) \text{ is a polynomial,} \\ \gcd(k_1, p-1) - 1, & \text{if } g(X) = aX^{k_1} \text{ is a monomial.} \end{cases}$$

5.1.3 Main Results

Our main results are the theorems given in this section.

Theorem 5.1.1. *Let $\Psi(X)$ be a trinomial of the form (5.1.2) with $a, b, c \in \mathbb{F}_p^*$. Define*

$$d = \gcd(k, p-1), \qquad e = \gcd(\ell, p-1), \qquad f = \gcd(m, p-1)$$

and

$$g = \frac{d}{\gcd(d, f)}, \qquad h = \frac{e}{\gcd(e, f)}.$$

Suppose $f \geqslant g \geqslant h$, then

$$S_\chi(\Psi) \ll ph^{-1/4} + \begin{cases} p^{7/8} f^{1/8}, & \text{if } h \geqslant (p \log p)^{1/2}, \\ p^{15/16} (f/h)^{1/8} (\log p)^{1/16}, & \text{if } g \geqslant (p \log p)^{1/2} > h, \\ p(f/gh)^{1/8} (\log p)^{1/8}, & \text{if } g < (p \log p)^{1/2}. \end{cases}$$

Note that the assumption $f \geqslant g \geqslant h$ of Theorem 5.1.1 does not present any additional restriction 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.

Theorem 5.1.2. *Let $\Psi(X)$ be a quadrinomial of the form (5.1.3) with $a, b, c, d \in \mathbb{F}_p^*$. Define*

$$\alpha = \gcd(k, p-1),\ \beta = \gcd(\ell, p-1),\ \gamma = \gcd(m, p-1),\ \delta = \gcd(n, p-1)$$

and

$$f = \frac{\alpha}{\gcd(\alpha, \delta)}, \qquad g = \frac{\beta}{\gcd(\beta, \delta)}, \qquad h = \frac{\gamma}{\gcd(\gamma, \delta)}.$$

Suppose $f \geqslant g \geqslant h$. Then $p/\delta > f$ and

$$S_\chi(\Psi) \ll pg^{-1/8} + \begin{cases} p^{15/16}\delta^{1/32}, & \text{if } g \geqslant p^{1/2}\log p, \\ p^{31/32}\delta^{1/32}g^{-1/16+o(1)}, & \text{if } f \geqslant p^{1/2}\log p > g, \\ p\delta^{1/32}(fg)^{-1/16+o(1)}, & \text{if } p/\delta \geqslant p^{1/2}\log p > f, \\ p^{31/32+o(1)}\delta^{3/32}(fg)^{-1/16}, & \text{if } p/\delta < p^{1/2}\log p. \end{cases}$$

Similarly to Theorem 5.1.1, we mention that our result is independent of the size of our powers k, l, m, n and is strongest when δ is small and f, g, h are large. Here $o(1)$ represents some power of a log and is used here, and other times in this chapter, to simplify the presentation and calculation of logarithmic factors. As mentioned in the previous section, many previous results become trivial for quadrinomials of large degree. It is easy to see that our bound is non-trivial and improves previous results for a wide range of exponents k, ℓ, m and n. By Theorem 5.1.2 we present the following example as a corollary.

Corollary 5.1.3. *Let $\Psi(X)$ be a quadrinomial of the form (5.1.3) with $a, b, c, d \in \mathbb{F}_p^*$. Suppose $p/2 > |n| > |k| > |\ell| > |m| \geqslant p^{1/2}\log p$, $\delta = 1$ and $k, \ell | p-1$, where δ is defined as in Theorem 5.1.2. Then*

$$S_\chi(\Psi) \ll p^{15/16}.$$

Clearly in the above example both (5.1.4) and (5.1.5) are trivial. We compare this to (5.1.6). One can see (5.1.6) gives a weaker bound than Theorem 5.1.1 when $\gamma < p^{1/8}$. One can also check that in this instance our bound also gives something stronger than [13, Theorem 1.2]. Indeed, it is possible to give results in which Theorem 5.1.1 is stronger than (5.1.6) for all four bounds of Theorem 5.1.1 by restricting the size of h, as in the above example.

Here we also mention one can get a similar result to Theorem 5.1.2 using [30, Theorem 1.4], however this gives strictly weaker results due to the results in Section 5.2 being stronger in the case of subgroups rather than subsets.

Using Theorem 5.1.2, as well as the results mentioned in Section 5.1.2, we can give classes of quadrinomials where we have savings in terms of p. For example we have the following result using Theorem 5.1.1 and the bounds (5.1.4), (5.1.5) and (5.1.6).

Corollary 5.1.4. *Let $\Psi(X)$ be a quadrinomial of the form (5.1.3) with $a, b, c, d \in \mathbb{F}_p^*$. Suppose $k, \ell, m | p-1$, $\gcd(n, p-1) = 1$ and $k \geqslant \ell \geqslant m \geqslant n$. Then*

$$S_\chi(\Psi) \ll p^{15/16+o(1)}.$$

Additionally, using [13, Theorem 1.2], as well as the results of Section 5.1.2, we get the following bound which does not depend on the size of n.

Corollary 5.1.5. *Let $\Psi(X)$ be a quadrinomial of the form (5.1.3) with $a, b, c, d \in \mathbb{F}_p^*$. Suppose $k, \ell, m | p-1$, $\gcd(n, p-1) = 1$ and $k \geqslant \ell \geqslant m$. Then*

$$S_\chi(\Psi) \ll p^{71/72+o(1)}.$$

Finally, we give a bound on multinomial exponential sums that extends past quadrinomials. The following is a consequence of Theorem 4.2.1.

Theorem 5.1.6. *Let $\Psi(X)$ be a multinomial of the form (5.1.1), with coefficients $a_i \in \mathbb{F}_p^*$ for $i = 1, \dots, t$. We define*

$$\alpha_{k_i} = \gcd(k_i, p-1)$$

and

$$\beta_{k_i} = \frac{\alpha_{k_i}}{\gcd(\alpha_{k_i}, \alpha_{k_t})}.$$

Suppose $\beta_{k_1} \geqslant \cdots \geqslant \beta_{k_{t-1}}$. Then

$$\begin{aligned} &S_\chi(\Psi) \\ &\ll p\left(\left(\frac{\alpha_{k_t}}{p-1}\right)^{\frac{1}{2}} + \beta_{k_1}^{\frac{-1}{2^2}} + \cdots + \beta_{k_{t-1}}^{\frac{-1}{2^t}} + p^{\frac{1}{2^t}} C_t(\alpha_{k_t}) \prod_{i=1}^{t-2} D_t(\beta_{k_i})\right) \end{aligned}$$

where

$$C_t(\alpha) = \begin{cases} \alpha^{\frac{3}{2^{t+1}}} p^{-\frac{3}{2^{t+1}}}, & \text{if } \alpha \geqslant p^{\frac{1}{2}} \log p, \\ \alpha^{\frac{1}{2^{t+1}}} p^{-\frac{1}{2^t}}, & \text{if } \alpha < p^{\frac{1}{2}} \log p, \end{cases}$$

and

$$D_t(\beta) = \begin{cases} p^{-\frac{1}{2^t(t-2)}}, & \text{if } \beta \geqslant p^{\frac{1}{2}} \log p, \\ \beta^{-\frac{1}{2^{t-1}(t-2)}}, & \text{if } \beta < p^{\frac{1}{2}} \log p. \end{cases}$$

We mention that Theorem 5.1.6 returns the same bound as 5.1.2 when $t = 4$.

5.2 Trinomial and Quadrinomial Exponential Sums

5.2.1 Preliminaries

We define $D_{\times}(\mathcal{U})$ to be the number of solutions of

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

We also define the multiplicative energy $\mathrm{E}^{\times}(\mathcal{U}, \mathcal{V})$ to be the number of solutions of

$$u_1 v_1 = u_2 v_2 \qquad u_i \in \mathcal{U},\ v_i \in \mathcal{V},\ i = 1, 2.$$

When $\mathcal{U} = \mathcal{V}$, we write $\mathrm{E}^{\times}(\mathcal{U},\mathcal{U}) = E^{\times}(\mathcal{U})$.

We have the following lemma as a consequence of Theorem 2.1.2 and the proof of Lemma 2.2.6.

Lemma 5.2.1. *For a multiplicative subgroup $\mathcal{G} \subset \mathbb{F}_p^*$, we have*

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

We also have the following lemma which comes as a result of (2.3.19).

Lemma 5.2.2. *Let $\mathcal{G}$ be a multiplicative subgroup of $\mathbb{F}_p^*$. Then for any $\lambda \in \mathbb{F}_p^*$, we have*

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

We immediately obtain the following result by observing the dominant term from Lemma 5.2.2.

Corollary 5.2.3. *Let $\mathcal{G}$ be a multiplicative subgroup of $\mathbb{F}_p^*$. Then for any $\lambda \in \mathbb{F}_p^*$, we have*

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

We define $N(\mathcal{F}, \mathcal{G}, \mathcal{H})$ to be the number of triples of solutions to the equation $f_1(g_1 - g_2) = f_2(h_1 - h_2)$ where $f_i \in \mathcal{F}, g_i \in \mathcal{G}, h_i \in \mathcal{H}$ for $i = 1, 2$. Using Corollary 5.2.3 we obtain the following result.

Lemma 5.2.4. *Let $\mathcal{F}, \mathcal{G}, \mathcal{H}$ be multiplicative subgroups of $\mathbb{F}_p^*$ with cardinalities F, G, H respectively with $G \geqslant H$. Additionally, let $M = \max(F, G)$. Then*

$$N(\mathcal{F}, \mathcal{G}, \mathcal{H}) \ll \frac{F^2}{M^{1/2}} \begin{cases} G^2H^2p^{-1/2}, & \text{if } H \geqslant p^{1/2}\log p, \\ G^2H^{3/2+o(1)}p^{-1/4}, & \text{if } G \geqslant p^{1/2}\log p > H, \\ (GH)^{3/2+o(1)}, & \text{if } G < p^{1/2}\log p. \end{cases}$$

Proof. By multiplying both sides of $f_1(g_1 - g_2) = f_2(h_1 - h_2)$ by the inverses f_2^{-1} and h_2^{-1} and taking a factor of g_2 from the left hand side, and defining

$$S = \{fgh : f \in \mathcal{F}, g \in \mathcal{G}, h \in \mathcal{H}\}$$

we have

$$N(\mathcal{F}, \mathcal{G}, \mathcal{H}) = \frac{F^2GH}{|S|} \sum_{\lambda \in S} |\{(g, h) \in \mathcal{G} \times \mathcal{H} : \lambda(g - 1) = h - 1\}|.$$

By two applications of the Cauchy-Schwartz inequality,

$$\begin{aligned} N(\mathcal{F}, \mathcal{G}, \mathcal{H})^2 &\leqslant \frac{F^4G^2H^2}{|S|} \left| \left\{ (g_i, h_i) \in \mathcal{G} \times \mathcal{H},\ i = 1, 2 : \frac{h_1 - 1}{g_1 - 1} = \frac{h_2 - 1}{g_2 - 1} \right\} \right| \\ &\leqslant \frac{F^4G^2H^2}{|S|} (\mathrm{E}^{\times}(\mathcal{G} - 1)\mathrm{E}^{\times}(\mathcal{H} - 1))^{1/2}. \end{aligned}$$

By Corollary 5.2.3,

$$N(\mathcal{F}, \mathcal{G}, \mathcal{H})^2 \ll \frac{F^4G^2H^2}{|S|} \begin{cases} G^2H^2/p, & \text{if } H \geqslant p^{1/2}\log p, \\ G^2H^{1+o(1)}p^{-1/2}, & \text{if } G \geqslant p^{1/2}\log p > H, \\ (GH)^{1+o(1)}, & \text{if } G < p^{1/2}\log p. \end{cases}$$

Since $|S| \geqslant M$ we complete our proof. □

5.2.2 Bounds On Trilinear and Quadrilinear Exponential Sums Over Subgroups

Applying Lemma 5.2.1 and Lemma 5.2.4 in the proof of [30, Theorem 1.4], we obtain the following result on quadrilinear sums over subgroups.

Lemma 5.2.5. *For any multiplicative subgroups $\mathcal{F}, \mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_p^*$ of cardinalities F, G and H, respectively, with $F \geqslant G \geqslant H$ and weights $\rho = (\rho_{u,v})$, $\sigma = (\sigma_{u,w})$ and $\tau = (\tau_{v,w})$ with*

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

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

$$T \ll FGH^{3/4} + \begin{cases} F^{7/8}GH, & \text{if } H \geqslant (p\log p)^{1/2}, \\ p^{1/16}F^{7/8}GH^{7/8}\,(\log p)^{1/16}, & \text{if } G \geqslant (p\log p)^{1/2} > H, \\ p^{1/8}F^{7/8}G^{7/8}H^{7/8}\,(\log p)^{1/8}, & \text{if } G < (p\log p)^{1/2}, \end{cases}$$

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

Proof. We see from [30, 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 [30, Theorem 1.3], expressing K via multiplicative character sums and using the Cauchy-Schwartz inequality, we obtain $K^2 \leqslant D_\times(\mathcal{G})D_\times(\mathcal{H})$. Applying Lemma 5.2.1, instead of [30, Equation 3.9], we now obtain

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

Taking 8th roots we complete the proof. □

Clearly, the bound of Lemma 5.2.5 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 $F \geqslant G \geqslant H \geqslant p^{1/3+\varepsilon}$ then the exponential sums of Lemma 5.2.5 are bounded by $O(FGHp^{-\delta})$.

Lemma 5.2.6. *For any multiplicative subgroups $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z} \subseteq \mathbb{F}_p^*$ of cardinalities W, X, Y and Z, respectively, with $W \geqslant X \geqslant Y \geqslant Z$ and weights $\vartheta = (\vartheta_{w,x,y})$, $\rho = (\rho_{w,x,z})$, $\sigma = (\sigma_{w,y,z})$ and $\tau = (\tau_{x,y,z})$ with*

$$\max_{(w,x,y)\in\mathcal{W}\times\mathcal{X}\times\mathcal{Y}} |\vartheta_{w,x,y}| \leqslant 1, \quad \max_{(w,x,y)\in\mathcal{W}\times\mathcal{X}\times\mathcal{Z}} |\rho_{w,x,z}| \leqslant 1,$$

$$\max_{(w,x,y)\in\mathcal{W}\times\mathcal{Y}\times\mathcal{Z}} |\sigma_{w,y,z}| \leqslant 1, \quad \max_{(w,x,y)\in\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}} |\tau_{x,y,z}| \leqslant 1,$$

for the sums

$$T = \sum_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} \sum_{z\in\mathcal{Z}} \vartheta_{w,x,y}\rho_{w,x,z}\sigma_{w,y,z}\tau_{x,y,z}\, \mathbf{e}_p(awxyz)$$

we have

$$|T| \ll WXZY^{7/8} + \begin{cases} W^{31/32}XYZp^{-1/32}, & \text{if } Y \geqslant p^{1/2}\log p, \\ W^{31/32}XY^{15/16+o(1)}Z, & \text{if } X \geqslant p^{1/2}\log p > Y, \\ W^{31/32}(XY)^{15/16+o(1)}Zp^{1/32}, & \text{if } W \geqslant p^{1/2}\log p > X, \\ W^{29/32+o(1)}(XY)^{15/16}Zp^{1/16}, & \text{if } W < p^{1/2}\log p, \end{cases}$$

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

Proof. We see from [30, p. 24] that

$$|T|^8 \ll (WXY)^6Z^7 \sum_{\mu\in\mathbb{F}_p^*} \sum_{\lambda\in\mathbb{F}_p} J(\mu)I(\lambda)\eta_\mu\, \mathbf{e}_p(\lambda\mu) + (WXZ)^8Y^7,$$

where η_μ, $\mu \in \mathbb{F}_p^*$ are complex numbers with $|\eta_\mu| = 1$, $J(\mu)$ is the number of quadruples $(x_1, x_2, y_1, y_2) \in \mathcal{X}^2 \times \mathcal{Y}^2$ such that $(x_1 - x_2)(y_1 - y_2) = \mu \in \mathbb{F}_p^*$ and $I(\lambda)$ is the number of triples $(w_1, w_2, z) \in \mathcal{W}^2 \times \mathcal{Z}$ such that $z(w_1 - w_2) = \lambda \in \mathbb{F}_p$. We estimate $J(\mu)$ as in [30, Equation 3.10] but using our bound from Lemma 5.2.1 to obtain

$$\sum_{\mu\in\mathbb{F}_p^*} J(\mu)^2 \ll \begin{cases} X^4Y^4/p, & \text{if } Y \geqslant p^{1/2}\log p, \\ X^4Y^{3+o(1)}p^{-1/2}, & \text{if } X \geqslant p^{1/2}\log p > Y, \\ (XY)^{3+o(1)}, & \text{if } X < p^{1/2}\log p. \end{cases} \tag{5.2.1}$$

Now

$$\begin{aligned} &\sum_{\lambda\in\mathbb{F}_p} I(\lambda)^2 \\ &\quad = |\{w_1, w_2 \in \mathcal{W}, z_i \in \mathcal{Z}, i = 1, 2, 3, 4 : z_1(w_1 - w_2) = z_2(w_3 - w_4)\}| \\ &\quad = N(Z, W, W). \end{aligned}$$

Therefore, by Lemma 5.2.4,

$$\sum_{\lambda\in\mathbb{F}_p} I(\lambda)^2 \ll \begin{cases} Z^2W^{7/2}p^{-1/2}, & \text{if } W \geqslant p^{1/2}\log p, \\ Z^2W^{5/2+o(1)}, & \text{if } W < p^{1/2}\log p. \end{cases} \tag{5.2.2}$$

Applying the classical bound on bilinear exponential sums from Lemma 4.1.3 together with (5.2.1) and (5.2.2), we get

$$\begin{aligned} |T|^8 \ll & (WXZ)^8Y^7 \\ & + \begin{cases} W^{31/4}X^8Y^8Z^8p^{-1/4}, & \text{if } Y \geqslant p^{1/2}\log p, \\ W^{31/4}X^8Y^{15/2+o(1)}Z^8, & \text{if } X \geqslant p^{1/2}\log p > Y, \\ W^{31/4}(XY)^{15/2+o(1)}Z^8p^{1/4}, & \text{if } W \geqslant p^{1/2}\log p > X, \\ W^{29/4+o(1)}(XY)^{15/2}Z^8p^{1/2}, & \text{if } W < p^{1/2}\log p. \end{cases} \end{aligned}$$

Hence,

$$\begin{aligned} |T| \ll & WXZY^{7/8} \\ & + \begin{cases} W^{31/32}XYZp^{-1/32}, & \text{if } Y \geqslant p^{1/2}\log p, \\ W^{31/32}XY^{15/16+o(1)}Z, & \text{if } X \geqslant p^{1/2}\log p > Y, \\ W^{31/32}(XY)^{15/16+o(1)}Zp^{1/32}, & \text{if } W \geqslant p^{1/2}\log p > X, \\ W^{29/32+o(1)}(XY)^{15/16}Zp^{1/16}, & \text{if } W < p^{1/2}\log p. \end{cases} \end{aligned}$$

This completes the proof. □

We compare our bound for subgroups from Lemma 5.2.6 with that for arbitrary sets coming from [30, Theorem 1.4]

$$\begin{aligned} \left|\sum_{w\in\mathcal{W}}\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}}\sum_{z\in\mathcal{Z}} \vartheta_{w,x,y}\rho_{w,x,z}\sigma_{w,y,z}\tau_{x,y,z}\,\mathbf{e}_p(awxyz)\right| & \\ \ll p^{1/16}W^{15/16}(XY)^{61/64}Z^{31/32}. & \end{aligned} \tag{5.2.3}$$

For example, if $W = X = Y = Z = p^{1/2+o(1)}$ then the bounds become $p^{125/64+o(1)}$ and $p^{63/32+o(1)}$ respectively.

5.2.3 Proof of Theorem 5.1.1

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,

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

where

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

Clearly, the set $\mathcal{X} = \{x^m : x \in \mathbb{F}_p^*\}$ of non-zero mth 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 we have $f \geqslant g \geqslant h$ and invoke Lemma 5.2.5, which gives us,

$$\begin{aligned}
S_\chi(\Psi) &\ll \frac{f \gcd(d,f) \gcd(e,f)}{de} \times (p/f) g h^{3/4} + \frac{f \gcd(d,f) \gcd(e,f)}{de} \times \\
&\qquad \begin{cases} (p/f)^{7/8} gh, & \text{if } h \geqslant p^{1/2} \log p, \\ p^{1/16} (p/f)^{7/8} g h^{7/8} (\log p)^{1/16}, & \text{if } g \geqslant (p \log p)^{1/2} > h, \\ p^{1/8} (p/f)^{7/8} g^{7/8} h^{7/8} (\log p)^{1/8}, & \text{if } g < (p \log p)^{1/2}, \end{cases} \\
&= ph^{-1/4} \\
&\qquad + \begin{cases} p^{7/8} f^{1/8}, & \text{if } h \geqslant (p \log p)^{1/2}, \\ p^{15/16} f^{1/8} h^{-1/8} (\log p)^{1/16}, & \text{if } g \geqslant (p \log p)^{1/2} > h, \\ p f^{1/8} g^{-1/8} h^{-1/8} (\log p)^{1/8}, & \text{if } g < (p \log p)^{1/2}. \end{cases}
\end{aligned}$$

This concludes the proof.

5.2.4 Proof of Theorem 5.1.2

Let $\mathcal{G}_\alpha, \mathcal{G}_\beta, \mathcal{G}_\gamma$ be the subgroups of $\mathbb{F}_p^*$ generated by the elements of orders α, β and γ respectively. Then,

$$\begin{aligned}
S_\chi(\Psi) &= \frac{1}{\alpha\beta\gamma} \sum_{x\in\mathcal{G}_\alpha} \sum_{y\in\mathcal{G}_\beta} \sum_{z\in\mathcal{G}_\gamma} \sum_{w\in\mathbb{F}_p^*} \chi(wxyz)\, \mathbf{e}_p(\Psi(wxyz)) \\
&= \frac{1}{\alpha\beta\gamma} \sum_{x\in\mathcal{G}_\alpha} \sum_{y\in\mathcal{G}_\beta} \sum_{z\in\mathcal{G}_\gamma} \sum_{w\in\mathbb{F}_p^*} \\
&\qquad \chi(wxyz)\, \mathbf{e}_p(aw^k y^k z^k + bw^\ell x^\ell z^\ell + cw^m x^m y^m + dw^n x^n y^n z^n) \\
&= \frac{1}{\alpha\beta\gamma} \sum_{x\in\mathcal{G}_\alpha} \sum_{y\in\mathcal{G}_\beta} \sum_{z\in\mathcal{G}_\gamma} \sum_{w\in\mathbb{F}_p^*} \vartheta_{w,x,y}\rho_{w,x,z}\sigma_{w,y,z}\, \mathbf{e}_p(dw^n x^n y^n z^n)
\end{aligned}$$

where we choose

$$\vartheta_{w,x,y} = \chi(wxy)\, \mathbf{e}_p(cw^m x^m y^m), \quad \rho_{w,x,z} = \chi(z)\, \mathbf{e}_p(bw^\ell x^\ell z^\ell)$$

and

$$\sigma_{w,y,z} = \mathbf{e}_p(aw^k y^k z^k).$$

Now the image $\mathcal{W} = \{w^n : w \in \mathbb{F}_p^*\}$ of non-zero nth powers contains $(p-1)/\delta$ elements, each appearing with multiplicity δ. Similarly, we can see that the images $\mathcal{X} = \{x^n : x \in \mathcal{G}_\alpha\}, \mathcal{Y} = \{y^n : y \in \mathcal{G}_\beta\}$ and $\mathcal{Z} = \{z^n : z \in \mathcal{G}_\gamma\}$ contain f, g and h elements with multiplicity $\gcd(\alpha,\delta), \gcd(\beta,\delta)$ and $\gcd(\gamma,\delta)$ respectively. We apply Lemma 5.2.6, recalling our assumption that $f \geqslant g$ and noticing $f\delta = \operatorname{lcm}(\alpha,\delta) < p-1$, hence $f < p/\delta$, which gives us

$$\begin{aligned}
S_\chi(\Psi) \ll& \frac{\delta \gcd(\alpha,\delta)\gcd(\beta,\delta)\gcd(\gamma,\delta)}{\alpha\beta\gamma}(p/\delta) f g^{7/8} h \\
&+ \frac{\delta \gcd(\alpha,\delta)\gcd(\beta,\delta)\gcd(\gamma,\delta)}{\alpha\beta\gamma} \\
&\times \begin{cases}
(p/\delta)^{31/32} fghp^{-1/32}, & \text{if } g \geqslant p^{1/2}\log p, \\
(p/\delta)^{31/32} fg^{15/16+o(1)}h, & \text{if } f \geqslant p^{1/2}\log p > g, \\
(p/\delta)^{31/32} (fg)^{15/16+o(1)} hp^{1/32}, & \text{if } p/\delta \geqslant p^{1/2}\log p > f, \\
(p/\delta)^{29/32+o(1)} (fg)^{15/16} hp^{1/16}, & \text{if } p/\delta < p^{1/2}\log p,
\end{cases} \\
=& pg^{-1/8} \\
&+ \begin{cases}
p^{15/16}\delta^{1/32}, & \text{if } g \geqslant p^{1/2}\log p, \\
p^{31/32}\delta^{1/32} g^{-1/16+o(1)}, & \text{if } f \geqslant p^{1/2}\log p > g, \\
p\delta^{1/32}(fg)^{-1/16+o(1)}, & \text{if } p/\delta \geqslant p^{1/2}\log p > f, \\
p^{31/32+o(1)}\delta^{3/32}(fg)^{-1/16}, & \text{if } p/\delta < p^{1/2}\log p.
\end{cases}
\end{aligned}$$

This concludes the proof.

5.3 Multinomial Exponential Sums

5.3.1 Preliminaries

The aim of this section is to extend the results of the previous section beyond the cases of trinomials and quadrinomials, to more general multinomial sums.

Combining Corollary 5.2.3 with (4.2.5) and observing which term dominates we get the following corollary.

Corollary 5.3.1. *Let $\mathcal{G} \subseteq \mathbb{F}_p^*$ be a multiplicative subgroup with $|\mathcal{G}| = G$. Then*

$$D_k^{\times}(\mathcal{G}) \ll \begin{cases} G^{4k}p^{-1} & \text{if } G \geqslant p^{\frac{1}{2}}\log p, \\ G^{4k-2+o(1)}, & \text{if } G < p^{\frac{1}{2}}\log p. \end{cases}$$

We also have the following result as a consequence of Lemma 5.2.4

Lemma 5.3.2. *Let $\mathcal{G}, \mathcal{H} \subset \mathbb{F}_p^*$ be multiplicative subgroups with cardinalities G, H respectively with $G \geqslant H$. Then,*

$$N(\mathcal{H}, \mathcal{G}, \mathcal{G}) \ll \begin{cases} H^2G^{\frac{7}{2}}p^{-\frac{1}{2}} & \text{if } G \geqslant p^{\frac{1}{2}}\log p, \\ H^2G^{\frac{5}{2}+o(1)}, & \text{if } G < p^{\frac{1}{2}}\log p. \end{cases}$$

We then have the following result on multilinear exponential sums over subgroups, which may be of independent interest to the reader.

Lemma 5.3.3. *Let $\mathcal{X}_i \subset \mathbb{F}_p$ be multiplicative subgroups with $|\mathcal{X}_i| = X_i$, $X_1 \geqslant X_2 \geqslant \cdots \geqslant X_n$, $n \geqslant 4$. Then with $S(\mathcal{X}_1, \ldots, \mathcal{X}_n; \omega_1, \ldots, \omega_n)$ as given in* (4.2.1),

$$S(\mathcal{X}_1, \ldots, \mathcal{X}_n; \omega_1, \ldots, \omega_n) \ll_n (X_1 \ldots X_n)p^{\frac{1}{2^n}} A_n(\mathcal{X}_1) \prod_{i=2}^{n-1} B_n(\mathcal{X}_i) + (X_1 \ldots X_n)\left(\frac{1}{X_n^{1/2}} + \cdots + \frac{1}{X_1^{1/2^n}}\right)$$

where

$$A_n(\mathcal{X}_1) = \begin{cases} X_1^{-\frac{1}{2^{n+1}}}p^{-\frac{1}{2^{n+1}}}, & \text{if } X_1 \geqslant p^{\frac{1}{2}}\log p, \\ X_1^{-\frac{3}{2^{n+1}}+o(1)}, & \text{if } X_1 < p^{\frac{1}{2}}\log p, \end{cases}$$

and

$$B_n(\mathcal{X}_i) = \begin{cases} p^{-\frac{1}{2^n(n-2)}}, & \text{if } X_i \geqslant p^{\frac{1}{2}}\log p, \\ X_i^{-\frac{1}{2^{n-1}(n-2)}}, & \text{if } X_i < p^{\frac{1}{2}}\log p. \end{cases}$$

Proof. The proof follows that of Theorem 4.2.1, however we use Corollary 5.3.1 and Lemma 5.3.2 in place of their relevant results on arbitrary sets. □

5.3.2 Proof of Theorem 5.1.6

Let $\alpha_{k_i} = \gcd(k_i, p-1)$ for each $i = 1, \dots, t$. We then let $\mathcal{G}_{\alpha_i}$ be the subgroups of $\mathbb{F}_p^*$ generated by the elements of order α_{k_i}. Then

$$\begin{aligned}
S_\chi(\Psi) &= \frac{1}{\alpha_{k_1} \dots \alpha_{k_{t-1}}} \sum_{x_1 \in \mathcal{G}_{\alpha_1}} \dots \sum_{x_{t-1} \in \mathcal{G}_{\alpha_{t-1}}} \\
&\qquad \sum_{x_t \in \mathbb{F}_p^*} \chi(x_1 \dots x_t)\, \mathbf{e}_p(\Psi(x_1 \dots x_t)) \\
&= \frac{1}{\alpha_{k_1} \dots \alpha_{k_{t-1}}} \sum_{x_1 \in \mathcal{G}_{\alpha_1}} \dots \sum_{x_{t-1} \in \mathcal{G}_{\alpha_{t-1}}} \sum_{x_n \in \mathbb{F}_p^*} \chi(x_1 \dots x_t) \\
&\mathbf{e}_p(a_1(x_2 \dots x_t)^{k_1}) \dots \mathbf{e}_p(a_{t-1}(x_1 \dots x_{t-2}x_t)^{k_{t-1}})\, \mathbf{e}_p(a_t(x_1 \dots x_t)^{k_t}) \\
&= \frac{1}{\alpha_{k_1} \dots \alpha_{k_{t-1}}} \sum_{x_1 \in \mathcal{G}_{\alpha_1}} \dots \sum_{x_{t-1} \in \mathcal{G}_{\alpha_{t-1}}} \\
&\qquad \sum_{x_t \in \mathbb{F}_p^*} \omega_1(\mathbf{x}) \dots \omega_t(\mathbf{x})\, \mathbf{e}_p(a_t(x_1 \dots x_t)^{k_t}).
\end{aligned}$$

Now the image $\mathcal{X}_t = \{x_t^{k_t} : x_t \in \mathbb{F}_p^*\}$ of non-zero $k_t th$ powers contains $(p-1)/\alpha_{k_t}$ elements, each appearing with multiplicity α_{k_t}. Similarly, we notice the images $\mathcal{X}_i = \{x_i^{k_t} : x_i \in \mathcal{G}_{\alpha_{k_i}}\}$ contain $\alpha_{k_i}/\gcd(\alpha_{k_i}, \alpha_{k_t})$ elements, each appearing with multiplicity $\gcd(\alpha_{k_i}, \alpha_{k_t})$, for $i = 1, \dots, t-1$. Hence, we apply Lemma 5.3.3 to obtain

$$\begin{aligned}
S_\chi(\Psi) &\ll_t \frac{\alpha_{k_t}}{\beta_{k_1} \dots \beta_{k_{t-1}}} \cdot \left(p^{\frac{1}{2^t}} \beta_{k_{t-1}} A_t \left(\frac{p-1}{\alpha_{k_t}} \right) \prod_{i=1}^{t-2} B_t(\beta_{k_i}) \right) \\
&+ \frac{\alpha_{k_t}}{\beta_{k_1} \dots \beta_{k_{t-1}}} \cdot \frac{p-1}{\alpha_{k_t}} \beta_{k_1} \dots \beta_{k_{t-1}} \left(\left(\frac{\alpha_{k_t}}{p-1} \right)^{\frac{1}{2}} + \beta_{k_1}^{\frac{-1}{2^2}} + \dots + \beta_{k_{t-1}}^{\frac{-1}{2^t}} \right).
\end{aligned}$$

By simplifying we reach the required result.

5.4 Open Problems

In this chapter we were able to give stronger bounds on weighted multilinear exponential sums for when our sets are multiplicative subgroups of $\mathbb{F}_p$. One could also consider analogues over other interesting sets, such as intervals or sets contained in arithmetic progressions for example. In these cases we can take advantage of our subsets having small sum-sets, which may lead us to some stronger bounds.

It would also be interesting to consider short multinomial exponential sums or sums over some other choices of sets. Our techniques here unfortunately don't lend

themselves naturally to such applications. However, it should be possible to apply similar ideas when the sets are subgroups of $\mathbb{F}_p$.

Finally, another possible direction one could take this problem would be to consider taking the sum over composite moduli, rather than a prime p. Again, it seems that in this case new techniques will need to be developed and considered to provide new bounds.

References

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, and I. D. Shkredov, *Growth estimates in positive characteristic via collisions*, Int. Math. Res. Not. IMRN (2017), no. 23, 7148–7189.

[2] A. Balog and T. D. Wooley, *A low-energy decomposition theorem*, Q. J. Math. **68** (2017), no. 1, 207–226.

[3] J. Bourgain, *Multilinear exponential sums in prime fields under optimal entropy condition on the sources*, Geom. Funct. Anal. **18** (2009), no. 5, 1477–1502.

[4] ———, *On exponential sums in finite fields*, An irregular mind, Bolyai Soc. Math. Stud., vol. 21, János Bolyai Math. Soc., Budapest, 2010, pp. 219–242.

[5] J. Bourgain and M. Z. Garaev, *On a variant of sum-product estimates and explicit exponential sum bounds in prime fields*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 1, 1–21.

[6] J. Bourgain and A. Glibichuk, *Exponential sum estimates over a subgroup in an arbitrary finite field*, J. Anal. Math. **115** (2011), 51–70.

[7] 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. (2) **73** (2006), no. 2, 380–398.

[8] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), no. 1, 27–57.

[9] T. Cochrane, J. Coffelt, and C. Pinner, *A further refinement of Mordell's bound on exponential sums*, Acta Arith. **116** (2005), no. 1, 35–41.

[10] ———, *A system of simultaneous congruences arising from trinomial exponential sums*, J. Théor. Nombres Bordeaux **18** (2006), no. 1, 59–72.

[11] T. Cochrane and C. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. **133** (2005), no. 2, 313–320.

[12] ———, *Using Stepanov's method for exponential sums involving rational functions*, J. Number Theory **116** (2006), no. 2, 270–292.

[13] ———, *Bounds on fewnomial exponential sums over $\mathbb{Z}_p$*, Math. Proc. Cambridge Philos. Soc. **149** (2010), no. 2, 217–227.

[14] ———, *Explicit bounds on monomial and binomial exponential sums*, Q. J. Math. **62** (2011), no. 2, 323–349.

[15] P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in pure mathematics, Birkhäuser, Basel, 1983, pp. 213–218.

[16] M. Z. Garaev, *Sums and products of sets and estimates for rational trigonometric sums in fields of prime order*, Uspekhi Mat. Nauk **65** (2010), no. 4(394), 5–66.

[17] D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Q. J. Math. **51** (2000), no. 2, 221–235.

[18] B. Kerr and S. Macourt, *Multilinear exponential sums with a general class of weights*, ArXiv e-prints (2019).

[19] S. V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums*, IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) (Tula, 2001), Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002, pp. 86–114.

[20] S. V. Konyagin and I. D. Shkredov, *New results on sums and products in $\mathbb{R}$*, Tr. Mat. Inst. Steklova **294** (2016), no. Sovremennye Problemy Matematiki, Mekhaniki i Matematicheskoĭ Fiziki. II, 87–98.

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

[22] ———, *Incidence results and bounds of trilinear and quadrilinear exponential sums*, SIAM Journal on Discrete Mathematics **32** (2018), no. 2, 815–825.

[23] ———, *Decomposition of subsets of finite fields*, Funct. Approx. Comment. Math. **61** (2019), no. 2, 243–255.

[24] 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), no. 6, 1319–1338.

[25] D. A. Mit'kin, *Estimation of the total number of rational points of a set of curves over a finite prime field*, Chebyshevskiĭ Sb. **4** (2003), no. 4(8), 94–102.

[26] A. Mohammadi, *Szemerédi-Trotter type results in arbitrary finite fields*, ArXiv e-prints (2018).

[27] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev, and I. D. Shkredov, *New results on sum-product type growth over fields*, ArXiv e-prints (2017).

[28] A. Ostafe, *Polynomial values in affine subspaces of finite fields*, J. Anal. Math. **138** (2019), no. 1, 49–81.

[29] G. Petridis, *Collinear triples and quadruples for Cartesian products in* $\mathbb{F}_p^2$, ArXiv e-prints (2016).

[30] G. Petridis and I. E. Shparlinski, *Bounds of trilinear and quadrilinear exponential sums*, J. Anal. Math. **138** (2019), no. 2, 613–641.

[31] O. Roche-Newton, I. E. Shparlinski, and A. Winterhof, *Analogues of the Balog-Wooley decomposition for subsets of finite fields and character sums with convolutions*, Ann. Comb. **23** (2019), no. 1, 183–205.

[32] M. Rudnev, *On the number of incidences between points and planes in three dimensions*, Combinatorica **38** (2018), no. 1, 219–254.

[33] M. Rudnev, I. D. Shkredov, and S. Stevens, *On the energy variant of the sum-product conjecture*, ArXiv e-prints (2016).

[34] I. D. Shkredov, *On exponential sums over multiplicative subgroups of medium size*, Finite Fields Appl. **30** (2014), 72–87.

[35] ———, *On tripling constant of multiplicative subgroups*, Integers **16** (2016), Paper No. A75, 9.

[36] ———, *Differences of subgroups in subgroups*, Int. J. Number Theory **14** (2018), no. 4, 1111–1134.

[37] ———, *On asymptotic formulae in some sum-product questions*, ArXiv e-prints (2018).

[38] I. D. Shkredov and I. V. Vyugin, *On additive shifts of multiplicative subgroups*, Mat. Sb. **203** (2012), no. 6, 81–100.

[39] I. E Shparlinski, *On bounds of Gaussian sums*, Matem. Zametki **50** (1991), 122–130.

[40] Yu. N. Shteĭnikov, *Estimates of trigonometric sums over subgroups and some of their applications*, Mat. Zametki **98** (2015), no. 4, 606–625.

[41] S. Stevens and F. de Zeeuw, *An improved point-line incidence bound over arbitrary fields*, Bull. Lond. Math. Soc. **49** (2017), no. 5, 842–858.

[42] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006.

[43] A. Weil, *Basic number theory*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, Reprint of the second (1973) edition.