DOUBLE SUMS OF KLOOSTERMAN SUMS IN FINITE FIELDS

SIMON MACOURT AND IGOR E. SHPARLINSKI

Abstract. We bound double sums of Kloosterman sums over a finite field \( \mathbb{F}_q \), with one or both parameters ranging over an affine space over its prime subfield \( \mathbb{F}_p \subseteq \mathbb{F}_q \). These are finite fields analogues of a series of recent results by various authors in finite fields and residue rings. Our results are based on recent advances in additive combinatorics in arbitrary finite field.

1. Introduction

1.1. Background. The motivation behind this work comes from recent advances in estimating various bilinear sums of Kloosterman sums which have found a wealth of applications to various arithmetic problems, see [1, 4, 6–8, 10, 11] and references therein.

Here we extend some of these results to the settings of finite fields. Our approach is modelled from that of [10, 11] however at one significant point it deviates and we employ some very recent results of [9] from additive combinatorics in arbitrary finite fields.

For a prime power \( q \), let \( \mathbb{F}_q \) denote the finite field \( \mathbb{K} = \mathbb{F}_q \) of \( q \) elements.

We fix a nontrivial additive character \( \psi \) of \( \mathbb{F}_q \) and for integers \( u, v \in \mathbb{F}_q \) we define the Kloosterman sum

\[
\mathcal{K}_\psi(u, v) = \sum_{x \in \mathbb{F}_q^*} \psi(ux + vx^{-1}) .
\]

We consider sums of Kloosterman sums

\[
S_\psi(U, V) = \sum_{u \in U} \sum_{v \in V} \mathcal{K}_\psi(u, v)
\]
over some subsets $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_q$ and also of more general sums,

$$S_\psi(\alpha; \mathcal{U}, \mathcal{V}) = \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \alpha_v K_\psi(u, v),$$

with a sequence of complex weights $\alpha = \{\alpha_v\}_{v \in \mathcal{V}}$.

By the Weil bound we have

$$|K_\psi(u, v)| \leq 2q^{1/2},$$

see [5, Corollary 11.12]. Hence we immediately obtain

$$|S_\psi(\alpha; \mathcal{U}, \mathcal{V})| \leq 2Uq^{1/2} \sum_{v \in \mathcal{V}} |\alpha_v|,$$

where $U = \#\mathcal{U}$ is the cardinality of $\mathcal{U}$.

We are interested in studying cancellations amongst Kloosterman sums and thus improvements of the trivial bound (1.1). We note that the sums $S_\psi(\mathcal{U}, \mathcal{V})$ and $S_\psi(\alpha; \mathcal{U}, \mathcal{V})$ are finite field analogues of similar sums studied in [1, 4, 6–8, 10, 11] in the settings of prime fields and residue rings. Hence, adopting the model of $\mathbb{F}_q$ as

$$\mathbb{F}_q \cong \mathbb{F}_p[X]/f(x)$$

for a prime field $\mathbb{F}_p$ and an irreducible over $\mathbb{F}_p$ polynomial $f$ (of degree $\deg f = [\mathbb{F}_q : \mathbb{F}_p]$) we expect that our bounds can be used for similar arithmetic applications in function fields. Since in the above works, the case of averaging over intervals plays a vital role, here we consider the case when one or both of the sets $\mathcal{U}$ and $\mathcal{V}$ is an affine subspace of $\mathbb{F}_q$, considered as a vector space over its prime subfield $\mathbb{F}_p \subseteq \mathbb{F}_q$. More precisely, we consider the sums

- $S_\psi(\mathcal{A}, \mathcal{B})$ with two affine spaces $\mathcal{A}$ and $\mathcal{B}$,
- $S_\psi(\alpha; \mathcal{A}, \mathcal{V})$ with an affine space $\mathcal{A}$ and an arbitrary set $\mathcal{V}$.

Our approach is similar to that of [10, 11] however some ingredients used in [10, 11] are either unknown or do not exist in function field settings. Hence we use a different approach based on additive combinatorics and in particular we rely on recent results of Mohammadi [9].

1.2. **Our results.** We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that the inequality $|U| \leq cV$ holds with some constant $c > 0$, which is absolute throughout this paper.

We start with the sums $S_\psi(\mathcal{A}, \mathcal{B})$.

**Theorem 1.1.** Assume that $q = p^{2k+1}$ is an odd power of a prime $p$. Let $\mathcal{A}$ and $\mathcal{B}$ be affine subspaces of $\mathbb{F}_q$ of cardinalities $A = \#\mathcal{A}$ and
B = \#B, respectively, with \( A \leq B \). Then

\[
S_\psi(A, B) \ll AB \max \{q^{52/153}, (q/A)^{831/832}, (q/A)^{761/760}q^{-1/760}\}.
\]

Clearly Theorem (1.1) is only non-trivial for \( A \geq q^{415/831} \) as otherwise the bound \( |S_\psi(A, B)| \leq 2ABq^{1/2} \), implied by (1.1), is stronger.

Given a sequence of complex weights \( \alpha = \{\alpha_v\}_{v \in V} \) supported on a set \( V \) and \( \rho > 0 \), as usual, we define

\[
\|\alpha\|_\rho = \left( \sum_{\eta \in V} |\alpha_\eta|^\rho \right)^{1/\rho}.
\]

**Theorem 1.2.** Assume that \( q = p^{2k+1} \) is an odd power of a prime \( p \).

Let \( A \) be an affine subspace of \( \mathbb{F}_q \) of cardinality \( A = \#A \) and let \( V \subseteq \mathbb{F}_q \)
be an arbitrary set of cardinality \( V = \#V \). Then, for any sequence of complex weights \( \alpha = \{\alpha_v\}_{v \in V} \) we have

\[
S_\psi(\alpha; A, V) \ll Aq^{1/4}\sqrt{|\alpha|_1|\alpha|_2}
\]

\[
\max \left\{ q^{13/51}, \left( \frac{q}{A} \right)^{935/1248}, q^{-1/1140} \left( \frac{q}{A} \right)^{214/285} \right\}.
\]

If we suppose that \( |\alpha_v| \ll 1 \) for all \( v \in V \), then clearly Theorem 1.2 is only non-trivial for \( A^{935/623}V^{312/623} > q \). If we suppose \( V = A \) then we have Theorem 1.2 is non-trivial provided \( A > q^{623/1247} \).

2. **Background from additive combinatorics**

For a set \( S \subseteq \mathbb{F}_q \), we use \( E(S) \) to denote its additive energy, that is, the number of solutions to the equation

\[
s_1 + s_2 = s_3 + s_4, \quad s_1, s_2, s_3, s_4 \in S.
\]

Also, as usual, we denote

\[
S^{-1} = \{s^{-1} : s \in S\} \quad \text{and} \quad 2S = \{s + t : s + t \in S\}.
\]

Then by [9, Corollary 5] we have

**Lemma 2.1.** Let \( S \subseteq \mathbb{F}_q \) with

\[
\#S = S \quad \text{and} \quad \#(2S) = T
\]

and such that \( T \geq (\#G)^{52/51} \) for any proper subfield \( G \) of \( \mathbb{F}_q \). Then

\[
E(S^{-1}) \ll \left( T^{173/104} + q^{-1/285}T^{476/285} \right) S^{4/3}.
\]

It is easy to see that the Cauchy inequality implies the well-known inequality

\[
S^4 \leq \#(2S^{-1}) E(S^{-1}).
\]
Hence from Lemma 2.1 we derive the following (see also [9, Corollary 5]).

**Corollary 2.2.** Let $S \subseteq \mathbb{F}_q$ with
\[
\#S = S, \quad \#(2S) = T, \quad \#(2S^{-1}) = U
\]
d and such that $T \geq (\#G)^{52/51}$ for any proper subfield $G$ of $\mathbb{F}_q$. Then
\[
\max\{T, U\} \geq \min\{S^{832/831}, q^{1/761}S^{760/761}\}.
\]

3. **Proof of Theorem 1.1**

Changing the order of summation, we obtain

\[
S_{\psi}(A, B) = \sum_{x \in \mathbb{F}_q^*} \sum_{a \in A} \psi(ax) \sum_{b \in B} \psi(bx^{-1}).
\]

Clearly if $A$ is a translate of a linear space $L$ then

\[
\sum_{a \in A} \psi(ax) = \begin{cases} A, & \text{if } x \in L^\perp, \\ 0, & \text{otherwise}, \end{cases}
\]

where $L^\perp$ denotes the orthogonal complement of $L$.

Similarly if $B$ is a translate of a linear space $M$ then

\[
\sum_{b \in B} \psi(bx^{-1}) = \begin{cases} B, & \text{if } x^{-1} \in M^\perp, \\ 0, & \text{otherwise}. \end{cases}
\]

Hence, substituting (3.2) and (3.3) in (3.1), we obtain

\[
S_{\psi}(A, B) \ll ABS
\]

where $S = \#S$ and the set $S$ is defined as follows

\[
S = \{ x \in \mathbb{F}_q^* : x \in L^\perp \text{ and } x^{-1} \in M^\perp \}.
\]

If $S \leq q^{52/153}$ the result follows immediately. Otherwise we see that

\[
\#(2S) \geq \#S \geq (\#G)^{52/51}
\]

for any proper subfield $G$ of $\mathbb{F}_q$ (since $q$ is not a perfect square we have $\#G \leq q^{1/3}$). Hence Corollary 2.2 applies to $S$.

Since $L^\perp$ and $M^\perp$ are linear spaces, we obviously have

\[
2S \subseteq L^\perp \quad \text{and} \quad 2S^{-1} \subseteq M^\perp.
\]

Consequently,

\[
\#(2S) \leq \#L^\perp = q/A \quad \text{and} \quad \#(2S^{-1}) \leq \#M^\perp = q/B.
\]

Invoking Corollary 2.2, we obtain

\[
\min\{S^{832/831}, q^{1/761}S^{760/761}\} \ll \max\{q/A, q/B\} \leq q/A.
\]
as $A \leq B$. Thus

$$S \ll \max\{(q/A)^{831/832}, (q/A)^{761/760}q^{-1/760}\}$$

which after substitution in (3.4) implies the result.

4. Proof of Theorem 1.2

By changing the order of summation we have

$$|S_{\psi}(\alpha; A, V)| = \left| \sum_{x \in F_q^*} \sum_{v \in V} \alpha_v \psi(vx^{-1}) \sum_{a \in A} \psi(ax) \right|.$$

As previously, if $A$ is a translate of a linear space $L$ then

$$\sum_{a \in A} \psi(ax) = \begin{cases} A, & \text{if } x \in L^\perp, \\ 0, & \text{otherwise}, \end{cases}$$

where $L^\perp$ denotes the orthogonal complement $L$. It follows that

$$|S_{\psi}(\alpha; A, V)| = A \left| \sum_{x \in L^\perp} \sum_{v \in V} \alpha_v \psi(vx^{-1}) \right| \leq A \sum_{v \in V} |\alpha_v| \left| \sum_{x \in L^\perp} \psi(vx^{-1}) \right| \leq A \sum_{v \in V} |\alpha_v|^{1/2} |\alpha_v^{\perp}|^{1/2} \left| \sum_{x \in L^\perp} \psi(vx^{-1}) \right|.$$

Applying the Cauchy–Schwarz inequality twice, we obtain

$$|S_{\psi}(\alpha; A, V)|^4 \leq A^4 \left( \sum_{v \in V} |\alpha_v| \right)^2 \sum_{v \in V} |\alpha_v|^2 \sum_{v \in V} \sum_{x \in L^\perp} \psi(vx^{-1})^4 \leq A^4 |\alpha_1|^2 |\alpha_2|^2 \sum_{x \in L^\perp} \sum_{w, x, y, z \in L^\perp} \psi(v(w^{-1} + x^{-1} - y^{-1} - z^{-1})).$$

If $2L^\perp = L^\perp < (\#G)^{52/51}$, we use the trivial bound on additive energy, that is $E((L^\perp)^{-1}) \leq (\#L^\perp)^3$, and the result follows immediately.
Otherwise, we apply Lemma 2.1, observing \( \#L = q/A \), to obtain
\[
S_{\psi}(\alpha; A, V) \ll Aq^{1/4} \sqrt{|\alpha_1|/\alpha_2} \left( \left( \frac{q}{A} \right)^{173/104} + q^{-1/285} \left( \frac{q}{A} \right)^{476/285} \right) \left( \frac{q}{A} \right)^{4/3} \right)^{1/4}
\]
\[
\ll Aq^{1/4} \sqrt{|\alpha_1|/\alpha_2} \max \left\{ \left( \frac{q}{A} \right)^{935/1248}, q^{-1/1140} \left( \frac{q}{A} \right)^{214/285} \right\}.
\]
This completes the proof.

5. Comments

Some of the motivation to this paper comes from an intention to obtain function field analogues of the asymptotic formulas, with a power saving, from [1, 2, 10, 12] for 4th moments of \( L \)-functions. However, despite recent progress in this direction due to Florea [3], some ingredients, used in the groundbreaking work of Young [12], remain missing in the function field case.

Finally, we need to impose the condition on \( q = p^{2k+1} \) to avoid the existence of large subfields. It is certainly interesting to drop this restriction and extend our results to even degree extensions.

Acknowledgements

The authors are grateful to Goran Djanković for very illuminating discussions.

This work was supported in part by ARC Grant DP170100786.

REFERENCES

[1] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, ‘On moments of twisted \( L \)-functions’, Amer. J. Math. 139 (2017), 707–768.
[2] V. Blomer, É. Fouvry, E. Kowalski, P. Michel and D. Milićević, ‘Some applications of smooth bilinear forms with Kloosterman sums’, Trudy Matem. Inst. Steklov 296 (2017), 24–35.
[3] A. Florea, ‘The fourth moment of quadratic Dirichlet \( L \)-functions over function fields’, Geom. Funct. Anal. 27 (2017), 541–595.
[4] É. Fouvry, E. Kowalski and P. Michel, ‘Algebraic trace functions over the primes’, Duke Math. J. 163 (2014), 1683–1736.
[5] H. Iwaniec and E. Kowalski, Analytic number theory, Amer. Math. Soc., Providence, RI, 2004.
[6] K. Liu, I. E. Shparlinski and T. P. Zhang, ‘Divisor problem in arithmetic progressions modulo a prime power’, Adv. Math. 325 (2018), 459–481.
[7] E. Kowalski, P. Michel and W. Sawin, ‘Bilinear forms with Kloosterman sums and applications’, Ann. Math. 186 (2017), 413–500.
[8] E. Kowalski, P. Michel and W. Sawin, ‘Bilinear forms with generalized Kloosterman sums’, Preprint, 2018 (available from http://arxiv.org/abs/1802.09849). 1, 2

[9] A. Mohammadi, ‘Szemerédi–Trotter type results in arbitrary finite fields’, Preprint, 2018 (available from http://arxiv.org/abs/1808.05543). 1, 2, 3, 4

[10] I. E. Shparlinski, ‘On sums of Kloosterman and Gauss sums’, Trans. Amer. Math. Soc., (to appear). 1, 2, 6

[11] I. E. Shparlinski and T. P. Zhang, ‘Cancellations amongst Kloosterman sums’, Acta Arith., 176 (2016), 201–210. 1, 2

[12] M. Young, ‘The fourth moment of Dirichlet L-functions’, Annals Math., 173 (2011), 1–50. 6

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

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: igor.shparlinski@unsw.edu.au