Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Bilinear forms with exponential sums with binomials

Kui Liu [a], Igor E. Shparlinski [b], Tianping Zhang [c,*]

[a] *School of Mathematics and Statistics, Qingdao University, No. 308, Ningxia Road, Shinan, Qingdao, Shandong, 266071, PR China*
[b] *Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia*
[c] *School of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710019 Shaanxi, PR China*

ARTICLE INFO

Article history:
Received 29 October 2017
Received in revised form 12 December 2017
Accepted 19 December 2017
Available online xxxx
Communicated by S.J. Miller

MSC:
11D79
11L07

Keywords:
Binomial sums
Cancellation
Bilinear form

ABSTRACT

We obtain several estimates for bilinear forms with exponential sums with binomials $mx^k + nx^\ell$. In particular we show the existence of nontrivial cancellations between such sums when the coefficients m and n vary over rather sparse sets of general nature.

* Corresponding author.
E-mail addresses: liukui@qdu.edu.cn (K. Liu), igor.shparlinski@unsw.edu.au (I.E. Shparlinski), tpzhang@snnu.edu.cn (T.P. Zhang).

https://doi.org/10.1016/j.jnt.2017.12.011
0022-314X/

1. Introduction

1.1. Background and motivation

For a positive integer q, we denote by $\mathbb{Z}_q$ the residue ring modulo q and also denote by $\mathbb{Z}_q^*$ the group of units of $\mathbb{Z}_q$.

For fixed integers k and ℓ, we consider exponential sums with binomials

$$S_{k,\ell,q}(m,n) = \sum_{x \in \mathbb{Z}_q^*} \mathbf{e}_q\left(mx^k + nx^\ell\right),$$

where for negative powers of x are computed modulo q and

$$\mathbf{e}_q(z) = \exp(2\pi i z/q).$$

The case $(k,\ell) = (1,-1)$ corresponds to the case of Kloosterman sums. We note that when both k and ℓ are positive there is no reason to restrict the summation to $\mathbb{Z}_q^*$. However, motivated by the choice $(k,\ell) = (-2,1)$ which is important for applications to square-free numbers in progressions, see [13] we only consider this case. It is also important for the validity of the bound (1.3) below.

Furthermore, given two sets $\mathcal{M}, \mathcal{N} \subseteq \mathbb{Z}_q$ and two sequences of weights $\boldsymbol{\alpha} = \{\alpha_m\}_{m\in\mathcal{M}}$ and $\boldsymbol{\beta} = \{\beta_n\}_{n\in\mathcal{N}}$, we define the following bilinear forms with the binomial sums $S_{k,\ell,q}(m,n)$:

$$\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha},\boldsymbol{\beta};\mathcal{M},\mathcal{N}) = \sum_{m\in\mathcal{M}} \sum_{n\in\mathcal{N}} \alpha_m \beta_n S_{k,\ell,q}(m,n).$$

We also consider the following special cases

$$\begin{aligned} \mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha};\mathcal{M},\mathcal{N}) &= \mathcal{S}_{k,\ell,q}\left(\boldsymbol{\alpha},\{1\}_{n\in\mathcal{N}};\mathcal{M},\mathcal{N}\right) \\ &= \sum_{m\in\mathcal{M}} \sum_{n\in\mathcal{N}} \alpha_m S_{k,\ell,q}(m,n), \end{aligned} \tag{1.1}$$

and

$$\begin{aligned} \mathcal{S}_{k,\ell,q}(\mathcal{M},\mathcal{N}) &= \mathcal{S}_{k,\ell,q}\left(\{1\}_{m\in\mathcal{M}},\{1\}_{n\in\mathcal{N}};\mathcal{M},\mathcal{N}\right) \\ &= \sum_{m\in\mathcal{M}} \sum_{n\in\mathcal{N}} S_{k,\ell,q}(m,n). \end{aligned} \tag{1.2}$$

For $(k,\ell) = (1,-1)$, that is, for Kloosterman sums, such bilinear forms have been introduced by Fouvry, Kowalski and Michel [3] who have also demonstrated the importance of estimating them beyond of what follows immediately from the Weil bound of Kloosterman sums (see, for example, [7, Chapter 11]), that is, better than the bound (1.3) below.

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

More generally, for arbitrary modulus q and exponents (k, ℓ) one can apply the general bound of [16, Theorem 1] on exponential sums with few nomials to derive

$$|\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha}, \boldsymbol{\beta}; \mathcal{M}, \mathcal{N})| \le MNq^{1/2+o(1)} \max_{m \in \mathcal{M}} |\alpha_m| \max_{n \in \mathcal{N}} |\beta_n|, \tag{1.3}$$

to which we refer as the *trivial bound*.

Further progress in the case $(k, \ell) = (1, -1)$ has been achieved in [1,2,11,17,18]. In [22] this question has been studied on average over the moduli q. We also recall recent results of [10,12,21] when cancellations among Kloosterman sums are studied for moduli of special arithmetic structure. Furthermore, the case of a prime $q = p$ and $(k, \ell) = (2, -1)$ has been studied by Nunes [13], via the method of Fouvry, Kowalski and Michel [3]. Then these sums have been used to investigate the distribution of squarefree integers in arithmetic progressions; see Section 5 for exact formulations of the results of Nunes [13] and their comparison with our bounds.

We remark that the method introduced by Fouvry, Kowalski and Michel [3], and then further developed and used in [1,11,13], relies heavily on such deep tools as the Weil and Deligne bounds, see [7, Chapter 11]. As a result, this approach works well only for prime moduli p, while the methods of [17,18] are of elementary nature, and in particular work without any losses of strength for composite q. On the other hand, the method of [1,3,11,22] works for much more general objects than Kloosterman and other similar exponential sums.

1.2. General notation

We remark that our bounds involve only the norms of the weights $\boldsymbol{\alpha}$ but do not explicitly depend on the size of the set $\mathcal{M}$ on which they are supported. Hence, without loss of generality, we can assume that $\mathcal{M} = \mathbb{Z}_q$. On the other hand, our method does not apply to general sets $\mathcal{N}$ and works only when $\mathcal{N}$ is an interval, and thus, for the sums with weights we simplify the notation as

$$\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha}; \mathcal{J}) = \sum_{m \in \mathbb{Z}_q} \sum_{n \in \mathcal{J}} \alpha_m S_{k,\ell,q}(m, n), \tag{1.4}$$

where $\mathcal{J} = \{L+1, \ldots, L+N\} \subseteq \mathbb{Z}_q$ is a set of N consecutive residues of $\mathbb{Z}_q$ (with $q-1$ followed by 0). Furthermore, in the case of the sums without weights we only estimate such sums when the set $\mathcal{M} = \mathcal{I} = \{K+1, \ldots, K+M\} \subseteq \mathbb{Z}_q$ is another interval, and thus we write $\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J})$.

The case of $\ell = -1$ is somewhat special as it admits some extra treatment and is also important for many applications, see [13] for example. Thus we introduce special notations

$$\mathcal{S}^*_{k,q}(\mathcal{I}, \mathcal{J}) = \mathcal{S}_{k,-1,q}(\mathcal{I}, \mathcal{J}) \quad \text{and} \quad \mathcal{S}^*_{k,q}(\boldsymbol{\alpha}; \mathcal{J}) = \mathcal{S}_{k,-1,q}(\boldsymbol{\alpha}; \mathcal{J}), \tag{1.5}$$

which shorten (1.1) and (1.4), respectively.

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

For an integer u we define

$$\langle u \rangle_q = \min_{k \in \mathbb{Z}} |u - kq|$$

as the distance to the closest integer, which is a multiple of q.

We also define the norms

$$\|\boldsymbol{\alpha}\|_\infty = \max_{m \in \mathcal{M}} |\alpha_m| \qquad \text{and} \qquad \|\boldsymbol{\alpha}\|_\sigma = \left(\sum_{m \in \mathcal{M}} |\alpha_m|^\sigma \right)^{1/\sigma},$$

where $\sigma > 0$, and similarly for the weights $\boldsymbol{\beta}$.

Throughout the paper, as usual $A \ll B$ is equivalent to the inequality $|A| \le cB$ with some constant $c > 0$, which may depend on the integers k and ℓ, and occasionally, where obvious, the real parameter $\varepsilon > 0$ and on the integer parameter $\nu \ge 1$.

The letter p always denotes a prime number and we say that q is *squarefree* if it is not divisible by p^2 for any p.

2. New results

2.1. Bounds for every q

We start with the sums $\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha}; \mathcal{J})$, defined in (1.4), which are medium level of complexity as one variable still runs through a continuous interval. The proof is based on the method from [18], coupled with a result of Pierce [15, Theorem 4].

Theorem 2.1. *If k and ℓ are fixed nonzero integers such that k/ℓ is not a positive integer, then, for any fixed positive integer ν, squarefree $q \ge 1$ and*

$$\mathcal{J} = \{L+1, \ldots, L+N\} \subseteq \mathbb{Z}_q,$$

we have

$$\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha}; \mathcal{J}) \ll \min\Big\{ \|\boldsymbol{\alpha}\|_2 N^{1/2} q,\ \|\boldsymbol{\alpha}\|_1^{1-1/\nu} \|\boldsymbol{\alpha}\|_2^{1/\nu} \Big(q + q^{(2\nu^2+\nu+1)/2\nu(\nu+1)} N^{1/(\nu+1)} \Big) q^{o(1)} \Big\}.$$

In particular, when α_m is the characteristic function of the interval $\mathcal{I} = \{K+1, \ldots, K+M\}$ we obtain a bound on the sums $\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J})$, defined by (1.2). We also see that in the case of the sums $\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J})$ the roles of M and N can be interchanged.

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

Corollary 2.2. *If k and ℓ are fixed nonzero integers such that k/ℓ and ℓ/k are not positive integers, then, for any fixed positive integer ν, squarefree $q \geq 1$ and*

$$\mathcal{I} = \{K+1, \dots, K+M\}, \ \mathcal{J} = \{L+1, \dots, L+N\} \subseteq \mathbb{Z}_q,$$

we have

$$\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J}) \leq X^{1-1/2\nu} \left(q + q^{(2\nu^2+\nu+1)/2\nu(\nu+1)} Y^{1/(\nu+1)}\right) q^{o(1)},$$

where $X = \min\{M, N\}$, $Y = \max\{M, N\}$.

In particular, with $\nu = 2$ we obtain from Corollary 2.2 that

$$\mathcal{S}_{k,\ell,q}(\mathcal{I}, \mathcal{J}) \leq q^{1+o(1)} N^{3/4} + q^{11/12+o(1)} M^{1/3} N^{3/4}. \tag{2.1}$$

This improves the trivial bound (1.3) provided that

$$M^4 N \geq q^{2+\varepsilon} \qquad \text{and} \qquad M^8 N^3 \geq q^{5+\varepsilon} \tag{2.2}$$

for some fixed $\varepsilon > 0$, and in particular for $M = N \geq q^{5/11+\varepsilon}$. Note that in (2.1) and (2.2) the roles of M and N can be interchanged.

In the case $M, N = q^{1/2+o(1)}$ crucial for many applications, Corollary 2.2 implies the bound $MNq^{1/2-1/24+o(1)}$, saving $q^{1/24}$ compared to the trivial bound (1.3).

2.2. Bounds for almost all q

We also show that in the case of $\ell = -1$ for almost all q in a dyadic interval $[Q, 2Q]$ stronger versions of the results of Section 2.1 hold. In particular, we recall our special notations in this case, given by (1.5).

We also have an analogue of the second bound in Theorem 2.1, but only for the sums $\mathcal{S}^*_{k,q}(\boldsymbol{\alpha}; \mathcal{J})$.

Theorem 2.3. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν, fixed real $\varepsilon > 0$ and sufficiently large real $Q \geq 1$, we have*

$$\frac{1}{Q} \sum_{q \in [Q, 2Q]} |\mathcal{S}^*_{k,q}(\boldsymbol{\alpha}; \mathcal{J})|^{2\nu} \ll \|\boldsymbol{\alpha}\|_1^{2\nu-2} \|\boldsymbol{\alpha}\|_2^2 \left(Q^{2\nu} + Q^{\nu+1} N^{\nu}\right) Q^{o(1)}.$$

We now immediately derive:

Corollary 2.4. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν, fixed real $\varepsilon > 0$ and sufficiently large real $Q \geq 1$, for all but $O(Q^{1-\varepsilon})$ integers $q \in [Q, 2Q]$, we have*

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

$$\mathcal{S}^*_{k,q}(\boldsymbol{\alpha}; \mathcal{J}) \ll \|\boldsymbol{\alpha}\|_1^{1-1/\nu} \|\boldsymbol{\alpha}\|_2^{1/\nu} \left(q + q^{(\nu+1)/2\nu} N^{1/2}\right) q^{\varepsilon}.$$

We also have the following version of Corollary 2.2 (however this time we cannot interchange the roles of M and N).

Corollary 2.5. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν, fixed real $\varepsilon > 0$ and sufficiently large real $Q \geq 1$, for all but $O(Q^{1-\varepsilon})$ integers $q \in [Q, 2Q]$, we have*

$$\mathcal{S}^*_{k,q}(\mathcal{I}, \mathcal{J}) \ll M^{1-1/2\nu} \left(q + q^{(\nu+1)/2\nu} N^{1/2}\right) q^{\varepsilon}.$$

We see that Corollary 2.5 gives a nontrivial bound if for some integer $\nu \geq 1$ we have

$$MN^{2\nu} \geq q^{\nu} \qquad \text{and} \qquad MN^{\nu} \geq q.$$

3. Preparations

3.1. Linear and bilinear exponential sums

We need the following well-known simple results.

First we recall the following bound of linear sums [7, bound (8.6)].

Lemma 3.1. *For any integers u, L and $N \geq 1$, we have*

$$\sum_{n=L+1}^{L+N} \mathbf{e}_q(nu) \ll \min\left\{N, \frac{q}{\langle u \rangle_q}\right\}.$$

We also need the following well-known result, which dates back to Vinogradov [20, Chapter 6, Problem 14.a].

Lemma 3.2. *For arbitrary set $\mathcal{U}, \mathcal{V} \subseteq \mathbb{Z}_q$ and sequences of complex weights $\boldsymbol{\varphi} = \{\varphi_u\}_{u \in \mathcal{U}}$ and $\boldsymbol{\psi} = \{\psi_v\}_{v \in \mathcal{V}}$ we have*

$$\left|\sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \varphi_u \psi_v \, \mathbf{e}_q(uv)\right| \leq \|\boldsymbol{\varphi}\|_2 \|\boldsymbol{\psi}\|_2 q^{1/2}.$$

3.2. Some equations and congruences

We start with a very simple result on the monomial congruences. It can be derived elementary via a combination of the *Chinese Remainder Theorem* and *Hensel Lifting*, however we simply appeal to the general bound of Huxley [6].

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

Lemma 3.3. *If k is a nonzero integer then for any $a \in \mathbb{Z}_q$ the congruence*

$$x^k \equiv a \pmod q, \qquad x \in \mathbb{Z}_q^*,$$

has at most $q^{o(1)}$ solutions.

Proof. Clearly we can assume that $a \in \mathbb{Z}_q^*$ as otherwise there is no solution. Then the discriminant of the polynomial $X^k - a$ has a bounded greatest common divisor with q and the result follows from [6]. □

We also need several results of Pierce [15], which in turn generalises previous results of Heath-Brown [5, Lemma 1] (which corresponds to $\ell = -1$). We present these results in slightly more general forms (which are however implicitly contained in the argument of [15]).

For an integer $\nu \ge 1$ and real U let $I_{k,\ell,\nu,q}(U)$ be the number of solutions to the system of congruences

$$\begin{aligned} v_1 + \ldots + v_\nu &\equiv v_{\nu+1} + \ldots + v_{2\nu} \pmod q, \\ u_i^k &\equiv v_i^\ell \pmod q, \quad i = 1, \ldots, 2\nu, \end{aligned}$$

with $1 \le u_1, \ldots, u_{2\nu} \le U$ and unrestricted variables $v_1, \ldots, v_{2\nu} \in \mathbb{Z}_q$. We have the following slight extension of the bound of Pierce [15, Equation (6.2)] (which is free of the restriction $U \le q^{(\nu+1)/2\nu}$).

We recall that all implied constants are allowed to depend on ν.

Lemma 3.4. *If k and ℓ are fixed nonzero integers such that k/ℓ is not a positive integer, then, for any fixed positive integer ν, squarefree $q \ge 1$ and $U \le q$ we have*

$$I_{k,\ell,\nu,q}(U) \le \left(U^{2\nu} q^{-1} + U^{2\nu^2/(\nu+1)}\right) q^{o(1)}.$$

Proof. We use the following inequality given (in a slightly more precise form) in [15, Section 6.3]:

$$I_{k,\ell,\nu,q}(U) \le \left(Q^{-1} U^{2\nu-1} + Q^\nu U^\nu\right) q^{o(1)},$$

holds for any Q, satisfying the conditions

$$Q < U \qquad \text{and} \qquad 8QU \le q.$$

Thus taking

$$Q = \min\left\{U^{(\nu-1)/(\nu+1)}, q/8U\right\},$$

we obtain the result. □

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

In particular, if $U \le q^{(\nu+1)/2\nu}$ the bound of Lemma 3.4 is essentially of the same form as [15, Equation (6.2)].

In the case $\ell = -1$, following our previous convention, we denote

$$I^*_{k,\nu,q}(U) = I_{k,-1,\nu,q}(U).$$

We now show that one can get a better bound on $I^*_{k,\nu,q}(U)$ on average over q in a dyadic interval $[Q, 2Q]$. Indeed, let $J_{k,\nu}(U)$ be the number of solutions to the equation

$$\frac{1}{u_1^k} + \ldots + \frac{1}{u_\nu^k} = \frac{1}{u_{\nu+1}^k} + \ldots + \frac{1}{u_{2\nu}^k}, \qquad 1 \le u_1, \ldots, u_{2\nu} \le U. \tag{3.1}$$

We have the following bound, which is a slight modification of a result of Karatsuba [8], corresponding to $k = 1$ and presented in the proof of [8, Theorem 1].

Lemma 3.5. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν, we have*

$$J_{k,\nu}(U) \le U^{\nu + o(1)}.$$

Proof. Clearing the denominators in (3.1), we see that if $p \mid u_i$ for some component $i = 1, \ldots, 2\nu$ of a solution, then we also have $p \mid u_j$ for some $j \ne i$. This means that for any solution to (3.1), the product $u_1 \ldots u_{2\nu}$ is squarefull. Since any interval $[1, W]$ contains $O(W^{1/2})$ squarefull integers, see [19], applying this with $W = U^{2\nu}$ and then using the classical bound on the divisor function, see [7, Equation (1.81)], we obtain the result. □

Now repeating the argument of the proof of [4, Lemma 2.3] and using Lemma 3.5 in the appropriate place, we obtain:

Lemma 3.6. *If $k > 1$ is a fixed integer, then, for any fixed positive integer ν and sufficiently large real $1 \le U \le Q$, we have*

$$\frac{1}{Q} \sum_{Q \le q \le 2Q} I^*_{k,\nu,q}(U) \le \left(U^{2\nu} Q^{-1} + U^\nu\right) Q^{o(1)}.$$

4. Proofs of the main results

4.1. Proof of Theorem 2.1

Changing the order of summation, we obtain

$$\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha}; \mathcal{J}) = \sum_{x \in \mathbb{Z}_q^*} \sum_{m \in \mathbb{Z}_q} \alpha_m \, \mathbf{e}_q(mx^k) \sum_{n \in \mathcal{J}} \mathbf{e}_q(nx^\ell).$$

Recalling Lemma 3.1, we obtain

$$\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha};\mathcal{J}) = \sum_{m\in\mathbb{Z}_q}\sum_{x\in\mathbb{Z}_q^*}\alpha_m\gamma_x\,\mathbf{e}_q(mx^k),$$

where

$$|\gamma_x| \le \min\left\{N, \frac{q}{\langle x^\ell\rangle_q}\right\}.$$

We define $I = \lceil \log q\rceil$ and write

$$\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha};\mathcal{J}) \ll |\Sigma_{0,q}| + \sum_{i=1}^{I}|\Sigma_{i,q}|, \tag{4.1}$$

where

$$\Sigma_{0,q} = \sum_{m\in\mathbb{Z}_q}\sum_{\substack{x\in\mathbb{Z}_q^*\\ \langle x^\ell\rangle_q\le q/N}}\alpha_m\gamma_x\,\mathbf{e}_q(mx^k),$$

$$\Sigma_{i,q} = \sum_{m\in\mathbb{Z}_q}\sum_{\substack{x\in\mathbb{Z}_q^*\\ e^{i+1}q/N\ge\langle x^\ell\rangle_q>e^iq/N}}\alpha_m\gamma_x\,\mathbf{e}_q(mx^k), \qquad i=1,\dots,I.$$

Now using Lemmas 3.2 and 3.3, we have

$$|\Sigma_{0,q}| \le \|\boldsymbol{\alpha}\|_2 N\sqrt{(q/N)q^{1+o(1)}} \le \|\boldsymbol{\alpha}\|_2 N^{1/2}q^{1+o(1)}. \tag{4.2}$$

Also, for $i=1,\dots,I$, using that if $e^{i+1}q/N \ge \langle x^\ell\rangle_q > e^iq/N$ then $\gamma_x \ll Ne^{-i}$, hence, again by Lemmas 3.2 and 3.3, we obtain

$$\begin{aligned}\Sigma_{i,q} &= \sum_{m\in\mathbb{Z}_q}\sum_{\substack{x\in\mathbb{Z}_q^*\\ e^{i+1}q/N\ge\langle x^k\rangle_q>e^iq/N}}\alpha_m\gamma_x\,\mathbf{e}_q(mx^\ell)\\ &\le \|\boldsymbol{\alpha}\|_2(q^{o(1)}N^2e^{-2i}e^iq/N)^{1/2}q^{1/2} = e^{-i/2}\|\boldsymbol{\alpha}\|_2N^{1/2}q^{1+o(1)}.\end{aligned}$$

Therefore,

$$\sum_{i=1}^{I}|\Sigma_{i,q}| \le \|\boldsymbol{\alpha}\|_2N^{1/2}q^{1+o(1)}\sum_{i=1}^{I}e^{-i/2} \le \|\boldsymbol{\alpha}\|_2N^{1/2}q^{1+o(1)}. \tag{4.3}$$

Combining (4.2) and (4.3), we obtain the first bound.

For the second bound we turn to use the method of [17]. For a fixed integer $\nu\ge 2$, using the Hölder inequality, we obtain

$$|\Sigma_{0,q}|^{2\nu} \le \left(\sum_{m\in\mathbb{Z}_q} |\alpha_m|\right)^{2\nu-2} \sum_{m\in\mathbb{Z}_q} |\alpha_m|^2 W_{0,q} \\ = \|\boldsymbol{\alpha}\|_1^{2\nu-2} \|\boldsymbol{\alpha}\|_2^2 W_{0,q}, \tag{4.4}$$

where

$$W_{0,q} = \sum_{m\in\mathbb{Z}_q} \left| \sum_{\substack{x\in\mathbb{Z}_q^* \\ \langle x^\ell\rangle_q \le q/N}} \gamma_x \, \mathbf{e}_q(mx^k) \right|^{2\nu}.$$

Opening up the inner sum, changing the order of summation and using the orthogonality of exponential functions, we obtain

$$W_{0,q} = \sum_{m\in\mathbb{Z}_q} \sum_{\substack{x_1,\dots,x_{2\nu}\in\mathbb{Z}_q^* \\ \langle x_i^\ell\rangle_q \le q/N, i=1,\dots,2\nu}} \cdots \sum \prod_{j=1}^{\nu} \gamma_{x_j} \overline{\gamma_{x_{\nu+j}}} \, \mathbf{e}_q\left(m \sum_{j=1}^{\nu} (x_j^k - x_{\nu+j}^k)\right)$$

$$= q \sum_{\substack{\langle x_i^\ell\rangle_q \le q/N, i=1,\dots,2\nu \\ x_1^k+\dots+x_\nu^k \equiv x_{\nu+1}^k+\dots+x_{2\nu}^k \pmod q}} \cdots \sum \prod_{j=1}^{\nu} \gamma_{x_j} \overline{\gamma_{x_{\nu+j}}}$$

$$\le N^{2\nu} q \sum_{\substack{\langle x_i^\ell\rangle_q \le q/N, i=1,\dots,2\nu \\ x_1^k+\dots+x_\nu^k \equiv x_{\nu+1}^k+\dots+x_{2\nu}^k \pmod q}} \cdots \sum 1.$$

Let $u_i = \langle x_i^\ell\rangle_q$, $v_i = x_i^k$, then we have

$$v_1 + \dots + v_\nu \equiv v_{\nu+1} + \dots + v_{2\nu} \pmod q,$$
$$u_i^k \equiv \pm v_i^\ell \pmod q, \qquad 0 < u_i \le q/N,$$

which implies

$$v_1 + \dots + v_\nu \equiv v_{\nu+1} + \dots + v_{2\nu} \pmod q,$$
$$u_i^{2k} \equiv v_i^{2\ell} \pmod q, \qquad 0 < u_i \le q/N.$$

Applying Lemma 3.4, we have

$$W_{0,q} \le N^{2\nu} q^{1+o(1)} \left(\left(\frac{q}{N}\right)^{2\nu} q^{-1} + \left(\frac{q}{N}\right)^{2\nu^2/(\nu+1)} \right).$$

Then, we see from (4.4)

$$|\Sigma_{0,q}|^{2\nu} \le \|\boldsymbol{\alpha}\|_1^{2\nu-2}\|\boldsymbol{\alpha}\|_2^2 \left(q^{2\nu} + q^{(2\nu^2+\nu+1)/(\nu+1)}N^{2\nu/(\nu+1)}\right) q^{o(1)}. \tag{4.5}$$

Similarly, we also obtain

$$\begin{aligned}|\Sigma_{i,q}|^{2\nu} \le \|\boldsymbol{\alpha}\|_1^{2\nu-2}\|\boldsymbol{\alpha}\|_2^2 \\ \left(q^{2\nu} + q^{(2\nu^2+\nu+1)/(\nu+1)}N^{2\nu/(\nu+1)}e^{-2i\nu/(\nu+1)}\right) q^{o(1)},\end{aligned} \tag{4.6}$$

and the result now follows from (4.1).

4.2. Proof of Theorem 2.3

We see from (4.1) that by the Hölder inequality,

$$\mathcal{S}_{k,\ell,q}(\boldsymbol{\alpha};\mathcal{J})^{2\nu} \ll I^{2\nu-1}\left(|\Sigma_{0,q}|^{2\nu} + \sum_{i=1}^{I}|\Sigma_{i,q}|^{2\nu}\right).$$

Now, using Lemma 3.6 instead of Lemma 3.4 we obtain

$$\sum_{q\in[Q,2Q]}|\Sigma_{0,q}|^{2\nu} \le \|\boldsymbol{\alpha}\|_1^{2\nu-2}\|\boldsymbol{\alpha}\|_2^2\left(Q^{2\nu-1} + Q^{\nu+2}N^{\nu}\right)Q^{o(1)}$$

instead of (4.5) and

$$\sum_{q\in[Q,2Q]}|\Sigma_{i,q}|^{2\nu} \le \|\boldsymbol{\alpha}\|_1^{2\nu-2}\|\boldsymbol{\alpha}\|_2^2\left(Q^{2\nu-1} + Q^{\nu+2}N^{\nu}e^{-i\nu}\right)Q^{o(1)}$$

instead of (4.6). The result now follows.

5. Comparison with previous results

We note that for a prime $q = p$, in our notation for the functions $K_1(t)$ and $K_2(t)$ from [13] we have

$$K_1(mn) = p^{-1/2}S_{-2,1,p}(ab^2m^2, n) = p^{-1/2}S_{2,-1,p}(ab^2m^2, n)$$

and

$$K_2(mn^2) = p^{-1/2}S_{-2,1,p}(ab^2m, n) = p^{-1/2}S_{2,-1,p}(ab^2m, n).$$

Recalling the definition (1.1), we now see that the results of Nunes [13] can be written as

$$\mathcal{S}^*_{2,p}(\boldsymbol{\alpha};\mathcal{M}_1,\mathcal{J}) \le \sqrt{\|\boldsymbol{\alpha}\|_1\|\boldsymbol{\alpha}\|_2}p^{3/4+o(1)}M^{1/16}N^{5/8} \tag{5.1}$$

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

provided that $1 \le M \le N^2$ and $MN^2 \le p^2$ and also

$$\mathcal{S}^*_{2,p}(\boldsymbol{\alpha}; \mathcal{M}_2, \mathcal{J}) \le \sqrt{\|\boldsymbol{\alpha}\|_1 \|\boldsymbol{\alpha}\|_2} p^{3/4+o(1)} M^{1/12} N^{7/12} \tag{5.2}$$

provided that $1 \le M \le N^2$ and $MN \le p^{3/2}$, where

$$\mathcal{M}_1 = \{\alpha j \ : \ j = 1, \ldots, M\} \qquad \text{and} \qquad \mathcal{M}_2 = \{\alpha j^2 \ : \ j = 1, \ldots, M\}$$

(with some $\alpha \in \mathbb{F}_p^*$) and $\mathcal{J}$ is an interval of length $N < p$. Using Theorem 2.1 with $\nu = 2$ (and recalling that its bound does not depend on the support $\mathcal{M}$ of the weights $\boldsymbol{\alpha}$, see (1.4)), we obtain

$$\mathcal{S}^*_{2,p}(\boldsymbol{\alpha}; \mathcal{M}_j, \mathcal{J}) \le \sqrt{\|\boldsymbol{\alpha}\|_1 \|\boldsymbol{\alpha}\|_2} \left(p + p^{11/12} N^{1/3}\right) p^{o(1)}, \qquad j = 1, 2.$$

This bound improves (5.1) for

$$MN^{10} \ge p^{4+\varepsilon} \qquad \text{and} \qquad M^3 N^{14} \ge p^{8+\varepsilon}$$

and improves (5.2) for

$$MN^7 \ge p^{3+\varepsilon} \qquad \text{and} \qquad MN^3 \ge p^{2+\varepsilon}$$

with some fixed $\varepsilon > 0$. In particular, if M and N are of similar sizes, that is, $N = M^{1+o(1)}$, this happens for $M \ge p^{8/17+\varepsilon}$ and $M \ge p^{1/2+\varepsilon}$, respectively.

We further note that for applications to squarefree numbers in arithmetic progressions only the bound (5.1) matters and only in the case of constant weights and thus it has to be compared with that of Corollary 2.2 (it is easy to see that for $\ell = 1$ it can be extended to the set $\mathcal{M}_1 = \alpha\mathcal{I}$). In particular, in this case the bound (2.1) is better when

$$M^{13} N^{-2} \ge p^{4+\varepsilon} \qquad \text{and} \qquad M^{23} N^{-6} \ge p^{8+\varepsilon},$$

or similarly with M and N can be interchanged, see also (2.2) for the range when it is nontrivial.

One also easily observes that all our results can be extended, without any changes in their formulations and proofs, to much more general sums of the shape

$$S_{k,\ell,q}(\boldsymbol{\xi}; m, n) = \sum_{x \in \mathbb{Z}_q^*} \xi_x \, \mathbf{e}_q\left(mx^k + nx^\ell\right),$$

with some complex weights $\boldsymbol{\xi} = (\xi_x)_{x \in \mathbb{Z}_q^*}$ satisfying $\|\boldsymbol{\xi}\|_\infty \le 1$. For example ξ_x can be the Möbius function or the indicator function of primes. Note that the sums $S_{k,\ell,q}(\boldsymbol{\xi}; m, n)$ cannot be treated within the approach of [1,3,11,13].

In particular, in the regime when $N = M^{1+o(1)}$, which is crucial for many applications, the bound (2.1) is both better and nontrivial for $M \ge p^{8/17+\varepsilon}$. However, the potential

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011

improvement of [13], which is implied by our bounds seems to be of the same strength as in the follow up work of Nunes [14], where this is achieved via a different approach.

Finally, we remark that the squarefreeness restriction on the modulus in Theorem 2.1 comes from Lemma 3.4. For arbitrary integer q one can use much more general but weaker bounds of Kerr [9, Theorem 3.1].

Acknowledgments

The authors are grateful to Ramon Nunes for very useful discussions, in particular for the information about his results in [14] and their comparison with potential improvements coming from our new bounds. The authors are grateful to the anonymous referee for helpful comments and suggestions. Thanks also go to Will Sawin for his very important comments.

The first and the third authors gratefully acknowledge the support, hospitality and excellent conditions of the School of Mathematics and Statistics of UNSW during their visit.

This work was supported by NSFC Grant 11401329 (for K. Liu), by ARC Grant DP170100786 (for I. E. Shparlinski) and by NSFC Grant 11471258, 11201275, the Natural Science Foundation of Shaanxi Province of China Grant 2016JM1017 and the Fundamental Research Funds for the Central Universities GK201802011 (for T. P. Zhang).

References

[1] V. Blomer, É. Fouvry, E. Kowalski, P. Michel, D. Milićević, On moments of twisted L-functions, Amer. J. Math. 139 (2017) 707–768.
[2] V. Blomer, É. Fouvry, E. Kowalski, P. Michel, D. Milićević, Some applications of smooth bilinear forms with Kloosterman sums, Tr. Mat. Inst. Steklova (Proc. Steklov Math. Inst.) 296 (2017) 24–35.
[3] É. Fouvry, E. Kowalski, P. Michel, Algebraic trace functions over the primes, Duke Math. J. 163 (2014) 1683–1736.
[4] É. Fouvry, I.E. Shparlinski, On a ternary quadratic form over primes, Acta Arith. 150 (2011) 285–314.
[5] D.R. Heath-Brown, The least square-free number in an arithmetic progression, J. Reine Angew. Math. 332 (1982) 204–220.
[6] M.N. Huxley, A note on polynomial congruences, in: Recent Progress in Analytic Number Theory, vol. 1, Academic Press, 1981, pp. 193–196.
[7] H. Iwaniec, E. Kowalski, Analytic Number Theory, American Mathematical Society, Providence, RI, 2004.
[8] A.A. Karatsuba, Analogues of Kloosterman sums, Izv. Ross. Akad. Nauk Ser. Mat. (Russian Acad. Sci. Izv. Math.) 55 (5) (1995) 93–102, in Russian.
[9] B. Kerr, Solutions to polynomial congruences in well shaped sets, Bull. Aust. Math. Soc. 88 (2013) 435–447.
[10] R. Khan, The divisor function in arithmetic progressions modulo prime powers, Mathematika 62 (2016) 898–908.
[11] E. Kowalski, P. Michel, W. Sawin, Bilinear forms with Kloosterman sums and applications, Ann. of Math. (2) 186 (2017) 413–500.
[12] K. Liu, I.E. Shparlinski, T.P. Zhang, Divisor problem in arithmetic progressions modulo a prime power, Adv. Math. 325 (2018) 459–481.
[13] R.M. Nunes, Squarefree numbers in large arithmetic progressions, Preprint, available from http://arxiv.org/abs/1602.00311, 2016.

[14] R.M. Nunes, On the least squarefree number in an arithmetic progressions, Mathematika 63 (2017) 483–498.
[15] L.B. Pierce, The 3-part of class numbers of quadratic fields, J. Lond. Math. Soc. 71 (2005) 579–598.
[16] I.E. Shparlinski, On exponential sums with sparse polynomials and rational functions, J. Number Theory 60 (1996) 233–244.
[17] I.E. Shparlinski, Bilinear forms with Kloosterman and Gauss sums, Trans. Amer. Math. Soc. (2018), forthcoming.
[18] I.E. Shparlinski, T.P. Zhang, Cancellations amongst Kloosterman sums, Acta Arith. 176 (2016) 201–210.
[19] D. Suryanarayana, R. Sitaramachandra Rao, The distribution of square-full integers, Ark. Mat. 11 (1973) 195–201.
[20] I.M. Vinogradov, Elements of Number Theory, Dover Publ., NY, 1954.
[21] J. Wu, P. Xi, Arithmetic exponent pairs for algebraic trace functions and applications, Preprint, available from http://arxiv.org/abs/1603.07060, 2016.
[22] P. Xi, Large sieve inequalities for algebraic trace functions, Int. Math. Res. Not. IMRN 2017 (2017) 4840–4881, with an appendix by É. Fouvry, E. Kowalski and P. Michel.

Please cite this article in press as: K. Liu et al., Bilinear forms with exponential sums with binomials, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.12.011