Mathematika 65 (2019) 475–487 © 2019 University College London
doi:10.1112/S0025579318000554

CANCELLATIONS BETWEEN KLOOSTERMAN SUMS MODULO A PRIME POWER WITH PRIME ARGUMENTS

KUI LIU, IGOR E. SHPARLINSKI AND TIANPING ZHANG

Abstract. We obtain a non-trivial bound for cancellations between the Kloosterman sums modulo a large prime power with a prime argument running over very short intervals, which in turn is based on a new estimate on bilinear sums of Kloosterman sums. These results are analogues of those obtained by various authors for Kloosterman sums modulo a prime. However, the underlying technique is different and allows us to obtain non-trivial results starting from much shorter ranges.

§1. *Introduction.*

1.1. *Background and motivation.* For an integer $q \geqslant 1$ and arbitrary integers m and n, we define the Kloosterman sums

$$\mathcal{K}(m,n;q) = \frac{1}{q^{1/2}} \sideset{}{^*}\sum_{b \bmod q} e\left(\frac{mb+n\overline{b}}{q}\right),$$

where $\sum^*$ means summing over reduced residue classes, $\overline{b}$ is given by $b\overline{b} \equiv 1 \bmod q$ and for a real x we denote

$$e(x) = \mathrm{e}^{2\pi \mathrm{i} x}.$$

First we recall that the Weil bound, yields the estimate

$$|\mathcal{K}(m,n;q)| \leqslant \sqrt{\gcd(m,n,q)}q^{o(1)}, \tag{1.1}$$

see [7, equation (14.52)], which gives an optimal bound on individual Kloosterman sums. So any further progress in their applications is possible only via studying their finer structure and possible cancellations in various families of these sums.

Indeed, starting from the groundbreaking results of Kuznetsov [12] towards the Linnik conjecture [13] on cancellations between Kloosterman sums, this has been a very active area of research. The initial conjecture of Linnik [13] predicts cancellations when the coefficients m and n are fixed but the modulus q varies, see [18] for results towards a uniform version of this conjecture.

The dual question, concerning cancellations between Kloosterman sums $\mathcal{K}(m,n;q)$ modulo the same integer q but with varying coefficients m and n

Received 30 August 2018, published online 29 January 2019.
MSC (2010): 11L05, 11T23 (primary).

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

when one of both runs through a consecutive interval, can be found in [6, 15, 19], see also the references therein. Questions of this type usually become much harder when one imposes arithmetic conditions on the parameters m and n, such as square-freeness, smoothness or primality. In this direction, Fouvry *et al* [5, Theorem 1.5], in the case of prime moduli $q = p$, have shown the existence of non-trivial cancellations between the Kloosterman sums $\mathcal{K}(\ell, a; p)$ when ℓ runs over primes up to some parameter $X \geqslant q^{3/4+\varepsilon}$ for any fixed $\varepsilon > 0$ (with the goal to have X as small as possible compared to q). Blomer *et al* [2, Theorem 1.8] have improved the bound from [5] however not the range $X \geqslant q^{3/4+\varepsilon}$.

In this paper, using a different technique, we obtain analogues of these results in the case where $q = p^k$ is a power of an odd prime p for some sufficiently large integer k, which in fact allows us to reduce the amount of averaging down to $X \geqslant q^{\varepsilon}$ for any fixed $\varepsilon > 0$.

As in [2], our approach is based on bounding certain bilinear forms of Kloosterman sums. Namely, given two sequences of weights $\mathcal{A} = \{\alpha_m\}_{m=1}^{M}$ and $\mathcal{B} = \{\beta_n\}_{n=1}^{N}$ with

$$\max_{m=1,\dots,M} |\alpha_m| \leqslant 1 \quad \text{and} \quad \max_{n=1,\dots,N} |\beta_n| \leqslant 1,$$

we consider the bilinear sums

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) = \sum_{m=1}^{M} \sum_{n=1}^{N} \alpha_m \beta_n \mathcal{K}(mn, a; q).$$

Recently a series of bounds has been obtained, by various methods, on the sum $S_{a,q}(\mathcal{A}, \mathcal{B}; M, N)$ when $q = p$ is prime, see [1, 2, 10, 11, 20, 21] and references therein. Here, using a different technique, we obtain analogues of these results in the case where $q = p^k$ is a large power of an odd prime p. We believe this bound can be of independent interest and may find some other applications.

1.2. *Main results.* Before we formulate our results we need to recall that the notations $U \ll V$ and $U = O(V)$, are equivalent to $|U| \leqslant cV$ for some constant $c > 0$. We note that we do not number implicit constants, which we usually also denote by c so they are allowed to change their values in different statements.

We write $\ll_\rho$ and O_ρ to indicate that this constant may depend on the parameter ρ.

We also note that since Kloosterman sums $\mathcal{K}(m, n; q)$ are periodic with period q with respect to both m and n, it is sufficient to consider only the case when $1 \leqslant M, N < q$.

THEOREM 1.1. *Let $q = p^k$, $k \in \mathbb{N}$, be a power of an odd prime p. Then for any fixed constant $0 < \lambda < 1$ and $q^\lambda < M, N < q$, there exist a constant $H_1(\lambda) > 0$ depending only on λ and an absolute constant $c > 0$ such that for any $k > H_1(\lambda)$ and $\tau(\lambda) = c\lambda^3$ we have*

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \ll_\lambda MNq^{-\tau(\lambda)},$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on λ.

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

It is certainly interesting to try to obtain a version of Theorem 1.1 in terms of other norms of the weights, say, involving their L^1 and L^2 norms, rather than their L^∞ norm. However, the current approach splits summation over a rather large family of arithmetic progressions and thus it is not clear how to adapt it to this setting.

We note that for some applications one also needs to restrict the summation to truncated hyperbolic domain, that is, for points $(u, v) \in \mathbb{Z}^2$ with $uv \leqslant X$, $u \geqslant U$, $v \geqslant V$. The restrictions $u \geqslant U$, $v \geqslant V$ are needed as it is necessary to stay away from the cusps of the hyperbola to ensure that both summations are long enough.

COROLLARY 1.2. *Let $q = p^k$, $k \in \mathbb{N}$, be a power of an odd prime p. Then for any fixed constant $0 < \lambda < 1$ and $q^\lambda < U, V < X$ with $X < q$, there exist a constant $H_2(\lambda) > 0$ depending only on λ and an absolute constant $c > 0$ such that for any $k > H_2(\lambda)$ and $\vartheta(\lambda) = c\lambda^3$ we have*

$$\sum_{\substack{m \geqslant U, n \geqslant V \\ mn \leqslant X}} \alpha_m \beta_n \mathcal{K}(mn, a; q) \ll_\lambda Xq^{-\vartheta(\lambda)},$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on λ.

We use Corollary 1.2 in a combination with the main result of [**14**] to derive the following theorem.

THEOREM 1.3. *Let $q = p^k$, $k \in \mathbb{N}$, be a power of an odd prime p and $q^\varepsilon < X \leqslant q$. Then there exist a constant $H_3(\varepsilon) > 0$ depending only on ε and an absolute constant $c > 0$ such that for any $k > H_3(\varepsilon)$ and $\delta(\varepsilon) = c\varepsilon^3$ we have*

$$\sum_{\substack{\ell \leqslant X \\ \ell \text{ prime}}} \mathcal{K}(\ell, a; q) \ll_\varepsilon Xq^{-\delta(\varepsilon)}$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on ε.

§2. *Preliminaries.*

2.1. *Some bounds on Kloosterman sums.*

Let $\Re z$ denote the real part of a complex number z.

First we record the following explicit formula, see, for example, [**7**, equation (12.39)].

LEMMA 2.1. *Let $q = p^k$ with p being an odd prime and $k \geqslant 2$, $k \in \mathbb{N}$. Then for $\gcd(a, q) = 1$ we have*

$$\mathcal{K}(n, a; q) = \begin{cases} 2\left(\dfrac{r}{p}\right)^k \Re \vartheta_q e\left(\dfrac{2r}{q}\right), & \text{if } \left(\dfrac{na}{p}\right) = 1, \\ 0, & \text{if } \left(\dfrac{na}{p}\right) = -1, \end{cases}$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

where r is a solution of $r^2 \equiv na \bmod q$, (r/p) is the Legendre symbol, ϑ_q equals 1 if $q \equiv 1 \bmod 4$ and i if $q \equiv 3 \bmod 4$.

Easy calculations show the following well-known fact (see also [14]).

LEMMA 2.2. *Let p be an odd prime and $k \geqslant 2$ be a positive integer. If $\gcd(a, p) = 1$ and $p \mid n$, then the Kloosterman sums $\mathcal{K}(n, a; p^k) = 0$.*

One of our principal technical tools is the following estimate from [14] on the cancellations amongst Kloosterman sums.

LEMMA 2.3. *Let $q = p^k$, $k \in \mathbb{N}$ be a power of an odd prime p. Then for any fixed constant $0 < \lambda < 1$ and $q^\lambda < N < q$, there exist a constant $K_0(\lambda)$ depending only on λ and an absolute constant $c > 0$ such that for any $k > K_0(\lambda)$ and $\tau(\lambda) = c\lambda^3$ we have*

$$\sum_{1 \leqslant n \leqslant N} \mathcal{K}(n, a; q) \ll_\lambda N q^{-\tau(\lambda)}$$

uniformly over odd primes p and integers a with $\gcd(a, p) = 1$, where the implied constant depends only on λ.

2.2. *Short exponential sums with special polynomials.* The following bound is contained in the proof of [14, Theorem 1.2] (and in fact is in the core of this proof).

LEMMA 2.4. *Let $q = p^k$, $k \in \mathbb{N}$ be a power of an odd prime p. For any fixed η with $0 < \eta < 1$ being a fixed constant, there exists a constant $k_0(\eta) > 0$ such that for $q^\eta < N < q$ and the polynomial*

$$f(X) = \sum_{j=0}^{\lfloor k/s \rfloor} g(j) \gamma^j p^{js} X^j, \tag{2.1}$$

where γ is an arbitrary integer with $\gcd(\gamma, p) = 1$,

$$s = \left\lfloor \frac{\eta \log N}{3000 \log p} \right\rfloor,$$

$g(0) = 1$ and $g(j)$ with $1 \leqslant j \leqslant \lfloor k/s \rfloor$ are integers given by

$$g(j) \equiv \frac{1/2(1/2 - 1) \cdots (1/2 - j + 1)}{j!} \bmod p^k, \quad 0 \leqslant g(j) < p^k,$$

and any $k > k_0(\eta)$, uniformly over integers h with $\gcd(h, q) = 1$, we have

$$\sum_{n \leqslant N} e\left(\frac{hf(n)}{q}\right) \ll_\eta N q^{-\rho(\eta)},$$

where $\rho(\eta) = c\eta^3$ with some absolute constant $c > 0$ and the implied constant depends only on η.

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

Proof. Our choice of s corresponds to [14, equation (3.1)], and thus the polynomial f is as in [14, equation (3.5)]. It is now easy to see that the result we claim is a combination of bounds [14, equation (3.7)] and [14, equation (3.13)]. □

2.3. *Vaughan identity.* As usual, we use $\Lambda(n)$ to denote the von Mangoldt function

$$\Lambda(n) = \begin{cases} \log \ell & \text{if } n \text{ is a power of a prime } \ell, \\ 0 & \text{otherwise.} \end{cases}$$

We use the following result of Vaughan [24] in the form given by Davenport [4, Ch. 24].

LEMMA 2.5. *For any complex-valued function $f(n)$ and any real numbers $1 < U, V \leqslant X$, we have*

$$\sum_{n \leqslant X} \Lambda(n) f(n) \ll \Sigma_1 + \Sigma_2 \log(UV) + \Sigma_3 \log X + |\Sigma_4|,$$

where

$$\Sigma_1 = \left| \sum_{n \leqslant U} \Lambda(n) f(n) \right|,$$

$$\Sigma_2 = \sum_{v \leqslant UV} \left| \sum_{s \leqslant X/v} f(sv) \right|,$$

$$\Sigma_3 = \sum_{v \leqslant V} \max_{w \geqslant 1} \left| \sum_{w \leqslant s \leqslant X/v} f(sv) \right|$$

and

$$\Sigma_4 = \sum_{\substack{uv \leqslant X \\ u > U,\, v > V}} \Lambda(u) \left(\sum_{d \mid v,\, d \leqslant V} \mu(d) \right) f(uv).$$

§3. *Proof of main results.*

3.1. *Proof of Theorem 1.1.* Note that due to the symmetry of the sum and the claimed bound with respect to M and N, we can always assume that $M \geqslant N$.

Let $1 \leqslant s \leqslant k$ be a parameter to be determined. Write

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) = \sum_{u,v=1}^{p^s} \sum_{\substack{m \leqslant M \\ m \equiv u \bmod p^s}} \sum_{\substack{n \leqslant N \\ n \equiv v \bmod p^s}} \alpha_m \beta_n \mathcal{K}(mn, a; q).$$

Then by Lemmas 2.1 and 2.2, we have

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \leqslant \sideset{}{^*}\sum_{\substack{u,v=1 \\ (auv/p)=1}}^{p^s} \sum_{\substack{n \leqslant N \\ n \equiv v \bmod p^s}} \left| \sum_{\substack{m \leqslant M \\ m \equiv u \bmod p^s}} \alpha_m \mathcal{K}(mn, a; q) \right|.$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

Now by Lemma 2.1, we derive

$$S_{a,q}(\mathcal{A},\mathcal{B};M,N) \leqslant 2 \sum_{\substack{u,v=1\\(auv/p)=1}}^{p^s}{}^{*} \sum_{n\leqslant N \atop n\equiv v \bmod p^s} \Bigg| \sum_{\substack{m\leqslant M\\ m\equiv u \bmod p^s\\(amn/p)=1}} \alpha_m \left(\frac{r_{m,n}}{p}\right)^k \Re\vartheta_q e\left(\frac{2r_{m,n}}{q}\right)\Bigg|,$$

where $r_{m,n}$ is a solution to $r_{m,n}^2 \equiv amn \bmod q$ (the inequality holds for any choice of this solution). In particular, we see that

$$S_{a,q}(\mathcal{A},\mathcal{B};M,N) \leqslant 2 \sum_{\substack{u,v=1\\(auv/p)=1}}^{p^s}{}^{*} T_s(u,v), \tag{3.1}$$

where

$$T_s(u,v) = \sum_{\substack{n\leqslant N\\ n\equiv v \bmod p^s}} \Bigg| \sum_{\substack{m\leqslant M\\ m\equiv u \bmod p^s}} \alpha_m \left(\frac{r_{m,n}}{p}\right)^k \Re\vartheta_q e\left(\frac{2r_{m,n}}{q}\right)\Bigg|. \tag{3.2}$$

Note that $r_{m,n}^2 \equiv amn \equiv auv \bmod p$, and thus the Legendre symbol $(r_{m,n}/p)$ depends only on u and v. We now use the Cauchy inequality and derive

$$T_s(u,v)^2 \leqslant (Np^{-s}+1) \sum_{\substack{m_1,m_2\leqslant M\\ m_1\equiv u \bmod p^s\\ m_2\equiv u \bmod p^s}} \Bigg| \sum_{n\leqslant N \atop n\equiv v \bmod p^s} e\left(\frac{2(r_{m_1,n}-r_{m_2,n})}{q}\right)\Bigg|,$$

with $r_{m_i,n}$ being a solution of the congruence $r^2 \equiv m_i na \bmod q$ for $i = 1, 2$.

Now we consider the inner sum over n. Note that for $i = 1, 2$, we have $\gcd(am_i, q) = 1$, then we use the following argument, which is similar to that in [3, 8] and [14]. In fact these ideas date back to earlier work of Postnikov [16, 17] where they were used for polynomials, and then extended by Stepanov and Shparlinski [22, 23] for algebraic functions.

By $n \equiv v \bmod p^s$, there exists $t \in \mathbb{Z}$, such that

$$n = v + p^s t. \tag{3.3}$$

Now we have

$$r_{m_i,n}^2 \equiv am_i(v+p^s t) \equiv am_i v(1+\bar{v}p^s t) \bmod q,$$

with $v\bar{v} \equiv 1 \bmod q$. Note that $am_i v \equiv auv \bmod p$, then

$$\left(\frac{am_i v}{p}\right) = 1.$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

By the *Hensel lifting*, there exists an integer ω, such that $0 \leqslant \omega < p^s$ and

$$\omega^2 \equiv auv \bmod p^s,$$

and also for each m_i there exists an integer ω_{m_i} such that

$$\omega_{m_i}^2 \equiv am_i v \bmod q$$

and $\omega_{m_i} \equiv \omega \bmod p^s$ for $i = 1, 2$. Thus

$$r_{m_i,n}^2 \equiv am_i v \equiv \omega_{m_i}^2(1 + \bar{v}p^s t) \bmod q.$$

We remark that ω_{m_i} is determined by a, m_i and v, and does not depend on n. Consider $1 + \bar{v}p^s t$ in the p-adic field $\mathbb{Q}_p$. By the Taylor expansion (see [**9**, Ch. IV.1]), we have

$$(1 + \bar{v}p^s t)^{1/2} = 1 + \sum_{j=1}^{\infty} \binom{1/2}{j} \bar{v}^j p^{js} t^j$$

for $s \geqslant 1$ with the coefficients

$$\binom{1/2}{j} = \frac{1/2(1/2-1)\cdots(1/2-j+1)}{j!}, \quad j = 1, 2, \ldots,$$

which are p-adic integers, since p is an odd prime. Then we have

$$(1 + \bar{v}p^s t)^{1/2} \equiv 1 + \sum_{j=1}^{\lfloor k/s \rfloor} g(j)\bar{v}^j p^{js} t^j \bmod p^k,$$

where $g(j)$ with $1 \leqslant j \leqslant \lfloor k/s \rfloor$ are integers given by

$$g(j) \equiv \binom{1/2}{j} \bmod p^k, \quad 0 \leqslant g(j) < p^k.$$

Thus we have two solutions to the quadratic congruence of $r_{m_i,n}$ in the inner sum in (3.2).

$$r_{m_i,n} \equiv \pm\omega_{m_i} f(t) \bmod q,$$

where the polynomial $f(X)$ is given by (2.1) as in Lemma 2.4 with $\gamma = \bar{v}$ and t is defined by (3.3).

Choosing the solution $r_{m_i,n} \equiv \omega_{m_i} f(t) \bmod q$, then we have

$$T_s(u, v)^2 \leqslant (Np^{-s} + 1) \sum_{\substack{m_1,m_2 \leqslant M \\ m_1 \equiv u \bmod p^s \\ m_2 \equiv u \bmod p^s}} \left| \sum_{t \leqslant (N-v)/p^s} e\left(\frac{2(\omega_{m_1} - \omega_{m_2}) f(t)}{q}\right) \right|. \tag{3.4}$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

We now choose

$$B(\lambda) = 3000/\lambda > 3000 \quad \text{and} \quad s = \left\lfloor \frac{\log N}{B(\lambda)\log p} \right\rfloor. \tag{3.5}$$

Since $q^{\lambda} < N \leqslant M < q = p^k$, then we have $s \leqslant k/B(\lambda)$. Hence,

$$N/p^s \geqslant q^{\lambda/2} \quad \text{and} \quad k - 3s > k/2. \tag{3.6}$$

In particular, we see from (3.6) that

$$Np^{-s} + 1 \ll Np^{-s}.$$

Thus (3.4) can be simplified as

$$T_s(u, v)^2 \ll Np^{-s} \sum_{\substack{m_1, m_2 \leqslant M \\ m_1 \equiv u \bmod p^s \\ m_2 \equiv u \bmod p^s}} \left| \sum_{t \leqslant (N-v)/p^s} e\left(\frac{2(\omega_{m_1} - \omega_{m_2}) f(t)}{q}\right) \right|. \tag{3.7}$$

Let $\mathrm{ord}_p(n)$ denote the p-adic order of integer n. For a fixed m_1, we claim that

$$\sharp\{m_2 \leqslant M : m_2 \equiv m_1 \bmod p^s, \mathrm{ord}_p(\omega_{m_1} - \omega_{m_2}) \geqslant 3s\} \leqslant Mp^{-3s} + 1.$$

To see this, we note that $\mathrm{ord}_p(\omega_{m_1} - \omega_{m_2}) \geqslant 3s$ implies

$$\omega_{m_1}^2 \equiv \omega_{m_2}^2 \bmod p^{3s}.$$

Since $\gcd(av, q) = 1$, then by the definition of ω_{m_i}, we have the congruence $m_2 \equiv m_1 \bmod p^{3s}$, which yields our claim.

We estimate the contribution of this case to $T_s(u, v)^2$ trivially as

$$Np^{-s} \sum_{\substack{m_1 \leqslant M \\ m_1 \equiv u \bmod p^s}} \sum_{\substack{m_2 \leqslant M \\ m_2 \equiv m_1 \bmod p^s \\ \mathrm{ord}_p(\omega_{m_1} - \omega_{m_2}) \geqslant 3s}} \sum_{t \leqslant (N-v)/p^s} 1 \ll MN^2 p^{-3s}(Mp^{-3s} + 1).$$

Hence, we only need to estimate the exponential sum

$$\sum_{t \leqslant (N-v)/p^s} e\left(\frac{2(\omega_{m_1} - \omega_{m_2}) f(t)}{q}\right),$$

with $\mathrm{ord}_p(\omega_{m_1} - \omega_{m_2}) < 3s$. After cancelling the power of p, which divides factor p^{3s-1}, we obtain a similar exponential sum of the type

$$\sum_{t \leqslant (N-v)/p^s} e\left(\frac{hf(t)}{p^r}\right),$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

with $\gcd(h, q) = 1$ and $r > k - 3s$. To bound this sum, we recall our choice (3.5) and thus the inequality (3.6). Hence we can apply Lemma 2.4 and obtain

$$\sum_{t \leqslant (N-v)/p^s} e\left(\frac{2(\omega_{m_1} - \omega_{m_2}) f(t)}{q}\right) \ll Np^{-s} q^{-\rho(\lambda/2)},$$

for $k \geqslant 2k_0(\lambda/2)$, where k_0 and ρ are the same as in Lemma 2.4. Inserting this bound to (3.7), we derive

$$\begin{aligned} T_s(u, v)^2 &\ll M^2 N^2 p^{-4s} q^{-\rho(\lambda/2)} + MN^2 p^{-3s}(Mp^{-3s} + 1) \\ &= M^2 N^2 p^{-4s} q^{-\rho(\lambda/2)} + M^2 N^2 p^{-6s} + MN^2 p^{-3s}. \end{aligned}$$

Then we have

$$T_s(u, v) \ll MNp^{-2s} q^{-\rho(\lambda/2)/2} + MNp^{-3s} + M^{1/2} Np^{-3s/2},$$

which after the substitution in (3.1) yields

$$S_{a,q}(\mathcal{A}, \mathcal{B}; M, N) \ll MNq^{-\rho(\lambda/2)/2} + MNp^{-s} + M^{1/2} Np^{s/2}.$$

Note that the definition of s implies that

$$\begin{aligned} s &\geqslant \frac{\log N}{B(\lambda) \log p} - 1 = \frac{\lambda \log N}{3000 \log p} - 1 \\ &= \frac{\lambda k \log N}{3000 \log q} - 1 \geqslant \frac{\lambda k \log N}{6000 \log q} = \frac{\log N}{2B(\lambda) \log p}, \end{aligned}$$

provided that k is large enough (we also recall that $q > M \geqslant N > q^\lambda$). Hence

$$N^{1/(2B(\lambda))} \leqslant p^s \leqslant N^{1/B(\lambda)},$$

from which the result follows.

3.2. *Proof of Corollary 1.2.* Separating the summation over m in dyadic ranges and slightly reducing the constant c in the definition of $\vartheta(\lambda)$, it is enough to show that for any M_1, M_2 with

$$M_2 \leqslant 2M_1 \quad \text{and} \quad U \leqslant M_1 < M_2 \leqslant 2X/V,$$

we have

$$\sum_{m=M_1}^{M_2} \sum_{V \leqslant n \leqslant X/m} \alpha_m \beta_n \mathcal{K}(mn, a; q) \ll_\lambda Xq^{-\vartheta(\lambda)}. \tag{3.8}$$

Let $L = \lfloor X/M_1 \rfloor$. Clearly we can assume that $L \geqslant V$ as otherwise the sum over n is void and there is nothing to prove. In particular, we can assume that

$$L \geqslant q^\lambda.$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

By the orthogonality of exponential functions, we write

$$\begin{aligned}\sum_{m=M_1}^{M_2} \sum_{V\leqslant n\leqslant X/m} & \alpha_m\beta_n\mathcal{K}(mn,a;q)\\ &= \sum_{m=M_1}^{M_2} \sum_{V\leqslant n\leqslant L} \frac{1}{L}\sum_{z=0}^{L-1}\sum_{w=0}^{X/m} e(z(w-n)/L)\alpha_m\beta_n\mathcal{K}(mn,a;q)\\ &= \frac{1}{L}\sum_{z=0}^{L-1}\sum_{m=M_1}^{M_2}\sum_{w=0}^{X/m} e(zw/L)\sum_{V\leqslant n\leqslant L}\alpha_m\beta_n e(-zn/L)\mathcal{K}(mn,a;q).\end{aligned}$$

Using that for $z = 0, \dots, L-1$ we have

$$\sum_{w=0}^{X/m} e(zw/L) \ll \frac{L}{1+\min\{z, L-z\}},$$

see [7, Bound (8.6)], we now derive

$$\begin{aligned}\sum_{m=M_1}^{M_2} \sum_{V\leqslant n\leqslant X/m} & \alpha_m\beta_n\mathcal{K}(mn,a;q)\\ &= \sum_{z=0}^{L-1}\frac{1}{1+\min\{z, L-z\}}\sum_{m=M_1}^{M_2}\sum_{V\leqslant n\leqslant L}\widetilde{\alpha}_{z,m}\widetilde{\beta}_{z,n}\mathcal{K}(mn,a;q), \qquad (3.9)\end{aligned}$$

with some weights $|\widetilde{\alpha}_{z,m}| \leqslant 1$ and $|\widetilde{\beta}_{z,n}| \leqslant 1$ (in particular, $\widetilde{\beta}_{z,n} = \beta_n e(-zn/L)$). Thus, by Theorem 1.1 for every $z = 0, \dots, L-1$, for the double sum over m and n we have the bound

$$\sum_{m=M_1}^{M_2}\sum_{V\leqslant n\leqslant L}\widetilde{\alpha}_{z,m}\widetilde{\beta}_{z,n}\mathcal{K}(mn,a;q) \ll M_2 L q^{-\tau(\lambda)} \ll X q^{-\tau(\lambda)},$$

which after substitution in (3.9) implies (3.8) and concludes the proof.

3.3. *Proof of Theorem 1.3.* Using partial summation, one can easily see that it is enough to estimate the sum

$$\widetilde{S}(X;a,q) = \sum_{n\leqslant X}\Lambda(n)\mathcal{K}(n,a;q).$$

We now apply Lemma 2.5 (with $f(n) = \mathcal{K}(n,a;q)$) where we take $U = V = X^{1/3}$, for which we need to estimate the sums:

$$\Sigma_1 = \left|\sum_{n\leqslant U}\Lambda(n)\mathcal{K}(n,a;q)\right|,$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

$$\Sigma_2 = \sum_{v \leqslant UV} \Big| \sum_{s \leqslant X/v} \mathcal{K}(sv, a; q) \Big|,$$

$$\Sigma_3 = \sum_{v \leqslant V} \max_{w \geqslant 1} \Big| \sum_{w \leqslant s \leqslant X/v} \mathcal{K}(sv, a; q) \Big|$$

and

$$\Sigma_4 = \sum_{\substack{uv \leqslant X \\ u > U,\ v > V}} \Lambda(u) \Big(\sum_{d \mid v,\, d \leqslant V} \mu(d) \Big) \mathcal{K}(uv, a; q).$$

We note that by Lemma 2.2 we can always satisfy the coprimality conditions $\gcd(s, p) = \gcd(u, p) = \gcd(v, p) = 1$ in the summation ranges.

Using the Weil bound (1.1), or its more precise version given in Lemma 2.1, we have

$$\Sigma_1 \ll_\varepsilon X^{1/3} q^{\varepsilon/3} < X q^{-\varepsilon/3}.$$

For Σ_2, using Lemma 2.2, we write

$$\Sigma_2 = \sum_{\substack{v \leqslant UV \\ \gcd(v,p)=1}} \Big| \sum_{s \leqslant X/v} \mathcal{K}(sv, a; q) \Big| = \sum_{\substack{v \leqslant UV \\ \gcd(v,p)=1}} \Big| \sum_{s \leqslant X/v} \mathcal{K}(s, a\overline{v}; q) \Big|.$$

Since $v \leqslant UV = X^{2/3}$ we have $X/v \geqslant X^{1/3} > q^{\varepsilon/3}$. Now Lemma 2.3 can be applied to the sum over s. Hence there exist constants $K_1(\varepsilon) > 0$ and $\tau_1(\varepsilon) > 0$ such that

$$\Sigma_2 \ll_\varepsilon X q^{-\tau_1(\varepsilon)}$$

holds uniformly for any odd prime p and $k > K_1(\varepsilon)$.

For Σ_3, write the inner sum over s into

$$\sum_{w \leqslant s \leqslant X/v} \mathcal{K}(sv, a; q) = \sum_{s \leqslant X/v} \mathcal{K}(sv, a; q) - \sum_{s < w} \mathcal{K}(sv, a; q).$$

The contribution of the first sum on the right side can be bounded similarly as Σ_2. For the contribution of the second sum. If $w < q^{\varepsilon/4}$, then by the Weil bound we have

$$\sum_{s \leqslant w} \mathcal{K}(sv, a; q) \ll_\varepsilon q^{\varepsilon/3}.$$

If $w \geqslant q^{\varepsilon/4}$, then Lemma 2.3 can be applied to the above sum. It follows from the above treatment that there exist constants $K_2(\varepsilon) > 0$ and $\tau_2(\varepsilon) > 0$ such that

$$\Sigma_3 \ll_\varepsilon X q^{-\tau_2(\varepsilon)}$$

holds uniformly for any odd prime p and $k > K_2(\varepsilon)$.

For Σ_4, by Corollary 1.2 there exist constants $K_3(\varepsilon) > 0$ and $\tau_3(\varepsilon) > 0$ such that

$$\Sigma_4 \ll_\varepsilon X q^{-\tau_3(\varepsilon)}$$

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

holds uniformly for any odd prime p and $k > K_3(\varepsilon)$. It is also easy to see that for the functions $\tau_\nu(\varepsilon)$ we can take $\tau_\nu(\varepsilon) = c_\nu \varepsilon^3$ for some absolute constants $c_\nu > 0$, for every $\nu = 1, 2, 3$.

Now the desired bound on $\widetilde{S}(X; a, q)$ and thus Theorem 1.3 follows from the above estimates.

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

This work was supported in part by NSFC Grant 11401329 (for K. Liu), by ARC Grant DP 170100786 (for I. E. Shparlinski), by NSFC Grants 11871317, 11471258, and the Fundamental Research Funds for the Central Universities GK201802011 (for T. P. Zhang).

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. *Proc. Steklov Math. Inst.* **296** (2017), 18–29.
3. V. Blomer and D. Milićević, The second moment of twisted modular L-functions. *Geom. Funct. Anal.* **25** (2015), 453–516.
4. H. Davenport, *Multiplicative Number Theory*, 2nd edn., Springer (New York, 1980).
5. É. Fouvry, E. Kowalski and P. Michel, Algebraic trace functions over the primes. *Duke Math. J.* **163** (2014), 1683–1736.
6. É. Fouvry, P. Michel, J. Rivat and A. Sárközy, On the pseudorandomness of the signs of Kloosterman sums. *J. Aust. Math. Soc.* **77** (2004), 425–436.
7. H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society (Providence, RI, 2004).
8. R. Khan, The divisor function in arithmetic progressions modulo prime powers. *Mathematika* **62** (2016), 898–908.
9. N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-functions* (*Graduate Texts in Mathematics* **58**), 2nd edn., Springer (New York, 1984).
10. E. Kowalski, P. Michel and W. Sawin, Bilinear forms with Kloosterman sums and applications. *Ann. of Math. (2)* **186** (2017), 413–500.
11. E. Kowalski, P. Michel and W. Sawin, Bilinear forms with Kloosterman sums, II. *Preprint*, 2018, arXiv:1802.09849.
12. N. V. Kuznetsov, The Petersson conjecture for cusp forms of weight zero and the Linnik conjecture. Sums of Kloosterman sums. *Math. USSR-Sb.* **39** (1981), 299–342.
13. Y. V. Linnik, Additive problems and eigenvalues of the modular operators. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, Institut Mittag–Leffler (Djursholm, 1963), 270–284.
14. K. Liu, I. E. Shparlinski and T. P. Zhang, Divisor problem in arithmetic progressions modulo a prime power. *Adv. Math.* **325** (2018), 459–481.
15. H. Niederreiter, The distribution of values of Kloosterman sums. *Arch. Math.* **56** (1991), 270–277.
16. A. G. Postnikov, On the sum of characters with respect to a modulus equal to a power of a prime number. *Izv. Akad. Nauk SSSR. Ser. Mat.* **19** (1955), 11–16 (in Russian).
17. A. G. Postnikov, On Dirichlet L-series with the character modulus equal to the power of a prime number. *J. Indian Math. Soc.* **20** (1956), 217–226.
18. P. Sarnak and J. Tsimerman, On Linnik and Selberg's conjecture about sums of Kloosterman sums. In *Algebra, Arithmetic, and Geometry: in Honor of Yu. I. Manin, Vol. II* (*Progress in Mathematics* **270**), Birkhaüser (Boston, MA, 2009), 619–635.
19. I. E. Shparlinski, Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average. *Michigan Math. J.* **56** (2008), 99–111.
20. I. E. Shparlinski, On sums of Kloosterman and Gauss sums. *Trans. Amer. Math. Soc.* (to appear).
21. I. E. Shparlinski and T. P. Zhang, Cancellations amongst Kloosterman sums. *Acta Arith.* **176** (2016), 201–210.

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press

22. S. A. Stepanov and I. E. Shparlinski, Estimation of trigonometric sums with rational and algebraic functions (Russian). In *Automorphic Functions and Number Theory, Part I*, Akad. Nauk SSSR (Dal'nevostochn. Otdel., Vladivostok, 1989), 5–18.
23. S. A. Stepanov and I. E. Shparlinski, An estimate for the incomplete sum of multiplicative characters of polynomials (Russian). *Diskret. Mat.* **2** (1990), 115–119. Engl. transl., *Discrete Math. Appl.* **2** (1992), 169–174.
24. R. C. Vaughan, An elementary method in prime number theory. *Acta Arith.* **37** (1980), 111–115.

Kui Liu,
School of Mathematics and Statistics,
Qingdao University,
No. 308, Ningxia Road,
Shinan, Qingdao,
Shandong 266071,
P.R. China
E-mail: liukui@qdu.edu.cn

Tianping Zhang,
School of Mathematics and Information Science,
Shaanxi Normal University,
Xi'an 710119 Shaanxi,
P.R. China
E-mail: tpzhang@snnu.edu.cn

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

https://doi.org/10.1112/S0025579318000554 Published online by Cambridge University Press