BILINEAR SUMS WITH EXPONENTIAL FUNCTIONS

IGOR E. SHPARLINSKI

(Communicated by Wen-Ching Winnie Li)

Abstract. Let \( g \not= 0, \pm 1 \) be a fixed integer. Given two sequences of complex numbers \((\varphi_m)_{m=1}^{\infty}\) and \((\psi_n)_{n=1}^{\infty}\) and two sufficiently large integers \( M \) and \( N \), we estimate the exponential sums

\[
\sum_{p \leq M} \sum_{\gcd(a, p) = 1} \varphi_p \psi_n e_p (a g^n), \quad a \in \mathbb{Z},
\]

where the outer summation is taken over all primes \( p \leq M \) with \( \gcd(a, p) = 1 \).

1. Introduction

Let us fix an integer \( g \not= 0, \pm 1 \). Various questions concerning the distribution of residues of the exponential function \( g^x \) in residue rings when \( x \) takes consecutive integer values and also when it runs through some general and special sequences (such as smooth or prime numbers) have always been intensively studied; see \([1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 17]\) and the references therein. For example, for \( g = 2 \) they have a natural interpretation as results about the distribution of Mersenne numbers in residue classes; see \([1, 4, 11, 12]\). They are also related to various questions about the distribution \( g \)-ary digits of rational fractions; see \([13, 14]\). Furthermore, these results also have various applications to such areas as cryptography and pseudorandom number generators; see \([16, 18]\). Most of the applications are based on estimates of corresponding exponential sums.

More precisely, for an integer \( m \geq 1 \) and a complex \( z \), we define

\[
e_m(z) = \exp(2\pi i z/m).
\]

Several estimates have recently been obtained for exponential sums

\[
\sum_{1 \leq \ell \leq N} e_p \left( a g^\ell \right), \quad a \in \mathbb{Z},
\]

over primes \( \ell \leq N \); see \([1, 4]\). Furthermore, in \([11, 12]\) more general sums

\[
\sum_{k=1}^{K} e_p \left( a g^{s_k} \right), \quad a \in \mathbb{Z},
\]

have been considered.
have been estimated on average over \( p \leq M \), for arbitrary sequences of integers \( S = (s_k)_{k=1}^{\infty} \), provided that \( S \) is sufficiently dense. In particular, if \( M \leq K (\log K)^{2+\varepsilon} \) for some fixed \( \varepsilon > 0 \), then the result of M. Z. Garaev [11] applies to arbitrary sequences \( S \) with \( 0 \leq s_k \leq k^{15/14+o(1)} \); however, for shorter sums it loses its power even if the sequence \( S \) is very dense.

Here we consider more general exponential sums and in particular extend the results [11, 12] to a different range of parameters. Roughly speaking, the results of [11, 12] require less averaging but apply to longer sums, while we need more averaging but instead treat shorter (and more general) sums.

More precisely, given two sequences of complex numbers \( \Phi = (\varphi_m)_{m=1}^{\infty} \) and \( \Psi = (\psi_n)_{n=1}^{\infty} \) we consider the bilinear sums

\[
S_a(M, N; \Psi) = \sum_{p \leq M} \sum_{\gcd(a, p) = 1} \varphi_p \psi_n e_p (a^g n), \quad a \in \mathbb{Z},
\]

where the outer summation is taken over all primes \( p \leq M \) with \( \gcd(a, p) = 1 \). Note that we do not request that \( a \neq 0 \) since for \( a = 0 \) the summation range is empty.

Our method is different from that of M. Z. Garaev [11] and in fact originates from [3].

Throughout the paper, the implied constants in the symbols ‘\( O \)’ and ‘\( \ll \)’ may depend only on \( g \) and two more integer parameters \( r \) and \( s \) (we recall that \( A \ll B \) is equivalent to \( A = O(B) \)). We use the letters \( \ell, p \) and \( q \) exclusively to denote prime numbers, while \( m \) and \( n \) always denote positive integers.

2. Main result

In the case when some information is available about the growth of the elements of the sequence \( \Phi = (\varphi_m)_{m=1}^{\infty} \) (say if \( \varphi_m | \leq 1 \), \( 1 \leq m \leq M \)), which is almost always the case, it is easy to see that instead of the sums (1) it is enough to estimate the sums

\[
S_a(M, N; \Psi) = \sum_{p \leq M} \sum_{\gcd(a, p) = 1} \left| \sum_{1 \leq n \leq N} \psi_n e_p (a^g n) \right|, \quad a \in \mathbb{Z}.
\]

Theorem 1. For any integers \( r, s \geq 1 \) such that

\[
N^{r+2} \geq M^2,
\]

the following bound holds uniformly over all \( a \in \mathbb{Z} \):

\[
S_a(M, N; \Psi) \ll F \left( M^{1-1/2r(s+2)} N^{1/2+1/2rs} + M^{1+1/(s+2)} \right),
\]

where

\[
F = \sqrt{\sum_{1 \leq n \leq N} |\psi_n|^2}.
\]

Proof. Clearly for some complex numbers \( \varphi_m \) with \( |\varphi_m| = 1 \) for \( 1 \leq m \leq M \), we have

\[
S_a(M, N; \Psi) = \sum_{p \leq M} \varphi_p \sum_{\gcd(a, p) = 1} \sum_{1 \leq n \leq N} \psi_n e_p (a^g n).
\]
So, changing the order of summation we obtain

\[ |S_a(M, N; \Psi)| \leq \sum_{1 \leq n \leq N} |\psi_n| \left| \sum_{\substack{p \leq M \\ \gcd(ag, p) = 1}} \varphi_p e_p (ag^n) \right|. \]

Now, using the Cauchy inequality, we obtain

\[ (2) \quad |S_a(M, N; \Psi)| \leq FU^{1/2}, \]

where

\[ U = \sum_{1 \leq n \leq N} \left| \sum_{\substack{p \leq M \\ \gcd(ag, p) = 1}} \varphi_p e_p (ag^n) \right|^2 \]

\[ = \sum_{\substack{p, q \leq M \\ \gcd(ag, pq) = 1}} \varphi_p \varphi_q \sum_{1 \leq n \leq N} e_p (ag^n) e_q (-ag^n). \]

Let \( \mathcal{M} \) be the set of integers \( m \leq M^2 \) which are products of two distinct primes \( p < q \leq M \) with \( \gcd(ag, pq) = 1 \). Furthermore, for every \( m = pq \in \mathcal{M} \) we define \( a_m = a(q - p) \); thus

\[ e_p (ag^n) e_q (-ag^n) = e_m (a_m g^n). \]

We also remark that

\[ \gcd(a_m, m) = 1 \]

for every \( m \in \mathcal{M} \).

Estimating the contribution to \( U \) from at most the diagonal terms with \( p = q \) trivial as \( MN \), we derive

\[ (3) \quad U \leq MN + 2V, \]

where

\[ V = \sum_{m \in \mathcal{M}} \left| \sum_{1 \leq n \leq N} e_m (a_m g^n) \right|. \]

We now remark that for any integer \( h \geq 0 \) we have

\[ (5) \quad \sum_{1 \leq n \leq N} e_m (a_m g^n) = \sum_{1 \leq n \leq N} e_m (a_m g^{n+h}) + O(h). \]

Let \( H > 0 \) be an arbitrary integer, to be chosen later. Then, we see from \( \boxed{1} \) that

\[ (6) \quad V = \frac{W}{H} + O(H \# \mathcal{M}) = \frac{W}{H} + O(H M^2), \]

where

\[ W = \sum_{m \in \mathcal{M}} \sum_{h=1}^{H} \left| \sum_{1 \leq n \leq N} e_m (a_m g^{n+h}) \right|. \]
By the Hölder inequality, it follows that for any integer \( r \geq 1 \) we have

\[
W^r \leq H^{r-1}(\#M)^{r-1} \sum_{m \in M} \sum_{h=1}^{H} \left| \sum_{1 \leq n \leq N} e_m(a_m g^{n+h}) \right|^r
\]

\[
= H^{r-1}(\#M)^{r-1} \sum_{m \in M} \sum_{h=1}^{H} \vartheta_m(h) \left( \sum_{1 \leq n \leq N} e_m(a_m g^{n+h}) \right)^r
\]

for some complex numbers \( \vartheta_m(h) \) with \( |\vartheta_m(h)| = 1 \).

Now, let \( R_{m,k}(K, \lambda) \) denote the number of solutions of the congruence

\[
\sum_{i=1}^{k} g^{w_i} \equiv \lambda \pmod{m}, \quad 1 \leq w_1, \ldots, w_k \leq K.
\]

Then

\[
\left( \sum_{1 \leq n \leq N} e_m(a_m g^{n+h}) \right)^r = \sum_{\lambda=0}^{p-1} R_{m,r}(N, \lambda)e_m(a_m \lambda g^h).
\]

Therefore, after changing the order of summation (and also using the trivial bound \( \#M \leq M^2 \), we derive that

\[
W^r \leq H^{r-1} M^{2(r-1)} \sum_{m \in M} \sum_{\lambda=0}^{m-1} R_{m,r}(N, \lambda) \sum_{h=1}^{H} \vartheta_m(h) e_m(a_m \lambda g^h).
\]

For an integer \( s \geq 1 \), we write

\[
R_{m,r}(N, \lambda) = \left( R_{m,r}(N, \lambda)^2 \right)^{1/2s} \left( R_{m,r}(N, \lambda)^{(s-1)/s} \right).
\]

Using the Hölder inequality for a sum of products of three terms, we have

\[
W^{2rs} \leq H^{2(r-1)s} M^{4(r-1)s} \sum_{m \in M} \sum_{\lambda=0}^{m-1} R_{m,r}(N, \lambda)^2
\]

\[
\times \left( \sum_{m \in M} \sum_{\lambda=0}^{m-1} R_{m,r}(N, \lambda) \right)^{2s-2}
\]

\[
\times \sum_{m \in M} \sum_{\lambda=0}^{m-1} \sum_{h=1}^{H} \vartheta_m(h) e_m(a_m \lambda g^h)^{2s}.
\]

Clearly,

\[
\sum_{m \in M} \sum_{\lambda=0}^{m-1} R_{m,r}(N, \lambda) \leq \#MN^r \leq M^2 N^r
\]

and

\[
\sum_{m \in M} \sum_{\lambda=0}^{m-1} R_{m,r}(N, \lambda)^2 = \sum_{m \in M} T_{m,r}(N),
\]

where \( T_{m,k}(K) \) denotes the number of solutions of the congruence

\[
G_k(w_1, \ldots, w_{2k}) \equiv 0 \pmod{m}, \quad 1 \leq w_1, \ldots, w_{2k} \leq K,
\]
where
\[ G_k(w_1, \ldots, w_{2k}) = \sum_{i=1}^{2k} (-1)^i g^{w_i}. \]

Thus,
\[ W^{2rs} \leq H^{2(r-1)s} M^{4(r-1)s - 2} N^{2r(s-1)} \sum_{m \in \mathcal{M}} T_{m,r}(N) \times \sum_{m \in \mathcal{M}} \sum_{\lambda = 0}^{m-1} \left| \sum_{h=1}^{H} \vartheta_{m,h} e_m(a_m \lambda g^h) \right|^{2s}. \]

Furthermore,
\[ \sum_{\lambda = 0}^{m-1} \left| \sum_{h=1}^{H} \vartheta_{m,h} e_m(a_m \lambda g^h) \right|^{2s} = \sum_{h_1, \ldots, h_{2s}}^{H} \prod_{\lambda = 0}^{m-1} \left| \sum_{\lambda = 0}^{m-1} e_m(\lambda G_s(h_1, \ldots, h_{2s})) \right| \leq \sum_{h_1, \ldots, h_{2s}}^{H} \left| \sum_{\lambda = 0}^{m-1} e_m(\lambda G_s(h_1, \ldots, h_{2s})) \right| = m T_{m,s}(H) \leq M^2 T_{m,s}(H). \]

Hence,
\[ (7) \quad W^{2rs} \leq H^{2(r-1)s} M^{4rs - 2} N^{2r(s-1)} \sum_{m \in \mathcal{M}} T_{m,r}(N) \sum_{m \in \mathcal{M}} T_{m,s}(H). \]

We note that
\[ (8) \quad \sum_{m \in \mathcal{M}} T_{m,k}(K) = \sum_{w_1, \ldots, w_{2k} = 1}^{K} \sum_{m \in \mathcal{M}} 1. \]

Clearly, any nonzero value \( G_k(w_1, \ldots, w_{2k}) \neq 0 \) has at most
\[ \frac{\log(2kg^K)}{\log 2} \ll K \]
distinct prime divisors. Thus in this case there are at most \( O(K^2) \) values of \( m \in \mathcal{M} \) with \( m \mid G_k(w_1, \ldots, w_{2k}) \). Thus the total contribution from such terms is \( O(K^{2k+2}) \).

Furthermore, by the corollary to [15, Lemma 1, Chapter 15], there are at most \( 2^k K^k \) integer vectors \((w_1, \ldots, w_{2k})\) with \( 1 \leq w_1, \ldots, w_{2k} \leq K \) and such that \( G_k(w_1, \ldots, w_{2k}) = 0 \). For them we estimate the contribution from the sums over \( m \in \mathcal{M} \) trivially as \( M^2 \). Therefore,
\[ (9) \quad \sum_{m \in \mathcal{M}} T_{m,k}(K) \ll K^{2k+2} + K^k M^2. \]

Consequently, inserting (9) into (7), we obtain
\[ (10) \quad W^{2rs} \ll H^{2(r-1)s} M^{4rs - 2} N^{2r(s-1)} \left( N^{2r+2} + N^r M^2 \right) \left( H^{2s+2} + H^s M^2 \right). \]

We now choose
\[ H = \left[ M^{2/(s+2)} \right]. \]
so that \( H^{2s+2} + H^s M^2 \ll H^s M^2 \). Also, recalling that by the condition of the theorem we also have \( N^{2r+2} + N^r M^2 \ll N^{2r+2} \), we obtain from (10)

\[
W^{2rs} \ll H^{2rs-s} M^{4rs} N^{2rs+2}
\]

or

\[
W \ll H^{1-1/2r} M^2 N^{1+1/rs}.
\]

Substituting this estimate into (11) yields

\[ V \ll H^{-1/2r} M^2 N^{1+1/rs} + HM^2, \]

which in turn, after substituting into (3), gives

\[ U \ll H^{-1/2r} M^2 N^{1+1/rs} + HM^2 + MN \ll H^{-1/2r} M^2 N^{1+1/rs} + HM^2. \]

Inserting this into the inequality (2) and recalling the choice of \( H \) produce the desired estimate. \( \square \)

In particular, taking \( \Psi \) to be the indicator function of a sequence of integers \( S = (s_k)_{k=1}^\infty \), we obtain:

**Corollary 2.** Let \( r, s \geq 1 \) be two fixed integers. For any integers \( M \) and \( N \) with \( N \geq M^{2/(r+2)} \) and any sequence of \( K \geq 1 \) integers \( 1 \leq s_k \leq N \), \( k = 1, \ldots, K \), we have

\[
\sum_{p \leq M} \left| \sum_{k=1}^K \epsilon_p (ag^{s_k}) \right| \ll K^{1/2} M^{1-1/2r(s+2)} N^{1/2+1/2rs} + M^{1+1/(s+2)}
\]

uniformly over all \( a \in \mathbb{Z} \).

We note that Corollary 2 is nontrivial only if \( N^A \geq M \geq N^{1+\varepsilon} \) for some fixed \( A > 1 \) and \( \varepsilon > 0 \). In this case, taking a sufficiently large \( r \) (to ensure that \( N \geq M^{1/A} \geq M^{2/(r+2)} \)) and then a sufficiently large \( s \), we obtain

\[
K^{1/2} M^{1-1/2r(s+2)} N^{1/2+1/2rs} \ll K^{1/2} M N^{1-\delta}
\]

for some \( \delta > 0 \). Thus if the sequence \( s_1, \ldots, s_K \) is dense enough (for example, \( K \geq N^{1-\delta} \)), then Corollary 2 yields a nontrivial estimate.

On the other hand, the results of M. Z. Garaev \( [11] \) require a little less averaging and are nontrivial for smaller values of \( M \); however, they become trivial for \( M \geq N \).

### 3. Remarks and Open Questions

Clearly our estimates can be improved by a power of \( \log M \) (as on several occasions we have used the crude estimate \( \#M \leq M^2 \) instead of \( \#M \leq M^2 (\log M)^2 \)). It is also easy to see that a full analogue of Theorem 1 holds also for the sums

\[
\sum_{p \leq M} \max_{a_1, \ldots, a_{p-1}} \left| \sum_{1 \leq n \leq N} \psi_n \epsilon_p (ag^n) \right|, \quad a \in \mathbb{Z}.
\]

We note that an alternative way to estimate the sums \( S_a(M, N; \Psi) \) is via using the estimate due to J. Bourgain and M. Chang \( [7] \) directly to estimate the sum over \( n \) in (11); see also \( [3, 6] \) for further generalisations. However, this approach leads to less explicit estimates and also requires extending the estimates from \( [3, 6] \) to incomplete sums (it seems to be very plausible that such an extension is possible,
though). On the other hand, a clear advantage of this approach is that it can also be used to estimate sums of the type

$$\sum_{1 \leq m \leq M} \sum_{1 \leq n \leq N} \varphi_m \psi_n (ag^n), \quad a \in \mathbb{Z},$$

where the summation is taken over all positive integers $m \leq M$.

Finally, we remark that in [12] one can also find some bounds of multiplicative character sums. It is possible that the methods of [11] apply to multiplicative character sums as well. However the method of this paper does not seem to generalise to such sums. For example, obtaining good estimates on the sums

$$\sum_{p \leq M} \sum_{1 \leq n \leq N} \varphi_p \psi_n \left( \frac{g^n + a_p}{p} \right), \quad a \in \mathbb{Z},$$

where $(u/p)$ is the Legendre symbol modulo $p$, remains an open problem.

**References**


Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: igor@ics.mq.edu.au