PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 7, July 2009, Pages 2217–2224
S 0002-9939(09)09882-7
Article electronically published on March 4, 2009

BILINEAR SUMS WITH EXPONENTIAL FUNCTIONS

IGOR E. SHPARLINSKI

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. Let $g \neq 0, \pm 1$ 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

$$\sum_{\substack{p \le M \\ \gcd(ag,p)=1}} \sum_{1 \le n \le N} \varphi_p \psi_n \mathbf{e}_p\left(ag^n\right), \qquad a \in \mathbb{Z},$$

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

1. INTRODUCTION

Let us fix an integer $g \neq 0, \pm 1$. 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, 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 $m \ge 1$ and a complex z, we define

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

Several estimates have recently been obtained for exponential sums

$$\sum_{1 \le \ell \le N} \mathbf{e}_p\left(ag^{\ell}\right), \qquad a \in \mathbb{Z},$$

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

$$\sum_{k=1}^{K} \mathbf{e}_p\left(ag^{s_k}\right), \qquad a \in \mathbb{Z},$$

Received by the editors September 17, 2008.
2000 *Mathematics Subject Classification.* Primary 11L07, 11L26.
During the preparation of this paper, the author was supported in part by ARC grant No. DP0556431.

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

$$\sum_{\substack{p\le M\\ \gcd(ag,p)=1}} \sum_{1\le n\le N} \varphi_p \psi_n \mathbf{e}_p\left(ag^n\right), \qquad a\in\mathbb{Z}, \tag{1}$$

where the outer summation is taken over all primes $p \le M$ with $\gcd(ag, p) = 1$. Note that we do not request that $a \ne 0$ 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 ℓ, 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 $|\varphi_m| \le 1$, $1 \le m \le M$), which is almost always the case, it is easy to see that instead of the sums (1) it is enough to estimate the sums

$$S_a(M,N;\Psi) = \sum_{\substack{p\le M\\ \gcd(ag,p)=1}} \left| \sum_{1\le n\le N} \psi_n \mathbf{e}_p\left(ag^n\right)\right|, \qquad a\in\mathbb{Z}.$$

Theorem 1. *For any integers $r, s \ge 1$ such that*

$$N^{r+2} \ge M^2,$$

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

$$F = \sqrt{\sum_{1\le n\le N} |\psi_n|^2}.$$

Proof. Clearly for some complex numbers φ_m with $|\varphi_m| = 1$ for $1 \le m \le M$, we have

$$S_a(M,N;\Psi) = \sum_{\substack{p\le M\\ \gcd(ag,p)=1}} \varphi_p \sum_{1\le n\le N} \psi_n \mathbf{e}_p\left(ag^n\right).$$

So, changing the order of summation we obtain

$$|S_a(M,N;\Psi)| \le \sum_{1\le n\le N} |\psi_n| \left| \sum_{\substack{p\le M\\ \gcd(ag,p)=1}} \varphi_p \mathbf{e}_p\left(ag^n\right)\right|.$$

Now, using the Cauchy inequality, we obtain

$$|S_a(M,N;\Psi)| \le FU^{1/2}, \tag{2}$$

where

$$\begin{aligned} U &= \sum_{1\le n\le N} \left| \sum_{\substack{p\le M\\ \gcd(ag,p)=1}} \varphi_p \mathbf{e}_p\left(ag^n\right)\right|^2 \\ &= \sum_{\substack{p,q\le M\\ \gcd(ag,pq)=1}} \varphi_p\overline{\varphi_q} \sum_{1\le n\le N} \mathbf{e}_p\left(ag^n\right)\mathbf{e}_q\left(-ag^n\right). \end{aligned}$$

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

$$\mathbf{e}_p\left(ag^n\right)\mathbf{e}_q\left(-ag^n\right) = \mathbf{e}_m\left(a_m g^n\right).$$

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

$$U \le MN + 2V, \tag{3}$$

where

$$V = \sum_{m\in\mathcal{M}} \left| \sum_{1\le n\le N} \mathbf{e}_m\left(a_m g^n\right)\right|. \tag{4}$$

We now remark that for any integer $h \ge 0$ we have

$$\sum_{1\le n\le N} \mathbf{e}_m\left(a_m g^n\right) = \sum_{1\le n\le N} \mathbf{e}_m\left(a_m g^{n+h}\right) + O(h). \tag{5}$$

Let $H > 0$ be an arbitrary integer, to be chosen later. Then, we see from (5) that

$$V = \frac{W}{H} + O\left(H\#\mathcal{M}\right) = \frac{W}{H} + O\left(HM^2\right), \tag{6}$$

where

$$W = \sum_{m\in\mathcal{M}} \sum_{h=1}^{H} \left| \sum_{1\le n\le N} \mathbf{e}_m\left(a_m g^{n+h}\right)\right|.$$

By the Hölder inequality, it follows that for any integer $r \ge 1$ we have

$$\begin{aligned} W^r &\le H^{r-1}(\#\mathcal{M})^{r-1} \sum_{m\in\mathcal{M}} \sum_{h=1}^{H} \left| \sum_{1\le n\le N} \mathbf{e}_m\left(a_m g^{n+h}\right) \right|^r \\ &= H^{r-1}(\#\mathcal{M})^{r-1} \sum_{m\in\mathcal{M}} \sum_{h=1}^{H} \vartheta_{m,h} \left(\sum_{1\le n\le N} \mathbf{e}_m\left(a_m g^{n+h}\right) \right)^r \end{aligned}$$

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

$$\sum_{i=1}^{k} g^{w_i} \equiv \lambda \pmod m, \qquad 1 \le w_1, \dots, w_k \le K.$$

Then

$$\left(\sum_{1\le n\le N} \mathbf{e}_m\left(a_m g^{n+h}\right) \right)^r = \sum_{\lambda=0}^{p-1} R_{m,r}(N,\lambda)\mathbf{e}_m(a_m\lambda g^h).$$

Therefore, after changing the order of summation (and also using the trivial bound $\#\mathcal{M} \le M^2$, we derive that

$$W^r \le H^{r-1}M^{2(r-1)} \sum_{m\in\mathcal{M}} \sum_{\lambda=0}^{m-1} R_{m,r}(N,\lambda) \sum_{h=1}^{H} \vartheta_{m,h}\mathbf{e}_m(a_m\lambda g^h).$$

For an integer $s \ge 1$, we write

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

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

$$\begin{aligned} W^{2rs} &\le H^{2(r-1)s}M^{4(r-1)s} \sum_{m\in\mathcal{M}} \sum_{\lambda=0}^{m-1} R_{m,r}(N,\lambda)^2 \\ &\qquad \times \left(\sum_{m\in\mathcal{M}} \sum_{\lambda=0}^{m-1} R_{m,r}(N,\lambda) \right)^{2s-2} \\ &\qquad \times \sum_{m\in\mathcal{M}} \sum_{\lambda=0}^{m-1} \left| \sum_{h=1}^{H} \vartheta_{m,h}\mathbf{e}_m\left(a_m\lambda g^h\right) \right|^{2s}. \end{aligned}$$

Clearly,

$$\sum_{m\in\mathcal{M}} \sum_{\lambda=0}^{m-1} R_{m,r}(N,\lambda) \le \#\mathcal{M}N^r \le M^2N^r$$

and

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

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

$$G_k\left(w_1, \dots, w_{2k}\right) \equiv 0 \pmod m, \qquad 1 \le w_1, \dots, w_{2k} \le K,$$

where

$$G_k(w_1, \ldots, w_{2k}) = \sum_{i=1}^{2k} (-1)^i g^{w_i}.$$

Thus,

$$\begin{aligned} W^{2rs} \quad \le \quad & H^{2(r-1)s} M^{4(rs-1)} N^{2r(s-1)} \sum_{m \in \mathcal{M}} T_{m,r}(N) \\ & \times \sum_{m \in \mathcal{M}} \sum_{\lambda=0}^{m-1} \left| \sum_{h=1}^{H} \vartheta_{m,h} \mathbf{e}_m(a_m \lambda g^h) \right|^{2s}. \end{aligned}$$

Furthermore,

$$\begin{aligned} \sum_{\lambda=0}^{m-1} \left| \sum_{h=1}^{H} \vartheta_{m,h} \mathbf{e}_m\left(a_m \lambda g^h\right) \right|^{2s} &= \sum_{h_1,\ldots,h_{2s}=1}^{H} \prod_{i=1}^{2s} \vartheta_{m,h_i} \sum_{\lambda=0}^{m-1} \mathbf{e}_m\left(\lambda G_s\left(h_1, \ldots, h_{2s}\right)\right) \\ &\le \sum_{h_1,\ldots,h_{2s}=1}^{H} \left| \sum_{\lambda=0}^{m-1} \mathbf{e}_m\left(\lambda G_s\left(h_1, \ldots, h_{2s}\right)\right) \right| \\ &= m T_{m,s}(H) \le M^2 T_{m,s}(H). \end{aligned}$$

Hence,

$$W^{2rs} \le H^{2(r-1)s} M^{4rs-2} N^{2r(s-1)} \sum_{m \in \mathcal{M}} T_{m,r}(N) \sum_{m \in \mathcal{M}} T_{m,s}(H). \tag{7}$$

We note that

$$\sum_{m \in \mathcal{M}} T_{m,k}(K) = \sum_{w_1,\ldots,w_{2k}=1}^{K} \sum_{\substack{m \in \mathcal{M} \\ m \mid G_k(w_1,\ldots,w_{2k})}} 1. \tag{8}$$

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 $2^k k! K^k$ integer vectors $(w_1, \ldots, w_{2k})$ with $1 \le w_1, \ldots, w_{2k} \le K$ 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,

$$\sum_{m \in \mathcal{M}} T_{m,k}(K) \ll K^{2k+2} + K^k M^2. \tag{9}$$

Consequently, inserting (9) into (7), we obtain

$$W^{2rs} \ll H^{2(r-1)s} M^{4rs-2} N^{2r(s-1)} \left(N^{2r+2} + N^r M^2\right) \left(H^{2s+2} + H^s M^2\right). \tag{10}$$

We now choose

$$H = \left\lceil M^{2/(s+2)} \right\rceil$$

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 (6) 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. □

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

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

$$\sum_{\substack{p \le M \\ \gcd(ag,p)=1}} \left| \sum_{k=1}^{K} \mathbf{e}_p\left(a g^{s_k}\right) \right| \ll K^{1/2} M^{1-1/2r(s+2)} N^{1/2+1/2rs} + M^{1+1/(s+2)}$$

uniformly over all $a \in \mathbb{Z}$.

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

$$K^{1/2} M^{1-1/2r(s+2)} N^{1/2+1/2rs} \le K^{1/2} M N^{1/2-\delta}$$

for some $\delta > 0$. Thus if the sequence $s_1, \ldots, s_K$ is dense enough (for example, $K \ge N^{1-\delta}$), 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 $M \ge N$.

3. Remarks and open questions

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

$$\sum_{\substack{p \le M \\ \gcd(g,p)=1}} \max_{a=1,\ldots,p-1} \left| \sum_{1 \le n \le N} \psi_n \mathbf{e}_p\left(a g^n\right) \right|, \qquad a \in \mathbb{Z}.$$

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 (4); see also [5, 6] for further generalisations. However, this approach leads to less explicit estimates and also requires extending the estimates from [5, 6, 7] 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

$$\sum_{1\le m\le M}\sum_{1\le n\le N}\varphi_m\psi_n\mathbf{e}_m\left(ag^n\right), \qquad a\in\mathbb{Z},$$

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

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

$$\sum_{\substack{p\le M\\ \gcd(ag,p)=1}}\sum_{1\le n\le N}\varphi_p\psi_n\left(\frac{g^n+a}{p}\right), \qquad a\in\mathbb{Z},$$

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

References

[1] W. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, 'Exponential sums over Mersenne numbers', *Compos. Math.*, **140** (2004), 15–30. MR2004121 (2004j:11091)

[2] W. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, 'Character sums with exponential functions over smooth numbers', *Indag. Math.*, **17** (2006), 157–168. MR2321378 (2008e:11097)

[3] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Uniform distribution of fractional parts related to pseudoprimes', *Canad. J. Math.* (to appear).

[4] J. Bourgain, 'Estimates on exponential sums related the Diffie-Hellman distributions', *Geom. Funct. Anal.*, **15** (2005), 1–34. MR2140627 (2006h:11095)

[5] J. Bourgain, 'Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary', *J. Anal. Math.*, **97** (2005), 317–355. MR2274981 (2007j:11103)

[6] J. Bourgain, 'Exponential sum estimates in finite commutative rings and applications', *J. Anal. Math.*, **101** (2007), 325–355. MR2346549 (2008i:11108)

[7] J. Bourgain and M. Chang, 'Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors', *Geom. Funct. Anal.*, **16** (2006), 327–366. MR2231466 (2007d:11093)

[8] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Cambr. Phil. Soc.*, **146** (2008), 1–21.

[9] 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. Lond. Math. Soc.*, **73** (2006), 380–398. MR2225493 (2007e:11092)

[10] M. Dewar, D. Panario and I. E. Shparlinski, 'Distribution of exponential functions with k-full exponent modulo a prime', *Indag. Math.*, **15** (2004), 497–503. MR2114933 (2005k:11166)

[11] M. Z. Garaev, 'The large sieve inequality for the exponential sequence $\lambda^{[O(n^{15/14+o(1)})]}$ modulo primes', *Canad. J. Math.* (to appear).

[12] M. Z. Garaev and I. E. Shparlinski, 'The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes', *Intern. Math. Res. Notices*, **2005:39** (2005), 2391–2408. MR2181356 (2006i:11108)

[13] S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999. MR1725241 (2000h:11089)

[14] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Matem. Sbornik*, **89(131)** (1972), 654–670 (in Russian). MR0424660 (54:12619)

[15] A. G. Postnikov, *Ergodic aspects of the theory of congruences and of the theory of Diophantine approximations*, Trudy Mat. Inst. Steklov, vol. 82, 1966 (Russian); translated by the Amer. Math. Soc., Providence, R.I., 1967. MR0214561 (35:5410)

[16] I. E. Shparlinski, *Cryptographic applications of analytic number theory*, Birkhäuser Verlag, Basel, 2003. MR1954519 (2004h:94049)

[17] I. E. Shparlinski, 'Distribution of exponential functions with squarefull exponent in residue rings', *Indag. Math.*, **15** (2004), 283–289. MR2071861 (2005h:11183)
[18] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer, Dordrecht, 2007, 135–166. MR2278037 (2007m:11106)

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au