PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 129, Number 6, Pages 1617–1621
S 0002-9939(00)05921-9
Article electronically published on October 31, 2000

DOUBLE EXPONENTIAL SUMS OVER THIN SETS

JOHN B. FRIEDLANDER AND IGOR E. SHPARLINSKI

(Communicated by Dennis A. Hejhal)

ABSTRACT. We estimate double exponential sums of the form

$$S_a(\mathcal{X}, \mathcal{Y}) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \exp\left(2\pi i a \vartheta^{xy}/p\right),$$

where ϑ is of multiplicative order t modulo the prime p and $\mathcal{X}$ and $\mathcal{Y}$ are arbitrary subsets of the residue ring modulo t. In the special case $t = p - 1$, our bound is nontrivial for $|\mathcal{X}| \ge |\mathcal{Y}| \ge p^{15/16+\delta}$ with any fixed $\delta > 0$, while if in addition we have $|\mathcal{X}| \ge p^{1-\delta/4}$ it is nontrivial for $|\mathcal{Y}| \ge p^{3/4+\delta}$.

1

Let p be a prime and let $\mathbb{F}_p$ be a finite field of p elements. For an integer $m \ge 1$ we denote by $\mathbb{Z}_m = \{0, \ldots, m-1\}$ the residue ring modulo m. We also identify $\mathbb{F}_p$ with the set $\{0, \ldots, p-1\}$.

Finally we define $\mathbf{e}(z) = \exp(2\pi i/p)$ and use $\log z$ for the natural logarithm of z.

Throughout the paper the implied constants in symbols 'O', '$\ll$' and '$\gg$' may occasionally, where obvious, depend on the small positive parameter ε and are absolute otherwise (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$).

We fix an element $\vartheta \in \mathbb{F}_p$ of multiplicative order t, that is,

$$\vartheta^s \ne 1, \ 1 \le s < t, \qquad \vartheta^t = 1,$$

and consider double exponential sums

$$S_a(\mathcal{X}, \mathcal{Y}) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \mathbf{e}\left(a\vartheta^{xy}\right),$$

where $a \in \mathbb{F}_p$ and $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{Z}_t$. We also put $S_a(\mathcal{X}) = S_a(\mathcal{X}, \mathcal{X})$.

These sums are close relatives of the sums

$$\sum_{x=1}^{H} \mathbf{e}\left(a\vartheta^x\right) \qquad \text{and} \qquad \sum_{x=1}^{H} \chi(g^x + a),$$

Received by the editors September 16, 1999.

2000 *Mathematics Subject Classification.* Primary 11L07, 11T23; Secondary 11L26.

The first author was supported in part by NSERC grant A5123 and by an NEC grant to the Institute for Advanced Study.

The second author was supported in part by ARC grant A69700294.

where $1 \le H \le t$ and χ is a Dirichlet character of modulus p (see [7, 8, 9, 10] and [4], respectively), and also of the sums

$$\sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \mathbf{e}(uv) \qquad \text{and} \qquad \sum_{u \in \mathcal{U}} \sum_{v \in \mathcal{V}} \chi(u+v),$$

where $a \in \mathbb{F}_p$, $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p$. Such sums are well known in the literature and have proved to be useful in many applications; see [3, 5, 6, 11, 12] as well as Problem 14.a to Chapter 6 of [13], and the references therein.

In the case $\mathcal{X} = \mathcal{Y} = \mathbb{Z}_t$ it has been shown in [1, 2] that

$$\max_{a \in \mathbb{F}_p^*} |S_a(\mathbb{Z}_t)| \ll t p^{1/2} \tau(t),$$

where $\tau(t)$ is the number of integer divisors of t. In this paper we estimate sums $S_a(\mathcal{X}, \mathcal{Y})$ for arbitrary sets $\mathcal{X}$ and $\mathcal{Y}$.

In the special case that both sets are of the same cardinality $|\mathcal{X}| = |\mathcal{Y}| = N$ and $t = p - 1$, that is, ϑ is a primitive root of $\mathbb{F}_p$, our estimates are nontrivial for $N \ge p^{15/16+\delta}$ with any fixed $\delta > 0$. Further examples are given below.

Our results rely on the following estimate for certain double exponential sums from [1]; see the proof of Theorem 8 of that paper. Let $\lambda \in \mathbb{F}_p$ be of multiplicative order T. For any $a, b \in \mathbb{F}_p^*$ we have the bound

$$\sum_{u \in \mathbb{Z}_T} \left| \sum_{v \in \mathbb{Z}_T} \mathbf{e}(a\lambda^v + b\lambda^{uv}) \right|^4 \ll p T^{11/3}. \tag{1}$$

We also recall the well known fact (see Problem 11.c to Chapter 2 of [13]) that the number $\tau(m)$ of integer divisors of $m \ge 1$ satisfies

$$\tau(m) \le m^{o(1)}. \tag{2}$$

2

Our main estimate is the following.

Theorem. *For any sets $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{Z}_t$, the bound*

$$\max_{a \in \mathbb{F}_p^*} |S_a(\mathcal{X}, \mathcal{Y})| \ll |\mathcal{X}|^{1/2} |\mathcal{Y}|^{5/6} t^{1/2} p^{1/8+\varepsilon}$$

holds.

Proof. For a divisor $d|t$ we denote by $\mathcal{Y}(d)$ the subset of $y \in \mathcal{Y}$ with $\gcd(y, t) = d$. Then

$$|S_a(\mathcal{X}, \mathcal{Y})| \le \sum_{d|t} |\sigma_d|,$$

where

$$\sigma_d = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}(d)} \mathbf{e}(a\vartheta^{xy}).$$

Using the Cauchy inequality, we derive

$$\begin{aligned}|\sigma_d|^2 &\le |\mathcal{X}| \sum_{x\in\mathcal{X}} \left| \sum_{y\in\mathcal{Y}(d)} \mathbf{e}\left(a\vartheta^{xy}\right)\right|^2 \le \sum_{x\in\mathbb{Z}_t} \left| \sum_{y\in\mathcal{Y}(d)} \mathbf{e}\left(a\vartheta^{xy}\right)\right|^2 \\ &= |\mathcal{X}| \sum_{y,z\in\mathcal{Y}(d)} \sum_{x\in\mathbb{Z}_t} \mathbf{e}\left(a\left(\vartheta^{xy}-\vartheta^{xz}\right)\right).\end{aligned}$$

By the Hölder inequality we have

$$\begin{aligned}|\sigma_d|^8 &\le |\mathcal{X}|^4 |\mathcal{Y}(d)|^6 \sum_{y,z\in\mathcal{Y}(d)} \left| \sum_{x\in\mathbb{Z}_t} \mathbf{e}\left(a\left(\vartheta^{xy}-\vartheta^{xz}\right)\right)\right|^4 \\ &\le |\mathcal{X}|^4 |\mathcal{Y}(d)|^6 \sum_{y\in\mathcal{Y}(d)} \sum_{u\in\mathbb{Z}_{t/d}} \left| \sum_{x\in\mathbb{Z}_t} \mathbf{e}\left(a\left(\vartheta^{xy}-\vartheta^{xud}\right)\right)\right|^4.\end{aligned}$$

Because each element $y \in \mathcal{Y}(d)$ can be represented in the form $y = dv$ with $\gcd(v, t/d) = 1$ and $\vartheta_d = \vartheta^d$ is of multiplicative order t/d, we see that the double sum over u and x does not depend on y. Therefore,

$$\begin{aligned}|\sigma_d|^8 &\le |\mathcal{X}|^4 |\mathcal{Y}(d)|^7 \sum_{u\in\mathbb{Z}_{t/d}} \left| \sum_{x\in\mathbb{Z}_t} \mathbf{e}\left(a\left(\vartheta_d^x-\vartheta_d^{xu}\right)\right)\right|^4 \\ &= |\mathcal{X}|^4 |\mathcal{Y}(d)|^7 d^4 \sum_{u\in\mathbb{Z}_{t/d}} \left| \sum_{v\in\mathbb{Z}_{t/d}} \mathbf{e}\left(a\left(\vartheta_d^v-\vartheta_d^{vu}\right)\right)\right|^4.\end{aligned}$$

By (1) we obtain

$$|\sigma_d|^8 \ll |\mathcal{X}|^4 |\mathcal{Y}(d)|^7 p t^{11/3} d^{1/3}. \tag{3}$$

Using the bound $|\mathcal{Y}(d)| \le |\mathcal{Y}|$ for $d \le t/|\mathcal{Y}|$ and the bound $|\mathcal{Y}(d)| \le t/d$ for $d > t/|\mathcal{Y}|$, we obtain that

$$|\sigma_d| \ll |\mathcal{X}|^{1/2} |\mathcal{Y}|^{5/6} t^{1/2} p^{1/8}$$

for any divisor $d|t$. Applying the bound (2), we derive the desired result. □

Of course the sets $\mathcal{X}$ and $\mathcal{Y}$ can be interchanged in the above estimate. Combining those two bounds we obtain the following symmetric estimate:

$$\max_{a\in\mathbb{F}_p^*} |S_a(\mathcal{X}, \mathcal{Y})| \ll (|\mathcal{X}|^{-1/3} + |\mathcal{Y}|^{-1/3})^{-1} |\mathcal{X}|^{1/2} |\mathcal{Y}|^{1/2} t^{1/2} p^{1/8}$$

or, more simply, multiplying the two bounds and taking the square root we obtain the somewhat weaker result

$$\max_{a\in\mathbb{F}_p^*} |S_a(\mathcal{X}, \mathcal{Y})| \ll |\mathcal{X}|^{2/3} |\mathcal{Y}|^{2/3} t^{1/2} p^{1/8}.$$

In particular, if $|\mathcal{X}| = |\mathcal{Y}| = N$ and $t = p - 1$, then the bound takes the form

$$\max_{a\in\mathbb{F}_p^*} |S_a(\mathcal{X}, \mathcal{Y})| \ll N^{4/3} p^{5/8+\varepsilon}.$$

3

We remark that if some nontrivial information about the size of $\mathcal{Y}(d)$ is available, then the result can be improved. On the other hand if t does not have small proper divisors, then we obtain an improvement as well. For example, assume that t does not have proper divisors d in the interval $1 < d < t^{7/5}p^{-21/20}$. Then using the inequalities $|\mathcal{Y}(1)| \le |\mathcal{Y}|$ and $|\mathcal{Y}(d)| \le t/d$ for $d \ge t^{7/5}p^{-21/20}$ we obtain

$$\max_{a \in \mathbb{F}_p^*} |S_a(\mathcal{X}, \mathcal{Y})| \ll |\mathcal{X}|^{1/2} |\mathcal{Y}|^{7/8} t^{11/24} p^{1/8+\varepsilon}$$

(and this is the best that can be obtained by our method even for sets satisfying $|\mathcal{Y}(d)| \le |\mathcal{Y}|/d$ or even with $\gcd(y, p-1) = 1$ for $y \in \mathcal{Y}$).

It is of interest to remark that if $t = p-1$ our result can be reformulated as the bound

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in \mathcal{X}} \sum_{u \in \mathcal{U}} \mathbf{e}(au^x) \right| \ll \min \left\{ |\mathcal{X}|^{1/2} |\mathcal{U}|^{5/6}, |\mathcal{X}|^{5/6} |\mathcal{U}|^{1/2} \right\} p^{5/8+\varepsilon}$$

and hence

$$\max_{a \in \mathbb{F}_p^*} \left| \sum_{x \in \mathcal{X}} \sum_{u \in \mathcal{U}} \mathbf{e}(au^x) \right| \ll |\mathcal{X}|^{2/3} |\mathcal{U}|^{2/3} p^{5/8+\varepsilon}$$

for sets $\mathcal{X} \subseteq \mathbb{Z}_{p-1}$ and $\mathcal{U} \subseteq \mathbb{F}_p$. Thus the powers u^x, where $\mathcal{X} \subseteq \mathbb{Z}_{p-1}$ and $\mathcal{U} \subseteq \mathbb{F}_p$, are uniformly distributed modulo p, provided that $|\mathcal{X}|$ and $|\mathcal{U}|$ are large enough. For example it suffices for each of the two sets to have at least $p^{15/16+\delta}$ elements with some $\delta > 0$ or alternatively for one of them to be almost of positive density, say to have at least $p^{1-\delta/4}$ elements in which case the other one is required only to have density exceeding $p^{3/4+\delta}$.

If the sets $\mathcal{X}$ and $\mathcal{Y}$ are dense in the sense $|\mathcal{X}| \gg t^{1-\varepsilon}$ and $|\mathcal{Y}| \gg t^{1-\varepsilon}$, then our trivial estimate $\mathcal{Y}(d) \le t/d$ becomes almost optimal and we obtain the bound

$$S_a(\mathcal{X}, \mathcal{Y}) \ll t^{11/6} p^{1/8+\varepsilon},$$

which is nontrivial for $t \ge p^{3/4+\delta}$ with any fixed $\delta > 0$.

It would be interesting to extend these results to modular exponentiation modulo arbitrary integers m. In some cases, for example when m contains a large prime divisor, this can be done within the framework of this paper. Other moduli may require some new ideas.

Finally, it is clear that the arguments of the Theorem give the identical bound for the larger sum

$$T_a(\mathcal{X}, \mathcal{Y}) = \sum_{x \in \mathcal{X}} \left| \sum_{y \in \mathcal{Y}} \exp(2\pi i a \vartheta^{xy}/p) \right|$$

but then the roles of $\mathcal{X}$ and $\mathcal{Y}$ cannot be interchanged and the symmetrized bounds do not apply.

References

[1] R. Canetti, J. B. Friedlander, S. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski, 'On the statistical properties of Diffie–Hellman distributions', *Israel J. Math.* (to appear).

[2] R. Canetti, J. B. Friedlander and I. E. Shparlinski, 'On certain exponential sums and the distribution of Diffie–Hellman triples', *J. London Math. Soc.*, **59** (1999), 799–812. MR **2000g:**11079

[3] F. R. K. Chung, 'Several generalizations of Weil sums', *J. Number Theory*, **49** (1994), 95–106. MR **95h:**11085
[4] E. Dobrowolski and K. S. Williams, 'An upper bound for the sum $\sum_{n=a+1}^{a+H} f(n)$ for a certain class of functions f', *Proc. Amer. Math. Soc.*, **114** (1993), 29–35. MR **92c:**11086
[5] J. Friedlander and H. Iwaniec, 'Estimates for character sums', *Proc. Amer. Math. Soc.*, **119** (1993), 363–372. MR **93k:**11074
[6] H. Iwaniec and A. Sárközy, 'On a multiplicative hybrid problem', *J. Number Theory*, **26** (1987), 89–95. MR **88f:**11022
[7] S. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge Univ. Press, Cambridge, 1999. CMP 2000:05
[8] N. M. Korobov, 'On the distribution of digits in periodic fractions', *Matem. Sbornik*, **89** (1972), 654–670 (in Russian). MR **54:**12619
[9] N. M. Korobov, *Exponential sums and their applications*, Kluwer Acad. Publ., Dordrecht, 1992. MR **93a:**11068
[10] H. Niederreiter, 'Quasi-Monte Carlo methods and pseudo-random numbers', *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041. MR **80d:**65016
[11] A. Sárközy, 'On the distribution of residues of products of integers', *Acta Math. Hungar.*, **49** (1987), 397–401. MR **88e:**11004
[12] I. E. Shparlinski, 'On the distribution of primitive and irreducible polynomials modulo a prime', *Diskretnaja Matem.*, **1** (1989), no.1, 117–124 (in Russian).
[13] I. M. Vinogradov, *Elements of Number Theory*, Dover Publ., NY, 1954. MR **15:**933e

Department of Mathematics, University of Toronto, Toronto, Ontario, Canada M5S 3G3
E-mail address: frdlndr@math.toronto.edu

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