Bull. Aust. Math. Soc. **98** (2018), 64–69
doi:10.1017/S0004972718000205

BOUNDS FOR TRIPLE EXPONENTIAL SUMS WITH MIXED EXPONENTIAL AND LINEAR TERMS

KAM HUNG YAU

(Received 19 November 2017; accepted 21 February 2018; first published online 3 May 2018)

Abstract

We establish bounds for triple exponential sums with mixed exponential and linear terms. The method we use is by Shparlinski ['Bilinear forms with Kloosterman and Gauss sums', Preprint, 2016, arXiv:1608.06160] together with a bound for the additive energy from Roche-Newton *et al.* ['New sum-product type estimates over finite fields', *Adv. Math.* **293** (2016), 589–605].

2010 *Mathematics subject classification*: primary 11L07; secondary 11D79.

Keywords and phrases: exponential sums, exponential function, cancellation, solutions to congruences in small boxes.

1. Introduction

Bounds for exponential sums were first studied in number theory because they yield arithmetic information about certain Diophantine problems. For example, by obtaining estimates for exponential sums over primes, Vinogradov [9] was able to show that every sufficiently large odd integer can be written as a sum of three primes. Now, the study of bounds for exponential sums has both mathematical and arithmetic interest.

Let p be a prime and let g be an arbitrary integer with $\gcd(g, p) = 1$. Denote by T the multiplicative order of g modulo p. Given two intervals of consecutive integers

$$\mathcal{I} = \{K + 1, \dots, K + M\}, \quad \mathcal{J} = \{L + 1, \dots, L + N\}$$

and

$$\mathcal{K} = \{1, \dots, H\},$$

with integers H, K, L, M, N such that $0 < M \le p$, $0 < N \le T$, $0 < H < T$, and a complex sequence $\mathcal{A} = (\alpha_m)_{m\in\mathcal{I}}$, we define the exponential sum

$$\mathcal{S}_{a,T,p}(\mathcal{A}; \mathcal{I}, \mathcal{J}, \mathcal{K}) = \sum_{m\in\mathcal{I}} \sum_{n\in\mathcal{J}} \sum_{x\in\mathcal{K}} \alpha_m e_p(amg^x) e_T(nx)$$

The author is supported by an Australian Government Research Training Program (RTP) Scholarship.

for integers $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$, where $e_h(x) = e(2\pi i x/h)$. In particular, when $\mathcal{I} = \mathbb{Z}_p = \{0, 1, \dots, p-1\}$, we define

$$\mathcal{S}_{a,T,p}(\mathcal{A}; \mathcal{J}, \mathcal{K}) = \mathcal{S}_{a,T,p}(\mathcal{A}; \mathbb{Z}_p, \mathcal{J}, \mathcal{K}).$$

Similar double exponential sums arise frequently. In particular, sums of the form

$$S(\mathcal{A}, \mathcal{B}; \mathcal{I}, \mathcal{J}) = \sum_{m \in \mathcal{I}} \sum_{n \in \mathcal{J}} \alpha_m \beta_n e_p(amg^n)$$

have been considered by Shparlinski and Yau [8]. For the case where g is not necessarily a primitive root of p, bounds have been established under the condition $\mathcal{I} = \{1\}$ and $\alpha_m = \beta_n = 1$ by Kerr [2], but the method employed there also works for general $\mathcal{I}$ as the bounds depend only on the norm. Similar sums for multiplicative characters have also been studied in [7]. We refer the reader to [3] for a broader overview of exponential sums.

In this paper we establish bounds for $\mathcal{S}_{a,T,p}(\mathcal{A}; \mathcal{I}, \mathcal{J}, \mathcal{K})$ when $\mathcal{I} = \mathbb{Z}_p$. It will be clear the same method also works for general $\mathcal{I}$.

Our approach follows from Shparlinski [6]. In particular, after applying the triangle and Hölder inequalities to $\mathcal{S}_{a,T,p}(\mathcal{A}; \mathcal{I}, \mathcal{J}, \mathcal{K})$, we obtain a mean fourth moment of an exponential sum. By opening and changing the order of summation and appealing to the orthogonality of the exponential function, we can bound the sum by the number of solutions to a particular congruence (see Lemma 3.2).

2. Main result

The statements $A \ll B$ and $A = O(B)$ are both equivalent to the inequality $|A| \le cB$ for some positive absolute constant c. For any real number $\sigma > 0$, define

$$\|\mathcal{A}\|_\sigma = \Big(\sum_{m \in \mathcal{I}} |\alpha_m|^\sigma \Big)^{1/\sigma}.$$

Our main result is the following bound for $\mathcal{S}_{a,T,p}(\mathcal{A}; \mathcal{J}, \mathcal{K})$.

THEOREM 2.1. *For any prime p,*

$$S_{a,T,p}(\mathcal{A}; \mathcal{J}, \mathcal{K}) \ll \|\mathcal{A}\|_1^{1/2} \|\mathcal{A}\|_2^{1/2} p^{1/4} N^{3/8} T^{5/8}.$$

Using the same technique as in [5, Lemma 3.14] and the bound in [4, Corollary 19], we obtain the trivial bound

$$S_{a,T,p}(\mathcal{A}; \mathcal{J}, \mathcal{K}) \ll \|\mathcal{A}\|_1 N \min\{p^{1/8} H^{5/8}, p^{1/4} H^{3/8}\}. \tag{2.1}$$

Assuming $|\alpha_m| \le 1$, we have $\|\mathcal{A}\|_1 \ll M$ and $\|\mathcal{A}\|_2 \ll M^{1/2}$. We see that Theorem 2.1 provides a stronger bound

$$S_{a,T,p}(\mathcal{A}; \mathcal{J}, \mathcal{K}) \ll M^{3/4} p^{1/4} N^{3/8} T^{5/8}$$

https://doi.org/10.1017/S0004972718000205 Published online by Cambridge University Press

than (2.1), which becomes

$$S_{a,T,p}(\mathcal{A};\mathcal{J},\mathcal{K}) \ll MN \min\{p^{1/8}H^{5/8}, p^{1/4}H^{3/8}\},$$

when

$$pT^5 < M^2N^5H^5 \quad \text{and} \quad T^5 < M^2N^5H^3.$$

3. Preparation

For an integer u, we define

$$\langle u\rangle_r = \min_{k\in\mathbb{Z}} |u - kr|$$

as the distance to the nearest integral multiple of r.

We recall a well-known bound from [1, Bound (8.6)].

Lemma 3.1. *For integers u, W and $Z \geq 1$,*

$$\sum_{n=W+1}^{W+Z} e_r(nu) \ll \min\left\{Z, \frac{r}{\langle u\rangle_r}\right\}.$$

We recall that T is the multiplicative order of g modulo p. For any positive integer $K \leq T$, we define the *additive energy* $E_p(K)$ as the number of solutions to the congruence

$$g^{x_1} + g^{x_2} \equiv g^{x_3} + g^{x_4} \pmod{p} \tag{3.1}$$

where

$$(x_1, x_2, x_3, x_4) \in \{1, \dots, K\}^4.$$

Our approach to bounding $\mathcal{S}_{a,T,p}(\mathcal{A};\mathcal{I},\mathcal{J},\mathcal{K})$ is to reduce the problem to estimating $E_p(K)$.

Note that $(v_1, v_2, v_1, v_2) \in \{1, \dots, K\}^4$ is always a solution to (3.1); hence, we have the trivial lower bound $K^2 \leq E_p(K)$. If $(v_1, v_2, v_3, v_4) \in \{1, \dots, K\}^4$ is a solution to (3.1) then v_4 is dependent on v_1, v_2, v_3 and we obtain the trivial upper bound $E_p(K) \leq K^3$. In particular, $E_p(K)$ is an increasing function of K.

Set $A, B, C = \{g, \dots, g^K\}$. Then we have the trivial bounds $|A| \leq K$ and $|BC| \leq 2K$. Appealing to [4, Theorem 6], we can derive a nontrivial estimate for $E_p(K)$.

Lemma 3.2. *For any positive integer $1 \leq K \leq T$,*

$$E_p(K) \ll K^{5/2}.$$

https://doi.org/10.1017/S0004972718000205 Published online by Cambridge University Press

4. Proof of Theorem 2.1

We proceed similarly to the proof of [6, Theorem 2.1]. Rearranging then applying Lemma 3.1,

$$\begin{aligned}\mathcal{S}_{a,T,p}(\mathcal{A};\mathcal{J},\mathcal{K}) &= \sum_{x=1}^{H}\sum_{m=0}^{p-1}\alpha_m e_p(amg^x)\sum_{n=L+1}^{L+N} e_T(nx)\\ &= \sum_{x=1}^{H}\sum_{m=0}^{p-1}\alpha_m e_p(amg^x)\varphi_x\end{aligned}$$

where

$$|\varphi_x| \le \min\Big(N, \frac{T}{\langle x\rangle_T}\Big).$$

Define $I = \lceil \log N\rceil$ and define the sets

$$\mathcal{L}_0 = \{x \in \mathbb{Z} : 0 < x \le T/N\}$$

and

$$\mathcal{L}_i = \{x \in \mathbb{Z} : \min\{T, e^i T/N\} \ge x > e^{i-1}T/N\}$$

for $i = 1, \dots, I$. We obtain

$$\mathcal{S}_{a,T,p}(\mathcal{A};\mathcal{J},\mathcal{K}) \ll \sum_{i=0}^{I}|S_i|$$

where

$$S_i = \sum_{x\in\mathcal{L}_i}\sum_{m=0}^{p-1}\alpha_m e_p(amg^x)\varphi_x$$

for $i = 0, \dots, I$.

Applying the triangle and Hölder inequalities, we obtain

$$\begin{aligned}|S_i| &\le \sum_{m=0}^{p-1}|\alpha_m|^{1/2}|\alpha_m^2|^{1/4}\Big|\sum_{x\in\mathcal{L}_i}\alpha_m e_p(amg^x)\varphi_x\Big|\\ &\le \Big(\sum_{m=0}^{p-1}|\alpha_m|\Big)^{1/2}\Big(\sum_{m=0}^{p-1}|\alpha_m|^2\Big)^{1/4}\Big(\sum_{m=0}^{p-1}\Big|\sum_{x\in\mathcal{L}_i}e_p(amg^x)\varphi_x\Big|^4\Big)^{1/4}\\ &= \|\mathcal{A}\|_1^{1/2}\|\mathcal{A}\|_2^{1/2}\Big(\sum_{m=0}^{p-1}\Big|\sum_{x\in\mathcal{L}_i}e_p(amg^x)\varphi_x\Big|^4\Big)^{1/4} \qquad (4.1)\end{aligned}$$

https://doi.org/10.1017/S0004972718000205 Published online by Cambridge University Press

which is valid for $i = 0, \dots, I$. Opening the summation and changing the order of summation, we obtain

$$\sum_{m=0}^{p-1}\Big|\sum_{x\in\mathcal{L}_i} e_p(amg^x)\varphi_x\Big|^4 = \sum_{m=0}^{p-1}\sum_{x_1,\dots,x_4\in\mathcal{L}_i}\cdots\sum\varphi_{x_1}\varphi_{x_2}\overline{\varphi_{x_3}\varphi_{x_4}}e_p(am(g^{x_1}+g^{x_2}-g^{x_3}-g^{x_4}))$$
$$= \sum_{x_1,\dots,x_4\in\mathcal{L}_i}\cdots\sum\varphi_{x_1}\varphi_{x_2}\overline{\varphi_{x_3}\varphi_{x_4}}\sum_{m=0}^{p-1}e_p(am(g^{x_1}+g^{x_2}-g^{x_3}-g^{x_4})).$$

For all $x \in \mathcal{L}_i$, we have the bound $\varphi_x \ll e^{-i}N$, hence

$$\sum_{m=0}^{p-1}\Big|\sum_{x\in\mathcal{L}_i} e_p(amg^x)\varphi_x\Big|^4$$
$$\le \sum_{x_1,\dots,x_4\in\mathcal{L}_i}\cdots\sum|\varphi_{x_1}\varphi_{x_2}\overline{\varphi_{x_3}\varphi_{x_4}}|\sum_{m=0}^{p-1}e_p(am(g^{x_1}+g^{x_2}-g^{x_3}-g^{x_4}))$$
$$\ll e^{-4i}N^4\sum_{x_1,\dots,x_4\in\mathcal{L}_i}\cdots\sum\sum_{m=0}^{p-1}e_p(am(g^{x_1}+g^{x_2}-g^{x_3}-g^{x_4})).$$

By appealing to the orthogonality of the exponential function,

$$\sum_{m=0}^{p-1}\Big|\sum_{x\in\mathcal{L}_i} e_p(amg^x)\varphi_x\Big|^4 \ll pe^{-4i}N^4E_p(\lfloor e^iT/N\rfloor).$$

Therefore by Lemma 3.2

$$\sum_{m=0}^{p-1}\Big|\sum_{x\in\mathcal{L}_i} e_p(amg^x)\varphi_x\Big|^4 \ll pe^{-4i}N^4(e^iT/N)^{5/2}$$
$$\ll pe^{-3/2i}N^{3/2}T^{5/2}.$$

Substituting this bound into (4.1),

$$|S_i| \ll \|\mathcal{A}\|_1^{1/2}\|\mathcal{A}\|_2^{1/2}p^{1/4}e^{-3i/8}N^{3/8}T^{5/8}.$$

Finally,

$$\sum_{i=0}^{I}|S_i| \ll \|\mathcal{A}\|_1^{1/2}\|\mathcal{A}\|_2^{1/2}p^{1/4}N^{3/8}T^{5/8}$$

and the result follows immediately.

Acknowledgements

The author would like to thank the referee for many helpful comments and I. E. Shparlinski for the problem, helpful comments and proofreading of the paper.

https://doi.org/10.1017/S0004972718000205 Published online by Cambridge University Press

References

[1] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, 53 (American Mathematical Society, Providence, RI, 2004).

[2] B. Kerr, 'Incomplete exponential sums over exponential functions', *Q. J. Math.* **66**(1) (2015), 213–224.

[3] S. V. Konyagin and I. E. Shparlinski, *Character Sums with Exponential Functions and their Applications*, Cambridge Tracts in Mathematics, 136 (Cambridge University Press, Cambridge, 1999).

[4] O. Roche-Newton, M. Rudnev and I. D. Shkredov, 'New sum-product type estimates over finite fields', *Adv. Math.* **293** (2016), 589–605.

[5] I. E. Shparlinski, *Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness*, Progress in Computer Science and Applied Logic, 22 (Birkhäuser, Basel, 2013).

[6] I. E. Shparlinski, 'Bilinear forms with Kloosterman and Gauss sums', Preprint, 2016, arXiv:1608.06160.

[7] I. E. Shparlinski and K. H. Yau, 'Bounds of double multiplicative character sums and gaps between residues of exponential functions', *J. Number Theory* **167** (2016), 304–316.

[8] I. E. Shparlinski and K. H. Yau, 'Double exponential sums with exponential functions', *Int. J. Number Theory* **13** (2017), 2531–2543.

[9] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers* (Interscience Publishers, New York, NY, 1954).

KAM HUNG YAU, Department of Pure Mathematics,
University of New South Wales, Sydney, NSW 2052, Australia
e-mail: kamhung.yau@unsw.edu.au

https://doi.org/10.1017/S0004972718000205 Published online by Cambridge University Press