

Two-dimensional Weyl sums failing square-root cancellation along lines

Julia Brandes and Igor E. Shparlinski

Abstract. We show that a certain two-dimensional family of Weyl sums of length P takes values as large as $P^{3/4+o(1)}$ on almost all linear slices of the unit torus, contradicting a widely held expectation that Weyl sums should exhibit square-root cancellation on generic subvarieties of the unit torus. This is an extension of a result of J. Brandes, S. T. Parsell, C. Poulias, G. Shakan and R. C. Vaughan (2020) from quadratic and cubic monomials to general polynomials of arbitrary degree. The new ingredients of our approach are the classical results of E. Bombieri (1966) on exponential sums along a curve and R. J. Duffin and A. C. Schaeffer (1941) on Diophantine approximations by rational numbers with prime denominators.

1. Introduction

Given their central role in many number theoretic applications, it is no surprise that Weyl sums and their properties have been subject to thorough investigation over the years. For a collection φ of linearly independent polynomials $\varphi_1, \dots, \varphi_r \in \mathbb{Z}[X]$ with respective degrees k_1, \dots, k_r we consider the *Weyl sums*

$$f_\varphi(\boldsymbol{\alpha}) = \sum_{1 \leq x \leq P} \mathbf{e}(\alpha_1 \varphi_1(x) + \dots + \alpha_r \varphi_r(x)),$$

where $\mathbf{e}(z) = \exp(2\pi iz)$ and $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_r)$. We also write $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ for the unit torus, and refer to the end of this section for other notational conventions we use.

Whilst it is well known that $f_\varphi(\boldsymbol{\alpha})$ can be of order P when the entries of $\boldsymbol{\alpha}$ lie in the neighbourhood of fractions with a small denominator, the general expectation has always been that for a “typical” $\boldsymbol{\alpha}$ one should have the upper and lower bounds

$$(1.1) \quad P^{1/2} \ll |f_\varphi(\boldsymbol{\alpha})| \leq P^{1/2+o(1)}.$$

Key words and phrases: Exponential sums.

2010 Mathematics Subject Classification: primary 11L15; secondary 11J83, 11T23.

This question has recently been investigated in work by Chen and Shparlinski [7], which in particular implies that the bounds (1.1) hold for a subset of $\alpha \in \mathbb{T}^r$ of full Lebesgue measure whenever the polynomials φ have a non-vanishing Wronskian [7, Corollary 2.2]. A particularly strong version of this result, applicable to the situation when $\varphi_j(X) = X^j$ for $1 \leq j \leq r$, is available in subsequent work [6], where the interested reader can also find a more comprehensive bibliography on the subject.

In practical applications it is often necessary to control the size of $f_\varphi(\alpha)$ on linear slices of \mathbb{T}^r , where some of the α_i are fixed to lie in some set of full measure, whereas the remaining ones range over the entire unit interval. Such situations typically arise in “minor arcs” situations where some, but not all, entries of α may have a good rational approximation and thus lie in an anticipated exceptional set. This problem has recently been studied in a very general setup by Chen and Shparlinski [7] (see also [8]), refining an approach developed by Wooley [15]. Their main result [7, Theorem 2.1] asserts that whenever the polynomials φ have a non-vanishing Wronskian, then for almost all $(\alpha_1, \dots, \alpha_d) \in \mathbb{T}^d$ one has bounds of the shape

$$\sup_{\alpha_{d+1}, \dots, \alpha_r \in \mathbb{T}} |f_\varphi(\alpha_1, \dots, \alpha_r)| \leq P^{1/2 + \Gamma(d, \varphi) + o(1)},$$

where $\Gamma(d, \varphi)$ is a non-negative function depending on the degrees of the polynomials φ , for the precise definition of which we refer to [7]. Unfortunately, even though the bound of [7, Theorem 2.1] gives strong results in a number of configurations and notably implies that one can take $\Gamma(d, \varphi) = 0$ for all admissible r -tuples of polynomials when $d = r$, in many other cases the bounds it furnishes do not beat even the trivial bound. In such situations, one has to resort to the more classical methods employing bounds of Weyl or Hua type and their subsequent generalisations (see [14, Lemma 2.4 and Theorem 5.2] for the former, and [14, Lemma 2.5] as well as the results of [16, Section 14] for the latter). Bounds of this nature provide also the crucial input in the work by Erdoğan and Shakan [11], as well as in recent work by Chen and Shparlinski [9] in which, motivated by some links to certain questions on classical partial differential equations, they establish upper bounds along linear slices of the exponential sum associated with pairs of polynomials φ_1, φ_2 differing by a linear term. Several related results have recently been obtained by Barron [1]. However, as these bounds use Vinogradov’s mean value theorem (see [3, Theorem 1.1] or [16, Theorem 1.1]) as their main input, which is inefficient for Weyl sums whose degree exceeds their dimension, they are inherently unable to provide bounds stronger than $O(P^{1-c_k})$ for some positive parameter c_k of size $c_k \asymp k^{-2}$.

Whilst exponents of this magnitude are not believed to be sharp in general, Brandes et al. [4] have recently shown that one cannot hope to have $\Gamma(d, \varphi) = 0$ for

all choices of polynomials with non-vanishing Wronskian when $d < r$. In particular, for the choice $\varphi_1(x) = X^k + X$ and $\varphi_2(X) = X^k$ with $k=2$ or $k=3$, they show in [4, Theorem 1.3] that for all $\alpha_2 \in \mathbb{R} \setminus \mathbb{Q}$ and any $\tau > 0$ there exist arbitrarily large values of P for which we have the lower bound

$$(1.2) \quad \sup_{\alpha \in \mathbb{T}} |f_{\varphi}(\alpha_1, \alpha_2)| \gg P^{3/4-\tau},$$

and that for almost all $\alpha_2 \in \mathbb{T}$ this bound can be matched by a corresponding upper bound

$$\sup_{\alpha \in \mathbb{T}} |f_{\varphi}(\alpha_1, \alpha_2)| \leq P^{3/4+o(1)}.$$

To our knowledge, this is the first indication in the literature that the expectation that (1.1) should hold for all α on a linear slice of \mathbb{T}^r may be too naive. In [4] the authors speculate that the same behaviour as in (1.2) might continue to hold for polynomials $\varphi_1(X) = X^k + X$ and $\varphi_2(X) = X^k$ with $k \geq 4$.

The goal of this paper is therefore to extend the bound in (1.2) to more general polynomials, allowing also for higher degrees.

Theorem 1. *Let $\varphi \in \mathbb{Z}[X]$ be a polynomial of degree $k \geq 2$, and set*

$$(1.3) \quad f(\alpha_1, \alpha_2) = \sum_{1 \leq x \leq P} \mathbf{e}(\alpha_1(\varphi(x) + x) + \alpha_2\varphi(x)).$$

There exists a set $\mathcal{C} \subseteq \mathbb{T}$ of full Lebesgue measure such that for all $\alpha_2 \in \mathcal{C}$ one has the bound

$$\limsup_{P \rightarrow \infty} P^{-3/4} \sup_{\alpha_1 \in \mathbb{T}} |f(\alpha_1, \alpha_2)| = \infty.$$

Thus, whenever $\varphi = (\varphi_1, \varphi_2)$ is a pair of polynomials differing only by a linear term, the associated exponential sum is substantially larger than originally anticipated on almost all linear slices of \mathbb{T} . The fact that in our result the polynomials under consideration differ only by a linear term seems to play a role, since linear exponential sums do not exhibit square root cancellation in the same manner as their cousins of higher degree do. It is therefore an interesting question to investigate whether the behaviour observed in Theorem 1 persists, perhaps in a weaker form, even when the polynomials occurring in the exponential sum differ by more than a linear term.

Unlike in [4], our result in Theorem 1 is not complemented by a matching upper bound, however some nontrivial estimates can be found in [9]. The methods presented in [4] could conceivably be adapted to provide best possible upper bounds even in the more general case considered in the manuscript at hand for all α_2 lying in a subset of full measure of a suitably defined set of “major arcs”. This would

be sufficient when $k \leq 3$, as then the entire unit interval \mathbb{T} can be covered by such major arcs. For higher degrees, these methods fail and we have no improvements over the existing results of [9]. Nonetheless, we believe that these difficulties are of a technical rather than fundamental nature, and consequently it seems likely that the exponent $3/4$ should be sharp in those cases also.

Our argument is a streamlined version of that presented in [4, Section 8], which deals with the case of $\varphi(X) = X^k$ for $k = 2, 3$. However, we augment this approach by two classical results. Firstly, we appeal to a bound of Bombieri [2, Theorem 6] on exponential sums along a curve over a finite field, and secondly we make use of a result of Duffin and Schaeffer [10, Theorem I] which allows us to restrict to the case where the diophantine approximations we consider have a prime denominator.

Notation. Throughout the paper, we make use of the following conventions. When $x \in \mathbb{R}$ we denote by $\|x\|$ the distance from x to the nearest integer. Moreover, P always denotes a large positive number, and the letter p is reserved for primes. We use the Vinogradov ‘ \ll ’, ‘ \gg ’ and equivalent Bachmann–Landau notations ‘ $O(\cdot)$ ’ liberally, and here the implied constants are allowed to depend on φ and τ , but never on P or α .

2. Assembling the toolbox

2.1. Approximations by rational exponential sums

In our examination of the exponential sum (1.3) we rely heavily on our understanding of the closely related sum

$$g(\alpha, \gamma) = \sum_{1 \leq x \leq P} \mathbf{e}(\alpha x + \gamma \varphi(x))$$

and its associated approximations. Indeed, it is apparent from the respective definitions of these exponential sums that

$$(2.1) \quad f(\alpha_1, \alpha_2) = g(\alpha_1, \alpha_1 + \alpha_2).$$

When $\varphi(X) = X^k$, the latter one of these has been studied in [5] and [4], but it turns out that in the situation we are mainly interested in the pure power may be replaced by a more general polynomial. For $q \in \mathbb{N}$, $a, c \in \mathbb{Z}$ and $\beta \in \mathbb{R}$ set

$$S(q; a, c) = \sum_{x=1}^q \mathbf{e}\left(\frac{ax + c\varphi(x)}{q}\right) \quad \text{and} \quad I(\beta) = \int_0^P \mathbf{e}(\beta x) \, dx,$$

and recall that for non-vanishing β we can compute

$$(2.2) \quad |I(\beta)| = P \left| \frac{\sin(\pi\beta P)}{\pi\beta P} \right| \ll \min\{P, \|\beta\|^{-1}\},$$

while a classical Weil bound (see, for example, [13, Corollary II.2F]) shows that when p is prime and $p \nmid c$ one has

$$(2.3) \quad |S(p; a, c)| \leq (k-1)p^{1/2}.$$

The bound (2.3) is a special case of the bound of Bombieri [2, Theorem 6] for exponential sums along a curve. An important special case of [2, Theorem 6] can be formulated as follows.

Lemma 2. *Let $F(X, Y), G(X, Y)$ be polynomials over the finite field \mathbb{F}_p of p elements of degrees d_1 and d_2 , respectively. If the polynomial G is not constant along the curve $F(x, y) = 0$ then*

$$\left| \sum_{\substack{x, y \in \mathbb{F}_p \\ F(x, y) = 0}} \mathbf{e}(G(x, y)) \right| \leq (d_1^2 + 2d_1d_2 - 3d_1) p^{1/2} + d_1^2.$$

Next, we recall the following approximation result given by [14, Lemma 4.2] which we present in a slightly simplified form.

Lemma 3. *Suppose that F is a function with a continuous second derivative $F''(x)$ and a monotonic first derivative $F'(x)$ in the interval $[1, P]$, and such that for some integers H_1 and H_2 we have $H_1 < F'(\alpha) < H_2$ for all $\alpha \in [1, P]$. Then*

$$\sum_{1 \leq x \leq P} \mathbf{e}(F(x)) = \sum_{n=H_1}^{H_2} \int_1^P \mathbf{e}(F(\alpha) - h\alpha) d\alpha + O(\log H),$$

where $H = \max\{2, |H_1|, |H_2|\}$.

We also need the following elementary result whose proof can be obtained from that of [4, Lemma 2.2] by means of purely typographical changes (replacing x^k with $\varphi(x)$).

Lemma 4. *For any positive integer q and any integer c we have*

$$\sum_{b=1}^q |S(q; b, c)| \leq q^{3/2}.$$

We then have the following straightforward modification of [5, Theorem 3] or [14, Theorem 4.1].

Lemma 5. *Let $\varphi \in \mathbb{Z}[X]$ be a polynomial of degree $k \geq 2$. Suppose that $\gamma \in \mathbb{Q}$ with $\gamma = c/p$ in lowest terms, where p is a prime number, and fix $a \in \mathbb{Z}$ such that $|\alpha - a/p| \leq (2p)^{-1}$. Set then $\beta = \alpha - a/p$. In this notation we have*

$$g(\alpha, \gamma) = p^{-1}S(p; a, c)I(\beta) + O(p^{1/2} \log p).$$

Proof. Since $\gamma = c/p$ is in lowest terms, we have $c \not\equiv 0 \pmod{p}$.

Just like in the proof of [14, Theorem 4.1], we sort the variables into residue classes, which we then encode in terms of exponential sums. Thus

$$g(\alpha, \gamma) = \frac{1}{p} \sum_{b=1}^p S(p; a+b, c)g(\beta - b/p, 0).$$

By Lemma 3 we have $g(\beta - b/p, 0) = I(\beta - b/p) + O(1)$, so that together with Lemma 4 we find that

$$g(\alpha, \gamma) = \frac{1}{p} \sum_{b=1}^p S(p; a+b, c)I(\beta - b/p) + O(p^{1/2}).$$

Since $p \nmid c$, it follows upon deploying (2.2) and (2.3) that

$$g(\alpha, \gamma) - p^{-1}S(p; a, c)I(\beta) \ll p^{-1/2} \sum_{b=1}^{p-1} \|\beta - b/p\|^{-1} \ll p^{1/2} \log p,$$

where in the last step we use that

$$\|\beta - b/p\| \geq (2p)^{-1}$$

for all $b \not\equiv 0 \pmod{p}$. This completes the proof. \square

2.2. A lower bound on rational exponential sums

Our second main tool shows that the complete exponential sum $S(p; a, c)$ cannot be smaller than $p^{1/2}$ too often. It is useful to denote the leading coefficient of φ by $\text{lc}(\varphi)$.

Lemma 6. *Let p be a prime satisfying $p > (2k)^4$ with $p \nmid \text{lc}(\varphi)$, and let $c \in \mathbb{Z}$ with $p \nmid c$. Then there exists $a \in \mathbb{Z}$ with $p \nmid (a+c)$ such that*

$$|S(p; a, a+c)| \geq \frac{1}{2}p^{1/2}.$$

Proof. When $k=2$, the desired result follows from classical bounds on Gauss sums, so it is sufficient to consider the case when $k \geq 3$. By averaging and shifting the variable of summation, the result follows if we can show that

$$(2.4) \quad \sum_{a=1}^{p-1} |S(p; a-c, a)|^2 \geq \frac{1}{2}p^2$$

for all primes $p > (2k)^4$ not dividing $\text{lc}(\varphi)$.

We begin by noting that

$$\sum_{a=1}^{p-1} |S(p; a-c, a)|^2 = p \sum_{\substack{m,n=1 \\ \varphi(m)+m \equiv \varphi(n)+n \pmod{p}}}^p e\left(\frac{c(m-n)}{p}\right) - \left| \sum_{m=1}^p e\left(\frac{cm}{p}\right) \right|^2.$$

The second sum vanishes, and in the first one we make the change of variables $n=m-h$ and isolate the term corresponding to $h=0$. Hence

$$(2.5) \quad \sum_{a=1}^{p-1} |S(p; a-c, a)|^2 = p^2 + p \sum_{m=1}^p \sum_{\substack{h=1 \\ \Delta(m,h) \equiv 0 \pmod{p}}}^{p-1} e(ch),$$

where we put

$$\Delta(m, h) = (\varphi(m+h) - \varphi(m) + h)/h.$$

Hence, upon re-inserting in the term corresponding to $h=0$ in the sum on the right-hand side of (2.5) we discern that

$$(2.6) \quad \left| \sum_{m=1}^p \sum_{\substack{h=1 \\ \Delta(m,h) \equiv 0 \pmod{p}}}^{p-1} e(ch) \right| \leq \left| \sum_{\substack{m,h=1 \\ \Delta(m,h) \equiv 0 \pmod{p}}}^p e(ch) \right| + \left| \sum_{\substack{m=1 \\ \Delta(m,0) \equiv 0 \pmod{p}}}^p \right|.$$

If $k \geq 2$, then $\Delta(X, Y)$ is a nontrivial polynomial in two variables of degree exactly $k-1$, so the congruence

$$\Delta(m, h) \equiv 0 \pmod{p}$$

defines a curve over the finite field \mathbb{F}_p of p elements. In particular, since $\Delta(X, Y)$ is a nontrivial polynomial of degree exactly $k-1$ with respect to X with the leading monomial $k \text{lc}(\varphi) X^{k-1}$, for $p > k$ and $p \nmid \text{lc}(\varphi)$ the congruence

$$\Delta(m, 0) \equiv 0 \pmod{p}, \quad m \in \{1, \dots, p\},$$

has at most $k-1$ solutions, which bounds the second sum on the right hand side of (2.6). Moreover, the variable h is not constant along this curve, so we may apply

Lemma 2 (with $d_1=k-1$ and $d_2=1$) to the first sum. Thus altogether, after simple calculations, we find that

$$(2.7) \quad \left| \sum_{m=1}^p \sum_{\substack{h=1 \\ \Delta(m,h) \equiv 0 \pmod{p}}}^{p-1} e(ch) \right| \leq ((k-1)^2 + 2(k-1) - 3) \sqrt{p} + (k-1)^2 + k - 1.$$

Under our assumption $p > (2k)^4$, for the right hand side in (2.7) we have

$$\begin{aligned} & ((k-1)^2 + 2(k-1) - 3) \sqrt{p} + (k-1)^2 + k - 1 \\ &= (k^2 - 4) \sqrt{p} + k(k-1) < k^2 \sqrt{p} + k^2 < \frac{1}{4}p + \frac{1}{4}\sqrt{p} < \frac{1}{2}p. \end{aligned}$$

In view of (2.5), we derive (2.4), which is sufficient to establish the result. \square

3. Proof of the main result

The following result, going back to Duffin and Schaeffer [10], is a key ingredient in our arguments as it allows us to focus on those $\alpha \in \mathbb{T}$ whose rational approximations have prime denominators.

Lemma 7. *There is a set $\mathcal{C} \subseteq \mathbb{T}$ of full Lebesgue measure such that for any $\alpha \in \mathcal{C}$ there are infinitely many approximations*

$$\left| \alpha - \frac{a}{p} \right| < \frac{1}{p^2 \log \log p}$$

with $a \in \mathbb{Z}$ and p being a prime number.

Proof. Since

$$\sum_p \frac{1}{p \log \log p} = \infty \quad \text{and} \quad \sum_p \frac{p-1}{p \log \log p} \geq \frac{1}{2} \sum_p \frac{1}{\log \log p}$$

this is a direct application of [10, Theorem I]. \square

We also remark that Lemma 7 is a special case of the Duffin-Schaeffer conjecture, recently established as a theorem by Koukoulopoulos and Maynard [12].

We now have the wherewithal to embark on the proof of Theorem 1. Fix $\tau > 0$, and let $\alpha_2 \in \mathcal{C}$, where \mathcal{C} is as in Lemma 7. Then we can find an arbitrarily large prime number p , and $a_2 \in \mathbb{Z}$ not divisible by p , that satisfy $|\alpha_2 - a_2/p| \leq p^{-2}(\log \log p)^{-1}$. For any fixed such p satisfying $p > (2k)^4$ and not dividing $\text{lc}(\varphi)$, define P via the relation

$$(3.1) \quad P = \frac{1}{2}p^2 \log \log p.$$

Lemma 6 now guarantees the existence of an integer a_1 with $a_1 + a_2 \not\equiv 0 \pmod{p}$ and having the property that

$$(3.2) \quad |S(p; a_1, a_1 + a_2)| \gg p^{1/2}.$$

Take now $\beta_2 = \alpha_2 - a_2/p$ and $\beta_1 = -\beta_2$, and put $\alpha_1 = a_1/p + \beta_1$. Then upon recalling that $\gamma = \alpha_1 + \alpha_2$ in (2.1), we see that $\gamma = c/p$ with $c = a_1 + a_2 \not\equiv 0 \pmod{p}$, whereupon Lemma 5 yields the relation

$$g(\alpha_1, \gamma) = p^{-1} S(p; a_1, a_1 + a_2) I(\beta_1) + O(p^{1/2} \log p).$$

Recall now our definition of P from (3.1). Since

$$|\beta_1| = |\beta_2| \leq p^{-2} (\log \log p)^{-1} = (2P)^{-1},$$

and the elementary fact that $\eta^{-1} \sin \eta \geq 2/\pi$ for $|\eta| \leq \pi/2$, it follows further from (2.2) that

$$|I(\beta_1)| \geq P/2,$$

so upon inserting (3.2) we discern that

$$|g(\alpha_1, \gamma)| \gg P p^{-1/2} \gg P^{3/4} (\log \log P)^{1/4}.$$

In the light of (2.1) and Lemma 7, this establishes the desired result.

Acknowledgement. The authors would like to thank James Maynard for drawing our attention to a result of Duffin and Schaeffer [10, Theorem I] on Diophantine approximations with prime denominators.

During the preparation of this manuscript, JB was supported by Starting Grant no. 2017-05110 of the Swedish Science Foundation (Vetenskapsrådet) and IS was supported by the Australian Research Council Grant DP170100786.

References

1. BARRON, A., An L^4 maximal estimate for quadratic Weyl sums, to appear in *Int. Math. Res. Not. (IMRN)*. [MR4514444](#)
2. BOMBIERI, E., On exponential sums in finite fields, *Amer. J. Math.* **88** (1966), 71–105. [MR0200267](#)
3. BOURGAIN, J., DEMETER, C. and GUTH, L., Proof of the main conjecture in Vinogradov’s mean value theorem for degrees higher than three, *Ann. of Math.* **184** (2016), 633–682. [MR3548534](#)
4. BRANDES, J., PARSELL, S. T., POULIAS, C., SHAKAN, G. and VAUGHAN, R. C., On generating functions in additive number theory, II: lower order terms and applications to PDEs, *Math. Ann.* **379** (2021), 347–376. [MR4211090](#)

5. BRÜDERN, J. and ROBERT, O., Rational points on linear slices of diagonal hypersurfaces, *Nagoya Math. J.* **218** (2015), 51–100. [MR3345624](#)
6. CHEN, C., KERR, B., MAYNARD, J. and SHPARLINSKI, I. E., Metric theory of Weyl sums, to appear in *Math. Ann.* [MR4542717](#)
7. CHEN, C. and SHPARLINSKI, I. E., New bounds of Weyl sums, *Int. Math. Res. Not. IMRN* **2021** (2021), 8451–8491. [MR4298525](#)
8. CHEN, C. and SHPARLINSKI, I. E., On a hybrid version of the Vinogradov mean value theorem, *Acta Math. Hungar.* **163** (2021), 1–17. [MR4217954](#)
9. CHEN, C. and SHPARLINSKI, I. E., Hybrid bounds on two-parametric families of Weyl sums along smooth curves, to appear in *Michigan Math. J.* [MR4555223](#)
10. DUFFIN, R. J. and SCHAEFFER, A. C., Khintchine’s problem in metric Diophantine approximation, *Duke Math. J.* **8** (1941), 243–255. [MR0004859](#)
11. ERDOĞAN, M. B. and SHAKAN, G., Fractal solutions of dispersive partial differential equations on the torus, *Selecta Math. (N.S.)* **25** (2019), 1–26. Art., 11. [MR3910065](#)
12. KOUKOULOPOULOS, D. and MAYNARD, J., On the Duffin-Schaeffer conjecture, *Ann. of Math.* **192** (2020), 251–307. [MR4125453](#)
13. SCHMIDT, W. M., *Equations over finite fields – An elementary approach*, Lecture Notes in Mathematics **536**, Springer, Berlin, 1976. [MR0429733](#)
14. VAUGHAN, R. C., *The Hardy–Littlewood method*, Cambridge Tracts in Mathematics **125**, Cambridge University Press, Cambridge, 1997. [MR1435742](#)
15. WOOLEY, T. D., Perturbations of Weyl sums, *Int. Math. Res. Not. IMRN* **2016** (2016), 2632–2646. [MR3519125](#)
16. WOOLEY, T. D., Nested efficient congruencing and relatives of Vinogradov’s mean value theorem, *Proc. Lond. Math. Soc.* **118** (2019), 942–1016. [MR3938716](#)

Julia Brandes
Mathematical Sciences
University of Gothenburg and Chalmers
Institute of Technology
412 96 Göteborg
Sweden
brjulia@chalmers.se

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

Received February 8, 2022
in revised form November 17, 2022