Canad. Math. Bull. Vol. **64** (1), 2021, pp. 192–203
http://dx.doi.org/10.4153/S0008439520000363

Möbius Randomness Law for Frobenius Traces of Ordinary Curves

Min Sha and Igor E. Shparlinski

Abstract. Recently E. Bombieri and N. M. Katz (2010) demonstrated that several well-known results about the distribution of values of linear recurrence sequences lead to interesting statements for Frobenius traces of algebraic curves. Here we continue this line of study and establish the Möbius randomness law quantitatively for the normalised form of Frobenius traces.

1 Introduction

1.1 Background on Frobenius Traces

Throughout the paper, $\mathcal{C}$ denotes a smooth projective curve over a finite field $\mathbb{F}_q$ of q elements. Following Bombieri and Katz [4], we consider the sequence $A_{\mathcal{C}}(n)$ of *Frobenius traces* defined by

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = q^n + 1 - A_{\mathcal{C}}(n),$$

where $\#\mathcal{C}(\mathbb{F}_{q^n})$ is the cardinality of the set $\mathcal{C}(\mathbb{F}_{q^n})$ of $\mathbb{F}_{q^n}$-rational points on $\mathcal{C}$.

Let g be the genus of $\mathcal{C}$, and assume $g \geqslant 1$. Since by the Weil bound (see [17, Section VIII.5.9]), we have

$$|A_{\mathcal{C}}(n)| \leqslant 2gq^{n/2},$$

it is convenient to normalise the sequence $A_{\mathcal{C}}(n)$ as

$$a_{\mathcal{C}}(n) = \frac{A_{\mathcal{C}}(n)}{2gq^{n/2}} \in [-1,1], \tag{1.1}$$

which is called the *normalised Frobenius trace*.

1.2 Some Previous Results

Here we recall some previous results on the distribution of the sequence $a_{\mathcal{C}}(n)$ given by (1.1). First, we recall that Bombieri and Katz [4], using an interpretation of $A_{\mathcal{C}}(n)$ as a linear recurrence sequence of order $2g$, showed that $|a_{\mathcal{C}}(n)|$ is not too

Received by the editors November 5, 2019; revised March 25, 2020.
Published online on Cambridge Core May 15, 2020.
During the preparation of this paper, the first author was supported by the Australian Research Council Grant DE190100888, and the second author was partially supported by the Australian Research Council Grant DP180100201.
AMS subject classification: **11B37, 11G20, 11J25, 11J86, 11L07.**
Keywords: Möbius randomness law, smooth projective curve, Frobenius trace, Frobenius angle.

small. More precisely, by [4, Theorem 3.1], for any $\varepsilon > 0$, there is a constant $c(\varepsilon) > 0$ depending only on ε such that for every n, either $a_{\mathcal{C}}(n) = 0$ or $|a_{\mathcal{C}}(n)| \geqslant c(\varepsilon) g^{-1} q^{-n\varepsilon}$. However, unless $g = 1$ (that is, $\mathcal{C}$ is an elliptic curve), the constant $c(\varepsilon)$ is not effectively computable. Using the argument of [7, Theorem 2.6], one can give a stronger and fully effective bound of the form

$$|a_{\mathcal{C}}(n)| \geqslant n^{-\psi(n)},$$

which for any function $\psi(z) \to \infty$ as $z \to \infty$, holds for almost all n in the sense of asymptotic density.

The asymptotic distribution of the values $a_{\mathcal{C}}(n)$ in the interval $[-1, 1]$ was studied in [1], where it is shown that this distribution differs from the usually occurring Sato–Tate law [13, 14]. On the other hand, an asymptotic formula for the average ℓ-adic order of $A_{\mathcal{C}}(n)$ for a prime $\ell \nmid q$ was given in [21, Theorem 4].

Several related results about the distribution of Kloosterman and Birch sums have recently been given by Perret and Gentil [19].

We also note that using the upper bound of van der Poorten and Schlickewei [20, Theorem 1], on the number of zeros of linear recurrence sequences, one can estimate the number of zero values $a_{\mathcal{C}}(n) = 0$ in a better way that is outlined in [4, Section 5] (via uniform bounds on the number of zeros of linear recurrence sequences such as in [2, 8]).

The second part of our motivations comes from the so-called *Möbius randomness law* (see, for example, [12, Section 13.1] and also Sarnak's conjecture [23]), which roughly asserts that for any bounded sequence $s(n)$ of complex numbers, defined in terms that are not directly related to $\mu(n)$, we have

$$\sum_{n=1}^{N} \mu(n) s(n) = o(N), \quad \text{as } N \longrightarrow \infty.$$

Here, we establish quantitatively the Möbius randomness law for the sequence $a_{\mathcal{C}}(n)$ defined in (1.1).

1.3 Our Results

We recall that the Möbius function is defined as $\mu(n) = 0$ if an integer n is divisible by a prime squared and $\mu(n) = (-1)^r$ if n is a product of r distinct primes.

Our main result is Theorem 1.2. However, for the completeness, we also record Theorem 1.1.

Theorem 1.1 *For any $B > 0$ and for any integer $N \geqslant 2$, we have*

$$\left| \sum_{n=1}^{N} \mu(n) a_{\mathcal{C}}(n) \right| \leqslant c(B) N (\log N)^{-B},$$

where $c(B) > 0$ is a constant depending only on B.

When $\mathcal{C}$ is an *ordinary curve*, we can get a better result. Recall that $\mathcal{C}$ is called ordinary if and only if the number of p-torsion points on the Jacobian of $\mathcal{C}$ is exactly

https://doi.org/10.4153/S0008439520000363 Published online by Cambridge University Press

p^g, where p is the characteristic of $\mathbb{F}_q$ (see [11, Definition 3.1] for some equivalent definitions).

Recall that the assertion $U \ll V$ is equivalent to the inequality $|U| \leqslant cV$ with some *absolute* constant $c > 0$.

Theorem 1.2 *If $\mathcal{C}$ is an ordinary curve of genus $g \geqslant 1$, for any integer $N \geqslant 2$ we have*

$$\sum_{n=1}^{N} \mu(n) a_{\mathcal{C}}(n) \ll N^{1-1/\gamma(q,\,g)} (\log N)^4,$$

where

$$\gamma(q,\,g) = 2^{33} 3^3 \pi g^3 (\pi + \log q) \log(16g) + 4.$$

We remark that the constant $c(B)$ in Theorem 1.1 is currently not effectively computable. For the implied constant in Theorem 1.2, it is effectively computable (due to the effectiveness of Lemma 2.4), but getting an explicit value of this constant is beyond the scope of this paper.

To prove the above results, we first interpret the normalised Frobenius traces as linear recurrence sequences via the zeta function (see (2.11)). Then Theorem 1.1 is an immediate application of a result of Davenport [6], given by (2.6) below, on bounds on exponential sums with $\mu(n) \exp(2\pi i \alpha)$ for $\alpha \in \mathbb{R}$, and Theorem 1.2 is a consequence of an improvement of (2.6) when some Diophantine properties of α are known (see Lemma 2.5). More precisely, this improvement relies on a lower bound of the denominator in Dirichlet's approximation of an irrational number α when $\exp(2\pi i \alpha)$ is an algebraic number (see Lemma 2.3). Here, we are able to take advantage of this stronger bound in the case of Theorem 1.2 (see Lemma 2.7).

2 Preliminaries

2.1 Linear Form in the Logarithms of Algebraic Numbers

The main tool in this paper is Baker's theory of linear forms in the logarithms of algebraic numbers; see [5]. Here we restate one of its explicit forms due to Baker and Wüstholz [3].

First, recall that for a non-zero complex number z, the principal value of the natural logarithm of $z \in \mathbb{C}$ is

$$\log z = \log |z| + i \cdot \mathrm{Arg}(z),$$

where as usual, i is the imaginary unit, and $\mathrm{Arg}(z)$ is the principal value of the arguments of z ($0 \leqslant \mathrm{Arg}(z) < 2\pi$).

Let

$$\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + \cdots + b_n \log \alpha_n,$$

where $n \geqslant 2$, $b_1, \ldots, b_n \in \mathbb{Z}$, and $\alpha_1, \ldots, \alpha_n$ are non-zero elements of a number field K. Let $d = [K : \mathbb{Q}]$ and $B = \max\{|b_1|, \ldots, |b_n|\}$. For all $1 \leqslant j \leqslant n$, choose a real number

https://doi.org/10.4153/S0008439520000363 Published online by Cambridge University Press

A_j such that

$$A_j \geqslant \max\left\{\mathrm{h}(\alpha_j), |\log \alpha_j|/d, 1/d\right\},$$

where h stands for the logarithmic absolute Weil height (note that the height function used in [3] is different from ours).

Suppose that $\Lambda \neq 0$. Then we have

$$\log|\Lambda| > -C(n,d)A_1 \cdots A_n \cdot \max\{\log B, 1/d\}, \tag{2.1}$$

where

$$C(n,d) = 18(n+1)!n^{n+1}(32d)^{n+2}\log(2nd).$$

We remark that we in fact only need a lower bound on linear forms in two logarithms of the form in [16, Théorème 3]. However, the lower bound in [16, Théorème 3] essentially has the term $(\log B)^2$. This is not sufficient for our purpose. Alternatively, using [10, Theorem 2.1] one can obtain such a lower bound having the term $\log B$.

In addition, there is another explicit form of Baker's theory due to Matveev [18, Corollary 2.3]. However, for our purpose, Baker and Wüstholz [3] gives a slightly better result.

2.2 Lower Bounds for Diophantine Approximations

The famous theorem of Roth [22] states that given an irrational algebraic number α and $\varepsilon > 0$, there exists a constant $c(\alpha,\varepsilon) > 0$ such that for any integers r, s with $s > 0$, we have

$$\left|\alpha - \frac{r}{s}\right| > \frac{c(\alpha,\varepsilon)}{s^{2+\varepsilon}}. \tag{2.2}$$

Certainly, in general, for real transcendental numbers, no such bound is possible. Here, using Baker's theory of linear forms in logarithms (see [5]), we obtain such a lower bound for a special kind of real transcendental numbers, namely, for irrational arguments of algebraic numbers.

Now, let α be an irrational number. Define

$$\mathbf{e}(\alpha) = e^{2\pi i \alpha},$$

where, as usual, e is the base of the natural logarithm. If $\mathbf{e}(\alpha)$ is an algebraic number, then by the Gelfond–Schneider theorem, we know that α must be a transcendental number. Indeed, assume that α is an algebraic number; then by the Gelfond–Schneider theorem, $1 = \mathbf{e}(\alpha)^{1/\alpha}$ is a transcendental number, which is impossible.

The following result gives such a lower bound for any irrational number α when $\mathbf{e}(\alpha)$ is an algebraic number. This can be viewed as a Diophantine property of the arguments of algebraic numbers. In fact, $1 + \kappa(\alpha)$ is an upper bound of the *irrationality exponent* of α.

We also remark that the following result is essentially a variant of [4, Theorem 4.1]. Following the same strategy, we provide a proof for the convenience of the reader and also put it in a form suitable for our applications.

Lemma 2.1 *Let α be an irrational number. Assume that $\mathbf{e}(\alpha)$ is an algebraic number. Then, for any integers r, s with $s \geqslant 1$, we have*

$$\left|\alpha - \frac{r}{s}\right| > \frac{1}{\pi(2s)^{1+\kappa(\alpha)}},$$

where

$$\kappa(\alpha) = 2^{25}3^3\pi d^3 A_1 \log(4d),$$
$$d = [\mathbb{Q}(\mathbf{e}(\alpha)) : \mathbb{Q}],$$
$$A_1 = \max\{\mathrm{h}(\mathbf{e}(\alpha)), 2\pi\alpha/d, 1/d\}.$$

Proof We can always replace α with its fractional part $\{\alpha\}$. Hence, without loss of generality, we assume that $0 < \alpha < 1$ and $\gcd(r, s) = 1$. Then if $|r| > s$, we have

$$\left|\alpha - \frac{r}{s}\right| > \frac{1}{s},$$

which is better than the desired result. In the sequel, we assume $|r| \leqslant s$.

Denote

$$\Delta = \alpha - \frac{r}{s}.$$

Then, since $0 < \alpha < 1$, we have

$$\log \mathbf{e}(\alpha) = 2\pi i\alpha = 2\pi i\Big(\Delta + \frac{r}{s}\Big),$$

and so

$$2s\pi i\Delta = s\log \mathbf{e}(\alpha) - 2r\pi i = s\log \mathbf{e}(\alpha) - 2r\log(-1).$$

Denote

$$\Lambda = s\log \mathbf{e}(\alpha) - 2r\log(-1).$$

So,

$$|\Delta| = \frac{|\Lambda|}{2\pi s}. \tag{2.3}$$

Note that α is an irrational number. So, $\mathbf{e}(\alpha)$ is not a root of unity, and thus $\Lambda \neq 0$. Using (2.1) with $n = 2$, we obtain

$$\log|\Lambda| > -C(d)A_1A_2 \cdot \max\{\log B, 1/d\}, \tag{2.4}$$

where

$$C(d) = C(2, d) = 2^{25}3^3 d^4 \log(4d),$$
$$d = [\mathbb{Q}(\mathbf{e}(\alpha)) : \mathbb{Q}],$$
$$A_1 = \max\{\mathrm{h}(\mathbf{e}(\alpha)), 2\pi\alpha/d, 1/d\}, \quad A_2 = \pi/d,$$
$$B = \max\{s, 2|r|\}.$$

https://doi.org/10.4153/S0008439520000363 Published online by Cambridge University Press

Since $|r| \leqslant s$, we have $B \leqslant 2s$. In view of $s \geqslant 1$ and $d \geqslant 2$, we get

$$\max\{\log B, 1/d\} \leqslant \log(2s).$$

Hence, inequality (2.4) becomes

$$\log|\Lambda| > -2^{25}3^3\pi d^3 \log(4d) A_1 \log(2s),$$

which, together with (2.3), implies the desired result. ■

2.3 Dirichlet's Theorem

We first recall *Dirichlet's theorem* in Diophantine approximation; see, for example, [12, Equation (20.29)].

Lemma 2.2 *Let α be an irrational number. Then, for any integer $N \geqslant 2$, there are two integers r, s such that*

$$0 < \left|\alpha - \frac{r}{s}\right| \leqslant \frac{1}{sN}, \quad 1 \leqslant s \leqslant N, \ \gcd(r, s) = 1.$$

In Lemma 2.2, if N tends to infinity, then s also goes to infinity. It is natural to ask how large s can be. If α is an irrational algebraic number, combining Lemma 2.2 with the bound (2.2), we have

$$s > \left(c(\alpha, \varepsilon)N\right)^{1/(1+\varepsilon)}. \tag{2.5}$$

The next result follows directly from Lemmas 2.1 and 2.2.

Lemma 2.3 *Let α be an irrational number. Assume that $\mathbf{e}(\alpha)$ is an algebraic number. Then, for any integer $N \geqslant 2$, there are integers r, s such that*

$$0 < \left|\alpha - \frac{r}{s}\right| \leqslant \frac{1}{sN}, \quad 1 \leqslant s \leqslant N, \ \gcd(r, s) = 1,$$

and

$$s > \frac{1}{2}\left(N/(2\pi)\right)^{1/\kappa(\alpha)},$$

where $\kappa(\alpha)$ has been defined in Lemma 2.1.

2.4 Exponential Sums with Möbius Function

Recall the following bound of exponential sums with Möbius function, which depends on the Diophantine properties of the exponent α; see [12, Theorem 13.9]. It can be viewed as a variant of the modern form of the Vinogradov bound for exponential sums over primes; see [12, Section 13.5] for more details.

Lemma 2.4 *Suppose that the real α satisfies*

$$\left|\alpha - \frac{r}{s}\right| \leqslant \frac{1}{s^2}$$

for some integers r, s *with* $s > 0$ *and* $\gcd(r, s) = 1$. *Then, for any integer* $N \geqslant 2$, *we have*

$$\sum_{n=1}^{N} \mu(n)\mathbf{e}(n\alpha) \ll \left(s^{1/4}N^{1/4} + s^{-1/4}N^{1/2} + N^{2/5}\right)N^{1/2}(\log N)^4.$$

We remark that the implied constant in Lemma 2.4 is effectively computable, but getting an explicit value of this constant is beyond the scope of this paper.

In addition, Davenport [6] (see also [12, Theorem 13.10]) has established the following general result: for any real number α and $N \geqslant 2$, we have

$$\left|\sum_{n=1}^{N} \mu(n)\mathbf{e}(n\alpha)\right| \leqslant c(B)N(\log N)^{-B} \tag{2.6}$$

for any $B > 0$, where $c(B) > 0$ is a constant depending only on B. We remark that the constant $c(B)$ is currently not effectively computable. The upper bound in (2.6) has the very attractive feature that it is independent of α.

Involving the dependence on α, the bound (2.6) can be improved for some special cases.

Lemma 2.5 *Let* α *be an irrational number. Assume that* $\mathbf{e}(\alpha)$ *is an algebraic number. Then, for any integer* $N \geqslant 2$, *we have*

$$\sum_{n=1}^{N} \mu(n)\mathbf{e}(n\alpha) \ll N^{1-1/(4\kappa(\alpha)+4)}(\log N)^4,$$

where $\kappa(\alpha)$ *has been defined in Lemma 2.1.*

Proof By Lemma 2.3, for any integer $M \geqslant 2$, there are integers r, s such that

$$0 < \left|\alpha - \frac{r}{s}\right| \leqslant \frac{1}{sM}, \quad 1 \leqslant s \leqslant M, \ \gcd(r, s) = 1,$$

and

$$s > \frac{1}{2}\left(M/(2\pi)\right)^{1/\kappa(\alpha)},$$

where $\kappa(\alpha)$ has been defined in Lemma 2.1. Then, by Lemma 2.4, we have

$$\sum_{n=1}^{N} \mu(n)\mathbf{e}(n\alpha) \ll \left(s^{1/4}N^{1/4} + s^{-1/4}N^{1/2} + N^{2/5}\right)N^{1/2}(\log N)^4. \tag{2.7}$$

Note that

$$\frac{1}{2}\left(M/(2\pi)\right)^{1/\kappa(\alpha)} < s \leqslant M,$$

hence

$$s^{1/4}N^{1/4} + s^{-1/4}N^{1/2} \ll M^{1/4}N^{1/4} + M^{-1/(4\kappa(\alpha))}N^{1/2},$$

which with

$$M = \left\lceil N^{\kappa(\alpha)/(\kappa(\alpha)+1)} \geqslant 2\right\rceil$$

becomes

$$s^{1/4}N^{1/4} + s^{-1/4}N^{1/2} \ll N^{1/2-1/(4\kappa(\alpha)+4)}.$$

Substituting this into (2.7), we see that the term $N^{9/10}$ never dominates, and we obtain the desired result. ■

From the above proof, one can see that if an irrational number α has a Diophantine property as in Lemma 2.3, then the upper bound (2.6) can be improved similarly. For example, this can be done for irrational algebraic numbers by (2.5).

2.5 Frobenius Eigenvalues and Angles

We refer the reader to [17] for a background on curves and their zeta-functions.

For a smooth projective curve $\mathcal{C}$ over the finite field $\mathbb{F}_q$, we define the zeta-function of $\mathcal{C}$ as

$$Z(T) = \exp\Big(\sum_{n=1}^{\infty} \#\mathcal{C}(\mathbb{F}_{q^n})\frac{T^n}{n}\Big).$$

It is well known that if $\mathcal{C}$ is of genus $g \geqslant 1$, then

$$Z(T) = \frac{P(T)}{(1-T)(1-qT)},$$

where

$$P(T) = \prod_{j=1}^{2g}(1-\beta_j T)$$

is a polynomial of degree $2g$ with integer coefficients, and $\beta_1, \beta_2, \dots, \beta_{2g}$ are algebraic integers, called the *Frobenius eigenvalues*, which satisfy

$$|\beta_j| = q^{1/2}, \qquad j = 1, 2, \dots, 2g; \tag{2.8}$$

see [17, Section VIII.5]. Then, for each β_j, since all its conjugates have absolute value $q^{1/2}$, we have (via the Mahler measure, see [24, Lemma 3.10])

$$\mathrm{h}(\beta_j) = \frac{1}{2}\log q, \qquad j = 1, 2, \dots, 2g. \tag{2.9}$$

Furthermore, in view of (2.8), we write

$$\beta_j = q^{1/2}\mathbf{e}(\alpha_j), \tag{2.10}$$

with some $\alpha_j \in [0, 1)$, $j = 1, 2, \dots, 2g$. Usually, these $2\pi\alpha_j$ are called *Frobenius angles*. We then call α_j *normalised Frobenius angles*. Now simple combinatorial arguments lead to the well-known identity

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{2g}\beta_j^n,$$

https://doi.org/10.4153/S0008439520000363 Published online by Cambridge University Press

which implies

$$a_{\mathcal{C}}(n) = \frac{1}{2g}\sum_{j=1}^{2g} \mathbf{e}(n\alpha_j). \tag{2.11}$$

This is crucial for our approach.

2.6 Diophantine Properties of Normalised Frobenius Angles

We recall the following irrationality property of normalised Frobenius angles given by [1, Lemma 8]

Lemma 2.6 *Suppose that $\mathcal{C}$ is an ordinary smooth projective curve of genus $g \geqslant 1$ over $\mathbb{F}_q$. Then all its normalised Frobenius angles α_j, $j = 1, 2, \dots, 2g$, are irrational.*

Now, we can use Lemma 2.1 to obtain a Diophantine property for the normalised Frobenius angles.

Lemma 2.7 *Suppose that $\mathcal{C}$ is an ordinary smooth projective curve of genus $g \geqslant 1$ over $\mathbb{F}_q$. Let α be an arbitrary normalised Frobenius angle of $\mathcal{C}$. Then, for any integers r, s with $s \geqslant 1$, we have*

$$\left|\alpha - \frac{r}{s}\right| > \frac{1}{\pi(2s)^{1+\kappa(q,\,g)}},$$

where

$$\kappa(q,\, g) = 2^{31}3^3\pi g^3(\pi + \log q)\log(16g).$$

Proof Let β be the Frobenius eigenvalue corresponding to α as defined in (2.10). That is, $\beta = q^{1/2}\mathbf{e}(\alpha)$. Hence, $\mathbf{e}(\alpha)$ is an algebraic number. Besides, by Lemma 2.6, α is an irrational number. Then, appying Lemma 2.1, we have that for any integers r, s with $s \geqslant 1$,

$$\left|\alpha - \frac{r}{s}\right| > \frac{1}{\pi(2s)^{1+\kappa(\alpha)}},$$

where

$$\begin{aligned} \kappa(\alpha) &= 2^{25}3^3\pi d^3\log(4d)A_1, \\ d &= [\mathbb{Q}(\mathbf{e}(\alpha)) : \mathbb{Q}], \\ A_1 &= \max\{\mathrm{h}(\mathbf{e}(\alpha)), 2\pi\alpha/d, 1/d\}. \end{aligned}$$

Since $\deg\beta \leqslant 2g$, we have

$$d = \left[\mathbb{Q}(\mathbf{e}(\alpha)) : \mathbb{Q}\right] = \left[\mathbb{Q}(\beta q^{-1/2}) : \mathbb{Q}\right] \leqslant 2\deg\beta \leqslant 4g.$$

Using (2.9), we obtain

$$\mathrm{h}(\mathbf{e}(\alpha)) = \mathrm{h}(\beta q^{-1/2}) \leqslant \mathrm{h}(\beta) + \mathrm{h}(q^{1/2}) = \log q.$$

Note that we must have $d \geqslant 2$. So, we have $A_1 \leqslant \pi + \log q$. Hence, we get

$$\kappa(\alpha) \leqslant 2^{31} 3^3 \pi g^3 (\pi + \log q) \log(16g).$$

This completes the proof. ∎

3 Proofs of the Main Results

3.1 Proof of Theorem 1.1

By (2.11), we have

$$\Big|\sum_{n=1}^{N} \mu(n) a_{\mathcal{C}}(n)\Big| \leqslant \frac{1}{2g} \sum_{j=1}^{2g} \Big|\sum_{n=1}^{N} \mu(n) \mathbf{e}(n\alpha_j)\Big|.$$

Then the desired result follows directly from the bound (2.6).

3.2 Proof of Theorem 1.2

Let $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ be the normalised Frobenius angles of $\mathcal{C}$. For each α_j, using Lemmas 2.5 and 2.7, we have that for any integer $N \geqslant 2$,

$$\sum_{n=1}^{N} \mu(n) \mathbf{e}(n\alpha_j) \ll N^{1-1/(4\kappa(q,\, g)+4)} (\log N)^4, \tag{3.1}$$

where $\kappa(q,\ g)$ has been defined in Lemma 2.7.

So, combining (2.11) with (3.1), for any integer $N \geqslant 2$, we have

$$\begin{aligned} \Big|\sum_{n=1}^{N} \mu(n) a_{\mathcal{C}}(n)\Big| &= \frac{1}{2g} \Big|\sum_{n=1}^{N} \mu(n) \sum_{j=1}^{2g} \mathbf{e}(n\alpha_j)\Big| \\ &\leqslant \frac{1}{2g} \sum_{j=1}^{2g} \Big|\sum_{n=1}^{N} \mu(n) \mathbf{e}(n\alpha_j)\Big| \\ &\ll N^{1-1/(4\kappa(q,\, g)+4)} (\log N)^4. \end{aligned}$$

This completes the proof.

4 Comments

We remark that our methods also apply to the sequences of character sums

$$\mathcal{S}_R(n) = \frac{1}{q^{n/2}} \sum_{x \in \mathbb{F}_{q^n}^*} \psi\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(R(x))\right),$$

where $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$, ψ is a fixed additive character of $\mathbb{F}_q$ and $R(X) \in \mathbb{F}_q(X)$. We recall that if $R(X)$ is not of the form $R(X) = Q(X)^p - Q(X)$ for any other function $Q(X) \in \mathbb{F}_q(X)$, where p is the characteristic of $\mathbb{F}_q$, then $\mathcal{S}_R(n)$ can be expressed as a power sum of the same type as (2.11); see [12, Section 11.11]. Hence, a full analogue of Theorem 1.1 holds for these sums for any $R(X) \in \mathbb{F}_q(X)$, such that $R(X) \neq Q(X)^p - Q(X)$ for any $Q(X) \in \mathbb{F}_q(X)$.

The situation with an analogue of Theorem 1.2 is more complicated as one needs an irrationality of angles statement similar to Lemma 2.6, which does not seem to be readily available. There are some results in this direction in [4, 19], in particular showing that the required irrationality holds "generically" in some special cases, but they are not enough to make a conclusive statement about the sums $\mathcal{S}_R(n)$. Hence, we pose this as an question to find appropriate sufficient conditions on $R(X)$ for which an analogues of Theorem 1.2 holds for $\mathcal{S}_R(n)$.

Perhaps, it is natural to start with Kloosterman sums

$$\mathcal{K}(n) = \frac{1}{q^{n/2}} \sum_{x \in \mathbb{F}_{q^n}^*} \psi\left(\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\left(ax + x^{-1}\right)\right), \qquad n = 1, 2, \ldots,$$

where $a \in \mathbb{F}_q^*$ is a fixed element. Indeed, it is well known that for some $\vartheta \in \mathbb{C}$ with $|\vartheta| = q^{1/2}$, we have

$$\mathcal{K}(n) = \vartheta^n + \overline{\vartheta}^n, \qquad n = 1, 2, \ldots;$$

see [4, 19], where this representation is also exploited. We note that this setting is dual to that of [9, 15] where Kloosterman sums modulo a large fixed prime p (and more general trace functions) are ordered by the coefficient n in the exponent $nx + x^{-1}$, rather than by the degree of the field extension as in this setting.

Acknowledgment The authors are very grateful to the referee for valuable comments.

References

[1] O. Ahmadi and I. E. Shparlinski, *On the distribution of the number of points on algebraic curves in extensions of finite fields*. Math. Res. Lett. **17**(2010), 689–699. https://doi.org/10.4310/MRL.2010.v17.n4.a9

[2] F. Amoroso and E. Viada, *On the zeros of linear recurrence sequences.* Acta Arith. **147**(2011), 387–396. https://doi.org/10.4064/aa147-4-4

[3] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties.* J. Reine Angew. Math. **442**(1993), 19–62. https://doi.org/10.1515/crll.1993.442.19

[4] E. Bombieri and N. M. Katz, *A note on lower bounds for Frobenius traces*. Enseign. Math. **56**(2010), 203–227. https://doi.org/10.4171/LEM/56-3-1

[5] Y. Bugeaud, *Linear forms in logarithms and applications.* IRMA Lectures in Mathematics and Theoretical Physics, 28, European Math. Soc., Zürich, 2018. https://doi.org/10.4171/183

[6] H. Davenport, *On some infinite series involving arithmetical functions II.* Quart. J. Math. **8**(1937), 313–320.

[7] G. Everest, A. J. van der Poorten, I. E. Shparlinski, and T. B. Ward, Recurrence sequences. Mathematical Surveys and Mongraphs, 14, Amer. Math. Soc., Providence, RI, 2003. https://doi.org/10.1090/surv/104

[8] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*. Ann. of Math. **155**(2002), 807–836. https://doi.org/10.2307/3062133

[9] É. Fouvry, E. Kowalski, and P. Michel, *Algebraic trace functions over the primes.* Duke Math. J. **163**(2014), 1683–1736. https://doi.org/10.1215/00127094-2690587

[10] N. Gouillon, *Explicit lower bounds for linear forms in two logarithms*. J. Théor. Nombres Bordeaux **18**(2006), 125–146.

[11] E. Howe, *Principally polarized ordinary abelian varieties over finite fields.* Trans. Amer. Math. Soc. **347**(1995), 2361–2401. https://doi.org/10.2307/2154828

[12] H. Iwaniec and E. Kowalski, *Analytic number theory*. American Mathematical Society Colloquium Publications, 53, Amer. Math. Soc., Providence, RI, 2004. https://doi.org/10.1090/coll/053

[13] N. M. Katz, *Convolution and equidistribution: Sato–Tate theorems for finite field Mellin transforms*. Annals of Math. Studies, 80, Princeton University Press, Princeton, NJ, 2012.
[14] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*. American Mathematical Society Colloquium Publications, 45, Amer. Math. Soc., Providence, RI, 1999.
[15] M. A. Korolev and I. E. Shparlinski, *Sums of algebraic trace functions twisted by arithmetic functions.* Pacific J. Math. **304**(2020), 505–522. https://doi.org/10.2140/pjm.2020.304.505
[16] M. Laurent, M. Mignotte, and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation.* J. Number Theory **55**(1995), 285–321. https://doi.org/10.1006/jnth.1995.1141
[17] D. Lorenzini, *An invitation to arithmetic geometry*. Graduate Studies in Mathematics, 9, Amer. Math. Soc., Providence, RI, 1996. https://doi.org/10.1090/gsm/009
[18] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II*. Izv. Math. **64**(2000), 1217–1269. https://doi.org/10.1070/IM2000v064n06ABEH000314
[19] C. Perret-Gentil, *Roots of L-functions of characters over function fields, generic linear independence and biases.* Algebr. Number Theory 14(2020), 1291–1329. https://doi.org/10.2140/ant.2020.14.1291
[20] A. J. van der Poorten and H. P. Schlickewei, *Zeros of recurrence sequences*. Bull. Austral Math. Soc. **44**(1991), 215–223. https://doi.org/10.1017/S0004972700029646
[21] A. J. van der Poorten and I. E. Shparlinski, *On the number of zeros of exponential polynomials and related questions.* Bull. Austral Math. Soc. **46**(1992), 401–412. https://doi.org/10.1017/S0004972700012065
[22] K.F. Roth, *Rational approximations to algebraic numbers.* Mathematika **2**(1955), 1–20. https://doi.org/10.1112/S002557930000064
[23] P. Sarnak, *Three lectures on the Möbius function, randomness and dynamics*. Lecture notes, 2011. https://publications.ias.edu/node/512.
[24] M. Waldschmidt, *Diophantine approximation on linear algebraic groups. Transcendence properties of the exponential function in several variables*. Grundlehren der Mathematischen Wissenschaften, 326, Springer-Verlag, Berlin, 2000. https://doi.org/10.1007/978-662-11569-5

School of Mathematics and Statistics, University of New South Wales,Sydney, NSW 2052,Australia
e-mail: shamin2010@gmail.com igor.shparlinski@unsw.edu.au