Finite Fields and Their Applications 51 (2018) 298–305

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A note on exponential-Möbius sums over $\mathbb{F}_q[t]$

Sam Porritt

Department of Mathematics, University College London, 25 Gordon Street, London, England, United Kingdom

ARTICLE INFO

Article history:
Received 7 December 2017
Received in revised form 13 February 2018
Accepted 14 February 2018
Available online 27 February 2018
Communicated by Stephen D. Cohen

MSC:
11T23

Keywords:
Möbius function
Exponential sums
Function fields

ABSTRACT

In 1991, Baker and Harman proved, under the assumption of the generalized Riemann hypothesis, that

$$\max_{\theta\in[0,1)}\left|\sum_{n\leqslant x}\mu(n)e(n\theta)\right| \ll_\epsilon x^{3/4+\epsilon}.$$

The purpose of this note is to deduce an analogous bound in the context of polynomials over a finite field using Weil's Riemann Hypothesis for curves over a finite field. Our approach is based on the work of Hayes who studied exponential sums over irreducible polynomials.

© 2018 The Author. Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

Let μ be the Möbius function and write $e(\theta) = e^{2\pi i\theta}$. Baker and Harman [1] proved under the assumption of the generalized Riemann hypothesis that for all $\epsilon > 0$,

$$\max_{\theta\in[0,1)}\left|\sum_{n\leqslant x}\mu(n)e(n\theta)\right| \ll_\epsilon x^{\frac{3}{4}+\epsilon}. \tag{1}$$

E-mail address: samuel.porritt.15@ucl.ac.uk.

https://doi.org/10.1016/j.ffa.2018.02.005
1071-5797/© 2018 The Author. Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

It is conjecture that (1) holds for all $\epsilon > 0$ with $\frac{3}{4}$ replaced by $\frac{1}{2}$. The best unconditional result is due to Davenport [3] who showed that for all $A > 0$

$$\max_{\theta\in[0,1)} \left| \sum_{n\leqslant x} \mu(n)e(n\theta) \right| \ll_A \frac{x}{(\log x)^A}.$$

The purpose of this note is to deduce an analogue of (1) for the polynomial ring $\mathbb{F}_q[t]$. First, let us go through some definitions required to state the result. The function field analogue of the real numbers is the completion of the field of fractions of $\mathbb{F}_q[t]$ with respect to the norm defined by

$$|f/g| = \begin{cases} q^{\deg f - \deg g} & \text{if } f \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

This completion is naturally identified with the ring of formal Laurent series $\mathbb{F}_q((1/t)) = \{\sum_{i\leqslant j} x_i t^i \ : \ x_i \in \mathbb{F}_q,\ j \in \mathbb{Z}\}$. The norm defined above is extended to $x = \sum_{i\leqslant j} x_i t^i \in \mathbb{F}_q((1/t))$ by setting $|x| = q^j$ where j is the largest index with $x_j \neq 0$. The analogue of the unit interval is $\mathbb{T} := \{\sum_{i<0} x_i t^i \ : \ x_i \in \mathbb{F}_q\}$, and is a subring of $\mathbb{F}_q((1/t))$.

Define the additive character $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ by $\psi(x) = e(\mathrm{tr}(x)/p)$, where $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the usual trace map and p is the characteristic of $\mathbb{F}_q$. Define also the exponential map $\mathbf{e}_q : \mathbb{F}_q((1/t)) \to \mathbb{C}^\times$ by $\mathbf{e}_q(x) = \psi(x_{-1})$.

Now let $\mu(f)$ denote the Möbius function on the ring $\mathbb{F}_q[t]$, defined as $(-1)^k$ if f is the product of k distinct irreducibles and 0 otherwise and let $\phi(f)$ be the size of the unit group $(\mathbb{F}_q[t]/(f))^\times$, that is $|f|\prod_{\omega|f}(1-1/|\omega|)$, where the product is over all monic irreducibles dividing f. All sums over polynomials are sums over monic polynomials.

Theorem 1. *Suppose $n \geqslant 3$. Then*

$$\max_{\theta\in\mathbb{T}} \left| \sum_{\deg f = n} \mu(f)\mathbf{e}_q(f\theta) \right| \leqslant 4q^{\frac{3n+1}{4}} \left(\frac{3\sqrt{3}}{2}\right)^n.$$

Remark. It follows that for all $\epsilon > 0$ and q large enough with respect to ϵ we have

$$\max_{\theta\in\mathbb{T}} \left| \sum_{\deg f = n} \mu(f)\mathbf{e}_q(f\theta) \right| \leqslant q^{(\frac{3}{4}+\epsilon)n}.$$

Our proof of Theorem 1 will follow the strategy of Hayes employed in his study of the exponential sum

$$\sum_{\substack{\deg \omega = n \\ \omega \text{ irreducible}}} \mathbf{e}_q(\omega\theta).$$

Recently, Bienvenu and Lê have independently derived a similar result to Theorem 1 in [2]. Their Theorem 9 corresponds to our Lemma 1 and their Theorem 11 closely resembles our Theorem 1.

2. Lemmas

Let $\mathbb{F}_q[t]^\times$ be the multiplicative monoid of monic polynomials in $\mathbb{F}_q[t]$. Whilst investigating the distribution of irreducible polynomials over $\mathbb{F}_q$, Hayes [4] introduced certain congruences classes on $\mathbb{F}_q[t]^\times$ defined as follows. Let $s \geqslant 0$ be an integer and $g \in \mathbb{F}_q[t]$. We define an equivalence relation $\mathcal{R}_{s,g}$ on $\mathbb{F}_q[t]^\times$ by

$$a \equiv b \bmod \mathcal{R}_{s,g} \Leftrightarrow g \text{ divides } a-b \text{ and } \left|\frac{a}{t^{\deg a}} - \frac{b}{t^{\deg b}}\right| < \frac{1}{q^s}$$

It is easy to check that this is indeed an equivalence relation and that for all $c \in \mathbb{F}_q[t]^\times$,

$$a \equiv b \bmod \mathcal{R}_{s,g} \Rightarrow ac \equiv bc \bmod \mathcal{R}_{s,g}$$

so we can define the quotient monoid $\mathbb{F}_q[t]^\times/\mathcal{R}_{s,g}$. Hayes showed that an element of $\mathbb{F}_q[t]$ is invertible modulo $\mathcal{R}_{s,g}$ if and only if it is coprime to g and that the units of this quotient monoid form an abelian group of order $q^s\phi(g)$ which we denote $\mathcal{R}^*_{s,g} = (\mathbb{F}_q[t]^\times/\mathcal{R}_{s,g})^\times$. Given a character (group homomorphism) $\chi : \mathcal{R}^*_{s,g} \to \mathbb{C}$ we can lift this to a character of $\mathbb{F}_q[t]^\times$ by setting $\chi(f) = 0$ if f is not invertible modulo $\mathcal{R}_{s,g}$. Associated to each such character is the L-function $L(u,\chi)$ defined for $u \in \mathbb{C}$ with $|u| < 1/q$ by

$$L(u,\chi) = \sum_{f \in \mathbb{F}_q[t]^\times} \chi(f) u^{\deg f} = \prod_{\omega} (1 - \chi(\omega) u^{\deg \omega})^{-1}$$

where the product is over all monic irreducibles. When χ is a non-trivial character it can be shown that $L(u,\chi)$ is a polynomial which factorises as

$$L(u,\chi) = \prod_{i=1}^{d(\chi)} (1 - \alpha_i(\chi) u)$$

for some $d(\chi) \leqslant s + \deg g - 1$ and each $\alpha_i(\chi)$ satisfies $|\alpha_i(\chi)| = 1$ or $\sqrt{q}$. This follows from Weil's Riemann Hypothesis and appears to have been first proved by Rhin in [7].

When $\chi = \chi_0$ is the trivial character we have

$$L(u,\chi_0) = \sum_{\substack{f \in \mathbb{F}_q[t]^\times \\ (f,g)=1}} u^{\deg f} = \sum_{f \in \mathbb{F}_q[t]^\times} u^{\deg f} \prod_{\omega \mid g} (1 - u^{\deg \omega}) = \frac{1}{1-qu} \prod_{\omega \mid g} (1 - u^{\deg \omega}).$$

Lemma 1. *Let χ be a character modulo $\mathcal{R}^*_{s,g}$ and $\deg g \leqslant n/2$. Then*

$$\left|\sum_{\deg f=n} \mu(f)\chi(f)\right| \leqslant \begin{cases} \binom{n+s+\deg g-2}{s+\deg g-2} q^{n/2} & \text{if } \chi \neq \chi_0 \\ \binom{n+r-1}{r-1}(q+1) & \text{if } \chi = \chi_0 \end{cases}$$

where r is the number of distinct irreducible divisors of g.

Remark. The bound χ_0 is smaller than the one for $\chi \neq \chi_0$ when $n \geqslant 3$ because $\deg g$ is an upper bound for r and for $n \geqslant 3$

$$(q+1)\binom{n+\deg g-1}{n} \leqslant \binom{n+\deg g-2}{n} q^{n/2}.$$

Proof. Suppose first that $\chi \neq \chi_0$. Then

$$\sum_f \chi(f)\mu(f)u^{\deg f} = L(u,\chi)^{-1} = \prod_{i=1}^{d(\chi)}(1-\alpha_i(\chi)u)^{-1}$$

$$= \sum_{n\geqslant 0}\left(\sum_{\substack{r_1+\cdots r_{d(\chi)}=n \\ 0\leqslant r_i\leqslant n}} \prod_{i=1}^{d(\chi)} \alpha_i(\chi)^{r_i}\right) u^n.$$

Comparing coefficients and using the triangle inequality we get

$$\left|\sum_{\deg f=n}\chi(f)\mu(f)\right| = \left|\sum_{\substack{r_1+\cdots+r_{d(\chi)}=n \\ 0\leqslant r_i\leqslant n}} \prod_{i=1}^{d(\chi)}\alpha_i(\chi)^{r_i}\right| \leqslant \binom{n+d(\chi)-1}{d(\chi)-1} q^{n/2}$$

$$\leqslant \binom{n+s+\deg g-2}{s+\deg g-2} q^{n/2}.$$

When $\chi = \chi_0$ is the principal character

$$L(u,\chi_0)^{-1} = (1-qu)\prod_{\omega|g}(1+u^{\deg\omega}+u^{2\deg\omega}+\cdots).$$

If we write $\omega_1, \omega_2, \ldots, \omega_r$ for the distinct irreducible divisors of g then we get, by equating coefficients again,

$$\left|\sum_{\deg f=n}\chi_0(f)\mu(f)\right| \leqslant \sum_{\substack{a_i\in\mathbb{Z}_{\geqslant 0} \\ \sum_{1\leqslant i\leqslant r} a_i\deg\omega_i=n}} 1 + q \sum_{\substack{a_i\in\mathbb{Z}_{\geqslant 0} \\ \sum_{1\leqslant i\leqslant r} a_i\deg\omega_i=n-1}} 1$$

$$\leqslant (q+1) \sum_{\substack{b_i \in \mathbb{Z}_{\geqslant 0} \\ \sum_{1 \leqslant i \leqslant r} b_i = n}} 1$$
$$= (q+1)\binom{n+r-1}{r-1}. \quad \square$$

Lemma 2. *For each $\theta \in \mathbb{T}$ there exist unique coprime polynomials $a, g \in \mathbb{F}_q[t]$ with g monic and $\deg a < \deg g \leqslant n/2$ such that*

$$\left|\theta - \frac{a}{g}\right| < \frac{1}{q^{\frac{n}{2}+\deg g}}.$$

Proof. See Lemma 3 from [6]. $\square$

Lemma 3. *Let $\theta \in \mathbb{T}$ and let a, g be the unique polynomials defined as in Lemma 2 with respect to θ and n. Set $s = n - [\frac{n}{2}] - \deg g$. For any $f_1, f_2 \in \mathbb{F}_q[t]^\times$ of degree n such that $f_1 \equiv f_2$ mod $\mathcal{R}_{s,g}$ we have*

$$\boldsymbol{e}_q(f_1\theta) = \boldsymbol{e}_q(f_2\theta).$$

Proof. See Lemma 5.2 from [5]. $\square$

Lemma 4. *Suppose $g \in \mathbb{F}_q[t]$ is square-free. Then*

$$\sum_{d|g} \frac{1}{q^{\deg d}} \leqslant \left(1 + \frac{\log(\deg g)}{\log q}\right)e.$$

Proof. Order the monic irreducibles $\omega_1, \omega_2, \ldots, \omega_r$ dividing g and the monic irreducibles $P_1, \ldots$ in $\mathbb{F}_q[t]$ in order of degree (and those of the same degree arbitrarily). Let $\pi(k)$ be the number of monic irreducibles of degree k and define N by $\sum_{\deg P \leqslant N-1} \deg P < \deg g \leqslant \sum_{\deg P \leqslant N} \deg P$. Then g has at most $\sum_{1 \leqslant k \leqslant N} \pi(N)$ irreducible factors. Therefore, since $\deg P_i \leqslant \deg \omega_i$, we have

$$\sum_{d|g} \frac{1}{q^{\deg d}} = \prod_{\omega|g}\left(1 + \frac{1}{q^{\deg \omega}}\right) \leqslant \prod_{\deg P \leqslant N}\left(1 + \frac{1}{q^{\deg P}}\right) = \prod_{1 \leqslant k \leqslant N}\left(1 + \frac{1}{q^k}\right)^{\pi(k)}.$$

Using $\pi(k) \leqslant \frac{q^k}{k}$ this is bounded by

$$\prod_{1 \leqslant k \leqslant N}\left(1 + \frac{1}{q^k}\right)^{\frac{q^k}{k}} \leqslant \prod_{1 \leqslant k \leqslant N} e^{\frac{1}{k}} \leqslant e^{1+\log N} = Ne.$$

Now we bound N in terms of $\deg g$ as follows

$$\deg g > \sum_{\deg P \leqslant N-1} \deg p = \sum_{1 \leqslant k \leqslant N-1} \pi(k)k \geqslant \sum_{k|N-1} \pi(k)k = q^{N-1}$$

by the prime number theorem in $\mathbb{F}_q[t]$. This gives $N \leqslant 1 + \frac{\log(\deg g)}{\log q}$ which completes the proof of the Lemma. □

3. Proof of Theorem 1

Let $\theta \in \mathbb{T}$ and choose g and s as in Lemma 3. We start by giving an explicit description of a set a representatives for the equivalence relation $\mathcal{R}_{s,g}$. It is not hard to show that

$$\mathcal{S}_{s,g} = \{t^{[\frac{n}{2}]} g b_1 + b_2 \mid \deg b_1 = s, b_1 \text{ monic}, \deg b_2 < \deg g\}$$

is such a set. Furthermore,

$$\mathcal{S}^*_{s,g} = \{t^{[\frac{n}{2}]} g b_1 + b_2 \mid \deg b_1 = s, b_1 \text{ monic}, \deg b_2 < \deg g, (b_2, g) = 1\}$$

defines a set of reduced representatives modulo $\mathcal{R}_{s,g}$. See [5] Lemma 7.1 for details.

Then by Lemma 3 and the orthogonality of characters modulo $\mathcal{R}^*_{s,g}$ we can write

$$\begin{aligned}
&\sum_{\deg f = n} \mu(f)\mathbf{e}_q(f\theta) \\
&= \sum_{b \in \mathcal{S}_{s,g}} \sum_{\substack{\deg f = n \\ f \equiv b \bmod \mathcal{R}_{s,g}}} \mu(f)\mathbf{e}_q(f\theta) \\
&= \sum_{d|g} \sum_{\substack{b \in \mathcal{S}_{s,g} \\ (g,b)=d}} \mathbf{e}_q(b\theta) \sum_{\substack{\deg f = n \\ f \equiv b \bmod \mathcal{R}_{s,g}}} \mu(f) \\
&= \sum_{d|g} \sum_{\substack{b \in \mathcal{S}_{s,g/d} \\ (g/d,b)=1}} \mathbf{e}_q(bd\theta) \sum_{\substack{\deg f = n - \deg d \\ f \equiv b \bmod \mathcal{R}_{s,g/d}}} \mu(fd) \\
&= \sum_{d|g} \sum_{b \in \mathcal{S}^*_{s,g/d}} \mathbf{e}_q(bd\theta) \sum_{\deg f = n - \deg d} \frac{1}{q^s \phi(g/d)} \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \overline{\chi}(b)\chi(f)\mu(fd).
\end{aligned}$$

Notice that $\mu(fd) = \mu(f)\mu(d)\chi_d(f)$ where $\chi_d(f)$ is the trivial character modulo $\mathcal{R}^*_{s,d}$. We can therefore rewrite the above as

$$= \sum_{d|g} \frac{\mu(d)}{q^s \phi(g/d)} \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left(\sum_{b \in \mathcal{S}^*_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right) \left(\sum_{\deg f = n - \deg d} \mu(f)\chi\chi_d(f) \right).$$

Now χ is a character modulo $\mathcal{R}^*_{s,g/d}$ and χ_d is a character modulo $\mathcal{R}^*_{s,d}$. Therefore, $\chi\chi_d$ is a character modulo $\mathcal{R}^*_{s,g}$, and so using the triangle inequality and Lemma 1 we can bound this in absolute value by

$$q^{n/2} \sum_{\substack{d|g \\ g \text{ square-free}}} \frac{1}{q^{s+\deg d/2}\phi(g/d)} \binom{n-\deg d+s+\deg g-2}{s+\deg g-2}$$
$$\times \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left| \sum_{b\in\mathcal{S}_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right|.$$

We bound the Gauss sum over $\chi \bmod \mathcal{R}^*_{s,g/d}$ in the standard way using the Cauchy–Schwarz inequality and Parseval's identity as follows

$$\begin{aligned}
&\sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left| \sum_{b\in\mathcal{S}_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right| \\
&\leqslant \left(\sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} 1 \sum_{\chi \bmod \mathcal{R}^*_{s,g/d}} \left| \sum_{b\in\mathcal{S}_{s,g/d}} \mathbf{e}_q(bd\theta)\overline{\chi}(b) \right|^2 \right)^{1/2} \\
&= \left(q^s\phi(g/d) \sum_{b_1,b_2\in\mathcal{S}_{s,g/d}} \mathbf{e}_q(d(b_1-b_2)\theta) \sum_{\chi \bmod \mathcal{R}^*_{s,g}} \overline{\chi}(b_1)\chi(b_2) \right)^{1/2} \\
&= \left((q^s\phi(g/d))^2 \sum_{b_1=b_2\in\mathcal{S}^*_{s,g/d}} \mathbf{e}_q((b_1-b_2)\theta) \right)^{1/2} \\
&= (q^s\phi(g/d))^{3/2}.
\end{aligned}$$

Recall that $s+\deg g = n-[\frac{n}{2}] \geqslant n/2$ so that

$$\binom{n-\deg d+s+\deg g-2}{s+\deg g-2} \leqslant \binom{2n-[\frac{n}{2}]-2}{n-[\frac{n}{2}]-2}.$$

We can bound this binomial coefficient using the fact that for all positive integers k,

$$\sqrt{2\pi}k^{k+\frac{1}{2}}e^{-k+\frac{1}{12k+1}} < k! < \sqrt{2\pi}k^{k+\frac{1}{2}}e^{-k+\frac{1}{12k}}.$$

This precise form of Stirling's formula is due to Robbins [8]. It follows that if $k=[\frac{n}{2}]$ then

$$\binom{2n-[\frac{n}{2}]-2}{n-[\frac{n}{2}]-2} < \binom{3k}{k} < \frac{1}{\sqrt{2\pi}} e^{\frac{1}{36k}-\frac{1}{12k+1}-\frac{1}{24k+1}} \frac{(3k)^{3k+\frac{1}{2}}}{k^{k+\frac{1}{2}}(2k)^{2k+\frac{1}{2}}} < \frac{1}{\sqrt{4\pi k/3}} \left(\frac{3\sqrt{3}}{2}\right)^{2k}.$$

Putting it all together with $\phi(g/d) \leqslant q^{\deg g-\deg d}$ and Lemma 4 we get

$$\left|\sum_{\deg f=n}\mu(f)\mathbf{e}_q(f\theta)\right| \leqslant q^{n/2}\frac{1}{\sqrt{2\pi(n-1)/3}}\left(\tfrac{3\sqrt{3}}{2}\right)^n\sum_{d|g}\frac{(q^s\phi(g/d))^{1/2}}{q^{\deg d/2}}$$

$$\leqslant q^{n-\frac{1}{2}\left[\frac{n}{2}\right]}\frac{(1+\frac{\log n}{\log q})e}{\sqrt{2\pi(n-1)/3}}\left(\tfrac{3\sqrt{3}}{2}\right)^n$$

and Theorem 1 easily follows after a short numerical calculation.

Acknowledgments

We are very grateful to Pierre Bienvenu for pointing out a mistake in an earlier version of our proof of Theorem 1. We are also grateful to Andrew Granville for pointing out how to strengthen an earlier version of Theorem 1. Previously, we required both n and q to be large with respect to ϵ for the remark that follows Theorem 1 to hold. This work was supported by the Engineering and Physical Sciences Research Council EP/L015234/1 via the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College London.

References

[1] R.C. Baker, G. Harman, Exponential sums formed with the Möbius function, J. Lond. Math. Soc. (2) 43 (2) (1991) 193–198.
[2] P.-Y. Bienvenu, T.H. Lê, Linear and quadratic uniformity of the Möbius function over $\mathbb{F}_q[t]$, preprint, arXiv:1711.05358.
[3] H. Davenport, On some infinite series involving arithmetical functions (II), Q. J. Math. 8 (1) (1937) 313–320.
[4] D.R. Hayes, The distribution of irreducibles in GF$[q, x]$, Trans. Am. Math. Soc. 117 (1965) 101–127.
[5] D.R. Hayes, The expression of a polynomial as a sum of three irreducibles, Acta Arith. 11 (1966) 461–488.
[6] P. Pollack, Irreducible polynomials with several prescribed coefficients, Finite Fields Appl. 22 (2013) 70–78.
[7] G. Rhin, Répartition modulo 1 dans un corps de séries formelles sur un corps fini, Diss. Math. 95 (1972) 75.
[8] H. Robbins, A remark on Stirling's formula, Am. Math. Mon. 62 (1955) 26–29.