DISJOINTNESS OF THE MÖBIUS TRANSFORMATION AND MÖBIUS FUNCTION

El Houcein El Abdalaoui, Igor Shparlinski

DISJOINTNESS OF THE MÖBIUS TRANSFORMATION AND MÖBIUS FUNCTION

EL HOUCEIN EL ABDALAOUI AND IGOR E. SHPARLINSKI

Abstract. We study the distribution of the sequence of elements of the discrete dynamical system generated by the Möbius transformation $x \mapsto (ax+b)/(cx+d)$ over a finite field of p elements at the moments of time that correspond to prime numbers. Motivated by a recent conjecture of P. Sarnak, we obtain nontrivial estimates of exponential sums with such sequences that imply that trajectories of this dynamical system are disjoined with the Möbius function. We also obtain an equidistribution result for such trajectories at prime moments of time.

1. Introduction

1.1. **Motivation and background.** Let, as usual $\mu(n)$ denote the *Möbius function*, that is, $\mu(n) = 0$ if n is not squarefree and $\mu(n) = (-1)^s$ if n is a product of s distinct primes. Furthermore, given a compact topological space X and a homeomorphism $T : X \to X$, we consider the *flow* $\mathcal{X} = (T, X)$. The *Möbius disjointness conjecture* of Sarnak [34] asserts that for any flow $\mathcal{X} = (T, X)$ of topological entropy zero, we have

$$\sum_{n \le N} \mu(n) f\left(T^n x\right) = o(N), \qquad N \to \infty, \tag{1.1}$$

for any $x \in X$ and a continuous complex-valued function f on X. This conjecture has recently attracted very active interest and has actually been established for several classes of flows, see [2,10,11,13,16,19,20,23, 26,28,33] and references therein. Moreover, for the connection between the Sarnak and Chowla conjectures, we refer to very recent works of el Abdalaoui [1], Gomilko, Kwietniak and Lemańczyk [22], Tao [36] and Tao and Teräväinen [37].

2010 *Mathematics Subject Classification.* 11L07, 11N60, 11T23, 37P05.

Key words and phrases. Möbius function, Möbius transformation, Möbius disjointness, exponential sums over primes.

Here we consider a discrete analogue of this conjecture for the flow $\mathcal{M} = (A, \mathbb{F}_p)$ formed by the Möbius map

$$A : \ x \mapsto \frac{ax+b}{cx+d} \tag{1.2}$$

over a finite field $\mathbb{F}_p$ of p elements, where p is a sufficiently large prime. For $c \neq 0$ also extend the definition (1.2) by setting

$$A(-d/c) = a/c. \tag{1.3}$$

It is now easy to check that this extended map $x \mapsto A(x)$ induces a permutation of $\mathbb{F}_p$.

In fact, we always identify the map (1.2) with a nonsingular matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p),$$

and we also always assume that $c \neq 0$ (so A is not a linear map).

Moreover, after an appropriate scaling of the coefficient of A we can always assume that

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p). \tag{1.4}$$

Furthermore, for $\xi_0 \in \mathbb{F}_p$ we consider the trajectory

$$\xi_n = A\left(\xi_{n-1}\right) = A^n\left(\xi_0\right), \qquad n = 1, 2, \ldots, \tag{1.5}$$

generated by iterations of A.

It is easy to see that each sequence of the form (1.5) either terminates after finitely many steps (if $c\xi_{n-1} + d = 0$) of is eventually periodic, and then, as A is a permutation it is purely periodic.

It is known that showing (1.1) can be reduced to estimating exponentials sums along trajectories of $\mathcal{X}$ twisted by the Möbius function. In our case, we are interested in the sums

$$S_\psi(N) = \sum_{n \le N} \mu(n) \psi\left(\xi_n\right) \tag{1.6}$$

twisted by the Möbius function along the trajectory (1.5) with a nontrivial additive character ψ of $\mathbb{F}_p$.

We remark, that similar sums, however associated with a linear map $x \mapsto gx$ over $\mathbb{F}_p$, that is, of the sequence $\xi_0 g^n$, have been estimated in [5, Theorem 5.1]. In fact, using the ideas of [7] it is possible to improve [5, Theorem 5.1], see also [9]. Furthermore, exponential sums over primes, associated with similar dynamical systems on elliptic curves over $\mathbb{F}_p$

have been estimated in [6] (see also [31, Section 4]), and can easily be extended to sums with the Möbius function.

Exponential sums with the Möbius function are closely related to sums over primes, which is associated with the behaviour of dynamical systems at "prime" times, see [35] for a general point of view and also specific results for dynamical systems on $\mathrm{SL}_2(\mathbb{R})$. We note that the study of ergodic dynamical system along the primes, initiated by Bourgain [8] and Wierdl [40] has been studied quite extensively; we refer also to the results of Nair [29,30] and to the surveys by Rosenblatt and Wierdl [32] and by Thouvenot [38]. For several results on the Prime Ergodic Theorem and Ergodic Theorem with Arithmetical Weight, we refer to [3, 12, 15–17, 29, 30], see also the references therein and also to a very recent survey by Eisner and Lin [17].

For the orbits of the dynamical system $x \mapsto gx$ over $\mathbb{F}_p$ such results are given in [5,7,9,21]. We have already mentioned bounds from [6,31] on exponential sums over primes, associated with similar dynamical systems on elliptic curves over $\mathbb{F}_p$.

Thus, motivated by these results, together with the sums (1.6) we also obtain nontrivial bounds on the sums

$$T_\psi(N) = \sum_{\substack{\ell \le N \\ \ell \text{ prime}}} \psi\left(\xi_\ell\right). \tag{1.7}$$

Now, due to the finite nature of our dynamical systems instead the asymptotic relations of the typs (1.1), we are interested in obtaining upper bound on the sums (1.6) and (1.7) with an explicit saving depending on N and other parameters.

1.2. **Main results.** Throughout the paper, the implied constants in the symbols 'O', '$\ll$' and '$\gg$' may occasionally, where obvious, depend on the real positive parameter ε, and are absolute otherwise (we recall that $U \ll V$ and $V \gg U$ are both equivalent to $U = O(V)$).

In all our bounds we have to assume that

$$t \ge p^{1/2+\varepsilon}, \tag{1.8}$$

which is not a severe restriction as it is satisfied by the majority of the sequences, see, for example, [14].

Our main result is the following bound:

Theorem 1.1. *Let $\varepsilon > 0$ be sufficiently small. If the period length t of the sequence (1.5) satisfies (1.8) then, for any real*

$$\alpha \geq p^{-\varepsilon/2} \log p$$

and integer

$$N \geq t \exp\left(5\alpha^{-1} \left(\log(1/\alpha)\right)^6\right).$$

uniformly over all nontrivial additive character ψ of $\mathbb{F}_p$, we have

$$|S_\psi(N)| \ll \alpha N.$$

We remark that Theorem 1.1 yields a power saving, that is allows to take $\alpha = p^{-\eta}$ with some fixed positive $\eta < \varepsilon/2$, only to very large values of N, much larger that in the case of the linear transformation $x \mapsto gx$ and a similar map on elliptic curves, see [5, 7, 9, 21] and [6, 31] respectively. This is because in the case of the Möbius transformation we have not been able to use a canonical way via a version of the *Vaughan identity* for the Möbius function, see, for example, [5, Section 5]. Instead we use a much more robust approach due to Kátai [25] in the form given by Bourgain, Sarnak and Ziegler [11, Theorem 2].

To estimate the sums (1.7) we first estimate the sums

$$R_\psi(N) = \sum_{n \leq N} \Lambda(n) \psi\left(\xi_n\right) \tag{1.9}$$

with the von Mangoldt function, which is given by

$$\Lambda(n) = \begin{cases} \log \ell & \text{if } n \text{ is a power of a prime } \ell, \\ 0 & \text{if } n \text{ is not a prime power.} \end{cases}$$

We notice that the sums (1.9) are technically easier to work with.

As usual, we reduce the problem of estimating the sums $R_\psi(N)$ to bounding some single sums (Type I sums) and bilinear character sums (Type II sums). However, a direct application of the Vaughan identity, see [24, Section 13.4], does not seem to work. We circumvent this by applying a slightly different approach, which is based on the work of Bourgain, Sarnak and Ziegler [11, Theorem 2].

Theorem 1.2. *Let $\varepsilon > 0$ be sufficiently small. If the period length t of the sequence (1.5) satisfies (1.8) then, for any real α*

$$\alpha \geq p^{-\varepsilon/6} \log p \tag{1.10}$$

and integer

$$\exp\left(p^{\varepsilon/4}\right) \geq N \geq t p^{\varepsilon} \exp\left(5\alpha^{-1} \left(\log(1/\alpha)\right)^6\right). \tag{1.11}$$

uniformly over all nontrivial additive character ψ of $\mathbb{F}_p$, we have

$$|R_\psi(N)| \ll \alpha N$$

As usual, we use $\pi(N)$ to denote the number of primes $\ell \le N$. Then, by appealing to a classical argument, based on partial summation (see for example [4, Section 4.3]) we then derive:

Corollary 1.3. *Let $\varepsilon > 0$ be sufficiently small. If the period length t of the sequence (1.5) satisfies (1.8) then, for any real α and integer N satisfying (1.10) and (1.11) uniformly over all nontrivial additive character ψ of $\mathbb{F}_p$, we have*

$$|T_\psi(N)| \ll \alpha\pi(N).$$

1.3. **Further perspectives.** We also note that our results behind the estimates of Theorem 1.1 and 1.2, in particular Lemma 2.6 below can be applied to estimating exponential sum along sequences with other arithmetic constraints such as *square-freeness* (in which case one can expect stronger results) and *smoothness*.

One can also apply our approach to other dynamical systems such as polynomial dynamical systems $x \mapsto f(x)$ for a polynomial $f \in \mathbb{F}_p[X]$ of a fixed degree $d \ge 2$ or to monomial dynamical systems $x \mapsto x^e$ for an integer $e \ge 1$ with $\gcd(e, p-1) = 1$, which however can be rather large in terms of p.

2. Preliminaries

2.1. Möbius transformation and binary recurrences.

Lemma 2.1. *Let $f(Z) = Z^2 - eZ - 1 \in \mathbb{F}_p[Z]$, where $e = a + d$, be the characteristic polynomial of the matrix A of the form (1.4). Then there are two binary recurrence sequences u_n and v_n satisfying*

$$u_{n+2} = eu_{n+1} + u_n \qquad \text{and} \qquad v_{n+2} = ev_{n+1} + v_n$$

with the initial values

$$(u_0, u_1) = (\xi_0, a\xi_0 + b) \qquad \text{and} \qquad (v_0, v_1) = (1, c\xi_0 + d)$$

such that

$$\xi_n = u_n/v_n$$

for $n = 0, 1, \ldots$.

Proof. It is easy to check that the recursive definition of u_n and v_n can be rewritten as

$$\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = A \begin{pmatrix} u_n \\ v_n \end{pmatrix}, \qquad n = 0, 1, \ldots.$$

with the initial values

$$(u_0, u_1) = (\xi_0, a\xi_0 + b) \qquad \text{and} \qquad (v_0, v_1) = (1, c\xi_0 + d)$$

Then one verifies that the desired statement by induction on n. □

Using the well known expression of linear recurrence sequences via the roots of characteristic polynomials, see, for example, [18], we immediately derive from Lemma 2.1, in a straightforward fashion, the following explicit formula:

Lemma 2.2. *Let $f(Z) = Z^2 - eZ - 1 \in \mathbb{F}_p[Z]$, where $e = a + d$, be the characteristic polynomial of the matrix A of the form (1.4), which has two distinct roots ϑ and ϑ^{-1} in $\mathbb{F}_p$. Then there exist elements $\alpha, \beta, \gamma \in \mathbb{F}_p$ such that*

$$\xi_n = \alpha + \frac{\beta}{\vartheta^{2n} + \gamma}, \qquad n = 0, 1, \ldots.$$

2.2. **Bounds on single character sums.** Let p be the characteristic of $\mathbb{F}_p$ and let $\overline{\mathbb{F}}_p$ denote the algebraic closure of $\mathbb{F}_p$.

One of our main tools is the bound on hybrid sums of multiplicative and additive characters, which in its classical form is given by Weil [39, Example 12 of Appendix 5]; see also [27, Theorem 3 of Chapter 6].

Lemma 2.3. *For any polynomials $g(X), h(X) \in \mathbb{F}_p[X]$ such that the rational function $F(X) = h(X)/g(X)$ is not of the form $G(X)^p - G(X)$ with $G(X) \in \overline{\mathbb{F}}_p(X)$, and any nontrivial additive character ψ and arbitrary multiplicative character χ of $\mathbb{F}_p$ we have*

$$\left| \sum_{\substack{x \in \mathbb{F}_p \\ g(x) \neq 0}} \psi\left(F(x)\right) \chi(x) \right| \ll \max\{\deg g\,, \deg h\} p^{1/2}.$$

We now need a bound on the character sums

$$Q_\psi(u, v; k, m, N) = \sum_{n \le N} \psi\left(u\xi_{kn} + v\xi_{mn}\right)$$

with $u, v \in \mathbb{F}_p$ and non-negative integers k and m, along consecutive values of the trajectory (1.5).

Lemma 2.4. *Assume that the characteristic polynomial of the matrix A of the form (1.4) has two distinct roots in $\mathbb{F}_p$. If t is the period length of the sequence (1.5), then, for any $u, v \in \mathbb{F}_p$ with $(u, v) \neq (0, 0)$ and integers $0 \leq k < m$, for any $N \leq t$ we have*

$$Q_\psi(u, v; k, m, N) \ll mp^{1/2} \log p.$$

Proof. Let ϑ be as in Lemma 2.1. It is clear that t is the multiplicative order of ϑ^2. For every integer h, We now define the sums

$$Q_{h,\psi}(u, v; k, m) = \sum_{n=1}^{t} \psi\left(u\xi_{kn} + v\xi_{mn}\right) \mathbf{e}(hn/t),$$

where

$$\mathbf{e}(z) = \exp(2\pi i z).$$

Since ϑ^2 is of order t it can be written as $\vartheta^2 = g^s$ for $s = (p-1)/t$ and some primitive root g of $\mathbb{F}_p^*$. For $x \in \mathbb{F}_p^*$, we define $\operatorname{ind} x$ by the conditions

$$g^{\operatorname{ind} x} = x \qquad \text{and} \qquad 0 \leq \operatorname{ind} x \leq p-2.$$

Hence, using Lemma 2.2 and the additivity of ψ, we write

$$\begin{aligned}
&Q_{h,\psi}(u, v; k, m) \\
&\quad = \psi\left(\alpha\left(u+v\right)\right) \sum_{n=1}^{t} \psi\left(\frac{\beta u}{g^{kns}+\gamma} + \frac{\beta v}{g^{mns}+\gamma}\right) \mathbf{e}(hn/t) \\
&\quad = \psi\left(\alpha\left(u+v\right)\right) \sum_{n=1}^{t} \psi\left(\frac{\beta u}{g^{kns}+\gamma} + \frac{\beta v}{g^{mns}+\gamma}\right) \mathbf{e}(hsn/(p-1)) \\
&\quad = \frac{1}{s}\psi\left(\alpha\left(u+v\right)\right) \sum_{n=1}^{p-1} \psi\left(\frac{\beta u}{g^{kns}+\gamma} + \frac{\beta v}{g^{mns}+\gamma}\right) \mathbf{e}(hsn/(p-1)).
\end{aligned}$$

Now, denote $x = g^n$ and using that g is a primitive root, we obtain

$$\begin{aligned}
&Q_\psi(h, u, v; k, m) \\
&\quad = \frac{1}{s}\psi\left(\alpha\left(u+v\right)\right) \sum_{x \in \mathbb{F}_p^*} \psi\left(\frac{\beta u}{x^{ks}+\gamma} + \frac{\beta v}{x^{ms}+\gamma}\right) \mathbf{e}(hs \operatorname{ind} x/(p-1)).
\end{aligned}$$

Since the function $x \mapsto \mathbf{e}(hs \operatorname{ind} x/(p-1))$ is a multiplicative character of $\mathbb{F}_p^*$, recalling Lemma 2.3, we obtain

$$Q_{h,\psi}(u, v; k, m) \ll \frac{1}{s} smp^{1/2} = mp^{1/2}.$$

Using the standard reduction between complete and incomplete sums, see [24, Section 12.2], we conclude the proof. □

For sums with one term

$$R_\psi(u;m,N)=\sum_{n\le N}\psi\left(u\xi_{mn}\right)$$

with $u\in\mathbb{F}_p$ and a non-negative integer m, we have a slightly more precise statement.

Lemma 2.5. *Assume that the characteristic polynomial of the matrix A of the form (1.4) has two distinct roots in $\mathbb{F}_p$. If t is the period length of the sequence (1.5), then, for any $u\in\mathbb{F}_p^*$ and an integers $m>0$, for any $N\le t$ we have*

$$R_\psi(u;m,N)\ll \gcd(m,t)p^{1/2}\log p.$$

Proof. Let $d=\gcd(m,t)$. We set

$$k=m/d \qquad \text{and} \qquad s=t/d.$$

Let $B=A^k$. We also consider the sequences $\zeta_n=\xi_{kn}$ then instead of (1.5), we can write

$$\zeta_n=B\left(\zeta_{n-1}\right)=B^n\left(\xi_0\right), \qquad n=1,2,\ldots.$$

Hence, by the standard arguments as before, we see that the period of the sequence ζ_n $n=1,2,\ldots$, is t. Using a special case (with only one term) applied to $\zeta_{dn}=\xi_{mn}$ instead of ξ_n, we obtain the result. □

2.3. **Double sums and correlations with multiplicative functions.** Now, by applying the machinery in the proof of the criterion of Bourgain, Sarnak and Ziegler [11, Theorem 2] (which in turn improves the result of Kátai [25]), we obtain our main technical result.

We present it in a form which is more general and flexible than we need here, since we believe it may find other applications.

Lemma 2.6. *Let ν be a multiplicative function and F an arbitrary periodic arithmetic function with period t. Assume*

$$|\nu(n)|\le 1 \qquad \text{and} \qquad |F(n)|\le 1, \qquad n\in\mathbb{N}.$$

We further assume that for any primes $r\ne s$, and for any positive integer $h\le t$ we have

$$\left|\sum_{n\le h}F(nr)\overline{F}(ns)\right|\le \max\{r,s\}t\rho$$

for some real $\rho<1$. Then for any real

$$\alpha\ge\sqrt{\rho\log(1/\rho)} \tag{2.1}$$

and integer

$$N \geq t \exp\left(4\alpha^{-1} \left(\log(1/\alpha)\right)^6\right). \tag{2.2}$$

we have

$$\left|\sum_{n\leq N} \nu(n)F(n)\right| \ll \alpha N.$$

Proof. We follow the proof of [11, Theorem 2]. In particular, let $1 > \alpha > 0$ be some sufficiently small parameter, to be chosen later. As in [11, Equation (2.1)] we define

$$j_0 = \frac{\left(\log(1/\alpha)\right)^3}{\alpha} \qquad \text{and} \qquad j_1 = j_0^2. \tag{2.3}$$

For every integer $j \in [j_0, j_1 + 1]$ we also define

$$R_j = (1+\alpha)^j \qquad \text{and} \qquad M_j = N/R_{j+1}.$$

We note that we do not assume that these quantities are integer numbers.

Furthermore, for every integer $j \in [j_0, j_1]$ we define $\mathcal{P}_j$ as the set of primes in the interval $[R_j, R_{j+1}]$ and then we also define the set

$$\mathcal{Q}_j = \left\{ m \in [1, M_j] \ : \ m \text{ has no prime factors in } \bigcup_{i\leq j} \mathcal{P}_j \right\}.$$

We note that, by the prime number theorem (with an explicit bound on the error term, we do not however need the full power of the current knowledge such as [24, Corollary 8.30]), we have the following bound on the cardinality of $\mathcal{P}_j$, for every $j \in [j_0, j_1]$:

$$\#\mathcal{P}_j \leq R_j \left(\frac{1}{j} + \frac{1}{\alpha j^2} + O\left(\exp\left(-\sqrt{\alpha j}\right)\right)\right) \ll \frac{1}{j} R_j, \tag{2.4}$$

see [11, Equation (2.8)], where have also used that $\alpha j \geq \alpha j_0 \gg 1$.

As in the proof of [11, Theorem 2] we notice that the products of the mr with $r \in \mathcal{P}_j$, $m \in \mathcal{Q}_j$ for some $j \in [j_0, j_1]$ are pairwise distinct and obviously belong the interval $[1, N]$, so we conclude

$$\sum_{j_0 \leq j \leq j_1} \#\mathcal{P}_j \#\mathcal{Q}_j \leq N \tag{2.5}$$

which is also used in the derivation of [11, Equations (2.20) and (2.21)].

Furthermore, using (2.4) and recalling choice of the parameters (2.3), we obtain

$$\begin{aligned}\sum_{j_0\le j\le j_1} \#\mathcal{P}_j &\ll \sum_{j_0\le j\le j_1} \frac{1}{j}(1+\alpha)^j \le (1+\alpha)^{j_1} \sum_{j_0\le j\le j_1} \frac{1}{j}\\ &\le (1+\alpha)^{j_1}\log(j_1/j_0) \le \exp\left(\alpha j_1\right)\log j_0.\end{aligned}$$

Hence

$$\sum_{j_0\le j\le j_1} \#\mathcal{P}_j \ll \exp\left(1.5\alpha^{-1}\left(\log(1/\alpha)\right)^6\right), \tag{2.6}$$

provided that α is sufficiently small.

Now to establish the desired result, we recall that by [11, Equation (2.16)]

$$\sum_{n\le N} \nu(n)F(n) \ll \sum_{j_0\le j\le j_1} W_j + \alpha N, \tag{2.7}$$

where

$$W_j = \sum_{m\in\mathcal{Q}_j} \left|\sum_{r\in\mathcal{P}_j} \nu(r)F(mr)\right|, \qquad j_0 \le j \le j_1.$$

Using the Cauchy–Schwarz inequality, extending the range of summation over m to all positive integers up to M_j, changing the order of summation and recalling that $|\nu(n)| \le 1$, we obtain

$$W_j^2 \le \#\mathcal{Q}_j \sum_{r,s\in\mathcal{P}_j} \left|\sum_{m\le M_j} F(mr)\overline{F(ms)}\right|, \qquad j_0 \le j \le j_1, \tag{2.8}$$

see [11, Equation (2.17)].

The contribution $T_{1,j}$ to the right hand side of (2.8) from the diagonal terms can estimated as in [11, Equation (2.20)] by

$$T_{1,j} \ll M_j \#\mathcal{P}_j. \tag{2.9}$$

To estimate the remaining contribution $T_{2,j}$ from the off-diagonal terms we recall our assumption on bilinear sums with the function F. More precisely, splitting the interval of summation into at most M_j/t intervals of length t and at most 1 interval of length $h \le t$, we obtain

$$\left|\sum_{n\le M_j} F(nr)\overline{F}(ns)\right| \le \max\{r,s\}(M_j/t+1)t\rho.$$

Hence, using (for simplicity) that $r, s \le R_{j+1} \le 2R_j$ and $M_j R_j \le N$, we derive

$$T_{2,j} \le 2\left(\#\mathcal{P}_j\right)^2 R_j \left(M_j + t\right)\rho \ll \left(\#\mathcal{P}_j\right)^2 \left(N + R_j t\right)\rho. \tag{2.10}$$

Substituting the bound (2.9) and (2.10) in (2.8), we obtain

$$\begin{aligned} W_j^2 &\ll M_j \#\mathcal{P}_j \#\mathcal{Q}_j + \left(\#\mathcal{P}_j\right)^2 \left(N/t + R_j\right) t\rho \#\mathcal{Q}_j \\ &\le M_j \#\mathcal{P}_j \#\mathcal{Q}_j + N\left(\#\mathcal{P}_j\right)^2 \#\mathcal{Q}_j \rho + \left(\#\mathcal{P}_j\right)^2 \#\mathcal{Q}_j R_j t\rho, \end{aligned}$$

which after the substitution in (2.7) implies

$$\sum_{n \le N} \nu(n) F(n) \ll S_1 + S_2\sqrt{N\rho} + S_3\sqrt{t\rho} + \alpha N, \tag{2.11}$$

where

$$\begin{aligned} S_1 &= \sum_{j_0 \le j \le j_1} \left(M_j \#\mathcal{P}_j \#\mathcal{Q}_j\right)^{1/2}, \\ S_2 &= \sum_{j_0 \le j \le j_1} \#\mathcal{P}_j \left(\#\mathcal{Q}_j\right)^{1/2}, \\ S_3 &= \sum_{j_0 \le j \le j_1} \#\mathcal{P}_j \left(\#\mathcal{Q}_j R_j\right)^{1/2}. \end{aligned}$$

To bound the sum S_1, we use the Cauchy–Schwarz inequality and write

$$S_1 \ll \left(\sum_{j_0 \le j \le j_1} \#\mathcal{P}_j \#\mathcal{Q}_j\right)^{1/2} \left(\sum_{j_0 \le j \le j_1} M_j\right)^{1/2}.$$

We estimate the first sum using (2.5), while the second sums is easily estimated as

$$\begin{aligned} \sum_{j_0 \le j \le j_1} M_j &= N \sum_{j_0 \le j \le j_1} (1+\alpha)^{-j-1} \le N(1+\alpha)^{-j_0-1} \sum_{j=0}^{\infty} (1+\alpha)^{-j} \\ &= N\frac{1+\alpha}{\alpha}(1+\alpha)^{-j_0-1} \ll N\frac{1}{\alpha}\exp(-j_0 \log(1+\alpha)). \end{aligned}$$

Therefore, by the definition of j_0 in (2.3) combined with the inequality $\log(1+x) \ge x/2$ for $x \in [0,1]$, we obtain

$$S_1 \ll N \exp\left(-0.25\left(\log(1/\alpha)\right)^3\right). \tag{2.12}$$

Note that (2.12) is stronger that the bound recorded in [11, Equation (2.20)], however this does not affect the final result as it is dominated by the term αN, which is already present in (2.11).

For the sum S_2, writing

$$\#\mathcal{P}_j \left(\#\mathcal{Q}_j\right)^{1/2} = \left(\#\mathcal{P}_j \#\mathcal{Q}_j\right)^{1/2} \left(\#\mathcal{P}_j\right)^{1/2},$$

and applying again the Cauchy–Schwarz inequality, we obtain

$$S_2 \le \left(\sum_{j_0 \le j \le j_1} \#\mathcal{P}_j \#\mathcal{Q}_j\right)^{1/2} \left(\sum_{j_0 \le j \le j_1} \#\mathcal{P}_j\right)^{1/2}.$$

Now, we see from (2.4) and (2.5) that

$$S_2 \ll N^{1/2} \left(\log(1/\alpha)\right)^{1/2}. \tag{2.13}$$

Therefore, it remains to estimate the sum S_3. We notice that the trivial innequality $\#\mathcal{Q}_j R_j \le N$ yields

$$S_3 \le N^{1/2} \sum_{j_0 \le j \le j_1} \#\mathcal{P}_j,$$

which together with (2.6) implies

$$S_3 \ll N^{1/2} \exp\left(1.5\alpha^{-1} \left(\log(1/\alpha)\right)^6\right). \tag{2.14}$$

Substituting the bounds (2.12), (2.13) and (2.14) in (2.11), we derive

$$\sum_{n \le N} \nu(n) F(n) \ll N\left(\alpha + \sqrt{\rho \log(1/\alpha)}\right) + N^{1/2} t^{1/2} \rho^{1/2} \exp\left(1.5\alpha^{-1} \left(\log(1/\alpha)\right)^6\right).$$

Under the condition (2.1), we have

$$\sqrt{\rho \log(1/\alpha)} \ll \alpha,$$

while the condition (2.2) implies

$$N^{1/2} t^{1/2} \rho^{1/2} \exp\left(1.5\alpha^{-1} \left(\log(1/\alpha)\right)^6\right) \le N \rho^{1/2} \exp\left(-0.5\alpha^{-1} \left(\log(1/\alpha)\right)^6\right) \ll \alpha N,$$

and the result now follows. □

3. Proofs of Main Results

3.1. **Proof of Theorem 1.1.** We see from Lemma 2.4 and since we can take some

$$\rho \ll t^{-1} p^{1/2} \log p$$

in Lemma 2.6 we have $\rho \ll p^{-\varepsilon} \log p$, by (1.8). We thus get

$$\sqrt{\rho \log(1/\rho)} \le p^{-\varepsilon/2} \log p$$

provided that ε is sufficiently small. Now, after simple calculations, we conclude the proof.

3.2. **Proof of Theorem 1.2.** We recall the following classical identity, see [24, Section 13.4]

$$\Lambda(n) = \sum_{d|n} \mu(n/d) \log d.$$

from which we derive

$$R_\psi(N) = \sum_{\substack{d,m\geq 1\\ dm\leq N}} \mu(m)\psi\left(\xi_{dm}\right) \log d.$$

We now set

$$D = \frac{t^{1/2}\tau(t)^{1/2}}{p^{1/4}(\log p)^{1/2}} \tag{3.1}$$

where $\tau(k)$ is the divisor function, and note that by the classical bound

$$\tau(k) = k^{o(1)}, \tag{3.2}$$

(see, for example, [24, Equation (1.81)]) and the inequality (1.8), we have

$$D \geq p^{\varepsilon/2+o(1)}. \tag{3.3}$$

We now write

$$R_\psi(N) = R_I + R_{II}, \tag{3.4}$$

where

$$R_I = \sum_{d\leq t} \log d \left(\sum_{m\leq N/d} \mu(m)\psi\left(\xi_{dm}\right) \right),$$

$$R_{II} = \sum_{m\leq N/t} \mu(m) \left(\sum_{t<d\leq N/m} \psi\left(\xi_{dm}\right) \log d \right).$$

We thus need to estimate the sums R_I (a Type I sum) and R_{II} (a Type II sum).

To estimate R_I, similarly to the proof of Lemma 2.5, if we define $B = A^d$, then instead of (1.5), we can write

$$\xi_{dm} = B\left(\xi_{d(m-1)}\right) = B^m\left(\xi_0\right), \qquad m = 1, 2, \dots .$$

Hence for d with $\gcd(t,d) \le D$, we see from (1.8) that the period of the sequence ξ_{dm}, $m = 1, 2, \ldots$, is

$$\frac{t}{\gcd(t,d)} \ge t/D = \frac{t^{1/2} p^{1/4} (\log p)^{1/2}}{\tau(t)^{1/2}} \ge p^{1/2+\varepsilon/3}.$$

Thus, recalling (1.10), we see that we can apply the bound of Theorem 1.1 for every d with $\gcd(t,d) \le D$.

For d with $\gcd(t,d) > D$, we estimate the inner sum trivially as N/d. Thus, we can write

$$R_I \ll S + T, \tag{3.5}$$

where

$$S = \alpha N \sum_{\substack{d \le t \\ \gcd(d,t) \le D}} \frac{\log d}{d} \qquad \text{and} \qquad T = N \sum_{\substack{d \le t \\ \gcd(d,t) > D}} \frac{\log d}{d}.$$

To estimate S, we discard the condition $\gcd(d,t) \le D$ and thus obtain

$$S \ll \alpha N (\log t)^2 \ll \alpha N (\log p)^2. \tag{3.6}$$

To estimate T, for each divisor $s \mid t$ collecting together the values of d with $s \mid d$ and writing then as es, with $e \le t/s$, we obtain

$$T \le N \sum_{\substack{s \mid t \\ s \ge D}} \sum_{e \le t/s} \frac{\log(es)}{es} \ll \tau(t) N D^{-1} (\log p)^2. \tag{3.7}$$

Substituting (3.6) and (3.7) in (3.5), we obtain

$$R_I \le \alpha N (\log p)^2 + \tau(t) N D^{-1} (\log p)^2 \ll \alpha N (\log p)^2 \tag{3.8}$$

as by (3.2) and (3.3) the first term dominates for the above choice of parameters.

We now proceed to estimate the sum R_{II} for which by the triangle inequality, we write

$$|R_{II}| \le \sum_{m \le N/t} \left| \sum_{t < d \le N/m} \psi(\xi_{dm}) \log d \right|. \tag{3.9}$$

Furthermore, by Abel summation, we have

$$\begin{aligned}\sum_{t<d\le N/m}\psi(\xi_{dm})\log d&=\sum_{n\le N/m}\psi(\xi_{dm})\log(N/m)-\sum_{n\le t}\psi(\xi_{dm})\log D\\&\quad-\int_t^{N/m}\frac{1}{z}\sum_{n\le z}\psi(\xi_{mn})\,dz.\end{aligned}$$

We thus obtain

$$\begin{aligned}\sum_{t<d\le N/m}\psi(\xi_{dm})\log d&\ll\sup_{z\le N/m}\left|\sum_{n\le z}\psi(\xi_{mn})\right|\log(N/m)\\&\le\sup_{z\le N/m}\left|\sum_{n\le z}\psi(\xi_{mn})\right|\log N.\end{aligned}$$

This, combined with Lemma 2.5, yields

$$\begin{aligned}\sum_{t<d\le N/m}\psi(\xi_{dm})&\ll\left(\frac{N}{mt}+1\right)\gcd(m,t)p^{1/2}(\log p)\\&\ll\frac{N\gcd(m,t)p^{1/2}(\log p)}{mt}\end{aligned}$$

(as $m\le N/t$). We use this bound for $\gcd(m,t)\le D$ and $m\le N/t$ and use the trivial bound N/m otherwise. Hence, splitting the sum over m in (3.9) accordingly, we obtain

$$R_{II}\ll U+V, \tag{3.10}$$

where

$$\begin{aligned}U&=\sum_{\substack{m\le N/t\\ \gcd(m,t)\le D}}\left(\frac{N}{mt}+1\right)\gcd(m,t)p^{1/2}\log p,\\V&=N\sum_{\substack{m\le N/t\\ \gcd(m,t)>D}}\frac{1}{m}.\end{aligned}$$

We first estimate U as

$$U\le Dp^{1/2}\log p\sum_{m\le N/t}\left(\frac{N}{mt}+1\right)\le\frac{2NDp^{1/2}(\log N)(\log p)}{t}. \tag{3.11}$$

To estimate V, for each divisor $s \mid t$ collecting together the values of m with $s \mid m$ and writing then as ks, with $k \le N/(dt)$ we obtain

$$\begin{aligned} V &\le N \sum_{\substack{s \mid t \\ s \ge D}} \sum_{k \le N/(st)} \frac{1}{ks} \\ &\ll N D^{-1} \sum_{s \mid t} \sum_{k \le N/(st)} \frac{1}{k} \ll \tau(t) N D^{-1} \log N. \end{aligned} \tag{3.12}$$

Substituting (3.11) and (3.12) in (3.10) and recalling (3.1), we obtain

$$\begin{aligned} R_{II} &\ll N t^{-1} D p^{1/2} (\log N)(\log p) + \tau(t) N D^{-1} \log N \\ &\ll N \frac{\tau(t)^{1/2} p^{1/4} (\log p)^{1/2} \log N}{t^{1/2}}, \end{aligned} \tag{3.13}$$

as by appealing to (3.1) and (3.2), we conclude that the first term dominates again for the above choice of parameters.

Substituting (3.8) and (3.13) in (3.4), we see that

$$R_\psi(N) \ll \alpha N (\log p)^2 + N \frac{\tau(t)^{1/2} p^{1/4} (\log p)^{1/2} \log N}{t^{1/2}}.$$

Using that (1.8) implies $p^{1/4} t^{-1/2} \le p^{-\varepsilon/2}$, while (1.11) implies $\log N \le p^{\varepsilon/4}$, and recalling (1.10), we conclude that the first term dominates and the result follows.

Acknowledgement

This work started during a very enjoyable visit by the second author to the University of Rouen, whose support and hospitality are gratefully acknowledged.

During the preparation of this work the second author was supported in part by the Australian Research Council Grants DP170100786 and DP180100201.

References

[1] E. H. el Abdalaoui, 'On Veech's proof of Sarnak's theorem on the Möbius flow', *Preprint*, 2017, (available from https://arxiv.org/abs/1711.06326). (p. 1)

[2] E. H. el Abdalaoui, M. Lemańczyk and T. de la Rue, 'On spectral disjointness of powers for rank-one transformations and Möbius orthogonality', *J. Funct. Analysis*, **266** (2014), 284–317. (p. 1)

[3] E. H. el Abdalaoui, J. Kułaga-Przymus, M. Lemańczyk and T. de la Rue, 'The Chowla and the Sarnak conjectures from ergodic theory point of view', *Discr. Cont, Dynam. Syst., Ser. A*, **37** (2017), 2899–2944. (p. 3)

[4] T. M. Apostol, *Introduction to analytic number theory*, Undergrad, Texts in Math., Springer-Verlag, New York-Heidelberg, 1976. (p. 5)
[5] W. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski, 'Exponential sums over Mersenne numbers', *Compos. Math.*, **140** (2004), 15–30. (pp. 2, 3, and 4)
[6] W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, 'Double character sums over elliptic curves and finite fields', *Pure and Appl. Math. Quart.*, **2** (2006), 179–197. (pp. 3 and 4)
[7] W. D. Banks, J. B. Friedlander, M. Z. Garaev and I. E. Shparlinski, 'Exponential and character sums Mersenne numbers', *J. Aust. Math. Soc.*, **92** (2012), 1–13. (pp. 2, 3, and 4)
[8] J. Bourgain, 'On the pointwise ergodic theorem on L^p for arithmetic sets', *Israel J. Math.*, **61** (1988), 73–84. (p. 3)
[9] J. Bourgain, 'Estimates on exponential sums related to Diffie-Hellman distributions', *Geom. and Funct. Anal.*, **15** (2005), 1–34. (pp. 2, 3, and 4)
[10] J. Bourgain, 'On the correlation of the Möbius function with rank-one systems', *J. Anal. Math.*, **120** (2013), 105–130. (p. 1)
[11] J. Bourgain, P. Sarnak and T. Ziegler, 'Disjointness of Möbius from horocycle flow', *From Fourier Analysis and Number Theory to Radon Transforms and Geometry*, Devel. Math., vol. 28, Springer, New York, 2013, 67–83. (pp. 1, 4, 8, 9, 10, and 11)
[12] Z. Buczolich, 'Ergodic averages with prime divisor weights in L^1', *Ergodic Theory and Dynam. Syst.*, (to appear). (p. 3)
[13] D. Carmon and Z. Rudnick, 'The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field', *Quart. J. Math.*, **65** (2014), 53–61. (p. 1)
[14] W.-S. Chou, 'On inversive maximal period polynomials over finite fields', *Appl. Algebra Engrg. Comm. Comput.*, **6** (1995), 245–250. (p. 3)
[15] C. Cuny and M. Weber, 'Ergodic theorems with arithmetical weights', *Israel J. Math.*, **217** (2017), 139–180. (p. 3)
[16] T. Eisner, 'A polynomial version of Sarnak's conjecture', *C. R. Math. Acad. Sci., Paris*, **353** (2015), 569–572. (pp. 1 and 3)
[17] T. Eisner and M. Lin, 'On modulated ergodic theorems', *Preprint*, 2017, (available from https://arxiv.org/abs/1709.05322). (p. 3)
[18] G. Everest, A. van der Poorten, I. E. Shparlinski and T. Ward, *Recurrence sequences*, Math. Surveys and Monogr., **104**, Amer. Math. Soc., Providence, RI, 2003. (p. 6)
[19] S. Ferenczi, J. Kułaga-Przymus and M. Lemańczyk, 'Sarnak's conjecture – What's new', *Preprint*, 2017, (available from https://arxiv.org/abs/1710.04039) (p. 1)
[20] É. Fouvry and S. Ganguly, 'Strong orthogonality between the Möbius function, additive characters and Fourier coefficients of cusp forms', *Compos. Math.*, **150** (2014), 763–797. (p. 1)
[21] M. Z. Garaev and I. E. Shparlinski, 'The large sieve inequality with exponential functions and the distribution of Mersenne numbers modulo primes', *Intern. Math. Research Notices*, **39** (2005), 2391–2408. (pp. 3 and 4)

[22] A. Gomilko, D. Kwietniak and M. Lemańczyk, 'Sarnak's conjecture implies the Chowla conjecture along a subsequence', *Preprint*, 2017, (available from https://arxiv.org/abs/1710.07049). (p. 1)
[23] B. J. Green and T. Tao, 'The Möbius function is strongly orthogonal to nilsequences', *Ann. Math.*, **175** (2012), 541–566. (p. 1)
[24] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004. (pp. 4, 7, 9, and 13)
[25] I. Kátai. A remark on a theorem of H. Daboussi. Acta Math. Hungar. 47 (1986), 223-225. (pp. 4 and 8)
[26] J. Kułaga-Przymus and M. Lemańczyk, 'The Möbius function and continuous extensions of rotations', *Monat. Math.*, **178** (2015), 553–582. (p. 1)
[27] W.-C. W. Li, *Number theory with applications*, World Scientific, Singapore, 1996. (p. 6)
[28] J. Liu and P. Sarnak, 'The Möbius disjointness conjecture for distal flows', *Duke Math. J.*, **164** (2015), 1353–1399. (p. 1)
[29] R. Nair, 'On polynomials in primes and J. Bourgain's circle method approach to ergodic theorems', *Ergodic Th. Dyn. Syst.*, **11** (1991), 485–499. (p. 3)
[30] R. Nair, 'On polynomials in primes and J. Bourgain's circle method approach to ergodic theorems II', *Studia Math.*, **105** (1993), 207–233. (p. 3)
[31] A. Ostafe and I. E. Shparlinski, 'Exponential sums over points of elliptic curves with reciprocals of primes', *Mathematika*, **58** (2012), 21–33. (pp. 3 and 4)
[32] J. M. Rosenblatt and M. Wierdl, 'Pointwise ergodic theorems via harmonic analysis', *Ergodic Theory and its Connections with Harmonic Analysis (Alexandria, 1993)*, London Math. Soc. Lecture Note Ser., v. 205, Cambridge Univ. Press, Cambridge, 1995, 3–151. (p. 3)
[33] V. V. Ryzhikov, 'Bounded ergodic constructions, disjointness, and weak limits of powers', *Trans. Moscow Math. Soc.*, **74** (2013), 165–171. (p. 1)
[34] P. Sarnak, 'Möbius randomness and dynamics', *Not. South Afr. Math. Soc.*, **43** (2012), 89–97. (p. 1)
[35] P. Sarnak and A. Ubis, 'The horocycle flow at prime times', *J. Math. Pures Appl.*, **103** (2015), 575–618. (p. 3)
[36] T. Tao, 'Equivalence of the logarithmically averaged Chowla and Sarnak conjectures', *Number Theory – Diophantine problems, Uniform Distribution and Applications; Festschrift in Honour of Robert F. Tichy's 60th Birthday (C. Elsholtz and P. Grabner, eds.)*, Springer, 2017, 391–421. (p. 1)
[37] T. Tao and J. Teräväinen, 'The structure of logarithmically averaged correlations of multiplicative functions, with applications to the Chowla and Elliott conjectures', *Preprint*, 2017, (available from https://arxiv.org/abs/1708.02610). (p. 1)
[38] J.-P. Thouvenot, 'La convergence presque sûre des moyennes ergodiques suivant certaines sous-suites d'entiers (d'après Jean Bourgain)', *Séminaire Bourbaki, Vol. 1989/90. Astérisque* **189–190** (1990), Exp. No. 719, 133–153. (p. 3)
[39] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974. (p. 6)
[40] M. Wierdl, 'Pointwise ergodic theorem along the prime numbers', *Israel J. Math.*, **64** (1988), 315–336. (p. 3)

Laboratoire de Mathématiques Raphaël Salem, Université de Rouen Normandie, F76801 Saint-Étienne-du-Rouvray, France

E-mail address: elhoucein.elabdalaoui@univ-rouen.fr

School of Mathematics and Statistics, University of New South Wales, Sydney NSW 2052, Australia

E-mail address: igor.shparlinski@unsw.edu.au