ON THE CORRELATIONS BETWEEN CHARACTER SUMS OF DIVISION POLYNOMIALS UNDER SHIFTS

SUBHAM BHAKTA AND IGOR E. SHPARLINSKI

ABSTRACT. Let E be an elliptic curve over the finite field $\mathbb{F}_p$, and $P \in E(\mathbb{F}_p)$ be an $\mathbb{F}_p$-rational point. We study the sums

$$S_{\chi,P}(N,h) = \sum_{n=1}^{N} \chi(\psi_n(P))\chi(\psi_{n+h}(P)),$$

where $\psi_n(P)$ denotes the n-th division polynomial evaluated at P, and χ is a multiplicative character of $\mathbb{F}_p^*$. We estimate $S_{\chi,P}(N,h)$ on average over h over a rather short interval $h \in [1, H]$. We also obtain a multidimensional generalisation of this result.

CONTENTS

1. INTRODUCTION

1.1. **Set-up and motivation.** Let E be an elliptic curve over $\mathbb{F}_p$ of characteristic $p > 3$ given by the Weierstrass equation as following, with coefficients in $\mathbb{F}_p$.

$$y^2 = x^3 + ax + b.$$

For any integer $n \geqslant 0$, define the nth division polynomial $\psi_n \in \mathbb{F}_p[x,y]$ as follows.

$$\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y,$$
$$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$
$$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$

for more details, see [**?**, Exercise 3.7], combined with the discussion in [**?**, Chapter III.1].

Denote by $E(\mathbb{F}_p)$ the group of points on E defined over $\mathbb{F}_p$. We can interpret each ψ_n as rational functions on $E(\mathbb{F}_p)$. The multiplication

---

of $P \in E$ by n is given as a rational map by

$$[n](P) = \left(\frac{x(P)\psi_n^2(P) - \psi_{n-1}(P)\psi_{n+1}(P)}{\psi_n(P)^2}, \right.$$
$$\left. \frac{\psi_{n-1}(P)^2\psi_{n+2}(P) - \psi_{n-2}(P)\psi_{n+1}(P)^2}{4y(P)\psi_n(P)^3} \right).$$

It is well known that

$$\psi_{m+n}(P)\psi_{m-n}(P)\psi_r^2(P)$$
$$= \psi_{m+r}(P)\psi_{m-r}(P)\psi_n^2(P) - \psi_{n+r}(P)\psi_{n-r}(P)\psi_m(P)^2,$$

for any integers m, n, r, see, for example, [?, Exercise 3.7(g)]. It turns out that $\psi_n(P)$ is periodic, and the period T, which could be as large as $(p-1)\operatorname{ord} P$, where $\operatorname{ord} P$ is the order of P in the group $E(\mathbb{F}_p)$, see [?, Corollary 9].

Let χ be a multiplicative character of $\mathbb{F}_p^*$. We consider the sequence $\chi(\psi_n(P))$, where of course we set $\chi(0) = 0$. Then, $\chi(\psi_n(P))$ is periodic with a much smaller period (see Section ??), compared to the period of $\psi_n(P)$. For points $P \in E(\mathbb{F}_p)$ of large orders, Shparlinski and Stange [?] have studied the character sums of the form

$$S_{\chi,P}(N) = \sum_{n=1}^{N} \chi(\psi_n(P)),$$

for the quadratic character of $\mathbb{F}_p$ and optained a nontrivial bound provided $\operatorname{ord} P \geqslant N \geqslant p^{1/2+\varepsilon}$ for some fixed $\varepsilon > 0$.

Here, we study a related but more difficult question on the correlation of $\chi(\psi_n(P))$ with its shifts, that is, about bounding the sums

$$S_{\chi,P}(N, h) = \sum_{n=1}^{N} \chi(\psi_n(P))\chi(\psi_{n+h}(P))$$

with an integer $h \neq 0$. More precisely, we ask the following:

Question 1.1. *Let p be a prime, $P \in E(\mathbb{F}_p)$ be a point and χ be a multiplicative character of $\mathbb{F}_p^*$. When do we have*

$$S_{\chi,P}(N, h) = o(N)?$$

Due to the limitations of our techniques, we do not have an affirmative answer to the question above. However, we prove an average version. For instance, we estimate the following sum

$$\sum_{h=1}^{H} |S_{\chi,P}(N,h)| = \sum_{h=1}^{H} \left| \sum_{n=1}^{N} \chi(\psi_n(P))\chi(\psi_{n+h}(P)) \right|.$$

Question **??** itself, as well as our results, are motivated by the progress towards the Chowla conjecture for $\lambda(n)$ and $\mu(n)$, that is, for the Liouville and Möbius functions, respectively.

It is well-known that the prime number theorem is equivalent to any of the following statements

$$\sum_{n=1}^{N} \lambda(n) = o(N) \quad \text{and} \quad \sum_{n=1}^{N} \mu(n) = o(N), \qquad \text{as } N \to \infty,$$

Chowla [**?**] has conjectured that for any integer $h > 0$, the following holds

$$(1.1) \quad \sum_{n=1}^{N} \lambda(n)\lambda(n + h) = o(N) \quad \text{and} \quad \sum_{n=1}^{N} \mu(n)\mu(n + h) = o(N),$$

as $N \to \infty$.

Despite several striking results towards these conjectures, both remain widely open, see [**?, ?, ?, ?, ?**] and references therein. An averaged version of this conjecture has been studied in [**?**], in fact for a more general class of multiplicative functions. Our function $\chi(\psi_n(P))$ is not multiplicative, although it satisfies an *almost multiplicative* property, as stated in Lemma **??**. Thus, Question **??** essentially studies an elliptic analogue of Chowla's conjectures (**??**), for the function $\chi(\psi_n(P))$, and also remains widely open.

1.2. **Notation.**

Throughout the whole article, as usual, the notations $U = O(V)$, $U \ll V$, and $V \gg U$ are equivalent to $|U| \leqslant cV$ for some positive constant c, which may depend on the the order d of the multiplicative character χ and on the dimension m.

We use $\omega(n)$ and $\tau(n)$ to denote the number of distinct prime and positive integer factors of an integer $n \neq 0$ and use $\varphi(n)$ to denote the Euler function.

We also denote $\mathbf{e}_R(n) = \exp(2\pi i n/R)$.

Everywhere, we use p to denote a prime, and h, k, m, n are reserved for integers.

1.3. **Main result.**

Let χ be a multiplicative character on $\mathbb{F}_p^*$ of order d, and $P \in E(\mathbb{F}_p)$ be a point. Denote $\operatorname{ord} P$ be the order of P in $E(\mathbb{F}_p)$, and set

$$(1.2) \qquad\qquad R = d \operatorname{ord} P.$$

Applying [**?**, Lemma 3.1] for $s = d$, the sequences $\chi(\psi_n(P))$ is periodic with a period dividing R, as long as $\operatorname{ord} P \geqslant 3$.

Here, given m integers $h_1, \ldots, h_m$, we consider the following average values of multidimensional correlations between the values of $\chi(\psi_n(P))$:

$$U_{m,\chi,P}(H, N) = \frac{1}{H^{m-1}} \sum_{h_2,\ldots,h_m=1}^{H} \left| \sum_{n=1}^{N} \chi(\psi_n(P)) \prod_{j=2}^{m} \chi(\psi_{n+h_j}(P)) \right|,$$

$$V_{m,\chi,P}(H, N) = \frac{1}{H^m} \sum_{h_1,\ldots,h_m=1}^{H} \left| \sum_{n=1}^{N} \prod_{j=1}^{m} \chi(\psi_{n+h_j}(P)) \right|.$$

Theorem 1.2. *For any integer $m \geqslant 2$, and integers $1 \leqslant H, N \leqslant R$, we have*

$$U_{m,\chi,P}(H, N), V_{m,\chi,P}(H, N)$$

$$\text{(1.3)} \qquad\qquad \ll H^{-1/8} R \exp\left(O\left((\log R)^{1/2}/\log\log R\right)\right)$$

$$+ H^{1/2} R^{3/4} p^{1/8} \log R,$$

and if $R \geqslant p^{1/2} \exp\left(2.1 \log p / \log\log p\right)$, then we also have

$$U_{m,\chi,P}(H, N), V_{m,\chi,P}(H, N)$$

$$\text{(1.4)} \qquad\qquad \ll H^{-1/4} R^{7/6} p^{1/24} (\log R)(\log\log R)^{1/6}.$$

Remark 1.3. It is easy to see from the proof of Theorem **??** that for complete sums $N = R$, one can remove $\log R$ from the second term of the bound (**??**) and from the bound (**??**).

To understand the strength of Theorem **??** we consider the extreme case of very long sums with $R \geqslant N \gg R$. Then the bound (**??**) is nontrivial in the range

$$\exp\left(C(\log R)^{1/2}/\log\log R\right) \leqslant H \leqslant R^{1/2} p^{-1/4} (\log R)^{-2} f(p)^{-1}$$

for some absolute constant $C > 0$ and any function $f(p) \to 0$ as $p \to \infty$. In fact, for any fixed $\varepsilon > 0$, Remark **??** allows us to have a non-trivial bound in the extended lower range

$$H \geqslant \exp\left(C_\varepsilon (\log R)^\varepsilon\right),$$

where $C_\varepsilon > 0$ is a constant depending on ε.

On the other hand, the bound (**??**) is nontrivial only when H is quite large, namely $R \geqslant H \geqslant R^{2/3} p^{1/6} (\log\log R)^{2/3} F(p)$ with any function $F(p) \to \infty$ as $p \to \infty$.

Unfortunately there is a wide gap between this ranges as

$$R^{2/3} p^{1/6} / R^{1/2} p^{-1/4} \geqslant p^{5/12} R^{1/6} \gg p^{1/2}.$$

(since the we have $R \geqslant p^{1/2}$ for either of the bounds (**??**) and (**??**) to be nontrivial). Closing this gap is certainly an interesting open question.

Another interesting regime is $H = N$. In this case the bound (**??**) is always trivial, while (**??**) requires

$$R \geqslant H = N \geqslant R^{14/15} p^{1/30} (\log R)^{4/5} (\log \log R)^{2/15} F(p)$$

with $F(p) \to \infty$ as $p \to \infty$.

In a response to Question **??**, we have the following simple application of Theorem **??**. Namely, taking $m = 2$ and applying (**??**) we immediately derive the following result.

Corollary 1.4. *Let* $\Delta > 0$ *be an arbitrary real number. If* $R \geqslant p^{1/2} \exp\left(2.1 \log p / \log \log p\right)$ *then, we have*

$$\sharp \left\{1 \leqslant h \leqslant H : |S_{\chi,P,h}(N)| \geqslant \Delta N\right\}$$
$$\ll \Delta^{-1} H^{3/4} N^{-1} R^{7/6} p^{1/24} (\log \log R)^{1/6}.$$

We note that, ignoring logarithmic terms, Corollary **??** produces a meaningful result if $H^{1/4} N \geqslant R^{7/6} p^{1/24+\varepsilon}$ for some fixed $\varepsilon > 0$.

2. Preliminaries

2.1. **Some properties of division polynomials.** We have an *almost multiplicative* nature of $\chi(\psi_n(P))$, which is given in [**?**, Lemma 3.2].

Lemma 2.1. *Let* χ *be a multiplicative character. Then for any integers* m, n *we have*

$$\chi(\psi_{mn}(P)) = \chi(\psi_m(nP))\chi(\psi_n(P))^{m^2}.$$

As usual, for any $\Psi \in \mathbb{F}_p(E)$, we define

$$\deg \Psi = \sum_{\substack{P \in E(\overline{\mathbb{F}_p}) \\ \nu_P(\Psi) > 0}} \nu_P(\Psi),$$

where $\nu_P(\Psi)$ is the multiplicity of P as a zero of Ψ (and thus this is a finite sum over all zeros P of Ψ).

Moreover, we also need the following results to show that a certain class of functions satisfies the requirement of Lemma **??** below.

Lemma 2.2. *Let* m *be any integer such that* $\mathrm{ord}(P) \nmid m$. *For positive integers* $k \neq \ell$ *with* $\gcd(k\ell, R) = 1$, *we consider the function*

$$\Psi_P(Q) = \psi_k(Q) \cdot \psi_k^{-1}(Q + mP) \cdot \psi_\ell^{-1}(Q) \cdot \psi_\ell(Q + mP).$$

Then,
  (i) $\deg \Psi_P < 2(k^2 + \ell^2)$;
  (ii) Ψ_P *is not a non-trivial power of any function in the function field* $\overline{\mathbb{F}_p(E)}$.

Proof. Proof of (i) is clear, as each ψ_h has $h^2 - 1$ simple zeroes, see [**?**, Exercise III.3.7].

To prove (ii), let us assume that $\Psi_P = G^\nu$ for some $\nu \geqslant 2$ and $G \in \overline{\mathbb{F}_p(E)}$. In particular, the function

$$\widetilde{\Psi}_P(Q) = \Psi_P(Q) \cdot \psi_\ell^2(Q) \cdot \psi_k^2(Q + mP)$$

has the property that each zero of $\widetilde{\Psi}_P$ has multiplicity at least two.

Without loss of generality, let us assume that $k > \ell$. Since, as we have mentioned, the polynomial ψ_k has $k^2 - 1 > 1$ simple roots in $\overline{\mathbb{F}_p}$, each root Q_0 of ψ_k, is also a root at least one of the $\psi_k(Q_0 + mP)$, $\psi_\ell(Q_0)$ or $\psi_\ell(Q_0 + mP)$ is zero.

Of course, we have $k^2 - \ell^2 \geqslant 3$. Therefore, we can choose Q_0 so that $\psi_\ell(Q_0) \neq 0$. Now, if either of $\psi_k(Q_0 + mP) = 0$ or $\psi_\ell(Q_0 + mP) = 0$ is zero and thus $k\ell mP = 0$. However, since $\text{ord}\,P \nmid m$ this contradicts our assumption $\gcd(k\ell, \text{ord}\,P) = 1$ and concludes the proof. □

2.2. **Some character sums with division polynomials.** We now derive from [**?**, Lemma 4.2].

Lemma 2.3. *Let χ be any non-principal multiplicative character on $\mathbb{F}_p^*$, R be as in* (**??**)*, and $\Psi \in \mathbb{F}_p(E)$ be of degree $\deg \Psi$. Assume that Ψ is not a non-trivial power of a function in $\overline{\mathbb{F}_p(E)}$. Then, we have the following estimate for any integer a*

$$\sum_{n=1}^{R} \chi(\Psi(nP))\,\mathbf{e}_R(an) \ll \deg \Psi \cdot \sqrt{p}.$$

Proof. Since $R = dr$, where $r = \text{ord}\,P$, we can write

$$\sum_{n=1}^{R} \chi(\Psi(nP))\,\mathbf{e}_R(an) = \sum_{k=0}^{d-1}\sum_{n=1}^{r} \chi(\Psi((nd-k)P))\,\mathbf{e}_R(a(nd-k))$$

$$= \sum_{k=0}^{d-1} \mathbf{e}_R(-ak) \sum_{n=1}^{r} \chi(\Psi((nd-k)P))\,\mathbf{e}_r(an).$$

The result now follows by applying [**?**, Lemma 4.2] to each of the inner sums over n. □

Consequently, we deduce the following estimate.

Lemma 2.4. *Assume that $R \geqslant p^{1/2}\exp\left(2.1\log p/\log\log p\right)$. For any integer a, we have*

$$\sum_{n=1}^{R} \chi(\psi_n(P))\,\mathbf{e}_R(an) \ll p^{1/12}R^{5/6}(\log\log R)^{1/3}.$$

Proof. The proof proceeds in the same manner as that of [**?**, Theorem 5.1]; for completeness, we briefly sketch the argument. The only modification involves the choice of the set of integers

$$\mathcal{R}_d = \{1 \leqslant r \leqslant L : \ r \equiv 1 \bmod d, \ \gcd(r, R) = 1\},$$

for a suitably chosen parameter L. Let Q be the largest factor of R with $\gcd(d, Q) = 1$. Clearly for $r \equiv 1 \bmod d$ the condition $\gcd(r, R) = 1$ is equivalent to $\gcd(r, Q) = 1$. Writing $r = du + 1$, a simple inclusion–exclusion argument gives

$$\sharp \mathcal{R}_d = \sum_{e|Q} \mu(e) \sum_{\substack{0 \leqslant u \leqslant (L-1)/d \\ du+1 \equiv 0 \bmod e}} 1 = \sum_{e|Q} \mu(e) \left(\frac{L-1}{de} + \vartheta_e \right)$$

with some $\vartheta_e \in [-1, 1]$, $e \mid Q$. Hence, for some $\vartheta \in [-1, 1]$, we have

$$\sharp \mathcal{R}_d = \sum_{e|Q} \mu(e) \sum_{\substack{0 \leqslant u \leqslant (L-1)/d \\ du+1 \equiv 0 \bmod e}} 1 = \sum_{e|Q} \mu(e) \left(\frac{L-1}{de} + \vartheta_e \right)$$

$$= \frac{L-1}{d} \sum_{e|Q} \frac{\mu(e)}{e} + \vartheta \tau(Q) = \frac{L-1}{d} \prod_{\substack{\ell|Q \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell} \right) + \vartheta \tau(Q)$$

$$= \frac{\varphi(Q)(L-1)}{dQ} + \vartheta \tau(Q),$$

see [**?**, Theorem 62].

Thus, using the elementary observations

$$\frac{\varphi(Q)}{Q} \geqslant \frac{\varphi(R)}{R} \qquad \text{and} \qquad \tau(Q) \leqslant \tau(R)$$

and the following well-known estimates

$$\tau(R) \leqslant \exp\left((\log 2 + o(1)) \log R / \log \log R \right) \quad \text{and} \quad \varphi(R) \gg \frac{R}{\log \log R},$$

as $R \to \infty$, see [**?**, Theorems 317 and 328], we see that

$$\sharp \mathcal{R}_d \geqslant \frac{\varphi(R)(L-1)}{dR} - \tau(R) \gg \frac{L}{\log \log R}$$

provided that

(2.1) $$L \geqslant \exp\left(0.7 \log p / \log \log p \right).$$

The desired sum is then bounded by $|W|$, where

$$W = \frac{1}{\sharp \mathcal{R}_d} \sum_{r \in \mathcal{R}_d} \sum_{n=1}^{R} \chi(\psi_{nr}(P)) \, \mathbf{e}_R(anr).$$

We interchange the sums and apply the Cauchy–Schwarz inequality, as exactly done in [**?**, Theorem 5.1]. Thanks to Lemma **??**, we have the following identity for any $r \in \mathcal{R}_d$

$$\chi(\psi_{nr}(P)) = \chi(\psi_n(P))\chi(\psi_r(nP)).$$

Applying the identity, we have

$$W^2 \leqslant \frac{R}{(\sharp \mathcal{R}_d)^2} \sum_{n=1}^{R} \left| \sum_{r \in \mathcal{R}_d} \chi(\psi_r(nP)) \, \mathbf{e}_R(anr) \right|^2$$

$$\leqslant \frac{R}{(\sharp \mathcal{R}_d)^2} \sum_{r_1, r_2 \in \mathcal{R}_d} \left| \sum_{n=1}^{R} \chi(\Psi_{r_1,r_2}(nP)) \, \mathbf{e}_R(a(r_1 - r_2)n) \right|,$$

where $\Psi_{r_1,r_2} \in \mathbb{F}_p(E)$ is given by the following

$$\Psi_{r_1,r_2}(Q) = \psi_{r_1}(Q) \cdot \psi_{r_2}^{-1}(Q).$$

For any $r_1 \neq r_2$, it is clear that Ψ_{r_1,r_2} is not power of a function in $\overline{\mathbb{F}_p(E)}$ (since zeros of $\psi_r(Q)$ in the function field of E are exactly distinct torsion points of order dividing r, see also the proof of Lemma **??**).

Estimating the contributions from the integers $r_1 = r_2 \in \mathcal{R}_d$ trivially, and applying Lemma **??** for each such $r_1 \neq r_2 \in \mathcal{R}_d$, we have

$$W \ll R \, (\sharp \mathcal{R}_d)^{-1/2} + R^{1/2} L p^{1/4}$$

$$\ll R L^{-1/2} (\log \log R)^{1/2} + R^{1/2} L p^{1/4}.$$

The result follows by choosing $L = R^{1/3} p^{-1/6} (\log \log p)^{1/3}$, as clearly it satisfies (**??**) due to the assumption on R. $\square$

3. Bounds of some double character sums with division polynomials

3.1. **Small H.** We denote $\overline{\chi}$ to be the complex conjugate character of a multiplicative character χ of $\mathbb{F}_p^*$, that is, $\chi \overline{\chi} = 1$. To prove Theorem **??**, we first need the following estimate regarding the correlation between χ and $\overline{\chi}$.

Denote

$$T_{\chi,P}(H) = \sum_{h=1}^{H} \left| \sum_{n=1}^{R} \chi(\psi_n(P)) \overline{\chi}(\psi_{n+h}(P)) \right|^2.$$

Lemma 3.1. *Let R be as in (**??**). For any integer $1 \leqslant H \leqslant R$, we have*

$$T_{\chi,P}(H) \ll H^{1/2} R^2 \exp\left(O\left((\log R)^{1/2} / \log \log R \right) \right) + H^3 R p^{1/2}.$$

Proof. Let $\mathcal{E}$ be the set of positive integers $e \leqslant H$ which factors into primes which are also prime divisors of R. For each $e \in \mathcal{E}$ we consider the following set of integers

$$\mathcal{K}_e = \{1 \leqslant k \leqslant H/e : \ \gcd(k, R) = 1\}.$$

Clearly we have the following partition

$$\{1, \ldots, H\} = \bigsqcup_{e \in \mathcal{E}} (e\mathcal{K}_e)$$

in disjointed sets $e\mathcal{K}_e = \{ek : \ k \in \mathcal{K}_e\}$. Hence

$$(3.1) \qquad T_{\chi, P}(H, N) \leqslant \sum_{e \in \mathcal{E}} S_e,$$

where

$$S_e = \sum_{k \in \mathcal{K}_e} \left| \sum_{n=1}^{R} \chi(\psi_n(P)) \overline{\chi}(\psi_{n+ek}(P)) \right|^2.$$

Clearly, we can replace n in the inner sums with kn for any $k \in \mathcal{K}_e$, hence

$$S_e = \sum_{k \in \mathcal{K}_e} \left| \sum_{n=1}^{R} \chi(\psi_{kn}(P)) \overline{\chi}(\psi_{k(n+e)}(P)) \right|^2.$$

For any $k \in \mathcal{K}_e$, by Lemma **??** we have the following identity

$$\chi(\psi_{kn}(P)) \overline{\chi}(\psi_{k(n+e)}(P))$$
$$= \chi\left(\psi_k(nP) \psi_k^{-1}((n+e)P) \right) \chi\left(\psi_n(P) \psi_{n+e}^{-1}(P) \right)^{2k^2},$$

with the convention that if $\psi_k((n+e)P) = 0$ or $\psi_{n+e}(P) = 0$ then the whole expression is equal to zero. We follow a similar convention below as well.

Therefore,

$$(3.2) \qquad S_e \leqslant \sum_{j=1}^{d} W_{j,e},$$

with

$$W_{j,e} = \sum_{\substack{k \in \mathcal{K}_e \\ k \equiv j \bmod d}} \left| \sum_{n=1}^{R} \chi \left(\psi_k \left(nP \right) \psi_k^{-1} \left((n+e)P \right) \right) \right.$$

$$\left. \chi \left(\psi_n(P) \psi_{n+e}^{-1}(P) \right)^{2k^2} \right|^2$$

$$= \sum_{m,n=1}^{R} \chi \left(\psi_m(P) \cdot \psi_{m+e}^{-1}(P) \cdot \psi_n^{-1}(P) \cdot \psi_{n+e}(P) \right)^{2j^2}$$

$$\sum_{\substack{k \in \mathcal{K}_e \\ k \equiv j \bmod d}} \Xi_{k,m,n},$$

where we denote

$$\Xi_{k,m,n} = \chi \left(\psi_k \left(mP \right) \psi_k^{-1} \left((m+e)P \right) \right) \overline{\chi} \left(\psi_k \left(nP \right) \psi_k^{-1} \left((n+e)P \right) \right).$$

By the Cauchy–Schwarz inequality, and changing the order of summation, we see that

$$W_{j,e}^2 \leqslant R^2 \sum_{m,n=1}^{R} \left| \sum_{\substack{k \in \mathcal{K}_e \\ k \equiv j \bmod d}} \Xi_{k,m,n} \right|^2$$

$$= R^2 \sum_{\substack{k,\ell \in \mathcal{K}_e \\ k \equiv \ell \equiv j \bmod d}} \sum_{m,n=1}^{R} \Xi_{k,m,n} \overline{\Xi_{\ell,m,n}}.$$

Denoting

$$\Psi_{k,\ell}(Q) = \psi_k(Q) \cdot \psi_k^{-1}(Q + eP) \cdot \psi_\ell^{-1}(Q) \cdot \psi_\ell(Q + eP),$$

we see that

$$W_{j,e}^2 \leqslant R^2 \sum_{\substack{k,\ell \in \mathcal{K}_e \\ k \equiv \ell \equiv j \bmod d}} \sum_{m,n=1}^{R} \chi \left(\Psi_{k,\ell}(nP) \right) \overline{\chi \left(\Psi_{k,\ell}(mP) \right)}$$

$$= R^2 \sum_{\substack{k,\ell \in \mathcal{K}_e \\ k \equiv \ell \equiv j \bmod d}} \left| \sum_{n=1}^{R} \chi(\Psi_{k,\ell}(nP)) \right|^2.$$

By Lemma **??** we have

$$\deg \Psi_{k,\ell} \ll k^2 + \ell^2 \ll (H/e)^2.$$

In particular, using Lemma **??** for any distinct integers $k, \ell \in \mathcal{K}_e$ and estimating the contribution from $k = \ell$ trivially, since the implied constants may depend on d, we obtain

$$W_{j,e}^2 \ll R^2 \left(\sharp \mathcal{K}_e R^2 + (\sharp \mathcal{K}_e)^2 \left(\left(He^{-1} \right)^2 p^{1/2} \right)^2 \right).$$

Since $\sharp \mathcal{K}_e \leqslant H/e$, we see that

$$W_{j,e} \ll H^{1/2} R^2 e^{-1/2} + H^3 R p^{1/2} e^{-3}.$$

Substituting this bound in (**??**), we derive

$$S_e \ll H^{1/2} R^2 e^{-1/2} + H^3 R p^{1/2} e^{-3}.$$

Recalling (**??**), we see that

$$T_{\chi,P}(H) \ll \sum_{e \in \mathcal{E}} \left(H^{1/2} R^2 e^{-1/2} + H^3 R p^{1/2} e^{-3} \right)$$

(3.3)
$$\ll H^{1/2} R^2 \sum_{e \in \mathcal{E}} e^{-1/2} + H^3 R p^{1/2} \sum_{e \in \mathcal{E}} e^{-3}$$

$$\ll H^{1/2} R^2 \rho + H^3 R p^{1/2},$$

where

$$\rho = \sum_{e \in \mathcal{E}} e^{-1/2}.$$

Let $\nu = \omega(R)$ and let p_i denote the ith prime. Then

$$\rho \leqslant \prod_{p \mid R} \sum_{j=1}^{\infty} p^{-j/2} \leqslant \prod_{i=1}^{\nu} \sum_{j=1}^{\infty} p_i^{-j/2}$$

(3.4)
$$= \prod_{i=1}^{\nu} \left(1 + p_i^{-1/2} + O\left(p_i^{-1} \right) \right) = \exp \lambda,$$

where

$$\lambda = \sum_{i=1}^{\nu} \log \left(1 + p_i^{-1/2} + O(p_i^{-1}) \right) \ll \sum_{i=1}^{\nu} p_i^{-1/2}$$

(3.5)
$$\ll \sum_{i=1}^{\nu} (i \log i)^{-1/2} \ll \nu^{1/2} (\log \nu)^{-1/2}.$$

Since obviously $\nu! \leqslant R$, from the Stirling formula, we see that

$$\nu \ll \frac{\log R}{\log \log R}$$

and thus $\rho \leqslant \exp \left(O \left((\log R)^{1/2} / \log \log R \right) \right)$. Substituting this bound on ρ in (**??**), we conclude the proof. $\qquad \square$

Remark 3.2. Using the so-called Rankin method, that is, using that for any $\gamma > 0$, similarly to (**??**) and (**??**), we have

$$\rho = \sum_{e \in \mathcal{E}} e^{-1/2} \leqslant \sum_{\substack{e \in \mathbb{N} \\ p|e \Rightarrow p|R}} e^{-1/2} \left(\frac{H}{e}\right)^\gamma \ll H^\gamma \sum_{i=1}^\nu (i \log i)^{-1/2-\gamma}$$

$$= H^\gamma \nu^{1/2-\gamma} (\log \nu)^{-1/2-\gamma}$$

$$= H^\gamma \exp\left(O\left((\log R)^{1/2-\gamma}/\log\log R\right)\right),$$

and optimising the choice of γ one can obtain a slightly more precise bound when H is small.

3.2. **Large H.** In this section, we obtain a similar estimate for the correlation between χ and $\overline{\chi}$ as in Lemma **??**, for a large H.

We first estimate $T_{\chi,P}(H)$ for $H = R$.

Lemma 3.3. *Assume that $R \geqslant p^{1/2} \exp\left(2.1 \log p/\log\log p\right)$. Then, we have*

$$T_{\chi,P}(R) \ll R^{8/3} p^{1/6} (\log\log R)^{2/3}.$$

Proof. Using that $\chi(\psi_k(P))$, $k = 1, 2, \ldots$, is periodic with period R, we can derive

$$T_{\chi,P}(R)$$
$$= \sum_{h=1}^R \left|\sum_{n=1}^R \chi(\psi_n(P))\overline{\chi}(\psi_{n+h}(P))\right|^2$$
$$= \sum_{m,n=1}^R \chi(\psi_m(P))\overline{\chi}(\psi_n(P)) \sum_{h=1}^R \chi(\psi_{m+h}(P))\overline{\chi}(\psi_{n+h}(P))$$
$$= \sum_{\substack{m_1,m_2,n_1,n_2=1 \\ m_1-m_2 \equiv n_1-n_2 \bmod R}}^R \chi(\psi_{m_1}(P))\overline{\chi}(\psi_{n_1}(P)\chi(\psi_{m_2}(P))\overline{\chi}(\psi_{n_2}(P)).$$

Using the orthogonality of exponential functions, we write

$$
\begin{aligned}
T_{\chi,P}(R) & \\
&= \sum_{m_1,m_2,n_1,n_2=1}^{R} \chi(\psi_{m_1}(P))\overline{\chi}(\psi_{n_1}(P)\chi(\psi_{m_2}(P))\overline{\chi}(\psi_{n_2}(P)) \\
& \qquad\qquad\qquad\qquad \cdot \frac{1}{R}\sum_{\lambda=1}^{R} \mathbf{e}_R\left(\lambda\left(m_1 - m_2 - n_1 + n_2\right)\right) \\
&= \frac{1}{R}\sum_{\lambda=1}^{R} \left|\sum_{n=1}^{R}\chi(\psi_n(P))\,\mathbf{e}_R(\lambda n)\right|^2 \left|\sum_{n=1}^{R}\chi(\psi_n(P))\,\mathbf{e}_R(-\lambda n)\right|^2 .
\end{aligned}
$$

Applying Lemma **??** and the orthogonality of exponential functions to the remaining sum we see that

$$
\begin{aligned}
\sum_{h=1}^{R}\left|\sum_{n=1}^{R}\chi(\psi_n(P))\overline{\chi}(\psi_{n+h}(P))\right|^2 & \\
&\ll \left(R^{5/6}p^{1/12}(\log\log R)^{1/3}\right)^2 \frac{1}{R}\sum_{\lambda=1}^{R}\left|\sum_{n=1}^{R}\chi(\psi_n(P))\,\mathbf{e}_R(\lambda n)\right|^2 \\
&\ll \left(R^{5/6}p^{1/12}(\log\log R)^{1/3}\right)^2 R = R^{8/3}p^{1/6}(\log\log R)^{2/3},
\end{aligned}
$$

which concludes the proof. □

4. Proof of Theorem **??**

4.1. **Preliminaries.** We start with the following bound on weighted sums.

Lemma 4.1. *Let R be as in* (**??**)*, and let α_n, $n = 1,\ldots,R$, be a sequence of weights with $|\alpha_n| \leqslant 1$. Then, we have*

$$
\frac{1}{H}\sum_{h=1}^{H}\left|\sum_{n=1}^{R}\alpha_n\chi(\psi_{n+h}(P))\right| \ll H^{-1/4}\left(R^{1/2}\,|T_{\chi,P}(H)|^{1/4} + R\right).
$$

Proof. Denote

$$
S = \sum_{h=1}^{H}\left|\sum_{n=1}^{R}\alpha_n\chi(\psi_{n+h}(P))\right|.
$$

By the Cauchy–Schwarz inequality,

$$|S|^2 \leqslant H \sum_{h=1}^{H} \left| \sum_{n=1}^{R} \alpha_n \chi(\psi_{n+h}(P)) \right|^2$$

$$\leqslant H \sum_{m,n=1}^{R} \overline{\alpha_m} \alpha_n \sum_{h=1}^{H} \chi(\psi_{m+h}(P)) \overline{\chi}(\psi_{n+h}(P)).$$

In particular, we have

$$|S|^2 \leqslant H \sum_{m,n=1}^{R} \left| \sum_{h=1}^{H} \chi(\psi_{m+h}(P)) \overline{\chi}(\psi_{n+h}(P)) \right|.$$

Applying the Cauchy–Schwarz inequality again, we get

$$|S|^4 \leqslant H^2 R^2 \sum_{m,n=1}^{R} \left| \sum_{h=1}^{H} \chi(\psi_{m+h}(P)) \overline{\chi}(\psi_{n+h}(P)) \right|^2$$

$$= H^2 R^2 \sum_{m,n=1}^{R} \sum_{h,k=1}^{H} \chi(\psi_{m+h}(P)) \overline{\chi}(\psi_{n+h}(P))$$

$$\cdot \overline{\chi}(\psi_{m+k}(P)) \chi(\psi_{n+k}(P)).$$

By periodicity, we now have

$$|S|^4 \leqslant H^3 R^2 \sum_{|h| \leqslant H} \left| \sum_{m,n=1}^{R} \chi(\psi_m(P)) \overline{\chi}(\psi_n(P)) \overline{\chi}(\psi_{m+h}(P)) \chi(\psi_{n+h}(P)) \right|$$

$$= H^3 R^2 \sum_{|h| \leqslant H} \left| \sum_{n=1}^{R} \chi(\psi_n(P))) \overline{\chi}(\psi_{n+h}(P)) \right|^2$$

$$= 2H^3 R^2 \sum_{h=1}^{H} \left| \sum_{n=1}^{R} \chi(\psi_n(P))) \overline{\chi}(\psi_{n+h}(P)) \right|^2 + H^3 R^4$$

$$= 2H^3 R^2 T_{\chi,P}(H) + H^3 R^4,$$

and the result follows.   □

Let a be an arbitrary integer. Applying Lemma **??**, we have

$$\frac{1}{H^{m-1}} \sum_{h_2,\ldots,h_m=1}^{H} \left| \sum_{n=1}^{R} \chi(\psi_n(P)) \prod_{j=2}^{m} \chi(\psi_{n+h_j}(P)) \, \mathbf{e}_R(an) \right|$$

$$\ll H^{-1/4} \left(R^{1/2} |T_{\chi,P}(H)|^{1/4} + R \right).$$

On the other hand, by the periodicity and Lemma **??**, we have

$$\frac{1}{H^m} \sum_{h_1,\ldots,h_m=1}^{H} \left| \sum_{n=1}^{R} \chi(\psi_{n+h_1}(P)) \prod_{j=2}^{m} \chi(\psi_{n+h_j}(P)) \, \mathbf{e}_R(an) \right|$$

$$= \frac{1}{H^m} \sum_{h_1,\ldots,h_m=1}^{H} \left| \sum_{n=1}^{R} \chi(\psi_n(P)) \prod_{j=2}^{m} \chi(\psi_{n+h_j-h_1}(P)) \, \mathbf{e}_R(an) \right|$$

$$\ll H^{-1/4} \left(R^{1/2} \, |T_{\chi,P}(H)|^{1/4} + R \right).$$

By the completing technique, see [**?**, Lemma 12.1], we have

$$U_{m,\chi,P}(H,N), V_{m,\chi,P}(H,N) \ll H^{-1/4} \left(R^{1/2} \, |T_{\chi,P}(H)|^{1/4} + R \right) \log R.$$

4.2. **Concluding the proof.** Now, applying Lemma **??**, we have

$$U_{m,\chi,P}(H,N), V_{m,\chi,P}(H,N)$$
$$\ll H^{-1/8} R \exp \left(O \left((\log R)^{1/2} / \log \log R \right) \right)$$
$$+ H^{1/2} R^{3/4} p^{1/8} \log R + H^{-1/4} R \log R.$$

Clearly the first term always dominates the third, which can be omitted and thus we obtain (**??**).

Next, assume that $R \geqslant p^{1/2} \exp \left(2.1 \log p / \log \log p \right)$. Hence we can apply Lemma **??**, and derive

$$U_{m,\chi,P}(H,N), V_{m,\chi,P}(H,N)$$
$$\ll H^{-1/4} R^{7/6} p^{1/24} (\log R)(\log \log R)^{1/6} + H^{-1/4} R \log R.$$

Again, the first term always dominates and we obtain (**??**), which completes the proof.

References

[1] S. Chowla, The Riemann hypothesis and Hilbert's tenth problem, Math. and Its Appl., Vol. 4. Gordon and Breach Sci. Publ., New York- London-Paris, 1965.

[2] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford Univ. Press, Oxford, 1979.

[3] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[4] K. Matomäki, M. Radziwiłł and T. Tao, 'An averaged form of Chowla's conjecture, *Algebra Number Theory*, **9** (2015), 2167–2196.

[5] K. Matomäki, M. Radziwiłł, T. Tao, J. Teräväainen, and T. Ziegler. 'Higher uniformity of bounded multiplicative functions in short intervals on average', *Ann. of Math.*, **197** (2023), 739–857.

[6] I. E. Shparlinski and K. E. Stange, 'Character sums with division polynomials', *Can. Math. Bull.*, **55** (2012), 850–857.

[7] J. H. Silverman, '*p*-adic properties of division polynomials and elliptic divisibility sequences', *Math. Ann.*, **332** (2005), 443–471.

[8] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math., **106**, Springer, Dordrecht, 2009.

[9] T. Tao, 'Equivalence of the logarithmically averaged Chowla and Sarnak conjectures', *Number Theory - Diophantine Problems, Uniform Distribution and Applications*, Springer, Cham, 2017, 391–421.

[10] T. Tao and J. Teräväinen, 'The structure of logarithmically averaged correlations of multiplicative functions, with applications to the Chowla and Elliott conjectures', *Duke Math. J.*, **168** (2019), 1977–2027.

[11] T. Tao and J. Teräväinen, 'The structure of correlations of multiplicative functions at almost all scales, with applications to the Chowla and Elliott conjectures', *Algebra Number Theory*, **3** (2019), 2103–2150.

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia.
   Email address: subham.bhakta@unsw.edu.au

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia.
   Email address: igor.shparlinski@unsw.edu.au