Math. Proc. Camb. Phil. Soc. (2022), **172**, 563–590
doi:10.1017/S030500412100030X
First published online 15 April 2021

On the size of the maximum of incomplete Kloosterman sums

BY DANTE BONOLIS
IST Austria, Am Campus 1, 3400 *Klosterneuburg, Austria.*
e-mails: dante.bonolis@ist.ac.at

(*Received* 28 *November* 2018; *revised* 18 *January* 2021)

Abstract

Let $t:\mathbb{F}_p \to \mathbb{C}$ be a complex valued function on $\mathbb{F}_p$. A classical problem in analytic number theory is bounding the maximum

$$M(t) := \max_{0\leqslant H<p} \left|\frac{1}{\sqrt{p}}\sum_{0\leqslant n<H} t(n)\right|$$

of the absolute value of the incomplete sums $(1/\sqrt{p})\sum_{0\leqslant n<H} t(n)$. In this very general context one of the most important results is the Pólya–Vinogradov bound

$$M(t) \leqslant \left\|\hat{t}\right\|_\infty \log 3p,$$

where $\hat{t}:\mathbb{F}_p \to \mathbb{C}$ is the normalized Fourier transform of t. In this paper we provide a lower bound for certain incomplete Kloosterman sums, namely we prove that for any $\varepsilon > 0$ there exists a large subset of $a \in \mathbb{F}_p^\times$ such that for $\mathrm{kl}_{a,1,p} : x \mapsto e((ax+\overline{x})/p)$ we have

$$M(\mathrm{kl}_{a,1,p}) \geqslant \left(\frac{1-\varepsilon}{\sqrt{2\pi}} + o(1)\right)\log\log p,$$

as $p \to \infty$. Finally, we prove a result on the growth of the moments of $\{M(\mathrm{kl}_{a,1,p})\}_{a\in\mathbb{F}_p^\times}$.

2020 Mathematics Subject Classification: 11L03, 11T23 (Primary);
14F20, 60F10 (Secondary).

1. *Introduction*

Let p be a prime number and $t:\mathbb{F}_p \to \mathbb{C}$ be a complex valued function on $\mathbb{F}_p$. A classical problem in analytic number theory is to bound the incomplete sums

$$S(t, H) := \frac{1}{\sqrt{p}}\sum_{0\leqslant n<H} t(n),$$

for any $0 \leqslant H < p$. In this very general context, one of the most important results is the following:

THEOREM 1·1 (Pólya–Vinogradov bound, [25, 28]). *For any* $1 \leqslant H < p$ *one has*

$$|S(t, H)| \leqslant \left\|\hat{t}\right\|_\infty \log 3p,$$

where $\hat{t} : \mathbb{F}_p \to \mathbb{C}$ *is the normalised Fourier transform of* t

$$\hat{t}(y) := -\frac{1}{\sqrt{p}} \sum_{0 \leqslant x < p} t(x) e\left(\frac{yx}{p}\right),$$

$e(z) := e^{2\pi i z}$, *and* $\|\hat{t}\|_\infty := \max_{x \in \mathbb{F}_p} |\hat{t}(x)|$.

Pólya and Vinogradov proved this bound only in the case where $t = \chi$ is a multiplicative character over $\mathbb{F}_p^\times$. On the other hand, their methods can be applyed to any periodic function over $\mathbb{Z}$ (see [9, p. 2] for a proof of Theorem 1·1). Notice that this bound is non-trivial as soon as $H \geqslant \|\hat{t}\|_\infty \sqrt{p} \log 3p$. If one defines

$$M(t) := \max_{0 \leqslant H < p} |S(t, H)|,$$

then the Pólya-Vinogradov bound is equivalent to

$$M(t) \leqslant \left\|\hat{t}\right\|_\infty \log 3p.$$

A natural question that arises in this setting is the following: given a function $t : \mathbb{F}_p \to \mathbb{C}$, is the Pólya-Vinogradov bound sharp for t? And if it is not, what is the best possible bound?

1·1. *Kloosterman sums, Birch Sums and main results*

The aim of this paper is to study the cases of Kloosterman sums and Birch sums. We recall here the definitions of these two objects:

i) *Kloosterman sums.* For any $a, b \in \mathbb{F}_p^\times$, consider

$$\mathrm{kl}_{a,b,p} : x \mapsto e\left(\frac{ax + b\overline{x}}{p}\right)$$

where $\overline{x}$ denotes the inverse of x modulo p. The complete sum

$$\mathrm{Kl}(a, b;\, p) := \frac{1}{\sqrt{p}} \sum_{1 \leqslant x < p} e\left(\frac{ax + b\overline{x}}{p}\right)$$

is called the *Kloosterman sum associated to* a, b. The Riemann hypothesis for curves over finite fields implies $|\mathrm{Kl}(a, b;\, p)| \leqslant 2$ ([29]).

ii) *Birch sums.* For any $a, b \in \mathbb{F}_p^\times$, consider

$$\mathrm{bi}_{a,b,p} : x \mapsto e\left(\frac{ax + bx^3}{p}\right).$$

The *Birch sum associated to* a, b is

$$\mathrm{Bi}(a, b;\, p) := \frac{1}{\sqrt{p}} \sum_{1 \leqslant x < p} e\left(\frac{ax + bx^3}{p}\right).$$

In this case as well, an application of the Riemann hypothesis for curves over finite fields yields to the bound $|\mathrm{Bi}(a, b;\, p)| \leqslant 2$ ([29]).

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

Kloosterman sums and Birch sums arise in many different areas of analytic number theory such as applications of the circle method, spectral theory, the divisor problem, equidistribution questions, etc..

It is shown in [21, proposition 4·1] that $M(\mathrm{kl}_{a,1,p})$ and $M(\mathrm{bi}_{a,1,p})$ can be arbitrarily large when a varies over $\mathbb{F}_p^\times$ and p goes to infinity: in fact,

$$\lim_{p\to\infty}\max_{a\in\mathbb{F}_p^\times} M(\mathrm{kl}_{a,1,p}) = \lim_{p\to\infty}\max_{a\in\mathbb{F}_p^\times} M(\mathrm{bi}_{a,1,p}) = \infty.$$

We will prove the following lower bounds:

THEOREM 1·2. *Let* $0<\varepsilon<1$. *For all* p, *there exists* $S_{p,\varepsilon}\subset\mathbb{F}_p^\times$ *such that:*

(i) *for any* $a\in S_{p,\varepsilon}$ *one has*

$$M(\mathrm{kl}_{a,1,p}) \geqslant \left(\frac{1-\varepsilon}{\sqrt{2}\pi}+o(1)\right)\log\log p;$$

(ii) $|S_{p,\varepsilon}| \gg_\varepsilon p^{1-\frac{\log 16}{(\log p)^\varepsilon}}$.

The same holds if one replaces $M(\mathrm{kl}_{a,1,p})$ *by* $M(bi_{a,1,p})$.

Roughly speaking, the proof of Theorem 1·2 relies on the fact that we can simultaneously control the sign and the size of $2(\log p)^{1-\varepsilon}$ Kloosterman (or Birch) sums. Indeed we will prove

PROPOSITION 1·3. *Let* $0<\varepsilon<1$. *For every prime* p *there exists* $S_{p,\varepsilon}\subset\mathbb{F}_p^\times$ *such that for any* $a\in S_{p,\varepsilon}$ *and for every* $1\leqslant n\leqslant(\log p)^{1-\varepsilon}$

$$\mathrm{Kl}(an,1;p)\geqslant\sqrt{2},$$

and for every $-(\log p)^{1-\varepsilon}\leqslant n\leqslant -1$

$$\mathrm{Kl}(an,1;p)\leqslant-\sqrt{2}.$$

Moreover $|S_{p,\varepsilon}|\gg_\varepsilon p^{1-\frac{\log 16}{(\log p)^\varepsilon}}$. *The same is true if we replace* Kl *by* Bi.

Actually, we are going to prove a slightly more general version of Theorem 1·2 (see next section).

1·1·1. *The growth of the even moments*

In the second part of the paper, we focus our attention on the growth of the even moments of $\{M(\mathrm{kl}_{a,1,p})\}_{a\in\mathbb{F}_p^\times}$ and $\{M(\mathrm{bi}_{a,1,p})\}_{a\in\mathbb{F}_p^\times}$ as $p\to\infty$, obtaining:

THEOREM 1·4. *There exist two absolute constant* $0<c<1<C$ *such that as* $p\to\infty$ *one has*

$$(c^{2k}+o(1))(\log k)^{2k}\leqslant\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times}M(\mathrm{kl}_{a,1,p})^{2k}\leqslant((Ck)^{2k}+o(1))(\log\log p)^{2k},$$

for any fixed $k\geqslant 1$.

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

THEOREM 1·5. *There exist two absolute constant* $0<c<1<C$ *such that as* $p\to\infty$ *one has*

$$(c^{2k}+o(1))(\log k)^{2k}\leqslant\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times}M(bi_{a,1,p})^{2k}\leqslant(C^{2k}+o(1))P(k),$$

for any fixed $k\geqslant 1$, *where* $P(k):=\exp(4k\log\log k+k\log\log\log k+o(k))$.

From Theorem 1·5 we get the following

COROLLARY 1·6. *There exist two absolute constants* $B,b>0$ *such that as* $A\to\infty$,

$$\exp(-\exp(bA))\leqslant\liminf_{p\to\infty}\frac{1}{p-1}|\{a\in\mathbb{F}_p^\times : M(bi_{a,1,p})>A\}|\leqslant\exp\left(-\exp\left(BA^{1/2-o(1)}\right)\right).$$

1·2. *Remarks and related works*

(i) Notice that in Theorem 1·4 and 1·5 the lower bounds for the moments are identical but the upper bounds are substantially different: namely, the upper bound in Theorem 1·4 depends on both p and k, while the one in Theorem 1·5 is stronger, since it depends only on k. In the proof of Theorem 1·5, we use the estimate

$$\left|\sum_{N\leqslant x\leqslant N+H}e\left(\frac{ax+x^3}{p}\right)\right|\ll H^{1-\varepsilon}\tag{1·1}$$

uniformly for any $1<N<p$, $p^{1/2-\varepsilon/2}<H<p^{1/2+\varepsilon/2}$ and $a\in\mathbb{F}_p^\times$ which is a consequence of the Weyl inequality ([**16**, lemma 20·3]). The analogous estimate that would be used in Theorem 1·4 (to achieve the same upper bound as in Theorem 1·5) is

$$\left|\sum_{N\leqslant x\leqslant N+H}e\left(\frac{ax+\overline{x}}{p}\right)\right|\ll H^{1-\varepsilon}\tag{1·2}$$

uniformly for any $1<N<p$, $p^{1/2-\varepsilon/2}<H<p^{1/2+\varepsilon/2}$ and $a\in\mathbb{F}_p^\times$, but it is only conjectured (see for example Hooley's R^*-assumption, [**15**, p· 44]). We remark that this stronger bound for Theorem 1·4 would imply an analogous of 1·6 (obtained from Theorem 1·5) to Kloosterman sums.

(ii) We remark that Corollary 1·6 essentially recovers [**21**, theorem 1·6], with a slightly weaker upper bound. On the other hand, the techniques presented in [**21**] cannot provide any non trivial upper bound on the moments of the maximum of incomplete Kloosterman sums.

(iii) In [**1**], it is shown that there exists a constant $C>0$ such that for any $1\ll A\leqslant(2/\pi)(\log\log p-2\log\log\log p-C)$ one has that

$$\frac{1}{p-1}|\{a\in\mathbb{F}_p^\times : M(\mathrm{bi}_{a,1,p})>A\}|=\exp\left(-\exp\left(\frac{\pi A}{2}+O(1)\right)\right).\tag{1·3}$$

This is a much more precise result than Corollary 1·6, and it is obtained by a refinement of the argument presented in [**22**]. On the other hand, the argument in [**1**], [**22**] provides only a lower bound in the case of Kloosterman sums, i.e. one can show that there exists a constant $D > 0$ such that for any $1 \ll A \leqslant (2/\pi)(\log\log p - 2\log\log\log p - D)$ one has

$$\frac{1}{p-1}|\{a \in \mathbb{F}_p^\times : M(\mathrm{kl}_{a,1,p}) > A\}| \geqslant \exp\left(-\exp\left(\frac{\pi A}{2} + O(1)\right)\right). \qquad (1\cdot 4)$$

In particular, it seems that the upper bound in Theorem 1·4 is new. We remark that also in [1, 22] the difference between incomplete Birch sums and incomplete Kloosterman sums is due to the fact that the bound in (1·2) is only conjectured. Finally, we notice that (1·3) and (1·4) imply that there exist $S_p^1, S_p^2 \subset \mathbb{F}_p^\times$ such that $|S_p^1|, |S_p^2| \gg p^{1-\frac{1}{\log\log p}}$ and

$$M(\mathrm{Im}(\mathrm{kl}_{a_1,1,p})) \geqslant \left(\frac{2}{\pi} + o(1)\right)\log\log p, \quad M(\mathrm{Im}(\mathrm{bi}_{a_2,1,p})) \geqslant \left(\frac{2}{\pi} + o(1)\right)\log\log p \qquad (1\cdot 5)$$

for any $a_1 \in S_p^1$ and $a_2 \in S_p^2$.

(iv) One should compare our result with the case of incomplete character sums. Paley proved that the Pólya–Vinogradov bound is close to be sharp in this case; in [26] it is shown that there exist infinitely many primes p such that

$$M\left(\left(\frac{\cdot}{p}\right)\right) \gg \log\log p,$$

where $(\cdot/p)$ is the Legendre symbol modulo p. Similar results were achieved for non-trivial characters of any order by Granville and Soundararajan in [14], and by Goldmakher and Lamzouri in [12] and [13]. On the other hand, Montgomery and Vaughan ([23]) have shown that under the Generalised Rienann Hypothesis (GRH).

$$M(\chi) \ll \log\log p \qquad (1\cdot 6)$$

for any χ, which is the best possible bound up to evaluation of the constant.

1·3. *Notations and statement of general versions of the main results*

In this section we recall some notions regarding ℓ-adic trace functions. For a general introduction on this subject we refer the reader to [6]. Basic statements and references can also be found in [7] and [11]. In what follows, $p, \ell > 2$ are distinct primes and $i : \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$ is a fixed isomorphism. Let $\mathcal{F}$ be a middle-extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ pure of weight 0. For any $x \in \overline{\mathbb{A}}^1_{\mathbb{F}}(\mathbb{F}_{p^n})$ one defines

$$t_{\mathcal{F},n}(x) := i(\mathrm{Tr}(\mathrm{Fr}_{p^n} \mid \mathcal{F}_{\overline{x}})),$$

where Fr_{p^n} is the geometric Frobenius automorphism of $\mathbb{F}_{p^n}$ and $\mathcal{F}_{\overline{x}}$ is the stalk of $\mathcal{F}$ at a geometric point $\overline{x}$ over x. The function $t_{\mathcal{F},n}$ is called *the trace function attached to $\mathcal{F}$ over $\mathbb{F}_{p^n}$*. If there is no ambiguity, we denote by $t_{\mathcal{F}}$ the trace function $t_{\mathcal{F},1}$. The main examples of trace functions we should keep in mind are the following:

(i) for any $f \in \mathbb{F}_p[T]$, consider the function $x \mapsto e(f(T)/p)$; this is the trace function attached to the Artin-Schreier sheaf $\mathcal{L}_{e(f/p)}$ (see [4, chapter 6, sections 1-3]);

(ii) the Birch sums $b \mapsto \mathrm{Bi}(a, b; p)$ can be seen as the trace function attached to the sheaf $\mathrm{FT}(\mathcal{L}_{e((aT^3)/p)})$ ([17, 7·13, Sp-example (2)]);

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

(iii) the n–th HyperKloosterman sums: the map

$$x \longmapsto \mathrm{Kl}_n(x;\ p) := \frac{(-1)^{n-1}}{p^{(n-1)/2}} \sum_{\substack{y_1,\dots,y_n \in \mathbb{F}_p^\times \\ y_1\cdot\ldots\cdot y_n = x}} e\left(\frac{y_1+\cdots+y_n}{p}\right).$$

can be seen as the trace function attached to the *Kloosterman sheaf* $\mathcal{K}\ell_n$ (see [18] for the definition of such a sheaf and for its basic properties).

Definition 1·1. [7, Deinition 1·13] Let $\mathcal{F}$ be a middle extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ (see [17, 4·4,4·5]). The *conductor of* $\mathcal{F}$ is defined to be

$$c(\mathcal{F}) := \mathrm{Rank}(\mathcal{F}) + |\,\mathrm{Sing}(\mathcal{F})| + \sum_x \mathrm{Swan}_x(\mathcal{F}),$$

where:

(i) $\mathrm{Rank}(\mathcal{F}) = \dim \mathcal{F}_x$, for any x where $\mathcal{F}$ is lisse;
(ii) $\mathrm{Sing}(\mathcal{F}) = \{x \in \overline{\mathbb{P}}^1_{\mathbb{F}_p} : \mathcal{F}$ is not lisse at $x\}$;
(iii) $\mathrm{Swan}_x(\mathcal{F})$ for $x \in \overline{\mathbb{P}}^1_{\mathbb{F}_p}$, is the *Swan conductor of* $\mathcal{F}$ *at* x (see [18, chapter 1] for the definition of the Swan conductor).

Remark 1. If $\mathcal{F}$ is a middle extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ of weight zero, then for any $n \geqslant 1$ and $x \in \mathbb{F}_{p^n}$ one has that $|t_{\mathcal{F},n}(x)| \leqslant \mathrm{Rank}(\mathcal{F}) \leqslant c(\mathcal{F})$, i.e. $\|t\|_\infty \leqslant c(\mathcal{F})$ ([5, lemma 1·8·1]).

The formalism of trace functions is very powerful, mainly for the following two reasons. Firstly, because it is very flexible: the set of trace functions is closed under some basic operations such as sum, product, Fourier transform etc. Secondly, because once we have performed an operation, we can control the conductor of the output in terms of the conductors of the input data. Indeed, we have for example that:

(a) if $\mathcal{F}, \mathcal{G}$ are middle-extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ then $\mathcal{F} \oplus \mathcal{G}$ and $\mathcal{F} \otimes \mathcal{G}$ are still middle-extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ (see for example [11, section 3·4]). Moreover $t_{\mathcal{F}\oplus\mathcal{G},n}(x) = t_{\mathcal{F},n}(x) + t_{\mathcal{G},n}(x)$, and $t_{\mathcal{F}\otimes\mathcal{G},n}(x) = t_{\mathcal{F},n}(x) \cdot t_{\mathcal{G},n}(x)$ for any $n \geqslant 1$ and any $x \notin (\mathrm{Sing}(\mathcal{F}) \cup \mathrm{Sing}(\mathcal{G})) \cap \mathbb{F}_{p^n}$. Finally, $c(\mathcal{F} \oplus \mathcal{G}) \leqslant c(\mathcal{F}) + c(\mathcal{G})$, and $c(\mathcal{F} \otimes \mathcal{G}) \leqslant 5c(\mathcal{F})^2 c(\mathcal{G})^2$ ([6, pp· 6-7], [7, proposition 8·2]).
(b) Let $\mathcal{F}$ be a middle-extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ pure of weight 0 which is irreducible and not geometrically isomorphic to an Artin–Schreier sheaf of the form $\mathcal{L}_{e(aT/p)}$ for some $a \in \overline{\mathbb{F}}_p$. Then there exists an irreducible middle-extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ pure of weight 0, $\mathrm{FT}_{e(T/p)}(\mathcal{F})$, such that

$$t_{\mathrm{FT}_{e(T/p)}(\mathcal{F}),n}(x) = \frac{1}{p^{n/2}} \sum_{y \in \mathbb{F}_{p^n}} t_{\mathcal{F},n}(y) e(\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(xy)/p)$$

for any $n \geqslant 1$ and $x \in \mathbb{F}_{p^n}$. Moreover, $c(\mathrm{FT}_{e(T/p)}(\mathcal{F})) \leqslant 10c(\mathcal{F})^2$ (see [18, chapters 5, 8] and [7, proposition 8·2]). In what follows we will denote $\mathrm{FT}_{e(T/p)}(\mathcal{F}) = \mathrm{FT}(\mathcal{F})$ since there is not ambiguity;

(c) let $\mathcal{F}$ be a middle-extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ and $\gamma \in \mathrm{PGL}_2(\mathbb{F}_p)$. Then the pull-back $\gamma^*\mathcal{F}$ is a middle-extension ℓ-adic sheaf on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$. Moreover, $t_{\gamma^*\mathcal{F},n}(x) = t_{\mathcal{F},n}(\gamma(x))$ for any $n \geqslant 1$ and any $x \in \mathbb{F}_{p^n}$ and $c(\gamma^*\mathcal{F}, n) = c(\mathcal{F})$. Concretely, if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{F}_p)$, then $t_{\gamma^*\mathcal{F}}(x) = t_{\mathcal{F}}((ax+b)/(cx+d))$ for any $x \in \mathbb{F}_p$.

Definition 1·2. [8, definition 1·2] Let $p, \ell > 2$ be two distinct primes and let $r \geqslant 1$ be an integer. A middle-extension ℓ-adic sheaf, $\mathcal{F}$, is r-*bountiful* if

(i) $\mathcal{F}$ is pure of weight 0 and $\mathrm{Rank}(\mathcal{F}) \geqslant 2$,

(ii) the geometric and arithmetic monodromy groups of $\mathcal{F}$ satisfy $G^{\mathrm{arith}}_{\mathcal{F}} = G^{\mathrm{geom}}_{\mathcal{F}}$, and $G^{\mathrm{geom}}_{\mathcal{F}}$ is either $\mathrm{Sp}_r(\mathbb{C})$ or $\mathrm{SL}_r(\mathbb{C})$,

(iii) the projective automorphism group of $\mathcal{F}$

$$\mathrm{Aut}_0(\mathcal{F}) := \{\gamma \in \mathrm{PGL}_2(\mathbb{F}_p) : \gamma^*\mathcal{F} \cong \mathcal{F} \otimes \mathcal{L} \text{ for some rank 1 sheaf } \mathcal{L}\}$$

is trivial.

Definition 1·3. Let $p, \ell > 2$ be two distinct primes and let $r \geqslant 1$ be an integer. A family of ℓ-adic sheaves $(\mathcal{F}_a)_{a\in\mathbb{F}_p^\times}$ is a 1-*parameter family of sheaves of* Sp_{2g}-*type* if the following conditions are satisfied:

(i) for any $a \in \mathbb{F}_p^\times$, $\mathcal{F}_a$ is an irreducible middle-extension ℓ-adic Fourier sheaf on $\mathbb{A}^1_{\mathbb{F}_p}$ which is pointwise pure of weight 0. We denote by t_a the trace function attached to $\mathcal{F}_a$;

(ii) for any $a \in \mathbb{F}_p^\times$, the ℓ-adic Fourier transform $\mathrm{FT}(\mathcal{F}_a)$ is an $2g$-bountiful sheaf such that $G^{\mathrm{geom}}_{\mathrm{FT}(\mathcal{F}_a)} = \mathrm{Sp}_{2g}(\mathbb{C})$;

(iii) for every $y \in \mathbb{F}_p$, there exists $\tau_y \in \mathrm{PGL}_2(\mathbb{F}_p)$ such that $\tau_i \neq \tau_j$ if $i \neq j$ and

$$\hat{t}_a(y) = \hat{t}_1(\tau_y \cdot a)$$

for any $a \in \mathbb{F}_p^\times$, where $\hat{t}_a(\cdot)$ denotes the trace functions attached to $\mathrm{FT}(\mathcal{F}_a)$.

Definition 1·4. Let ℓ be a prime number. A family $\mathfrak{F} = (\mathcal{F}_{a,p})_{a\in\mathbb{F}_p^\times,p}$ is a *bounded family of* 1-*parameter families of sheaves of* Sp_{2g}-*type* if the following conditions hold:

(i) for any prime number $p \neq \ell$, the family $(\mathcal{F}_{a,p})_{a\in\mathbb{F}_p^\times}$ is an 1-parameter family of sheaves of Sp_{2g}-type;

(iii) there exists $C \geqslant 1$ such that for any p prime and $a \in \mathbb{F}_p^\times$

$$c(\mathcal{F}_{a,p}) \leqslant C.$$

We call the smallest C with this property the *conductor of the family* and denote it by $c_{\mathfrak{F}}$;

Remark 2. The last two definitions are similar to [1, definitions 9·4, 9·5]

Definition 1·5. Let $\mathfrak{F}$ be a bounded family of 1-parameter families of Sp_{2g}-type. For any $A > 0$ we define

$$D_{\mathfrak{F}}(A) := \liminf_{p\to\infty} \frac{1}{p-1} |\{a \in \mathbb{F}_p^\times : M(t_{a,p}) > A\}|,$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

where we recall that

$$M(t_{a,p}) = \max_{0\leqslant H<p} \left| \frac{1}{\sqrt{p}} \sum_{0\leqslant n<H} t_{a,p}(n) \right|.$$

Example 1·1. The following families are bounded families of 1-parameter families of Sp_2-type:

(i) the family of Artin–Schreier sheaves $\left(\mathcal{L}_{e(\frac{ax+\bar{x}}{p})}\right)_{a\in\mathbb{F}_p^\times,p}$. Indeed for any $a\in\mathbb{F}_p^\times$, $\mathcal{L}_{e(\frac{ax+\bar{x}}{p})}$ is a middle-extension ℓ-adic Fourier sheaf that is pointwise pure of weight 0, with $\mathrm{cond}(\mathcal{L}_{e(\frac{ax+\bar{x}}{p})})=2$. Moreover, $\mathrm{FT}(\mathcal{L}_{e(\frac{x+\bar{x}}{p})})=\mathcal{K}\ell_2$, the Kloosterman sheaf of rank 2 which is 2-bountiful ([8, paragraph 3·2]), and

$$\mathrm{FT}\left(e\left(\frac{ax+\bar{x}}{p}\right)\right)(y)=\mathrm{Kl}(a+y,1;\,p),$$

so we can take $\tau_y := \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}$ in Definition 1·3;

(ii) the family of Artin–Schreier sheaves $\left(\mathcal{L}_{e(\frac{x+b\bar{x}}{p})}\right)_{b\in\mathbb{F}_p^\times,p}$. It is enough to argue as above and to observe that

$$\mathrm{FT}\left(e\left(\frac{x+b\bar{x}}{p}\right)\right)(y)=\mathrm{Kl}(b(y+1),1;\,p),$$

so we can take $\tau_y := \begin{pmatrix} y+1 & 0 \\ 0 & 1 \end{pmatrix}$ in Definition 1·3;

(iii) fix $m\in\mathbb{Z}$. The family of Artin–Schreier sheaves $\left(\mathcal{L}_{e(\frac{ax+m\overline{ax}}{p})}\right)_{a\in\mathbb{F}_p^\times,p}$ is a bounded family of 1-parameter families of Sp_2-type. Also in this case one argues as above and observes that

$$\mathrm{FT}\left(e\left(\frac{ax+m\overline{ax}}{p}\right)\right)(y)=\mathrm{Kl}(my+m\bar{a},1;\,p),$$

so we can take $\tau_y := \begin{pmatrix} my & m \\ 1 & 0 \end{pmatrix}$ in Definition 1·3;

(iv) using similar arguments, one shows that the families

$$\left(\mathcal{L}_{e(\frac{ax+x^3}{p})}\right)_{a\in\mathbb{F}_p^\times,p},\quad \left(\mathcal{L}_{e(\frac{x+bx^3}{p})}\right)_{b\in\mathbb{F}_p^\times,p},\quad\text{and}\quad \left(\mathcal{L}_{e(\frac{ax+m(xa)^3}{p})}\right)_{a\in\mathbb{F}_p^\times,p}$$

are bounded families of 1-parameter families of Sp_2-type.

Then Theorem 1·2 is a consequence of the following:

THEOREM 1·7. *Let* $0<\varepsilon<1$. *Let* $\mathfrak{F}=(\mathcal{F}_{a,p})_{a\in\mathbb{F}_p^\times,p}$ *be a bounded family of* 1*-parameter families of* Sp_2*-type. For every prime* p *there exists* $S_{p,\varepsilon}\subset\mathbb{F}_p^\times$ *such that*:

(i) *for any* $a\in S_{p,\varepsilon}$,

$$M(t_{a,p})\geqslant\left(\frac{1-\varepsilon}{\sqrt{2}\pi}+o(1)\right)\log\log p;$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

(ii) $|S_{p,\varepsilon}| \gg_{\varepsilon, C_{\mathfrak{F}}} p^{1-\frac{\log 16}{(\log p)^{\varepsilon}}}$.

Similarly, Theorems 1·4 and 1·5 are a consequence of:

THEOREM 1·8. *Let $\mathfrak{F} = (\mathcal{F}_{a,p})_{a\in\mathbb{F}_p^\times, p}$ be a bounded family of 1-parameter families of Sp_{2g}-type. There exist two constants and $0 < c < 1 < C$ that depend only on $c_{\mathfrak{F}}$ such that for any fixed $k \geqslant 1$,*

$$((cg)^{2k} + o(1))(\log k)^{2k} \leqslant \frac{1}{p-1} \sum_{a\in\mathbb{F}_p^\times} M(t_{a,p})^{2k} \leqslant ((Ck)^{2k} + o(1))(\log\log p)^{2k}.$$

If, moreover, there exists $\varepsilon > 0$ such that

$$\Bigg| \sum_{N\leqslant x\leqslant N+H} t_{a,p}(x) \Bigg| \ll_{c_{\mathfrak{F}}} H^{1-\varepsilon} \tag{1·7}$$

uniformly for any $1 < N < p$, $p^{1/2-\varepsilon/2} < H < p^{1/2+\varepsilon/2}$ and $a \in \mathbb{F}_p^\times$, then for any fixed $k \geqslant 1$ one has

$$((cg)^{2k} + o(1))(\log k)^{2k} \leqslant \frac{1}{p-1} \sum_{a\in\mathbb{F}_p^\times} M(t_{a,p})^{2k} \leqslant (C^{2k} + o(1))P(k),$$

where $P(k) = \exp(4k\log\log k + k\log\log\log k + o(k))$.

We then obtain:

COROLLARY 1·9. *Under the same hypothesis as Theorem 1·8, we have that*:

(i) *for any $A > 0$,*

$$D_{\mathfrak{F}}(A) \geqslant \exp(-\exp(bA)),$$

where $b > 0$ depends only on $c_{\mathfrak{F}}$;

(ii) *if condition (1·7) holds, there exists a constant $B > 0$ depending only on $C_{\mathfrak{F}}$ such that for $A \to \infty$*

$$D_{\mathfrak{F}}(A) \leqslant \exp\left(-\exp\left(BA^{1/2-o(1)}\right)\right).$$

2. *Proof of Theorem 1·7*

2·1. *First step: Fourier expansion and Féjer Kernel*

The first step is to prove a quantitative version of the Fourier expansion for $(1/\sqrt{p})\sum_{x\leqslant\alpha p} t(x)$.

LEMMA 2·1. *Let $t : \mathbb{F}_p \to \mathbb{C}$ be a complex valued function on $\mathbb{F}_p$. Then for any $0 < \alpha < 1$ and $1 \leqslant N \leqslant p$ we have*

$$\frac{1}{\sqrt{p}} \sum_{x\leqslant\alpha p} t(x) = -\frac{1}{2\pi i} \sum_{1\leqslant|n|\leqslant N} \frac{\hat{t}(n)}{n}(1 - e(-\alpha n)) + \alpha\hat{t}(0) + O\left(\frac{\|t\|_\infty \sqrt{p}\log p}{N}\right),$$

where the implied constant is absolute.

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

Remark 3. In the case where $t=\chi$ is a multiplicative character, we recover [25] (and indeed the proof of Lemma 2·1 closely follows the one in [25]). The result in [25] has been extensively used in many works on the maximum of incomplete character sums, such as [2, 12–14, 23, 24, 26] among others.

Proof. Let us introduce the function

$$\Phi_\alpha(s)=\begin{cases}1 & \text{if } 0<s<2\pi\alpha,\\ \frac{1}{2} & \text{if } s=0 \text{ or } s=2\pi\alpha,\\ 0 & \text{if } 2\pi\alpha<s<2\pi.\end{cases}$$

Then the Fourier series of Φ_α is

$$\begin{aligned}\Phi_\alpha(s)&=\alpha+\sum_{n>0}\frac{\sin(2\pi\alpha n)}{\pi n}\cos(ns)-\frac{\cos(2\pi\alpha n-1)}{n\pi}\sin(ns)\\ &=\alpha+\frac{1}{\pi}T(s)-\frac{1}{\pi}T(s-2\pi\alpha),\end{aligned}$$

where

$$T(x):=\sum_{n>0}\frac{\sin(nx)}{n}.$$

Observe that for any $N>1$ one has

$$T(x)=\sum_{0<n\leqslant N}\frac{\sin(nx)}{n}+R_N(x),$$

with $R_N(0)=R_N(\pi)$, $R_N(2\pi-x)=-R_N(x)$ and $R_N(x)=O(1/(Nx))$ for any $x\in(0,\pi]$ [25, equation 10]. it follows that

$$\begin{aligned}\frac{1}{\sqrt{p}}\sum_{x\leqslant\alpha p}t(x)&=\frac{1}{\sqrt{p}}\sum_{x<p}t(x)\Phi_\alpha\left(\frac{2\pi x}{p}\right)+O(\|t\|_\infty/\sqrt{p})\\ &=\frac{1}{\sqrt{p}}\sum_{x<p}t(x)\left(\alpha+\frac{1}{\pi}T\left(\frac{2\pi x}{p}\right)-\frac{1}{\pi}T\left(\frac{2\pi x}{p}-2\pi\alpha\right)\right)+O\left(\frac{\|t\|_\infty}{\sqrt{p}}\right)\\ &=\frac{1}{\sqrt{p}}\sum_{x<p}t(x)\Bigg(\alpha+\frac{1}{\pi}\sum_{0<n\leqslant N}\frac{\sin\left(\frac{2\pi nx}{p}\right)}{n}+\frac{1}{\pi}R_N\left(\frac{2\pi x}{p}\right)\\ &\quad-\frac{1}{\pi}\sum_{0<n\leqslant N}\frac{\sin\left(\frac{2\pi nx}{p}-2\pi\alpha n\right)}{n}+\frac{1}{\pi}R_N\left(\frac{2\pi x}{p}-2\pi\alpha\right)\Bigg)+O\left(\frac{\|t\|_\infty}{\sqrt{p}}\right)\\ &=\frac{1}{\sqrt{p}}\sum_{x<p}t(x)\left(\frac{1}{\pi}\sum_{0<n\leqslant N}\frac{\sin\left(\frac{2\pi nx}{p}\right)}{n}-\frac{1}{\pi}\sum_{0<n\leqslant N}\frac{\sin\left(\frac{2\pi nx}{p}-2\pi\alpha n\right)}{n}\right)\\ &\quad+\alpha\hat{t}(0)+O\left(\frac{\|t\|_\infty\sqrt{p}\log p}{N}\right).\end{aligned}$$

On the other hand, we have

$$\sin\left(\frac{2\pi nx}{p}\right)=\frac{e\left(\frac{nx}{p}\right)-e\left(-\frac{nx}{p}\right)}{2i},\qquad \sin\left(\frac{2\pi nx}{p}-2\pi\alpha\right)=\frac{e\left(\frac{nx}{p}-\alpha n\right)-e\left(-\left(\frac{nx}{p}-\alpha n\right)\right)}{2i}.$$

Then,

$$\frac{1}{\sqrt{p}}\sum_{x\in\mathbb{F}_p}t(x)\left(\frac{e\left(\frac{nx}{p}\right)-e\left(-\frac{nx}{p}\right)}{2i}\right)=-\frac{1}{2i}(\hat{t}(n)-\hat{t}(-n)),$$

and similarly

$$\frac{1}{\sqrt{p}}\sum_{x\in\mathbb{F}_p}t(x)\left(\frac{e\left(\frac{nx}{p}-\alpha n\right)-e\left(-\left(\frac{nx}{p}-\alpha n\right)\right)}{2i}\right)=-\frac{1}{2i}(e(-\alpha n)\hat{t}(n)-e(\alpha n)\hat{t}(-n)).$$

Now we use the strategy of [26], introducing the Fejér kernel:

LEMMA 2·2. *For any* $t:\mathbb{F}_p\to\mathbb{C}$,

$$M(t)\geqslant\max_{\substack{\alpha\in[0,1]\\1\leqslant N<p}}\left|\frac{1}{4\pi}\sum_{1\leqslant|n|<N}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))\right|+O\left(\left\|\hat{t}\right\|_\infty\right).$$

Proof. The quantitative version of the Fourier transform (Lemma 2·1) leads to

$$\begin{aligned}\frac{1}{\sqrt{p}}\sum_{x\leqslant\alpha p}t(x)&=-\frac{1}{2\pi i}\sum_{1\leqslant|n|\leqslant p}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))+\alpha\hat{t}(0)+O(1)\\&=-\frac{1}{2\pi i}\sum_{1\leqslant|n|<p}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))+O\left(\left\|\hat{t}\right\|_\infty\right).\end{aligned}$$

We now extend the outer sum to all values modulo p using the Fejér kernel: for any $1<N<p$, we have

$$\begin{aligned}\frac{1}{2\pi i}\sum_{1\leqslant|n|\leqslant N}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))&=\frac{1}{2\pi i}\sum_{1\leqslant|n|\leqslant p}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))\cdot\\&\qquad\sum_{1<|a|\leqslant N}\phi(a)\int_0^1e((a-n)\vartheta)d\vartheta+O\left(\left\|\hat{t}\right\|_\infty\right)\qquad(2\cdot1)\\&=\int_0^1A(\vartheta)\Phi_N(\vartheta)d\vartheta+O\left(\left\|\hat{t}\right\|_\infty\right),\end{aligned}$$

where

$$\phi(a):=1-\frac{|a|}{N},\quad \Phi_N(\vartheta):=\sum_{|a|\leqslant N}\phi(a)e(a\vartheta)=\frac{1}{N}\left(\frac{\sin\frac{N\vartheta}{2}}{\sin\frac{\vartheta}{2}}\right)^2\qquad(2\cdot2)$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

is the Féjer Kernel, and

$$A(\vartheta) := \frac{1}{2\pi i}\sum_{1\leqslant |n|\leqslant p}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))e(-\vartheta n) = \frac{1}{2\pi i}\sum_{1\leqslant |n|\leqslant p}\frac{\hat{t}(n)}{n}(e(-\vartheta n)-1+1-e(-(\vartheta+\alpha)n))$$
$$-\frac{1}{2\pi i}\sum_{1\leqslant |n|\leqslant p}\frac{\hat{t}(n)}{n}(e(-\vartheta n)-1)+\frac{1}{2\pi i}\sum_{1\leqslant |n|\leqslant p}\frac{\hat{t}(n)}{n}(1-e(-(\vartheta+\alpha)n)).$$

By the triangle inequality,

$$\begin{aligned}\max_{\vartheta\in[0,1]}|A(\vartheta)| &\leqslant 2\max_{\alpha\in[0,1]}\left|\frac{1}{2\pi i}\sum_{1\leqslant |n|\leqslant p}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))\right| \\ &\leqslant 2\max_{\alpha\in[0,1]}\left|\frac{1}{\sqrt{p}}\sum_{x\leqslant \alpha p} t(x)\right| + O\left(\|\hat{t}\|_\infty\right) \\ &\leqslant 2M(t)+O\left(\|\hat{t}\|_\infty\right).\end{aligned}$$

Thus, we get

$$\left|\frac{1}{4\pi i}\sum_{1\leqslant |n|\leqslant N}\frac{\hat{t}(n)}{n}(1-e(-\alpha n))\right| \leqslant \left(M(t)+O\left(\|\hat{t}\|_\infty\right)\right)\cdot\int_0^1 \Phi_N(\vartheta)d\vartheta. \tag{2·3}$$

Using the fact that $\int_0^1 \Phi_N(\vartheta)d\vartheta = 1$, we conclude the proof.

To conclude the proof of Theorem 1·7, it is sufficient to prove the following generalisation of Proposition 1·3:

PROPOSITION 2·3. *For any prime p, let K be the trace function attached to an irreducible 2-bountiful sheaf $\mathcal{K}$ on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$. Fix $0<\varepsilon<1$. For every $1\leqslant |n|\leqslant (\log p)^{1-\varepsilon}$, set $\tau_n\in \mathrm{PGL}_2(\mathbb{F}_p)$ such that $\tau_n\neq\tau_m$ if $n\neq m$. Then there exists $S_{p,\varepsilon}\subset\mathbb{F}_p^\times$ such that for any $a\in S_{p,\varepsilon}$*

$$K(\tau_n\cdot a)\geqslant\sqrt{2}$$

for any $1\leqslant n\leqslant (\log p)^{1-\varepsilon}$, and

$$K(\tau_n\cdot a)\leqslant -\sqrt{2}$$

for any $-(\log p)^{1-\varepsilon}\leqslant n\leqslant -1$. Moreover $|S_{p,\varepsilon}|\gg_{\varepsilon,c(\mathcal{K})} p^{1-\frac{\log 16}{(\log p)^\varepsilon}}$.

Remark 4. Since $\mathrm{Sp}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})$, when considering a 2-bountiful sheaf $\mathcal{K}$ there is no need to specify the monodromy groups of $\mathcal{K}$.

Assuming this Proposition, whose proof is to be found in the next section, we prove Theorem 1·7. Applying Lemma 2·2 for $t = t_{a,p}$, and using the fact that $\|\hat{t}_{a,p}\|_\infty \leqslant c(\mathrm{FT}(\mathcal{F}_{a,p})) \leqslant 10c(\mathcal{F}_{a,p})^2 \leqslant 10c_{\mathfrak{F}}^2$ (see Remark 1 and [7, proposition 8·2]), we get

$$
\begin{aligned}
M(t_{a,p}) &= \max_{\alpha\in[0,1]} \left| \frac{1}{\sqrt{p}} \sum_{x\leqslant \alpha p} t_{a,p}(x) \right| \\
&\geqslant \frac{1}{4\pi} \max_{\substack{\alpha\in[0,1],\\ 1\leqslant N<p}} \left| \sum_{1\leqslant |n|\leqslant N} \frac{\hat{t}_{a,p}(n)}{n} (1-e(-\alpha n)) \right| + O_{c(\mathfrak{F})}(1) \\
&= \frac{1}{4\pi} \max_{\substack{\alpha\in[0,1],\\ 1\leqslant N<p}} \left| \sum_{1\leqslant |n|\leqslant N} \frac{\hat{t}_{1,p}(\tau_n\cdot a)}{n} (1-e(-\alpha n)) \right| + O_{c(\mathfrak{F})}(1) \\
&\geqslant \frac{1}{4\pi} \left| \sum_{1\leqslant |n|\leqslant (\log p)^{1-\varepsilon}} \frac{\hat{t}_{1,p}(\tau_n\cdot a)}{n} (1+(-1)^{n+1}) \right| + O_{c(\mathfrak{F})}(1),
\end{aligned}
$$

where the second step uses the fact that $\hat{t}_{a,p}(n) = \hat{t}_{1,p}(\tau_n \cdot a)$ (property (iii) in Definition 1·3). Applying Proposition 2·3 to $K = \hat{t}_{1,p}$, there exists $S_{p,\varepsilon} \subset \mathbb{F}_p^\times$ such that for any $a \in S_{p,\varepsilon}$

$$
M(t_{a,p}) \geqslant \frac{2\sqrt{2}}{4\pi} \sum_{\substack{1\leqslant |n|\leqslant (\log p)^{1-\varepsilon}\\ n\equiv 1(2)}} \frac{1}{n} + O_{c(\mathfrak{F})}(1) \geqslant \left(\frac{1-\varepsilon}{\sqrt{2}\pi} + o(1) \right) \log\log p,
$$

and this concludes the proof of Theorem 1·7.

2·2. *Preliminars for the proof of Proposition 2·3: Chebyshev polynomials*

Consider an irreducible 2-bountiful sheaf $\mathcal{K}$ on $\overline{\mathbb{A}}^1_{\mathbb{F}_p}$, and denote the trace function attached to it by $K(\cdot, r) = t_{\mathcal{K},r}(\cdot)$, where $K(\cdot) = K(\cdot, 1)$ if there is no ambiguity. Combining the fact that $G^{\mathrm{geom}}_{\mathcal{K}} = G^{\mathrm{arith}}_{\mathcal{K}} = \mathrm{SL}_2(\mathbb{C})$ (property (ii) in the definition of 2-bountiful) together with Deligne's Equidistribution Theorem ([**18**, chapter 3]), it follows that for any $r \geqslant 1$, and $a \in \mathbb{F}_{p^r}$ one has

$$
K(a, r) = 2\cos(\theta(a, r)) \tag{2·4}
$$

with $\theta(a, r) \in [0, \pi]$, and that when $r \to \infty$ the angles $\{\theta(a, r) : a \in \mathbb{F}_p^r\}$ equidistribute in the interval $[0, \pi]$ with respect to the pushforward of the Haar measure of $\mathrm{SU}_2(\mathbb{C}) \subset \mathrm{SL}_2(\mathbb{C})$, which is the Sato–Tate measure $\mu_{\mathrm{ST}} = (2/\pi) \int \sin^2 d\theta$ ([**18**, chapter 13]). Moreover, for any $n \geqslant 1$ one can consider the the middle-extension ℓ-adic sheaf $\mathrm{Sym}^n \mathcal{K}$. Then, for any $r \geqslant 1$ and $a \in \mathbb{F}_{p^r}$ one has that

$$
t_{\mathrm{Sym}^n \mathcal{K},r}(a) = \frac{\sin((n+1)\theta(a, r))}{\sin(\theta(a, r))} = U_n(K(a, r)),
$$

where the angles $\theta(a, r)$ are the same as in (2·4) and $U(n) \in \mathbb{Z}[\theta]$ (see [**18**, chapters 3, 13] for a discussion on the sheaf $\mathrm{Sym}^n \mathcal{K}$). In terms of representation theory, the polynomials U_n are all the irreducible characters of $\mathrm{SU}_2(\mathbb{C})$. In particular, by the Peter–Weyl Theorem, these polynomials form an orthonormal basis of $L^2([0, \pi], \mu_{\mathrm{ST}})$. Finally, we call a *trigonometric polynomial of degree* $s \geqslant 0$ any $Y \in L^2([0, \pi], \mu_{\mathrm{ST}})$ of the form

$$
Y = \sum_{j=0}^{s} y(j) U_j. \tag{2·5}
$$

with $y(s) \neq 0$. We refer to s as the *Chebyshev degree* of Y.

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

Remark 5. Let $f \in L^2([0,\pi],\mu_{ST})$. We can decompose f using the orthonormal basis $\{U_n\}_n$, i.e. we can write f as

$$f = \sum_n a_n U_n, \tag{2·6}$$

where

$$a_n = \int_0^\pi f(\theta) U_n(\theta) d\mu_{\mathrm{ST}}.$$

The decomposition (2·6) is called the *Chebyshev expansion of f*.

Let us begin by proving some properties of the sheaf $\mathrm{Sym}^n(\mathcal{K})$.

LEMMA 2·4. *Let $\mathcal{K}$ as above. For any $n > 0$:*

(i) *the geometric monodromy group of* $\mathrm{Sym}^n(\mathcal{K})$ *is given by*

$$G^{\mathrm{geom}}_{\mathrm{Sym}^n(\mathcal{K})} \cong \begin{cases} \mathrm{SL}_2(\mathbb{C}) & \text{if } n \text{ is odd,} \\ \mathrm{PSL}_2(\mathbb{C}) & \text{if } n \text{ is even;} \end{cases}$$

(ii) *the projective automorphism group*

$$\mathrm{Aut}_0(\mathrm{Sym}^n(\mathcal{K})) = \{\gamma \in \mathrm{PGL}_2(\mathbb{F}_p) : \gamma^* \mathrm{Sym}^n(\mathcal{K}) \cong \mathrm{Sym}^n(\mathcal{K}) \otimes \mathcal{L} \\ \text{for some rank 1 sheaf } \mathcal{L}\}$$

is trivial;

(iii) *the conductor of* $\mathrm{Sym}^n(\mathcal{K})$ *is bounded by*

$$c(\mathrm{Sym}^n(\mathcal{K})) \leqslant n \cdot c(\mathcal{K});$$

(iv) *if $n_1 \neq n_2$, then* $\mathrm{Sym}^{n_1}(\mathcal{K}) \ncong \mathrm{Sym}^{n_2}(\mathcal{K}) \otimes \mathcal{L}$ *for any rank one sheaf $\mathcal{L}$.*

Proof. For part (i), recall that by definition of the geometric monodromy group, $G^{\mathrm{geom}}_{\mathrm{Sym}^n(\mathcal{K})} = \mathrm{Sym}^n(G^{\mathrm{geom}}_{\mathcal{K}})$. Then the result follows since $G^{\mathrm{geom}}_{\mathcal{K}} = \mathrm{SL}_2(\mathbb{C})$ by hypothesis. For part (ii), let $\gamma \in \mathrm{PGL}_2(\mathbb{F}_p)$. First observe that for any $r \geqslant 1$, and $x \in \mathbb{F}_{p^r}$ we have that

$$t_{\mathrm{Sym}^n(\mathcal{K}),r}(x) = \frac{\sin((n+1)\theta(x,r))}{\sin(\theta(x,r))}, \qquad t_{\gamma^* \mathrm{Sym}^n(\mathcal{K}),r}(x) = \frac{\sin((n+1)\theta(\gamma\cdot x,r))}{\sin(\theta(\gamma\cdot x,r))},$$

where $\theta(x,r)$ is as in (2·4). By contradiction, assume that $\gamma^* \mathrm{Sym}^n(\mathcal{K}) \cong \mathrm{Sym}^n(\mathcal{K}) \otimes \mathcal{L}$ for some rank one sheaf, and let $U \subset \overline{\mathbb{A}}^1_{\mathbb{F}_p}$ be a dense open set where $\gamma^* \mathrm{Sym}^n(\mathcal{K})$, $\mathrm{Sym}^n(\mathcal{K})$ and $\mathcal{L}$ are all lisse. Then for any $x \in U(\mathbb{F}_{p^r})$,

$$t_{\gamma^* \mathrm{Sym}^n(\mathcal{K}),r}(x) = t_{\mathrm{Sym}^n(\mathcal{K})\otimes\mathcal{L},r}(x) = t_{\mathrm{Sym}^n(\mathcal{K}),r}(x) \cdot t_{\mathcal{L},r}(x).$$

On the other hand, $\gamma^* \mathrm{Sym}^n(\mathcal{K})$ and $\mathrm{Sym}^n(\mathcal{K})$ are pure of weight 0, and therefore $\mathcal{L}$ is pure of weight 0, i.e. we have that $|t_{\mathcal{L},r}(x)| = 1$ for any $r \geqslant 1$ and $x \in U(\mathbb{F}_{p^r})$. It follows that for any $x \in U(\mathbb{F}_{p^r})$

$$|t_{\gamma^* \mathrm{Sym}^n(\mathcal{K}),r}(x)| = |t_{\mathrm{Sym}^n(\mathcal{K}),r}(x)|. \tag{2·7}$$

Due to the fact that $\mathcal{K}$ is a bountiful sheaf, an application of the Goursat–Kolchin–Ribet criterion as stated in [8, lemma 2·4] combined with Deligne's equidistribution Theorem ([5, section 3·5]) implies that the angles $\{(\theta(x,r),\theta(\gamma\cdot x,r)) : x\in\mathbb{F}_{p^r}\}$ become equidistributed in $([0,\pi]\times[0,\pi],\mu_{\mathrm{ST}}\otimes\mu_{\mathrm{ST}})$ as $r\to\infty$. Now consider

$$\Theta_1=\left\{\theta\in[0,\pi]:\left|\frac{\sin((n+1)\theta)}{\sin(\theta)}\right|<\frac{1}{4}\right\},\quad \Theta_1=\left\{\theta\in[0,\pi]:\left|\frac{\sin((n+1)\theta)}{\sin(\theta)}\right|>\frac{3}{4}\right\}.$$

It easy to see that Θ_1, Θ_2 are non empty open subsets of $[0,\pi]$. Then we have that

$$\frac{|\{x\in\mathbb{F}_{p^r}:(\theta(x,r),\theta(\gamma\cdot x,r))\in\Theta_1\times\Theta_2\}|}{p^r}\longrightarrow\mu_{\mathrm{ST}}(\Theta_1)\cdot\mu_{\mathrm{ST}}(\Theta_2)>0,$$

when $r\to\infty$. Hence, for r large enough, we can find $x\in U(\mathbb{F}_{p^r})$ such that

$$|t_{\mathrm{Sym}^n(\mathcal{K}),r}(x)|<1/4,\qquad |t_{\gamma^*\,\mathrm{Sym}^n(\mathcal{K}),r}(x)|>3/4.$$

But this contradicts (2·7). The proof of part (iii) is included in the proof of Deligne's Equidistribution Theorem (see for example [18, paragraph 3·6]). For part (iv), it is enough to observe that the sheaves $\mathrm{Sym}^{n_1}(\mathcal{K})$ and $\mathrm{Sym}^{n_2}(\mathcal{K})$ are irreducible (see [11, p· 155]) and that $\mathrm{Rank}(\mathrm{Sym}^{n_1}(\mathcal{K}))=n_1+1$, while $\mathrm{Rank}(\mathrm{Sym}^{n_2}(\mathcal{K})\otimes\mathcal{L})=\mathrm{Rank}(\mathrm{Sym}^{n_2}(\mathcal{K}))=n_2+1$.

LEMMA 2·5. *Let $d\geqslant 0$. Let $(Y_i)_{i=0}^n$ be a family of trigonometric polynomials*

$$Y_i=\sum_{j=0}^{\deg Y_i}y_i(j)U_j$$

such that $\deg Y_i\leqslant d$ *for all i, and let $(\tau_i)_{i=1}^n\in\mathrm{PGL}_2(\mathbb{F}_p)^n$ be such that $\tau_i\neq\tau_j$ for $i\neq j$ then*

$$\Big|\sum_{a\in\mathbb{F}_p^\times}\prod_{i=0}^n Y_i(\theta(\tau_i\cdot a))-p\prod_{i=0}^n y_i(0)\Big|\leqslant 10n\cdot c(\mathcal{K})^2d^{2n+2}y^n\sqrt{p},\tag{2·8}$$

where $y=\max_{i,j}|y_i(j)|$.

Proof. It is enough to study

$$S=\sum_{a\in\mathbb{F}_p^\times}\prod_{i=0}^n U_{n_i}(K(\tau_i\cdot a)),$$

for any $n_i\geqslant 0$, by following the proof of [8, proposition 1·1] and [27, proposition 4·1]. Let us denote by $\mathcal{F}=\bigotimes_i\tau_i^*\,\mathrm{Sym}^{n_i}(\mathcal{K})$ and let $U\subset\overline{\mathbb{A}}^1_{\mathbb{F}_p}$ be the largest open subset on which $\mathcal{F}$ is lisse. Notice that $t_{\mathcal{F}}(a)=\prod_{i=0}^n U_{n_i}(K(\tau_i\cdot a))$ for any $a\in U(\mathbb{F}_p)$. Then

$$|S-\sum_{a\in U(\mathbb{F}_p)}\prod_{i=0}^n U_{n_i}(K(\tau_i\cdot a))|\leqslant\sum_i c(\tau_i^*\,\mathrm{Sym}^{n_i}(\mathcal{K})),$$

since all the sheaves are pure of weight 0. On the other hand, the Grothendieck–Lefschetz formula gives

$$\sum_{a\in U(\mathbb{F}_p)}\prod_{i=0}^n U_{n_i}(K(\tau_i\cdot a))=\sum_{i=0}^2(-1)^i\,\mathrm{Tr}(\mathrm{Fr}\,|H_c^i(U,\mathcal{F})).$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

Since $\mathcal{F}$ is a middle-extension sheaf (as the product of middle-extension sheaves is a middle-extension sheaf), it follows that $H_c^0(U, \mathcal{F}) = 0$. Moreover, according to parts (iii),(iv) to Lemma 2·4 and the discussion in [8, paragraph 3·1] we have that the $(n+1)$-tuple $\{\tau_i^* \operatorname{Sym}^{n_i}(\mathcal{K})\}_{i=0}^n$ is a strictly U-generous in the sense of [8, defintion 2·1]. Thus, we may use [8, theorem 2·7] to obtain

$$\dim\left(H_c^2\,(U, \mathcal{F})\right) = \prod_{i=0}^{n} M_{n_i}$$

where $M_{n_i} := \operatorname{Mult}(1, \operatorname{Sym}^{n_i} \operatorname{Std})$ is the multiplicity of the standard representation of $\mathrm{SL}_2(\mathbb{C})$, Std, in Sym^{n_i} Std. On the other hand, Sym^{n_i} Std is irreducible for any n_i, and it is trivial if and only if $n_i = 0$. Thus, we have that

$$M_{n_i} = \begin{cases} 1 & \text{if } n_i = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{2·9}$$

Hence,

$$\left|\sum_{a\in U(\mathbb{F}_p)} \prod_{i=0}^{n} U_{n_i}(K(\tau_i \cdot a)) - p\prod_{i=0}^{n} M_{n_i}\right| = |\operatorname{Tr}(\operatorname{Fr}|H_c^1(U, \mathcal{F}))| \leqslant \dim(H_c^1(U, \mathcal{F}))\sqrt{p},$$

by the Riemann Hypothesis over finite fields ([5]). It remains to bound $\dim(H_c^1(U, \mathcal{F}))$. We start by applying the Euler-Poincaré formula, obtaining

$$\begin{aligned}\dim(H_c^1(U, \mathcal{F})) &= (2 - (\operatorname{Sing} \mathcal{F}))\operatorname{Rank}(\mathcal{F}) + \sum_{x\in\overline{\mathbb{P}}^1_{\mathbb{F}_p}} \operatorname{Swan}_x(\mathcal{F}) + \dim(H_c^2(U, \mathcal{F}))\\ &\leqslant (2 - (\operatorname{Sing} \mathcal{F}))\operatorname{Rank}(\mathcal{F}) + \sum_{x\in\overline{\mathbb{P}}^1_{\mathbb{F}_p}} \operatorname{Swan}_x(\mathcal{F}) + 1,\end{aligned}$$

by (2·9). It is shown in [7, proposition 8·2] that

$$\operatorname{Rank}(\mathcal{F}) = \prod_i \operatorname{Rank}\left(\tau_i^* \operatorname{Sym}^{n_i}(\mathcal{K})\right) = \prod_i \operatorname{Rank}\left(\operatorname{Sym}^{n_i}(\mathcal{K})\right) \leqslant \max_i \left(\operatorname{Rank}\left(\operatorname{Sym}^{n_i}(\mathcal{K})\right)\right)^n$$

and that

$$|\operatorname{Sing}(\mathcal{F})| \leqslant \sum_i |\operatorname{Sing}\left(\tau_i^* \operatorname{Sym}^{n_i}(\mathcal{K})\right)| \leqslant n \max_i \left(c\left(\operatorname{Sym}^{n_i}(\mathcal{K})\right)\right).$$

Let us compute $\operatorname{Swan}_x(\mathcal{F})$ for every $x \in \overline{\mathbb{P}}^1_{\mathbb{F}_p}$. For any i, let $\lambda_i(x)$ be the largest break of $\operatorname{Sym}^{n_i}(\mathcal{K})$ at x and let λ_x be the largest break of $\mathcal{F}$ at x. Using [18, lemma 1·3], we get that

$$\lambda(x) \leqslant \max_i \lambda_i(x).$$

Hence,

$$\operatorname{Swan}_x(\mathcal{F}) \leqslant \operatorname{Rank}(\mathcal{F}) \cdot \lambda_x(\mathcal{F}) \leqslant \max_i(\operatorname{Rank}(\operatorname{Sym}^{n_i}(\mathcal{K})))^n \cdot \max_i(c(\operatorname{Sym}^{n_i}(\mathcal{K})))$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

and therefore

$$\dim(H_c^1(U,\mathcal{F})) \leqslant \mathrm{Rank}(\mathcal{F})|\,\mathrm{Sing}\,\mathcal{F}| + |\,\mathrm{Sing}(\mathcal{F})| \cdot \max_x \mathrm{Swan}_x(\mathcal{F})$$
$$\leqslant 10n \cdot (\max_i \mathrm{Rank}(\mathrm{Sym}^{n_i}(\mathcal{K}))^n \cdot (\max_i c(\mathrm{Sym}^{n_i}(\mathcal{K}))^2.$$

Putting it all together, we get that

$$\left| \sum_{a\in U(\mathbb{F}_p)} \prod_{i=0}^{n} U_{n_i}\,(K\,(\tau_i \cdot a)) - p \prod_{i=0}^{n} M_{n_i} \right| = |\,\mathrm{Tr}\left(\mathrm{Fr}\,|H_c^1\,(U,\mathcal{F})\right)| \leqslant L\sqrt{p},$$

where $L = 10n \cdot (\max_i \mathrm{Rank}(\mathrm{Sym}^{n_i}(\mathcal{K}))^n \cdot (\max_i c(\mathrm{Sym}^{n_i}(\mathcal{K}))^2$. And otherwise, if there exists an i for which $n_i \neq 0$, we have

$$|S| \leqslant L\sqrt{p}.$$

The result then follows from the fact that

$$\mathrm{Rank}(\mathrm{Sym}^{n_i}(\mathcal{K})) = n_i + 1 \leqslant 2d, \text{ and } c(\mathrm{Sym}^{n_i}(\mathcal{K})) \leqslant n_i c(\mathcal{K}) \leqslant dc(\mathcal{K}),$$

because $n_i \leqslant d$ for every i by assumption.

2·3. *Proof of Proposition 2·3*

Fix $m, \gamma \in \mathbb{N}$. To each $a \in \mathbb{F}_p^x$ we associate a point in $[0,\pi]^{2m}$ by defining

$$\boldsymbol{\theta}(a) = (\theta(\tau_{-m}.a), \cdots \theta(\tau_{-1}.a), \theta(\tau_1 \cdot a), \cdots, \theta(\tau_m \cdot a))),$$

where $\theta(\tau_i \cdot a)$ is the angle associated to $K(\tau_i \cdot a)$ accordingly with Section 2·2. Moreover, we denote by $\chi_{\frac{1}{\gamma}}(\cdot)$ (resp. $\chi_{-\frac{1}{\gamma}}(\cdot)$) the characteristic function of the interval $[0, \pi/2 - \pi/\gamma]$ (resp.$[\pi/2 + \pi/\gamma, \pi]$). To prove Proposition 2·3, we start by approximating the values of the product

$$\prod_{i=1}^{m} \chi_{\frac{1}{\gamma}}(\theta(\tau_i \cdot a)) \prod_{i=1}^{m} \chi_{-\frac{1}{\gamma}}(\theta(\tau_{-i} \cdot a))$$

using Chebyshev polynomials. We use the same method adopted in [20, section 3]: for any m, we find an integer $L \equiv -1(\mod 2\gamma)$ and two families of trigonometric polynomials $\{\alpha_{L,i}\}$, and $\{\beta_{L,i}\}$ such that for

$$A_L\left(\frac{\boldsymbol{\theta}(a)}{\pi}\right) = \prod_{1\leqslant |i| \leqslant m} \alpha_{L,i}\left(\frac{\theta(\tau_i \cdot a)}{\pi}\right),$$
$$B_L\left(\frac{\boldsymbol{\theta}(a)}{\pi}\right) = \sum_{1\leqslant |i| \leqslant m} \beta_{L,i}\left(\frac{\theta(\tau_i \cdot a)}{\pi}\right) \prod_{j\neq i} \alpha_{L,j}\left(\frac{\theta(\tau_i \cdot a)}{\pi}\right),$$

the following inequality holds for any $a \in \mathbb{F}_p$

$$A_L\left(\frac{\boldsymbol{\theta}(a)}{\pi}\right) - B_L\left(\frac{\boldsymbol{\theta}(a)}{\pi}\right) \leqslant \prod_{i=1}^{m} \chi_{\frac{1}{\gamma}}(\theta(\tau_i \cdot a)) \prod_{i=1}^{m} \chi_{-\frac{1}{\gamma}}(\theta(\tau_{-i} \cdot a)). \tag{2·10}$$

Moreover, this approximation satisfies the following properties.

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

LEMMA 2·6. *With the notations above, we have*:

(i) *there exist two constants $L_0 \geqslant 1$ and $c > 0$ depending only on γ, such that the contribution Δ of the constant term in the Chebyshev expansions of $A_L(\boldsymbol{\theta}/\pi) - B_L(\boldsymbol{\theta}/\pi)$ satisfies*:

$$\Delta \geqslant \frac{1}{2}\left(\frac{1}{2} - \frac{1}{\gamma}\right)^{2m},$$

when L is the smallest integer such that $L \equiv -1 \mod 2\gamma$ and $L \geqslant \max(cm, L_0)$;

(ii) *All the coefficients in the Chebyshev expansion (see Remark 5) of the factors in $A_L(\boldsymbol{\theta}/\pi)$ and all the terms in $B_L(\boldsymbol{\theta}/\pi)$ are bounded by* 1.

(iii) *The Chebyshev degree of the factors of $A_L(\boldsymbol{\theta}/\pi)$ and $B_L(\boldsymbol{\theta}/\pi)$ are $\leqslant 2L$.*

Assuming this Lemma, we can easily prove Proposition 2·3. Fix $\gamma = 1/4$ in Lemma 2·6 and denote

$$S_{p,m} := \{a \in \mathbb{F}_p^\times : K(\tau_n \cdot a) \geqslant \sqrt{2},\, K(\tau_{-n} \cdot a) \leqslant -\sqrt{2} \text{ for any } n = 1, ..., m\}.$$

Notice that $a \in S_{p,m}$ if and only if $\boldsymbol{\theta}(a) \in [-\frac{\pi}{2}, -\frac{\pi}{4}]^m \times [0, \frac{\pi}{4}]^m$. Let L be as in part (i) of Lemma 2·6; then

$$\begin{aligned}
|S_{p,m}| &= \sum_{a\in\mathbb{F}_p^\times} \prod_{i=1}^{m} \chi_{\frac{1}{4}}(\theta(\tau_i \cdot a)) \prod_{i=1}^{m} \chi_{-\frac{1}{4}}(\theta(\tau_{-i} \cdot a)) \\
&\geqslant \sum_{a\in\mathbb{F}_p^\times} \left(A_L\left(\frac{\boldsymbol{\theta}(a)}{\pi}\right) - B_L\left(\frac{\boldsymbol{\theta}(a)}{\pi}\right)\right) \\
&= p\Delta + O(mc(\mathcal{K})^2 L^{4m+2}\sqrt{p}) \\
&\geqslant \frac{1}{2}\left(\frac{1}{4}\right)^{2m} p + O(mc(\mathcal{K})^2 L^{4m+2}\sqrt{p}),
\end{aligned} \tag{2·11}$$

where in the second step we use Lemma 2·5. Also notice that:

(i) the condition $\tau_i \neq \tau_j$ for $i \neq j$ is satisfied by definition of 1-parameter family;

(ii) by part (ii) of Lemma 2·6 we have that y in Lemma 2·5 is equal to 1.

Let us denote $\delta = 1 - \varepsilon$ and consider $m = [(\log p)^\delta]$. By part (i) of Lemma 2·6 we know that $\max(cm, L_0) \leqslant L \leqslant \max(2\gamma cm, L_0)$. We may assume $cm \leqslant L \leqslant 2\gamma cm$, because L_0 is an absolute constant (it depends only on $\gamma = 1/4$). Then

$$\begin{aligned}
mc(\mathcal{K})^2 L^{2m+2}\sqrt{p} &\leqslant 2(\log p)^\delta c(\mathcal{K})^2 (2\gamma c(\log p)^\delta)^{4(\log p)^\delta + 2}\sqrt{p} \\
&= o((\log p)^{10\delta(\log p)^\delta}\sqrt{p}) \\
&= o(p^{\frac{1}{2}+\eta}),
\end{aligned} \tag{2·12}$$

for any $\eta > 0$. On the other hand, we have

$$\left(\frac{1}{4}\right)^{2m} \gg \left(\frac{1}{4}\right)^{2(\log p)^\delta} = e^{-\log 16 (\log p)^\delta} = e^{-\log 16 \frac{\log p}{(\log p)^\varepsilon}} = p^{-\frac{\log 16}{(\log p)^\varepsilon}}.$$

Thus, we obtain

$$|S_{p,[(\log p)^{1-\varepsilon}]}| \gg_\epsilon p^{1-\frac{\log 16}{(\log p)^\varepsilon}},$$

as we desired.

Proof of Lemma 2·6. The proof utilises ideas from [20, lemma 3·2] and [3]. Let $\mathbf{x} := (x_{-m}, \ldots, x_{-1}, x_1, \ldots x_m) \in [0,1]^{2m}$. We first construct the polynomial $A_L(\mathbf{x})$. Since $A_L(\mathbf{x}) = \prod_{1\leqslant|i|\leqslant m} \alpha_{L,i}(x_i)$, it is sufficient to define the $\alpha_{L,i}$s:

(i) if $1 \leqslant i \leqslant m$, $\alpha_{L,i}$ is a trigonometric polynomial in one variable

$$\sum_{|\ell|\leqslant L} \hat{\alpha}_{L,+}(\ell)e(\ell x),$$

where the $\hat{\alpha}_{L,+}(\ell)$s are defined as in [3, (2·2), lemma 5, (2·17)] with $u=0$, $v=1/2-1/\gamma$;

(ii) if $-m \leqslant i \leqslant 1$, $\alpha_{L,i}$ is a trigonometric polynomial in one variable

$$\sum_{|\ell|\leqslant L} \hat{\alpha}_{L,-}(\ell)e(lx)$$

where the $\hat{\alpha}_{L,-}(\ell)$s are defined as in [3, (2·2), lemma 5, (2·17)] with $u=1/2+1/\gamma$, $v=1$.

Let us focus on the definition of $B(\mathbf{x})$. Since we want $B_L(\mathbf{x}) = \sum_{1\leqslant|i|\leqslant m} \beta_{L,i}(x_i)\prod_{j\neq i}\alpha_{L,j}(x_i)$, in order to construct $B_L(\mathbf{x})$ it is sufficient to define $\beta_{L,i}$ for any $1\leqslant|i|\leqslant m$:

(i) for $1 \leqslant i \leqslant m$, define

$$\begin{aligned}\beta_{L,i}(x) &= \tfrac{1}{2(L+1)}\left(\sum_{|\ell|\leqslant L}\left(1-\tfrac{|\ell|}{L+1}\right)e(\ell x) + \sum_{|\ell|\leqslant L}\left(1-\tfrac{|\ell|}{L+1}\right)e\left(\ell\left(x-\tfrac{1}{2}+\tfrac{1}{\gamma}\right)\right)\right)\\ &= \tfrac{1}{2(L+1)}\left(2+\sum_{1\leqslant\ell\leqslant L}\left(1-\tfrac{\ell}{L+1}\right)\left(\cos\left(\pi\ell-\tfrac{2\pi\ell}{\gamma}\right)\right.\right.\\ &\qquad \left.\left.+\sin\left(\pi\ell+\tfrac{2\pi\ell}{\gamma}\right)+1\right)\cos(2\pi\ell x)\right);\end{aligned}$$

(ii) for $-m \leqslant i \leqslant 1$, define

$$\begin{aligned}\beta_{L,i}(x) &= \tfrac{1}{2(L+1)}\left(\sum_{|\ell|\leqslant L}\left(1-\tfrac{|\ell|}{L+1}\right)e\left(\ell\left(x-\tfrac{1}{2}-\tfrac{1}{\gamma}\right)\right) + \sum_{|\ell|\leqslant L}\left(1-\tfrac{|\ell|}{L+1}\right)e(\ell(x-1)\right)\\ &= \tfrac{1}{2(L+1)}\left(2+\sum_{1\leqslant\ell\leqslant L}\left(1-\tfrac{\ell}{L+1}\right)\left(\cos\left(-\pi\ell-\tfrac{2\pi\ell}{\gamma}\right)\right.\right.\\ &\qquad \left.\left.+\sin\left(-\pi\ell-\tfrac{2\pi\ell}{\gamma}\right)+1\right)\cos(2\pi\ell x)\right).\end{aligned}$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

Remember that the nth coefficients in the Chebychev expansions of $\alpha_{L,i}$ and $\beta_{L,i}$ are given by

$$\int_0^{\pi} \alpha_{L,i}\left(\frac{\theta}{\pi}\right) U_n(\theta) d\mu_{st} \text{ and } \int_0^{\pi} \beta_{L,i}\left(\frac{\theta}{\pi}\right) U_n(\theta) d\mu_{st}$$

respectively; then part (iii) immediately follows, since the above integrals vanish when $n > 2L$. In [3, lemma 5] it is shown that $0 \leqslant \alpha_{L,i}(x) \leqslant 1$ for $x \in [0, 1]$. On the other hand, one has that $0 \leqslant |\beta_{L,i}(x)| \leqslant 1$ for any i and for any $x \in [0, 1]$ by definition. Using the Cauchy-Schwarz inequality, we have

$$\left| \int_0^{\pi} \alpha_{L,i}\left(\frac{\theta}{\pi}\right) U_n(\theta) d\mu_{st}\right|^2 \leqslant \int_0^{\pi} |\alpha_{L,i}\left(\frac{\theta}{\pi}\right)|^2 d\mu_{st} \cdot \int_0^{\pi} |U_n(\theta)|^2 d\mu_{st} \leqslant 1,$$

and the same argument can be used for $\beta_{L,i}$, which proves part (ii). It remains to prove part (i). For any trigonometric polynomial Y, the constant term of its Chebyshev expansion is given by

$$\int_0^{\pi} Y(\theta) d\mu_{st}.$$

so we have that Δ in part (i) is given by

$$\begin{aligned}\Delta = &\left(\int_0^{\pi} \alpha_{L,1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^m \left(\int_0^{\pi} \alpha_{L,-1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^m \\ &- m\int_0^{\pi} \beta_{L,1}\left(\frac{\theta}{\pi}\right) d\mu_{st} \left(\int_0^{\pi} \alpha_{L,1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^{m-1} \left(\int_0^{\pi} \alpha_{L,-1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^m \\ &- m\int_0^{\pi} \beta_{L,-1}\left(\frac{\theta}{\pi}\right) d\mu_{st} \left(\int_0^{\pi} \alpha_{L,1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^{m} \left(\int_0^{\pi} \alpha_{L,-}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^{m-1}.\end{aligned}$$

Using the definition of $\beta_{L,\pm 1}$ we get

$$\int_0^{\pi} \beta_{L,\pm 1}(\tfrac{\theta}{\pi}) d\mu_{st} = \frac{1}{L+1},$$

so we can write Δ as

$$\begin{aligned}\Delta = &\left(\int_0^{\pi} \alpha_{L,1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^m \left(\int_0^{\pi} \alpha_{L,-1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^m \\ &- \frac{m}{L+1}\left(\int_0^{\pi} \alpha_{L,1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^{m-1} \left(\int_0^{\pi} \alpha_{L,-1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^m \\ &- \frac{m}{L+1}\left(\int_0^{\pi} \alpha_{L,1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^{m} \left(\int_0^{\pi} \alpha_{L,-1}\left(\frac{\theta}{\pi}\right) d\mu_{st}\right)^{m-1}.\end{aligned}$$

Notice that $\alpha_{L,\pm 1} \rightarrow \chi_{\pm\frac{1}{\gamma}}$ in $L^2([0, 1])$ $L \rightarrow \infty$. Moreover, from [3, (2·6)] one has

$$|\chi_{\pm\frac{1}{\gamma}}(x) - \alpha_{L,\pm 1}(x)| \leqslant |\beta_{L,\pm 1}(x)| \qquad 0 \leqslant x \leqslant 1.$$

From the Fourier expansion of $\beta_{L,\pm 1}(x)$,

$$||\beta_{L,\pm 1}||_{L^2}^2 \leqslant \frac{8+3L}{(2L+2)^2} \longrightarrow 0.$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

Thus,

$$\int_0^\pi \alpha_{L,1\pm}\left(\frac{\theta}{\pi}\right) d\mu_{st} \longrightarrow \int_0^\pi \chi_{\pm\frac{1}{\gamma}}\left(\frac{\theta}{\pi}\right) d\mu_{st} = \frac{1}{2} - \frac{1}{\gamma} + \frac{\sin\left(\frac{\pi}{\gamma}\right)\cos\left(\frac{\pi}{\gamma}\right)}{\pi}.$$

This implies that there exists L_0, such that $\int_0^\pi \alpha_{L,1\pm}\left(\frac{\theta}{\pi}\right) d\mu_{st} \geqslant 1/2 - 1/\gamma$. Hence,

$$\Delta \geqslant \left(\frac{1}{2} - \frac{1}{\gamma}\right)^{2m-2}\left(\left(\frac{1}{2} - \frac{1}{\gamma}\right)^2 - \frac{3m}{L+1}\right). \tag{2·13}$$

If we assume further that $L + 1 \geqslant 6m\,(1/2 - 1/\gamma)^{-2}$, we obtain

$$\Delta \geqslant \frac{1}{2}\left(\frac{1}{2} - \frac{1}{\gamma}\right)^{2m} \tag{2·14}$$

as desired.

3. *Moments: proof of Theorem 1·8*

3·1. *An auxiliary lemma*

The following Lemma will be instrumental to the proof of Theorem 1·8.

LEMMA 3·1. *Assume the notation of Theorem 1·8, and let $0 \leqslant \alpha < \beta \leqslant 1$. Then for every $k \geqslant 2$ there exist two constants C_1, $C_2 \geqslant 1$ depending only on $c_{\mathfrak{F}}$, such that*

$$\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times}\left|\frac{1}{\sqrt{p}}\sum_{\alpha p < x \leqslant \beta p} t_{a,p}(x)\right|^{2k} \leqslant C_1^{2k}(\log k)^{2k}\,(\beta-\alpha)^{\frac{2k}{\log k}} + C_2^{2k}p^{-\frac{1}{2}}(\log p)^{2k}.$$

Proof. We start by applying Lemma 2·1 to obtain

$$\frac{1}{\sqrt{p}}\sum_{\alpha p < x \leqslant \beta p} t_{a,p} = \frac{1}{2\pi i}\sum_{1\leqslant |n| \leqslant p/2}\frac{\hat{t}_{a,p}(n)}{n}(1 - e((\beta-\alpha)n))e(\alpha n) + (\beta-\alpha)\hat{t}_{a,p}(0) + O(1).$$

To simplify the notation, define for any $-p/2 \leqslant n \leqslant p/2$

$$c_n := \frac{(1 - e((\beta-\alpha)n))e(\alpha n)}{n},$$

so we can write the above equation as

$$\frac{1}{\sqrt{p}}\sum_{\alpha p < x \leqslant \beta p} t_{a,p}(x) = \frac{1}{2\pi i}\sum_{1 < |n| < p/2}\hat{t}_{a,p}(n)c_n + (\beta-\alpha)\hat{t}_{a,p}(0) + O(1).$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

By the triangle inequality,

$$\begin{aligned}\frac{1}{p-1}\sum_{a\in\mathbb{F}_a^\times}\left|\frac{1}{\sqrt{p}}\sum_{\alpha p<x\leqslant\beta p}t_{a,p}(x)\right|^{2k} &\leqslant \frac{1}{(p-1)\pi^{2k}}\sum_{a\in\mathbb{F}_p^\times}\left|\sum_{1<|n|<p/2}\hat{t}_{a,p}(n)c_n\right|^{2k}\\ &\quad + O\left(2^{4k}+2^{4k}(\beta-\alpha)^{2k}c_{\mathfrak{F}}^{2k}\right)\\ &= \frac{1}{(p-1)\pi^{2k}}\sum_{a\in\mathbb{F}_p^\times}\left|\sum_{1<|n|<p/2}\hat{t}_{1,p}(\tau_n\cdot a)c_n\right|^{2k}\\ &\quad + O\left(2^{4k}+2^{4k}(\beta-\alpha)^{2k}c_{\mathfrak{F}}^{2k}\right),\end{aligned} \tag{3·1}$$

where in the first inequality we use the fact that $\|\hat{t}_{a,p}\|_\infty \leqslant c(\mathrm{FT}(\mathcal{F}_{a,p})) \leqslant 10c(\mathcal{F}_{a,p})^2 \leqslant 10c_{\mathfrak{F}}^2$ (see Remark 1 and [7, proposition 8·2]). Moreover, since we are assuming that $G_{\mathcal{F}_{1,p}}^{\mathrm{geom}} = G_{\mathcal{F}_{1,p}}^{\mathrm{arith}} = \mathrm{Sp}_{2g}(\mathbb{C})$, it follows that $\hat{t}_{1,p}(\tau_y\cdot a)\in\mathrm{Tr}(\mathrm{USp}_{2g}(\mathbb{C}))=[-2g,2g]$, i.e. $\hat{t}_{a,p}$ is a real function for any p and $a\in\mathbb{F}_p^\times$. Let us bound the first term in the right-hand side of (3·1). Expanding the $2k$th power we get

$$\sum_{a\in\mathbb{F}_p^\times}\sum_{n_1}\cdots\sum_{n_k}\sum_{l_1}\cdots\sum_{l_k}\prod_{i=1}^{k}\hat{t}_{1,p}(\tau_{n_i}\cdot a)\hat{t}_{1,p}(\tau_{l_i}\cdot a)c_{n_i}\overline{c}_{l_i}.$$

Arguing as in Lemma 2·5, we obtain that

$$\left|\sum_{a\in\mathbb{F}_p^\times}\prod_{i=1}^{k}\hat{t}_{1,p}(\tau_{n_i}\cdot a)\hat{t}_{1,p}(\tau_{l_i}\cdot a)-m(\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}})p\right|\leqslant\delta_1^{2k}\sqrt{p},$$

where the constant δ_1 depends only on $c_{\mathfrak{F}}$, $\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}} := (\tau_{n_1},\ldots\tau_{n_k},\tau_{l_1},\ldots,\tau_{l_n})$, and

$$m(\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}})=\prod_{\tau\in\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}}}\mathrm{mult}_1(\mathrm{Std}^{\otimes m_\tau}),$$

where m_τ is the multiplicity of τ in the tuple $\tau_{\mathbf{n},\mathbf{l}}$ and Std is the standard representation of $\mathrm{Sp}_{2g}(\mathbb{C})$ ([8, corollary 1·7]). Notice that $m(\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}})\neq 0$ if and only if m_τ is even for any τ occurring in $\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}}$ ([8, corollary 1·6]). From this we get

$$\sum_{a\in\mathbb{F}_p^\times}\left|\sum_{1<|n|<p/2}\hat{t}_{a,p}(n)c_n\right|^{2k}\leqslant A+B,$$

where

$$A=p\left|\sum_{\mathbf{n},\mathbf{l}}c_{n_1}\cdot\ldots\cdot c_{n_k}\overline{c}_{l_1}\cdot\ldots\cdot\overline{c}_{l_k}m(\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}})\right|,$$

and

$$B=\left|\sqrt{p}\delta_1^{2k}\sum_{\mathbf{n},\mathbf{l}}c_{n_1}\cdot\ldots\cdot c_{n_k}\overline{c}_{l_1}\cdot\ldots\cdot\overline{c}_{l_k}\right|.$$

Let us first bound B:

$$B\leqslant\sqrt{p}\delta_1^{2k}\sum_{\mathbf{n},\mathbf{l}}|c_{n_1}|\cdot\ldots\cdot|c_{n_k}||c_{l_1}|\cdot\ldots\cdot|c_{l_k}|=\sqrt{p}\delta_1^{2k}\left(\sum_n|c_n|\right)^{2k}.$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

On the other hand

$$|c_n| \leqslant 2 \min\left(\frac{1}{n}, (\beta - \alpha)\pi\right) \leqslant \frac{2}{n},$$

hence $B \leqslant \sqrt{p} C_2^{2k} (\log p)^{2k}$ for some $C_2 > 0$ depending only on $c_{\mathfrak{F}}$. To bound A, we can proceed as follows: by definition, $m(\boldsymbol{\tau}_{\mathbf{n},\mathbf{l}}) \leqslant \gamma_1^{2k}$ for some γ_1 depending only on $c_{\mathfrak{F}}$. Thus,

$$A \leqslant \gamma_1^{2k} p \sum_m \sum_{(m_1 \cdots, m_{2k}) \in \nu(m)} c_{m_1} \cdots c_{m_{2k}}, \tag{3·2}$$

where $\nu(m) := \{(m_1, \ldots, m_{2k}) : m_1 \cdots m_{2k} = m \quad \text{any } m_i \text{ appears an even number of times}\}$. On the other hand, for any $(m_1, ..., m_{2k}) \in \nu(m)$ we have that

$$c_{m_1} \cdots c_{m_{2k}} \leqslant 2^{2k} \min\left(\frac{1}{m}, ((\beta - \alpha)\pi)^{2k}\right) =: c(m).$$

Let us focus our attention on the size of $|\nu(m)|$. First observe that by definition, $\nu(m) = 0$ when m is not a square. Moreover, for any $(m_1, \ldots, m_{2k}) \in \nu(m^2)$, we can find two sets $S_1, S_2 \subset \{1, ..., 2k\}$ such that

$$|S_1| = |S_2| = k, \qquad S_1 \cap S_2 = \emptyset, \qquad m = \prod_{i \in S_1} m_i = \prod_{j \in S_2} m_j.$$

Hence,

$$|\nu(m^2)| \leqslant \binom{2k}{k} d_k(m)^2,$$

where $d_k(m) := |\{(m_1, \ldots, m_k) : m_1 \cdots m_k = m\}|$. Inserting this into (3·2) we get

$$\begin{aligned} A &\leqslant \gamma_1^{2k} \binom{2k}{k} p \sum_m d_k(m)^2 c\left(m^2\right) \\ &\leqslant \gamma_1^{2k} \binom{2k}{k} p \sum_{m \leqslant p} d_k(m)^2 c\left(m^2\right) + O_{k,\varepsilon}\left(p^{\varepsilon}\right). \end{aligned}$$

It is shown in [**2**, lemma 4·1, pp. 437-438] that

$$\sum_{m \leqslant p} d_k(m)^2 c(m^2) \leqslant 2^k (\log k)^{2k} \left(\frac{\pi}{\beta - \alpha}\right)^{-\frac{2k}{\log k}}$$

which conclude the proof.

3·2. *Proof of Theorem 1·8*

We are finally ready to prove Theorem 1·8

Proof of Theorem 1·8. Let us start with the lower bound. By Lemma 2·2 for $t = t_{a,p}$, $N = k$ and $\alpha = 1/2$, we have that

$$M(t_{a,p}) \geqslant \frac{1}{2\pi} \left| \sum_{\substack{1 \leqslant n \leqslant k \\ n = 1(2)}} \frac{\hat{t}_{1,p}(\tau_n \cdot a)}{n} \right| + O_{c(\mathfrak{F})}(1) \tag{3·3}$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

for any p large enough and $a \in \mathbb{F}_p^\times$. By definition of a 1-parameter family of Sp_{2g}-type, the sheaf $\mathrm{FT}(\mathcal{F}_{1,p})$ is a bountiful sheaf of Sp_{2g}-type. This implies that the sheaves $\mathrm{FT}(\mathcal{F}_{1,p}),\ \tau_{-1}^* \mathrm{FT}(\mathcal{F}_{1,p}), \dots, \tau_{-k}^* \mathrm{FT}(\mathcal{F}_{1,p}),\ \tau_k^* \mathrm{FT}(\mathcal{F}_{1,p})$ satisfy the Goursat–Kolchin–Ribet criterion ([19, chapter 1·8]). Thus combining [8, lemma 2·4] with Deligne's equidistibution Theorem, we obtain that the sequence

$$\left\{\hat{t}_{1,p}(\tau_1 \cdot a),\ \hat{t}_{1,p}(\tau_{-1} \cdot a),\ \dots,\ \hat{t}_{1,p}(\tau_{-k} \cdot a),\ \hat{t}_{1,p}(\tau_k \cdot a)\right\}_{a\in\mathbb{F}_p}$$

become equidistributed in $(\prod_{i=1}^{2k}[-2g, 2g],\ \mu_{\mathrm{USp}_{2g}(\mathbb{C})}^{\otimes 2k})$ as $p \to \infty$, where $\mu_{\mathrm{USp}_{2g}(\mathbb{C})}$ is the pushforward of the Haar measure of $\mathrm{USp}_{2g}(\mathbb{C}) \subset \mathrm{Sp}_{2g}(\mathbb{C})$ (notice that $[-2g, 2g] = \mathrm{Tr}(\mathrm{USp}_{2g}(\mathbb{C}))$). Now if we define

$$\begin{aligned} S_{k,p} = \{a \in \mathbb{F}_p^\times : &\hat{t}_{1,p}(\tau_i \cdot a) > \sqrt{2}g\ \forall 0 < i < k, \\ &\hat{t}_{1,p}(\tau_{-i} \cdot a) < -\sqrt{2}g\ \forall 0 < i < k\}, \end{aligned}$$

we get that

$$M(t_{a,p}) \geqslant \left(\frac{g}{\sqrt{2\pi}} + o(1)\right) \log k$$

for any $a \in S_{k,p}$. Hence,

$$\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times} M\left(t_{a,p}\right)^{2k} \geqslant \frac{1}{p-1}\sum_{a\in S_{k,p}} M\left(t_{a,p}\right)^{2k} \geqslant \left(\frac{cg}{\sqrt{2\pi}} + o(1)\right)^{2k} (\log k)^{2k},$$

where $c = \mu_{\mathrm{USp}_{2g}(\mathbb{C})}((\sqrt{2}g, 2g]) \gg 1$. Let us now prove the upper bound. For any $a \in \mathbb{F}_p^\times$ let $N_{a,p}$ be the smallest integer such that

$$M(t_{a,p}) = \left|\frac{1}{\sqrt{p}}\sum_{x\leqslant N_{a,p}} t_{a,p}(x)\right|.$$

At this point we would like to apply Lemma 3·1 but the $N_{a,p}$'s might be very different from one another. To go around this issue, following the strategy of [24] and [2], we will use the Rademacher–Menchov trick: first of all expand $N_{a,p}/p$ in base 2

$$\frac{N_{a,p}}{p} = \sum_{j=1}^{\infty} a_j 2^{-j} \qquad a_j \in \{0, 1\},$$

and let $N_{a,p}(L_p)/p$ be the truncation of this series at the summand of power L_p. Then we have

$$M(t_{a,p}) \leqslant \left|\frac{1}{\sqrt{p}}\sum_{x\leqslant N_{a,p}(L_p)} t_{a,p}(x)\right| + E\left(a,\ p.L_p\right),$$

where

$$E(a, p, L_p) = \left|\frac{1}{\sqrt{p}}\sum_{N_{a,p}(L_p)<x\leqslant N_{a,p}} t_{a,p}(x)\right|.$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

Notice that the number of summands in $E(a,\ p.L_p)$ is $\leqslant p/2^{L_p}$. An application of the Hölder inequality leads to

$$M(t_{a,p})^{2k} \leqslant 2^{2k}\left(\sum_{l\leqslant L_p}\frac{1}{l^{\frac{2k\gamma}{2k-1}}}\right)^{2k-1}\left(\sum_{l\leqslant L_p} l^{2k\gamma}\left|\frac{1}{\sqrt{p}}\sum_{N_{a,p}(l)<x\leqslant N_{a,p}(l+1)} t_{a,p}(x)\right|^{2k}\right) + 2^{2k}E\left(a,\ p,\ L_p\right)^{2k}.$$

Observe first that $N_{a,p}(l+1) \leqslant N_{a,p}(l) + p2^{-(l+1)}$. Moreover, there are 2^{l-1} possibilities for the value of $N_{a,p}(l)$, so

$$M(t_{a,p})^{2k} \leqslant 2^{2k}\left(\sum_{l\leqslant L_p}\frac{1}{l^{\frac{2k\gamma}{2k-1}}}\right)^{2k-1}\left(\sum_{l\leqslant L_p} l^{2k\gamma}\sum_{0\leqslant m\leqslant 2^l-1}\left|\frac{1}{\sqrt{p}}\sum_{p\frac{m}{2^l}<x\leqslant p(\frac{m}{2^l}+2^{-(l+1)})} t_{a,p}(x)\right|^{2k}\right) + 2^{2k}E(a,\ p,\ L_p)^{2k}.$$

We can now apply Lemma 3·1 and choose $\gamma = 3/2$ to obtain

$$\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times} M(t_{a,p})^{2k} \leqslant 2^{2k}\left(\sum_{l\leqslant L_p}\frac{1}{l^{\frac{3k}{2k-1}}}\right)^{2k-1}\left(\sum_{l\leqslant L_p} l^{3k}2^l\left(\gamma^{2k}(\log k)^{2k}2^{-\frac{kl}{\log k}} + \delta^{2k}p^{-\frac{1}{2}}(\log p)^{2k}\right)\right) + \frac{2^{2k}}{p-1}\sum_{a\in\mathbb{F}_p^\times} E\left(a,\ p,\ L_p\right)^{2k}.$$

Choosing $L_p := \log_2\left(\frac{p^{\frac{1}{2}}}{(\log p)^{8k}}\right)$, we get

$$(2\delta)^{2k}\left(\sum_{l\leqslant L_p}\frac{1}{l^{\frac{3k}{2k-1}}}\right)^{2k-1}\sum_{l\leqslant L_p} l^{3k}2^l p^{-\frac{1}{2}}(\log p)^{2k} \ll_k (\log p)^{8k}2^{L_p}p^{-\frac{1}{2}} \ll_k 1,$$

where in the first step we are using the fact that

$$\sum_l \frac{1}{l^{\frac{3k}{2k-1}}} \ll 1.$$

Moreover, using the following inequality from [2, theorem 1·1, p. 440]

$$\sum_{l\leqslant L_p} l^{3k}2^l2^{-\frac{kl}{\log k}} \leqslant \exp(3k\log\log k + O(k)),$$

we get

$$(2\gamma)^{2k}(\log k)^{2k}\left(\sum_{l\leqslant L_p}\frac{1}{l^{\frac{2k}{2k-1}}}\right)^{2k-1}\sum_{l\leqslant L_p} l^{2k}2^l2^{-\frac{kl}{\log k}} \ll_k 1.$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

On the other hand, since the length of $E(a, p, L_p)$ is at most $p/2^{L_p} = p^{\frac{1}{2}}(\log p)^{8k}$, an application of [9, theorem 1·1] leads to

$$|E(a, p, L_p)| \leqslant 4c_{\mathfrak{F}} \log\left(4e^8(\log p)^{8k}\right).$$

Then

$$\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times} E\left(a, p, L_p\right)^{2k} \leqslant (Ck)^k(\log\log p)^{2k},$$

and this completes the proof of the first part of the Theorem. Now let us assume that

$$\Big|\sum_{N\leqslant x\leqslant N+H} t_{a,p}(x)\Big| \ll_{c_{\mathfrak{F}}} H^{1-\varepsilon} \tag{3·4}$$

holds uniformly for any $1 < N < p$, $p^{1/2-\varepsilon/2} < H < p^{1/2+\varepsilon/2}$ and $a \in \mathbb{F}_p^\times$. Starting again from

$$\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times} M(t_{a,p})^{2k} \leqslant 2^{2k}\left(\sum_{l\leqslant L_p}\frac{1}{l^{\frac{2\gamma k}{2k-1}}}\right)^{2k-1}\left(\sum_{l\leqslant L_p} l^{2k\gamma}2^l\left(\gamma^{2k}(\log k)^{2k}2^{-\frac{kl}{\log k}}\right.\right.$$
$$\left.\left.+\,\delta^{2k}p^{-\frac{1}{2}}(\log p)^{2k}\right)\right) + \frac{2^{2k}}{p-1}\sum_{a\in\mathbb{F}_p^\times} E\left(a, p, L_p\right)^{2k},$$

we choose $L_p = (1-\varepsilon)/2\log_2 p$, and obtain by (3·4) that there exists some $\varepsilon' > 0$ such that

$$E\left(a, p, L_p\right)^{2k} = \Big|\frac{1}{\sqrt{p}}\sum_{N_{a,p}(L_p)<x\leqslant N_{a,p}} t_{a,p}(x)\Big|^{2k} \ll_{c_{\mathfrak{F}}} p^{-\varepsilon'}$$

for any p and any $a \in \mathbb{F}_p^\times$. Hence,

$$\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times} E\left(a, p, L_p\right)^{2k} \ll_{c_{\mathfrak{F}}} p^{-\varepsilon'}.$$

Moreover,

$$\begin{aligned} p^{-\frac{1}{2}}(\delta\log p)^{2k}\left(\sum_{l\leqslant L_p} l^{2k\gamma}2^l\right) &\leqslant p^{-\frac{1}{2}}(\delta\log p)^{2k}\left(\sum_{l\leqslant L_p} L_p^{4k}2^l\right) \\ &\ll_{k,c_{\mathfrak{F}}} p^{-\frac{1}{2}}(\log p)^{2k}2^{L_p} \\ &\ll p^{-\varepsilon/2}(\log p)^{2k}. \end{aligned}$$

Putting it all together, we get

$$\frac{1}{p-1}\sum_{a\in\mathbb{F}_p^\times} M(t_{a,p})^{2k} \leqslant (2\gamma\log k)^{2k}\left(\sum_{l\leqslant L_p}\frac{1}{l^{\frac{2\gamma k}{2k-1}}}\right)^{2k-1}\left(\sum_{l\leqslant L_p} l^{2k\gamma}2^l2^{-\frac{kl}{\log k}}\right)$$
$$+\,O_{k,c_{\mathfrak{F}}}(p^{-\varepsilon''})$$

https://doi.org/10.1017/S030500412100030X Published online by Cambridge University Press

for some $\varepsilon'' > 0$. On the other hand, [2, theorem 1·1 p. 440] implies that

$$\sum_{l \leqslant L_p} \frac{1}{l^{\frac{2\gamma k}{2k-1}}} \leqslant (\gamma - 1)^{1-2k}, \qquad \sum_{l \leqslant L_p} l^{2k\gamma} 2^l 2^{-\frac{kl}{\log k}} \leqslant \exp(2k\gamma \log\log k + O(k)).$$

Hence, by choosing $\gamma = 1 + 1/\log\log k$ we obtain the desired result.

We conclude with the proof of Corollary 1·9.

Proof of Corollary 1·9. For part (i), observe that it follows from the proof of the lower bound of Theorem 1·8 that any element a in the set

$$S_{h,p} = \Big\{ a \in \mathbb{F}_p^\times : \quad \hat{t}_{1,p}(\tau_i \cdot a) > \sqrt{2}g \; \forall 0 < i < h, \\ \hat{t}_{1,p}(\tau_{-i} \cdot a) < -\sqrt{2}g \; \forall 0 < i < h \Big\}$$

satisfies that $M(t_{a,p}) > (r/(\sqrt{2}\pi) + o(1)) \log h$. Moreover we have that $|S_{h,p}| > c^{2h}$ for some absolute constant $0 < c < 1$. Choosing $h = \exp((g/(\sqrt{2}\pi) + o(1))^{-1} \cdot A)$ we get

$$D_{\mathfrak{F}}(A) \geqslant |S_{\exp((g/(\sqrt{2}\pi)+o(1))^{-1}\cdot A),p}|.$$

The proof of (ii) is exactly the same as in [2, theorem 1·3].

Acknowledgements. I am most thankful to my advisor, Emmanuel Kowalski, for suggesting this problem and for his guidance during these years. I also would like to thank Youness Lamzouri for informing me about his work on sum of incomplete Birch sums and Tal Horesh for her suggestions on a previous version of the paper. Finally, I am very grateful to the anonymous referee for their careful reading of the manuscript and their valuable comments.

REFERENCES

[1] P. Autissier, D. Bonolis and Y. Lamzouri. The distribution of the maximum of partial sums of Kloosterman sums and other trace functions. Submitted, 45 pages. arXiv:1909.03266.

[2] J.W. Bober and L. Goldmakher. The distribution of the maximum of character sums. *Mathematika* **59**(2) (2013), 427–442.

[3] J. T. Barton, H.L. Montgomery and J. D. Vaaler. Note on a Diophantine inequality in several variables. *Proc. Amer. Math. Soc.* **129**(2) (2001), 337–345.

[4] P. Deligne. Cohomologie étale (SGA $4\frac{1}{2}$). Lecture Notes in Math. Vol. 569 (Springer-Verlag, 1977).

[5] P. Deligne. La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.* (52) (1980), 137–252.

[6] É. Fouvry, E. Kowalski and P. Michel. Trace functions over finite fields and their applications. Colloquia. Ed. Norm. vol. 5 (Pisa, 2014).

[7] É. Fouvry, E. Kowalski and P. Michel. Algebraic twists of modular forms and Hecke orbits. *Geom. Funct. Anal.* **25**(2) (2015), 580–657.

[8] É. Fouvry, E. Kowalski and P. Michel. A study in sums of products. *Philos. Trans. Roy. Soc. A* **373**(2040) (2015), 26.

[9] É. Fouvry, E. Kowalski, P. Michel, C. S Raju, J. Rivat and K. Soundararajan. On short sums of trace functions. *Ann. Inst. Fourier (Grenoble)* **67**(1) (2019), 423–449.

[10] É. Fouvry, E. Kowalski and P. Michel. On the conductor of cohomological transforms. Submitted, arXiv:1310.3603.

[11] É. Fouvry, E. Kowalski, P. Michel and W. Sawin. Lectures on applied ℓ-adic cohomology. *Contemp. Math.* (2019).

[12] L. Goldmakher and Y. Lamzouri. Lower bounds on odd order character sums. *Int. Math. Res. Not. IMRN* (21) (2012), 5006–5013.

[13] L. GOLDMAKHER and Y. LAMZOURI. Large even order character sums. *Proc. Amer. Math. Soc.* **142**(8) (2014), 2609–2614.
[14] A. GRANVILLE and K. SOUNDARARAJAN. Large character sums: pretentious characters and the Pólya-Vinogradov theorem. *J. Amer. Math. Soc.* **20**(2) (2007), 357–384.
[15] C. HOOLEY. On the greatest prime factor of a cubic polynomial. *J. Reine Angew. Math.* 303/304 (1978), 21–50.
[16] H. IWANIEC and E. KOWALSKI. Analytic number theory. Amer. Math. Soc. Colloquium Publications. vol. 53 (American Mathematical Society, Providence, RI, 2004).
[17] N. M. KATZ. Sommes exponentielles. *Astérisque*. Société Mathématique de France, Paris, 1980.
[18] N. M. KATZ. Gauss sums, Kloosterman sums, and monodromy group. *Ann. Math. Stud.* (Princeton University Press, Princeton, NJ, 1988).
[19] N. M. KATZ. Exponential sums and differential equations. *Ann. Math. Stud.* (Princeton University Press, Princeton, NJ, 1990).
[20] E. KOWALSKI, Y.-K. LAU, K. SOUNDARARAJAN and J. WU. On modular signs. *Math. Proc. Camb. Phil. Soc.* 149(3) (2010), 389–411.
[21] E. KOWALSKI and W. SAWIN. Kloosterman paths and the shape of exponential sums. *Compos. Math.* **152**(7) (2016), 1489–1516.
[22] Y. LAMZOURI. On the distribution of the maximum of cubic exponential sums. *J. Inst. Math. Jussieu* 19(4) (2020), 1259–1286.
[23] H. L. MONTGOMERY and R. C. VAUGHAN. Exponential sums with multiplicative coefficients. *Invent. Math.* **43**(1) (1977), 69–82.
[24] H. L. MONTGOMERY and R. C. VAUGHAN. Mean values of character sums. *Canad. J. Math.* **31**(3) (1979), 476–487.
[25] G. PÓLYA. Über die Verteilung der quadratischen Reste und Nichtreste. Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse (1918), 21–29.
[26] R. E. A. C. PALEY. A Theorem on Characters. *J. London Math. Soc.* **7**(1) (1932), 28–32.
[27] C. PERRET-GENTIL. Gaussian distribution of short sums of trace functions over finite fields. *Math. Proc. Camb. Philos. Soc.* **163**(3) (2017), 385–422.
[28] I. M. VINOGRADOV. Sur la distribution des résidus et non-résidus des puissances. *Fiz.-Mat. Ob. Permsk. Gos. Univ*. 1, (1918), 94–98.
[29] A. WEIL. On some exponential sums. *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204–207.