Gaussian distribution of short sums of trace functions over finite fields

Corentin Perret-Gentil

Abstract. We show that under certain general conditions, short sums of ℓ-adic trace functions over finite fields follow a normal distribution asymptotically when the origin varies, generalizing results of Erdős-Davenport, Mak-Zaharescu and Lamzouri. In particular, this applies to exponential sums arising from Fourier transforms such as Kloosterman sums or Birch sums, as we can deduce from the works of Katz. By approximating the moments of traces of random matrices in monodromy groups, a quantitative version can be given as in Lamzouri's article, exhibiting a different phenomenon than the averaging from the central limit theorem.

Contents

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of cardinality q in characteristic p. For a function $t : \mathbb{F}_q \to \mathbb{C}$ and a subset $I \subset \mathbb{F}_q$, we let

$$S(t, I) = \sum_{x \in I} t(x)$$

be the partial sum over I. For I of various structures and sizes, such sums are omnipresent in analytic number theory (see e.g. [IK04, Chapter 12]). Due to oscillations, they often exhibit cancellation, and as a general phenomenon we can expect (or wish for) *square-root cancellation* $|S(t, I)| \ll \sqrt{|I|}$.

Date: September 2016. Last updated: February 2017.
2010 *Mathematics Subject Classification.* 11L05, 11T24, 11N64, 14F20, 15A52, 60G50.

1.1. **Sums over subsets with varying origin.** For $x \in \mathbb{F}_q$, we denote by $I + x = \{y + x : y \in I\}$ the translate of I by x. Given a family of functions $(t_q : \mathbb{F}_q \to \mathbb{C})_q$ and intervals $I_q \subset \mathbb{F}_q$, we are interested in the distribution of the complex random variable

$$\left(\frac{S(t_q, I_q + x)}{\sqrt{|I_q|}}\right)_{x \in \mathbb{F}_q,} \tag{1}$$

with respect to the uniform measure on $\mathbb{F}_q$, as $q, |I_q| \to \infty$.

Example 1.1. When $q = p$, the finite field $\mathbb{F}_p$ can be identified with the discrete interval $[1 \dots p]$. For an interval $I_H = [1 \dots H] \subset [1 \dots p]$ and $1 \leqslant x \leqslant p$ an integer, $S(t, I_H + x)$ is the partial sum

$$S(t, x, H) := \sum_{x < y \leqslant x + H} t(y)$$

of length H starting at $x + 1$. More generally, when $q = p^e$, we can consider "boxes" in $\mathbb{F}_q \cong \mathbb{F}_p^e$.

1.2. **The case of Dirichlet characters.** In the situation of Example 1.1 with $(t_p)_p = (\chi_p)_p$ a family of Dirichlet characters, the question of the distribution of the random variable (1) appears in the literature as follows:

(1) When χ_p is the Legendre symbol, Davenport and Erdős [DE52] showed that the real-valued random variable

$$\left(S(\chi_p, x, H_p)/\sqrt{H_p}\right)_{x \in \mathbb{F}_p}$$

converges in law to a normal distribution with mean 0 and unit variance when

$$p,\ H_p \to \infty \text{ with } \log H_p = o(\log p). \tag{2}$$

(2) Mak and Zaharescu [MZ11] generalized this result to short sums of the form

$$\tilde{S}_p(x, H_p) = \sum_{\substack{P=(x_1,x_2) \in C \\ x \leqslant x_1 < x + H_p \\ x_2 \in I}} \chi_p(g(P))\psi_p(f(P)),$$

where C is an absolutely irreducible affine plane curve over $\mathbb{F}_p$, $g, f \in \mathbb{F}_p(x, y)$ are rational functions, ψ_p (resp. χ_p) is an additive (resp. non-real multiplicative) character modulo p, and I is an interval. Under some technical conditions, they similarly obtain that the projection of the random variable $(\tilde{S}_p(x, H_p)/\sqrt{H_p})_{x \in \mathbb{F}_p}$ on any line through the origin converges in law to a normal distribution with mean 0 and unit variance when $p, H_p \to \infty$ under (2).

(3) Lamzouri [Lam13] showed that when χ_p is a non-real Dirichlet character, the random variable

$$\left(S(\chi_p, x, H_p)/\sqrt{H_p}\right)_{x \in \mathbb{F}_p}$$

converges in law to a normal distribution in $\mathbb{C}$ with mean 0 and covariance matrix $\frac{1}{2}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ when $p, H_p \to \infty$ with (2).

All of the above proceed by using the method of moments. To do so, one needs bounds on character sums that follow from the work of Weil on the Riemann hypothesis for curves over finite fields.

A particular aspect of Lamzouri's method in [Lam13] is to consider a *probabilistic model*, where the values of a multiplicative character are modeled as independent random variables uniformly distributed on the unit circle in $\mathbb{C}$. This model is shown to be accurate (in the sense of convergence in law) by bounding an exponential sum.

1.3. **Generalization to trace functions.** In this article, we will consider the question introduced above for families $(t_q : \mathbb{F}_q \to \mathbb{C})_q$ of *ℓ-adic trace functions over $\mathbb{F}_q$*, as they appear in particular in the works of Katz (see for example [Kat88] and [Kat90]), and more recently in the series of papers by Fouvry, Kowalski, Michel and others (see [FKM14b], [Pol14, Section 6] or [PG16] for surveys).

Using the results reviewed in [FKM15b], building upon Deligne's generalization of the Riemann Hypothesis over finite fields [Del80] and the works of Katz, we will show that under general assumptions on a family of ℓ-adic trace functions $(t_q : \mathbb{F}_q \to \mathbb{C})_q$, and a family of sets $I_q \subset \mathbb{F}_q$, the random variable (1) converges in law to a normal distribution in $\mathbb{C} \cong \mathbb{R}^2$ when q, $H_q = |I_q| \to \infty$ in the range (2). Hence, we generalize the results of Section 1.2 to trace functions.

For example, for the (normalized) Kloosterman sums of rank $n \geqslant 2$

$$\begin{aligned} t_q(x) &= \mathrm{Kl}_{n,q}(x) \\ &= \frac{(-1)^{n-1}}{q^{(n-1)/2}} \sum_{\substack{x_1,\dots,x_n \in \mathbb{F}_q^\times \\ x_1\cdots x_n = x}} e\left(\frac{\mathrm{tr}(x_1+\cdots+x_n)}{p}\right) \end{aligned} \tag{3}$$

(where $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace), we get the following:

Theorem. *Let $n \geqslant 2$ and for every prime power q, let $I_q \subset \mathbb{F}_q$. The complex random variable*

$$\left(\frac{S(\mathrm{Kl}_{n,q}, I_q + x)}{\sqrt{|I_q|}}\right)_{x \in \mathbb{F}_q}$$

(with respect to the uniform measure on $\mathbb{F}_q$) converges in law to a normal distribution $\mathcal{N}$ in $\mathbb{C} \cong \mathbb{R}^2$, with mean 0 and covariance matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ if n is even and $\frac{1}{2}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ if n is odd, when $q, |I_q| \to \infty$ with $\log|I_q| = o(\log q)$.

More precisely, for any $\varepsilon \in (0, 1/2)$ and for any closed rectangle $A \subset \mathbb{C}$ with sides parallel to the coordinate axes and Lebesgue measure $\mu(A)$, the probability

$$P\left(\frac{S(\mathrm{Kl}_{n,q}, I_q + x)}{\sqrt{|I_q|}} \in A\right) = \frac{|\{x \in \mathbb{F}_q : S(\mathrm{Kl}_{n,q}, I_q + x)/|I_q|^{1/2} \in A\}|}{q}$$

is given by

$$P(\mathcal{N} \in A) + O_\varepsilon\left(\mu(A)\left(q^{-\frac{1}{2}+\varepsilon} + \left(\frac{\log|I_q|}{\log q}\right)^{2/5} + \frac{1}{\sqrt{|I_q|}}\right)\right)$$

when q, $|I_q| \to \infty$ *under the range* $\log|I_q| = o(\log q)$ *if* n *is even and* $|I_q| = o\left((\log q)^{\frac{3}{2(1+\varepsilon)}}\right)$ *otherwise. As* $n \to \infty$ *or if* n *is even, the exponents* $2/5$ *and* $3/2$ *can be replaced by* $1/2$ *and* 1*, respectively.*

The general results will be stated in Section 2.

1.3.1. *Examples.* Examples of ℓ-adic trace functions over $\mathbb{F}_q$ we will consider include:

(a) Dirichlet characters χ modulo q or compositions $\chi \circ f$, where $f \in \mathbb{F}_q(T)$ is a rational function. This is the case considered in [Lam13] (if $f = \mathrm{id}$) and [MZ11], when $q = p$.
(b) Hyper-Kloosterman sums $\mathrm{Kl}_{n,q}$ of rank $n \geqslant 2$, or more generally hypergeometric sums, as studied by Katz in [Kat88] and [Kat90].
(c) General exponential sums of the form

$$t_q(x) = \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{F}_q} e\left(\frac{\mathrm{tr}(xf(y) + h(y))}{p}\right) \chi(g(y)), \tag{4}$$

for $f, g, h \in \mathbb{Q}(X)$ rational functions and $\chi : \mathbb{F}_q^\times \to \mathbb{C}$ a multiplicative character. This includes Birch sums

$$t_q(x) = \mathrm{Bi}(x, q) = \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{F}_q} e\left(\frac{\mathrm{tr}(xy + y^3)}{p}\right), \tag{5}$$

considered by Birch, Livné and Katz, and sums of the form

$$t_q(x) = \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{F}_q} e\left(\frac{\mathrm{tr}(xf(y))}{p}\right), \tag{6}$$

studied by Katz and Fouvry-Michel (see e.g. [Mic98]).
(d) Functions counting points on families of curves over $\mathbb{F}_q$ parametrized by varieties over $\mathbb{F}_q$, as surveyed in [KS91, Chapter 10].

Note that t_q can be complex or real-valued (the latter occurring for example for hyper-Kloosterman sums of even rank and Birch sums).

Acknowledgements. The author would like to thank his supervisor Emmanuel Kowalski for guidance and advice during this project. It is a pleasure to acknowledge in particular the influence of the works of Étienne Fouvry, Nicholas Katz, Emmanuel Kowalski, Youness Lamzouri and Philippe Michel. The computations present in this document have been performed with the SageMath [Sag15] software. This work was partially supported by DFG-SNF lead agency program grant 200021L_153647. The results also appear in the author's PhD thesis [PG16].

2. Statement of the results

2.1. **Trace functions over finite fields.** We briefly recall some definitions and terminology around ℓ-adic trace function over finite fields necessary to state our results, and refer the reader to [Kat88], [Kat90, Chapter 7], [Pol14, Section 6], [FKM14b], [FKM14a] or [PG16] for details and further references.

Definition 2.1. Let ℓ be a prime number distinct from the characteristic p of the finite field $\mathbb{F}_q$. We call *ℓ-adic sheaf over $\mathbb{F}_q$* a constructible sheaf $\mathcal{F}$ of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1/\mathbb{F}_q$ (with respect to the étale topology) which is middle-extension, i.e. for every nonempty open $j : U \to \mathbb{P}^1$ on which $\mathcal{F}$ is lisse, we have $\mathcal{F} \cong j_*j^*\mathcal{F}$. We write $\mathrm{Sing}(\mathcal{F}) = \mathbb{P}^1(\overline{\mathbb{F}}_q) - U_{\mathcal{F}}(\overline{\mathbb{F}}_q)$ for the set of *singularities* of $\mathcal{F}$, where $U_{\mathcal{F}}$ is the maximal open set of lissity[1] of $\mathcal{F}$.

There is an alternative point of view through ℓ-adic representations of étale fundamental groups that can be very convenient in practice:

Proposition 2.2. *There is an equivalence of categories between ℓ-adic sheaves $\mathcal{F}$ over $\mathbb{F}_q$ and continuous finite-dimensional ℓ-adic representations*

$$\rho_{\mathcal{F}} : \pi_{1,q} := \mathrm{Gal}\left(\mathbb{F}_q(T)^{\mathrm{sep}}/\mathbb{F}_q(T)\right) \to \mathrm{GL}(\mathcal{F}_{\overline{\eta}}) \cong \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell).$$

Moreover, $\mathcal{F}$ is lisse at $x \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ if and only if the inertia group $I_x \leqslant \pi_{1,q}$ acts trivially on $\overline{\mathbb{Q}}_\ell^n$. The integer n is the rank *of $\mathcal{F}$.*

Definition 2.3. Let $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ be a fixed isomorphism of fields. The *trace function* associated to an ℓ-adic sheaf $\mathcal{F}$ over $\mathbb{F}_q$ corresponding to a representation $\rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}(V)$ is the function

$$\begin{aligned} t_{\mathcal{F}} : \mathbb{F}_q &\to \mathbb{C} \\ x &\mapsto \iota \,\mathrm{tr}\left(\rho_{\mathcal{F}}(\mathrm{Frob}_{x,q}) \mid V^{I_x}\right), \end{aligned}$$

where $\mathrm{Frob}_{x,q} \in (D_x/I_x)^\sharp \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)^\sharp$ is the geometric Frobenius at $x \in \mathbb{F}_q$, for $D_x \leqslant \pi_{1,q}$ the decomposition group at x.

Definition 2.4. An ℓ-adic sheaf $\mathcal{F}$ over $\mathbb{F}_q$ is *pointwise pure of weight* 0 if for every finite extension $\mathbb{F}_{q'}/\mathbb{F}_q$ and every $x \in U_{\mathcal{F}}(\mathbb{F}_{q'})$, the eigenvalues of $\rho_{\mathcal{F}}(\mathrm{Frob}_{x,q'})$ are Weil numbers of weight 0, i.e. their images through any isomorphism of fields $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ have unit absolute value.

By a result of Deligne [Del80, 1.8], we have $||t_{\mathcal{F}}||_\infty \leqslant \mathrm{rank}(\mathcal{F})$ if $\mathcal{F}$ is pointwise pure of weight 0 (this is clear at points of lissity), so the former definition corresponds to a normalization assumption for the trace function.

By the Grothendieck-Lefschetz trace formula, the Euler-Poincaré formula of Grothendieck-Ogg-Safarevich and Deligne's generalization of the Riemann hypothesis over finite fields to weights of ℓ-adic sheaves [Del80], we have a precise control on sums of trace functions:

[1] One shows that such an open exists – it is where the stalk has generic rank – and that $\mathcal{F}$ is determined by its restriction to $U_{\mathcal{F}}$, see e.g. [Kat88, 8.5.1].

Theorem 2.5. *For $\mathcal{F}$ an ℓ-adic sheaf over $\mathbb{F}_q$ that is pointwise pure of weight 0, we have*

$$\sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x) = q\cdot \operatorname{tr}\left(\operatorname{Frob}_q \mid \mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}}\right) + O\left(E(\mathcal{F})\sqrt{q}\right),$$

where

$$1 \longrightarrow \pi_{1,q}^{\mathrm{geom}} = \operatorname{Gal}\left(\mathbb{F}_q(T)^{\mathrm{sep}}/\overline{\mathbb{F}}_q(T)\right) \longrightarrow \pi_{1,q} \longrightarrow \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow 1$$

is exact, $\operatorname{Frob}_q \in \operatorname{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ *is the geometric Frobenius,* $\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}}$ *is the space of coinvariants of the representation* $\rho_{\mathcal{F}}$ *of* $\pi_{1,q}^{\mathrm{geom}}$*, and*

$$E(\mathcal{F}) = \operatorname{rank}(\mathcal{F})\left[\,|\operatorname{Sing}(\mathcal{F})| - 1 + \sum_{x\in\operatorname{Sing}(\mathcal{F})} \operatorname{Swan}_x(\mathcal{F})\right]. \tag{7}$$

Proof. See [Del77, Exposé 6], [FKM14a, Chapter 4], [Kat88, Chapter 2] or [FKM15a, Section 9]. □

Remark 2.6. In the works of Fouvry-Kowalski-Michel and others, the error term is usually only given in terms of the *conductor*

$$\operatorname{cond}(\mathcal{F}) = \operatorname{rank}(\mathcal{F}) + |\operatorname{Sing}(\mathcal{F})| + \sum_{x\in\operatorname{Sing}(\mathcal{F})} \operatorname{Swan}_x(\mathcal{F}),$$

which is independent from q in most "natural" families of sheaves. We are more precise in (7) to be able to discuss cases where the conductor will be growing.

Definition 2.7. An ℓ-adic sheaf over $\mathbb{F}_q$ is *irreducible* (resp. *geometrically irreducible*) if the corresponding representation of $\pi_{1,q}$ (resp. of $\pi_{1,q}^{\mathrm{geom}}$) is irreducible.

Finally, we recall the definition of monodromy groups.

Definition 2.8. For a fixed isomorphism of fields $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$, the *geometric* (resp. *arithmetic*) *monodromy group* of an ℓ-adic sheaf $\mathcal{F}$ over $\mathbb{F}_q$ with rank n is the algebraic group

$$G_{\mathrm{geom}}(\mathcal{F}) = \overline{\iota\rho_{\mathcal{F}}\left(\pi_{1,q}^{\mathrm{geom}}\right)} \leqslant G_{\mathrm{arith}}(\mathcal{F}) = \overline{\iota\rho_{\mathcal{F}}\left(\pi_{1,q}\right)} \leqslant \mathrm{GL}_n(\mathbb{C}),$$

where $\overline{\cdot}$ denotes Zariski closure.

Remark 2.9. The main term in Theorem 2.5 can be rewritten as $q\operatorname{tr}(\operatorname{Frob}_q \mid \mathcal{F}_{G_{\mathrm{geom}}(\mathcal{F})})$, which is $q\dim(\mathcal{F}_G)$ if $G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F})$.

2.2. **Coherent families.** Finally, we introduce the class of families of trace functions to which our results will apply.

Definition 2.10. Let us fix a prime ℓ and an isomorphism of fields $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. A family $(\mathcal{F}_q)_q$ of pointwise pure of weight 0 and geometrically irreducible ℓ-adic sheaves over $\mathbb{F}_q$ (for q varying over powers of primes distinct from ℓ) is said to be *coherent* if:

(1) (Conductor) $\mathrm{cond}(\mathcal{F}_q)$ is bounded independently from q,

and either:

(2) *Kummer case*: For every q, $\mathcal{F}_q$ is a Kummer sheaf $\mathcal{L}_{\chi_q \circ f_q}$ for a character $\chi_q : \mathbb{F}_q^\times \to \mathbb{C}^\times$ and $f_q \in \mathbb{F}_q(X)$, and the characters χ_q are either all real-valued or all complex-valued.

(3) *Classical case*: There exists $G \in \{\mathrm{SL}_{n+1}(\mathbb{C}), \mathrm{Sp}_{2n}(\mathbb{C}), \mathrm{SO}_{n+1}(\mathbb{C})\} - \{\mathrm{SO}_8(\mathbb{C})\}$ for some $n \geqslant 1$ such that for every sheaf $\mathcal{F}_q$ over $\mathbb{F}_q$ in the family:
   (a) (Monodromy groups) The geometric and arithmetic monodromy groups of $\mathcal{F}_q$ coincide and are conjugate to G in $\mathrm{GL}_n(\mathbb{C})$.
   (b) (Independence of shifts) There is no geometric isomorphism

$$[+a]^*\mathcal{F}_q \cong \mathcal{F}_q \otimes \mathcal{L} \quad \text{or} \quad [+a]^*\mathcal{F}_q \cong D(\mathcal{F}_q) \otimes \mathcal{L} \tag{8}$$

   for a sheaf $\mathcal{L}$ of rank 1 over $\mathbb{F}_q$ and $a \in \mathbb{G}_m(\mathbb{F}_q)$, where $D(\mathcal{F}_q)$ denotes the dual sheaf (corresponding to the dual representation).

Definition 2.11. For $\mathcal{F}$ an ℓ-adic sheaf over $\mathbb{F}_q$ and $I \subset \mathbb{F}_q$, we say that $\mathcal{F}$ is *I-compatible* if, in the case where $\mathcal{F}$ is a Kummer sheaf $\mathcal{L}_{\chi(f)}$ with $\deg(f) > 1$, we have that $\sum_{i=1}^m x_i \neq 0$ for all $1 \leqslant m \leqslant \deg(f)$ and $x_1, \dots, x_m \in I$. If $\mathcal{F}$ is not a Kummer sheaf, it is always I-compatible.

Example 2.12. A Kummer sheaf $\mathcal{L}_{\chi(f)}$ is I-compatible if we have $I \subset [1 \dots p/\deg(f))^e \subset \mathbb{F}_q \cong \mathbb{F}_p^e$.

Remarks 2.13. As we shall see, these conditions are fairly generic for natural families arising in number theory. For example, geometric irreducibility and uniform boundedness of conductors are stable by ℓ-adic Fourier transform. In the classical case, the equality of monodromy groups is to control a main term through monodromy (see Remark 2.9), while the other conditions are to show that the monodromy group of a sheaf obtained as a sum of translates of the $\mathcal{F}_q$ is as large as possible, through the Goursat-Kolchin-Ribet criterion of Katz.

2.3. **Qualitative version.**

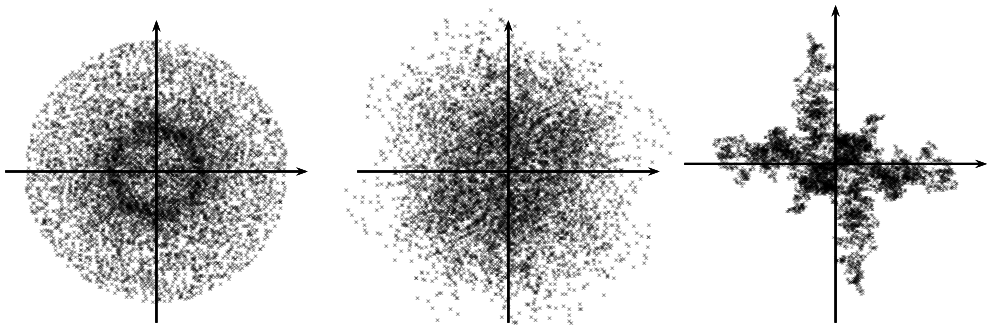
Theorem 2.14. *Let $(t_q : \mathbb{F}_q \to \mathbb{C})_q$ be a coherent family of trace functions and let $(I_q)_q$ be a family of subsets $I_q \subset \mathbb{F}_q$ such that $\mathcal{F}_q$ is I_q-compatible. Then the complex random variable*

$$\left(\frac{S(t_q, I_q + x)}{\sqrt{|I_q|}}\right)_{x \in \mathbb{F}_q}$$

(with respect to the uniform measure on $\mathbb{F}_q$) converges in law to a normal distribution $\mathcal{N}$ in $\mathbb{C} \cong \mathbb{R}^2$, with mean 0 and covariance matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ if } t_q \text{ has real values}, \quad \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ otherwise} \tag{9}$$

when $q, |I_q| \to \infty$ with $\log |I_q| = o(\log q)$.



(A) $H = 3$ (B) $H = 50$ (C) $H = 1000$

FIGURE 1. Distribution of sums of trace functions for a Dirichlet character modulo $p = 7927$ of order $p - 1$.

Remarks 2.15. (1) We do not require that I_q be an interval, but it can rather be *any* (small) subset.

(2) The result shows in particular that the limit has independent real and imaginary parts.

(3) As we shall see, the condition on t_q being real-valued can be reformulated as a condition on the monodromy group of the family.

To prove this theorem, we extend and adapt the method of [Lam13]. The values of the trace functions are modeled by random variables distributed like traces of random matrices uniform in maximal compact subgroups of the monodromy group with respect to the Haar measure (as in Deligne's equidistribution theorem), and the short sums by random walks.

The ℓ-adic formalism and Deligne's analogue of the Riemann hypothesis over finite fields applied to sum of products are used to show that this model is accurate, through the method of moments.

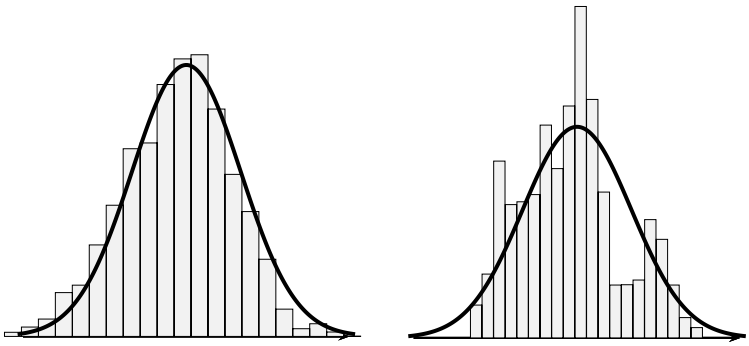
The conclusion then follows from the central limit theorem.

We mention that similar ideas are also used in [KS14] to study the paths obtained by joining partial Kloosterman and Birch sums, as stochastic processes.

2.4. **Quantitative version.** Actually, Lamzouri used more precise information than the central limit theorem: the first moments of the model correspond to those of a Gaussian, and are more generally bounded by them. This allows him to approximate the characteristic function of $(S(\chi_p, x, H_p))_{x\in\mathbb{F}_p}$ asymptotically, and in turn, gives a bound on the error term for the joint distribution function (what we will call a *quantitative version* of the convergence in law result) by using an identity of Selberg.

We also get a quantitative version for trace functions by using the fact that moments[2] of traces of random matrices in classical groups are also Gaussian (in $\mathbb{C} \cong \mathbb{R}^2$) as the rank grows, as already remarked and exploited

[2]For a complex-valued random variable X, we consider here the moments $\mathbb{E}(X^k\overline{X}^r)$ (and *not* $\mathbb{E}((\operatorname{Re} X)^k(\operatorname{Im} X)^r)$); see Remark 3.4 below.



(A) $H = 100$ (B) $H = 1300$

FIGURE 2. Distribution of sums of trace functions for the (real-valued) Kloosterman sum Kl_2 modulo $p = 7927$. In bold, the density function of a standard normal random variable.

for example by Diaconis-Shahshahani [DS94], Pastur-Vasilchuk [PV04], as well as Larsen [Lar90] in the context of trace functions.

More precisely, one rather needs subgaussian bounds on high order moments with respect to the rank, but exploiting the fact that they become exactly Gaussian allows to improve the error terms as the rank grows.

Hence, this uses a different phenomenon than the averaging of the central limit theorem: the random variables modeling the values of the trace function are themselves "close to Gaussian".

The following is then the extension of the main theorem of [Lam13] (rather than Theorem 2.14):

Theorem 2.16. *In the notations and hypotheses of Theorem 2.14, fix $\varepsilon \in (0, 1/2)$ and let R be the rank of the monodromy group of the family. For any closed rectangle $A \subset \mathbb{C} \cong \mathbb{R}^2$ with sides parallel to the coordinate axes and Lebesgue measure $\mu(A)$, the probability*

$$P\left(\frac{S(t_q, I_q + x)}{\sqrt{|I_q|}} \in A\right) = \frac{|\{x \in \mathbb{F}_q : S(t_q, I_q + x)/\sqrt{|I_q|} \in A\}|}{q}$$

is given by

$$P(\mathcal{N} \in A) + O_\varepsilon\left(\mu(A)\left(q^{-\frac{1}{2}+\varepsilon} + \left(\frac{\log|I_q|}{\log q}\right)^\beta + \frac{1}{\sqrt{|I_q|}}\right)\right)$$

when q, $|I_q| \to \infty$ with

$$\begin{cases} \log|I_q| = o(\log q) & \text{real-valued and Kummer cases} \\ |I_q| = o\left((\log q)^{\frac{2R}{(2R-1)(1+\varepsilon)}}\right) & \text{otherwise,} \end{cases}$$

where $\mathcal{N}$ is a normal random variable in $\mathbb{C}$ with mean 0 and covariance matrix as in Theorem 2.14, and

$$\beta = \begin{cases} 1/2 - \varepsilon & \text{real-valued and Kummer cases} \\ \frac{R-1}{2R-1} & \text{otherwise.} \end{cases}$$

Remark 2.17. By using a generalization of the Berry-Esseen inequality from [BRR86], we improve the method of Lamzouri, which is necessary in the non-real-valued case (see the outline at the beginning of Section 5). Moreover:

(1) In the self-dual case, Theorem 2.16 recovers the bound and the range of [Lam13], with an improvement on the power of $|I_q|$ (from 1/4 to 1/2), thanks to a modification of the method.
(2) In the non-self-dual case, we recover the bound valid for Dirichlet characters when the rank $R \to \infty$, but under the weaker range $|I_q| = o\left((\log q)^{\frac{R}{R-1}}\right)$ than the one for which Theorem 2.14 is valid. We will explain the reason for this later on.

2.5. **Examples.** In Section 7, we will prove that natural families arising from the examples of Section 1.3.1 are coherent, so that Theorems 2.14 and 2.16 apply to them.

To make the arithmetic and geometric monodromy groups coincide, we may eventually need to replace a family $(\mathcal{F}_q)_q$ by the twisted family $(\alpha_q \otimes \mathcal{F}_q)_q$ for $\alpha_q \in \overline{\mathbb{Q}}_\ell$ a Weil number of weight 0. This has simply the effect of multiplying the trace function by α_q, and the covariance matrix of Theorem 2.14 by the orthonormal matrix

$$\begin{pmatrix} \operatorname{Re}\alpha_q & -\operatorname{Im}\alpha_q \\ \operatorname{Im}\alpha_q & \operatorname{Re}\alpha_q \end{pmatrix},$$

where we identify α_q with its image through the fixed isomorphism $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$.

2.6. **Moments of random matrices in classical groups.** As we mentioned, an important ingredient in the proof of Theorem 2.16 is the following:

Proposition 2.18. *For $n \geqslant 1$, let G be $\mathrm{SL}_{n+1}(\mathbb{C})$, $\mathrm{Sp}_{2n}(\mathbb{C})$ or $\mathrm{SO}_{n+1}(\mathbb{C})$ with standard representation* Std. *Then, for $R = \mathrm{rank}(G)$ (namely n, n and $\lfloor (n+1)/2 \rfloor$ respectively):*

(1) If Std *is self-dual (i.e. in the symplectic case),*

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k}) = 0 \qquad (k \geqslant 0 \text{ odd}), \tag{10}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k}) = (k-1)!! \qquad (0 \leqslant k \leqslant R, \text{ even}), \tag{11}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k}) \leqslant (k-1)!! \qquad (k \geqslant 1). \tag{12}$$

(2) Otherwise,

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k} \otimes D(\mathrm{Std}^{\otimes k})) = k! \qquad (0 \leqslant k \leqslant R), \tag{13}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k} \otimes D(\mathrm{Std}^{\otimes r})) = 0 \qquad (0 \leqslant k \neq r \leqslant R), \tag{14}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k} \otimes D(\mathrm{Std}^{\otimes r})) \leqslant \sqrt{k!r!} \qquad (k, r \geqslant 0), \tag{15}$$

where $\mathrm{mult}_1(\cdot)$ *denotes the multiplicity of the trivial representation in a representation of* G*.*

New aspects compared to existing works are the bounds (12) and (15) that we need on the large order moments with respect to the rank.

Remark 2.19. Recall that (see Section 5.3):

- For $k, r \geqslant 0$ distinct integers, the (k,r)-th moment of a standard Gaussian in $\mathbb{R}^2 \cong \mathbb{C}$ is zero.
- For k odd, the kth moment of a standard Gaussian in $\mathbb{R}$ is zero.

In the self-dual case, odd moments are zero even for high rank, but in the non-self-dual case, we will see that there are infinitely many nonzero nondiagonal terms. This is the reason for the restricted range in the non-self-dual case of Theorem 2.16 noted in Remark 2.17.

3. Probabilistic model

We start by setting up a probabilistic model for the random variable $(S(t_q, I_q+x))_{x\in\mathbb{F}_q}$, motivated by Deligne's equidistribution theorem and Lamzouri's work [Lam13] for Dirichlet characters. We then compute its moments.

3.1. Deligne's equidistribution theorem.

Theorem 2.5 and Weyl's equidistribution criterion lead to the following, which shows that there is always an equidistribution result in a coherent family.

Theorem 3.1 (Deligne)**.** *Let us fix an isomorphism* $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$*, and let* $(\mathcal{F}_q)_q$ *be a coherent family of* ℓ*-adic sheaves over* $\mathbb{F}_q$ *with monodromy group* $G \leqslant \mathrm{GL}_n(\mathbb{C})$*. Let* $K \leqslant G(\mathbb{C})$ *be a maximal compact subgroup.*

For every $x \in U_{\mathcal{F}_q}(\mathbb{F}_q)$*, the semisimple part of the Jordan-Chevalley decomposition of* $\iota\rho_{\mathcal{F}_q}(\mathrm{Frob}_{x,q})$ *in* G *gives a well-defined conjugacy class* $\theta_{x,q} \in K^\sharp$ *such that* $t_{\mathcal{F}_q}(x) = \mathrm{tr}(\theta_{x,q})$*.*

When $q \to \infty$*, the set* $\{\theta_{x,q} : x \in U_{\mathcal{F}}(\mathbb{F}_q)\}$ *becomes equidistributed in* $K^\sharp$ *with respect to the pushforward of the normalized Haar measure of* K*.*

Proof. This is a variant of [Kat88, Chapter 3] and [KS91, Chapter 9]. □

3.2. Probabilistic model.

Theorem 3.1 suggests to model the random variable

$$\Big(\rho_{\mathcal{F}_q}(\mathrm{Frob}_{x,q})\Big)_{x\in U_{\mathcal{F}_q}(\mathbb{F}_q),}$$

(with respect to the uniform measure on $\mathbb{F}_q$) as $Y = \pi(X)$, where X is a random variable uniformly distributed in a maximal compact subgroup K of G with respect to the normalized Haar measure and $\pi : K \to K^\sharp$ is the projection to the conjugacy classes.

We shall then accordingly model the random variable

$$\Big(t_{\mathcal{F}_q}(x)\Big)_{x\in\mathbb{F}_q} \text{ by } Z = \mathrm{tr}(Y).$$

Remark 3.2. In [Lam13], the values of Dirichlet characters of order d are modeled by random variables uniformly distributed in the unit circle, while

in our model, by uniform random variables in the roots of unity of order d (the monodromy group of a Kummer sheaf associated to a Dirichlet character of order d) are used. Since the moments are the same (see Remark 5.5), this will make no difference.

3.2.1. *Sums of shifts.* Similarly, for $I \subset \mathbb{F}_q$ of size $H \geqslant 1$, we will model the random vector

$$\Big(\big(t_{\mathcal{F}_q}(x+a)\big)_{a\in I} \Big)_{x\in\mathbb{F}_q}$$

by $(Z_1, \dots, Z_H)$, for Z_i independent distributed like Z.

Therefore, the sum of shifts

$$\Big(S(t_{\mathcal{F}_q}, I+x)\Big)_{x\in\mathbb{F}_q} = \left(\sum_{y\in I} t_{\mathcal{F}_q}(y+x)\right)_{x\in\mathbb{F}_q}$$

will be modeled by the random walk $S(H) = Z_1 + \cdots + Z_H$, as in [Lam13].

3.3. **Computation of the moments.**

Proposition 3.3 (Probabilistic moments)**.** *For all integers $k, r \geqslant 0$ and $H \geqslant 1$, the moment*

$$M_{\mathrm{prob}}(k, r; H) := \mathbb{E}(S(H)^k \overline{S(H)^r})$$

is equal to

$$\sum_{\substack{k_1+\cdots+k_H=k\\ k_i\geqslant 0}} \sum_{\substack{r_1+\cdots+r_H=r\\ r_i\geqslant 0}} \binom{k}{k_1\dots k_H}\binom{r}{r_1\dots r_H} \times \prod_{i=1}^{H} \mathrm{mult}_1(\mathrm{Std}^{\otimes k_i} \otimes D(\mathrm{Std}^{\otimes r_i})),$$

where Std *is the standard representation of $G \leqslant \mathrm{GL}_n(\mathbb{C})$ and $D(\mathrm{Std})$ its dual.*

Proof. By independence and the multinomial formula, $M_{\mathrm{prob}}(k, r; H)$ equals

$$\sum_{\substack{k_1+\cdots+k_H=k\\ k_i\geqslant 0}} \sum_{\substack{r_1+\cdots+r_H=r\\ r_i\geqslant 0}} \binom{k}{k_1\dots k_H}\binom{r}{r_1\dots r_H} \prod_{i=1}^{H} \mathbb{E}(Z_i^{k_i}\overline{Z_i^{r_i}}).$$

By the Peter-Weyl Theorem,

$$\begin{aligned}\mathbb{E}(Z_i^k\overline{Z_i^r}) &= \int_{\mathbb{C}} x^k\overline{x^r}\, d(\mathrm{tr}_*\,\mu)(x) = \int_{K^\sharp} \mathrm{tr}(g)^k\overline{\mathrm{tr}(g)^r}\, d\mu(g)\\ &= \mathrm{mult}_1(\mathrm{Std}^{\otimes k}\otimes D(\mathrm{Std}^{\otimes r})),\end{aligned}$$

where μ is the normalized Haar measure on K, since tr (resp. $\overline{\mathrm{tr}}$) is the character associated to the standard representation of G (resp. its dual). □

Remark 3.4. The covariance matrix (9) of Theorem 2.14 is given with respect to the standard basis $1, i$ of $\mathbb{C}$ as $\mathbb{R}$-vector space, and a nice feature of the result is that the matrix is diagonal, i.e. the real and imaginary parts are independent. However, it will be more natural for the proof to make the

linear transformation $\binom{Z}{\overline{Z}} = \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)\binom{\operatorname{Re} Z}{\operatorname{Im} Z}$ and consider as in Proposition 3.3 the moments $\mathbb{E}(Z^k\overline{Z^r})$ instead of $\mathbb{E}((\operatorname{Re} Z)^k(\operatorname{Im} Z)^r)$. The reason is that conjugation has the algebraic interpretation of dualization of representations, characters, and trace functions. In the real-valued case, there is no difference.

Lemma 3.5. *We have $\mathbb{E}(Z) = 0$ and the covariance matrix of the random vector $Z = (\operatorname{Re} Z, \operatorname{Im} Z)$ is*

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ if Std is self-dual, } \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ otherwise.}$$

Proof. Since the sheaf is geometrically irreducible, Std is irreducible, so that $\mathbb{E}(Z) = \operatorname{mult}_1(\mathrm{Std}) = 0$ by Schur's Lemma. Moreover, for every integer $r \geqslant 0$ we have

$$\operatorname{mult}_1(\mathrm{Std}^{\otimes r}) = \int_K \operatorname{tr}(g)^r d\mu(g) = \int_K \overline{\operatorname{tr}(g)^r} d\mu(g) = \operatorname{mult}_1(D(\mathrm{Std})^{\otimes r})$$

where the second equality follows from the fact that $\operatorname{mult}_1(\mathrm{Std}^{\otimes r})$ is an integer. Using this, we find that the covariance matrix of Z is

$$\frac{1}{2}\begin{pmatrix} \operatorname{mult}_1(\mathrm{Std}^{\otimes 2}) + 1 & 0 \\ 0 & 1 - \operatorname{mult}_1(\mathrm{Std}^{\otimes 2}) \end{pmatrix}.$$

Finally, again by Schur's Lemma, $\operatorname{mult}_1(\mathrm{Std}^{\otimes 2}) = \operatorname{mult}_1(\mathrm{Std} \otimes D(D(\mathrm{Std}))) = \delta_{\text{Std self-dual}}$. □

Lemma 3.6. *Let $\mathcal{F}$ be a geometrically irreducible ℓ-adic sheaf over $\mathbb{F}_q$, pointwise pure of weight 0, with monodromy groups $G = G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F}) \leqslant \mathrm{GL}_n(\mathbb{C})$. The following are equivalent:*

(1) For any finite extension $\mathbb{F}_{q'}/\mathbb{F}_q$, the trace function $t : \mathbb{F}_{q'} \to \mathbb{C}$ is real-valued.
(2) The standard representation of $G \leqslant \mathrm{GL}_n(\mathbb{C})$ is self-dual.
(3) $\operatorname{mult}_1(\mathrm{Std}^{\otimes 2}) = \operatorname{mult}_1(\mathrm{Std} \otimes D(\mathrm{Std})) = 1$.

Proof. By a result of Deligne [Del80, 1.3.9] (see [KS91, 9.0.12]), we have G^0 semisimple, so that there is an equivalence of categories between representations of the algebraic group G, of the Lie group $G(\mathbb{C})$, or of K. Note that by assumption, Std is irreducible. By the Chebotarev density theorem, the Frobenius conjugacy classes $\mathrm{Frob}_{x,q'}$, for $\mathbb{F}_{q'}/\mathbb{F}_q$ a finite extension and $x \in U_{\mathcal{F}}(\mathbb{F}_{q'})$, are dense in $\pi_{1,q}$ (see [Ser89, I.2.2, Corollary 2 a)]). Thus, (1) is indeed equivalent to having $\iota(\operatorname{tr}(\rho_{\mathcal{F}}(\pi_{1,q}))) \subset \mathbb{R}$ for all q, which in turn holds if and only if $\operatorname{tr}(G) \subset \mathbb{R}$. Hence, (1) is equivalent to (2) by character theory of $G(\mathbb{C})$. If (2) holds, then

$$\operatorname{mult}_1(\mathrm{Std}^{\otimes 2}) = \operatorname{mult}_1(\mathrm{Std} \otimes D(\mathrm{Std})) = 1$$

by Schur's Lemma, so that (3) holds. If (3) holds, we have

$$1 = \int_K \operatorname{tr}(g)^2 dg = \left|\int_K \operatorname{tr}(g)^2 dg\right| \leqslant \int_K |\operatorname{tr}(g)|^2 dg = 1,$$

so that $\operatorname{tr}(g)^2 = |\operatorname{tr}(g)|^2$ for almost all $g \in K$. Hence, $\operatorname{tr}(g) \in \mathbb{R}$ almost everywhere in K, and this holds everywhere in K since a nonempty open

set has positive Haar measure. Thus (1) follows by the first statement in Theorem 3.1. □

Hence, we conclude by the two preceding Lemmas that the covariance matrix of Z is equal to that given in (9).

4. Qualitative version (Theorem 2.14)

4.1. **Strategy and comparison with other approaches.** The idea of the proof of Theorem 2.14 is the following:

(1) By the method of moments, it suffices to show that the moments of the random variable (1) tend to that of the Gaussian $\mathcal{N}$.
(2) We show that the probabilistic model of Section 3 is accurate, in the sense that the moments of (1) converge to that of the model.
(3) To conclude, it suffices to apply the central limit theorem (with convergence of moments) to the model.

This is to be compared with the approaches of earlier works which do not use the central limit theorem:

– Davenport-Erdős [DE52] and Mak-Zaharescu [MZ11] directly show that the moments of (1) are asymptotically Gaussian and apply the method of moments.
– Lamzouri [Lam13] first proves that his probabilistic model is accurate as in step (2) above. He then remarks that the random variable X modeling the values of the Dirichlet characters itself has moments bounded by those of a Gaussian. That allows to approximate the characteristic function of the model for the sums by that of a Gaussian. By using a method of Selberg, this finally gives an approximation for the joint characteristic function. We will comment more on this approach in Section 5.

We shall see that with the ℓ-adic formalism, the proof that the model is accurate becomes very natural and does not involve explicit computations of moments.

4.2. **Accuracy of the model.** Under the hypotheses and notations of Theorem 2.14, as in Proposition 3.3 the moment

$$M_q(k,r;I_q) := \mathbb{E}\left(S(t_q,I_q+x)^k\overline{S(t_q,I_q+x)^r}\right)$$

equals

$$\sum_{\substack{k_1+\cdots+k_H=k\\ k_i\geqslant 0}}\sum_{\substack{r_1+\cdots+r_H=r\\ r_i\geqslant 0}} \binom{k}{k_1\dots k_H}\binom{r}{r_1\dots r_H} \frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^{H} t_q(x+a_i)^{k_i}\overline{t_q(x+a_i)^{r_i}} \tag{16}$$

for all integers $k,r\geqslant 0$, where $I_q=\{a_1,\dots,a_H\}$. Thus, by Proposition 3.3, we need to compare "sums of products" of trace functions

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^{H} t_q(x+a_i)^{k_i}\overline{t_q(x+a_i)^{r_i}} \tag{17}$$

with products of the form

$$\prod_{i=1}^{H} \mathrm{mult}_1(\mathrm{Std}^{\otimes k_i} \otimes D(\mathrm{Std}^{\otimes r_i})) \tag{18}$$

when $k_i, r_i \geqslant 0$ are integers.

4.2.1. *Sums of products of trace functions.* The estimation of sums of the form $\sum_{x\in\mathbb{F}_q} \prod_{i=1}^{H} t_i(x)$ for t_i a trace function over $\mathbb{F}_q$ is precisely the question that is surveyed in [FKM15b], and the link between (17) and (18) can be made clear through a cohomological interpretation of the sum via Theorem 2.5:

– For $\boldsymbol{k}, \boldsymbol{r} \in \mathbb{N}^H$, let us consider the sheaf

$$\mathcal{G}^{\boldsymbol{k},\boldsymbol{r}} = \bigotimes_{1\leqslant i\leqslant H} \left([+a_i]^*\mathcal{F}_q^{\otimes k_i} \otimes D([+a_i]^*\mathcal{F}_q)^{\otimes r_i}\right).$$

By Theorem 2.5, under the hypotheses of Theorem 2.14, (17) is equal to

$$\mathrm{tr}\left(\mathrm{Frob}_q \mid \mathcal{G}^{\boldsymbol{k},\boldsymbol{r}}_{\pi_{1,q}^{\mathrm{geom}}}\right) + O(r^{S(\boldsymbol{k},\boldsymbol{r})}S(\boldsymbol{k},\boldsymbol{r})c^2q^{-1/2})$$

where the implicit constant is absolute, $r = \mathrm{rank}(\mathcal{F}_q)$, $c = \mathrm{cond}(\mathcal{F}_q)$, and $S(\boldsymbol{k},\boldsymbol{r}) = \sum_{i=1}^{H}(k_i + r_i)$.

– By the Goursat-Kolchin-Ribet criterion of Katz, if $\mathcal{F}_q$ is part of a coherent family in the classical case, then the arithmetic and geometric monodromy groups of

$$\mathcal{G} = \bigoplus_{1\leqslant i\leqslant H} [+a_i]^*\mathcal{F}_q$$

coincide and are as large as possible, i.e. isomorphic to G^H.

– Thus, by Remark 2.9,

$$\begin{aligned}\mathrm{tr}\left(\mathrm{Frob}_q \mid (\mathcal{G}_{\boldsymbol{k},\boldsymbol{r}})_{\pi_{1,q}^{\mathrm{geom}}}\right) &= \dim \Lambda_{G_{\mathrm{geom}}(\mathcal{G})} = \dim \Lambda_{G^H}\\ &= \dim \boxtimes_{1\leqslant i\leqslant H}\left(\mathrm{Std}^{\otimes k_i} \otimes D(\mathrm{Std})^{\otimes r_i}\right)_G\\ &= \prod_{1\leqslant i\leqslant H} \mathrm{mult}_1(\mathrm{Std}^{\otimes k_i} \otimes D(\mathrm{Std})^{\otimes r_i}),\end{aligned}$$

for the G^H-representation $\Lambda = \boxtimes_{1\leqslant i\leqslant H}\left(\mathrm{Std}^{\otimes k_i} \otimes D(\mathrm{Std})^{\otimes r_i}\right)$.

Remark 4.1. As mentioned in Remark 2.6, the conductor of $\mathcal{G}^{\boldsymbol{k},\boldsymbol{r}}$ is unbounded as $H \to \infty$, so that, in contrast with [FKM15b], we have to keep track of the dependency with the conductors in the error terms.

Finally, we get:

Proposition 4.2. *Let $(\mathcal{F}_q)_q$ be a coherent family of sheaves over $\mathbb{F}_q$, with monodromy group $G \leqslant \mathrm{GL}_n(\mathbb{C})$. Let $a_1, \dots, a_H \in \mathbb{F}_q$ be distinct. If $\mathcal{F}_q$ is*

$\{a_1,\dots,a_H\}$-compatible, then for all $\boldsymbol{k},\boldsymbol{r}\in\mathbb{N}^H$,

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{1\leqslant i\leqslant H}t_{\mathcal{F}_q}(x+a_i)^{k_i}\overline{t_{\mathcal{F}_q}(x+a_i)^{r_i}} = \prod_{1\leqslant i\leqslant H}\mathrm{mult}_1(\mathrm{Std}^{\otimes k_i}\otimes D(\mathrm{Std})^{\otimes r_i}) + O\left(r^{S(\boldsymbol{k},\boldsymbol{r})}S(\boldsymbol{k},\boldsymbol{r})q^{-1/2}\right)$$

where the implicit constant does not depend on q, and $S(\boldsymbol{k},\boldsymbol{r})=\sum_{i=1}^H(k_i+r_i)$.

Proof. The proof in the case of a classical monodromy group was sketched above; details can be found in [FKM15b] or [PG16]. For a Kummer sheaf $\mathcal{L}_{\chi(f)}$ with $\chi:\mathbb{F}_q^\times\to\mathbb{C}$ of order d and $f\in\mathbb{F}_q(T)$, the sum is by multiplicativity equal to

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\chi(g(x))=\frac{1}{q}\sum_{x\in\mathbb{F}_q}t_{\mathcal{L}_\chi(g)}(x),$$

where $g(X)=\prod_{1\leqslant i\leqslant H}f(X+a_i)^{k_i-r_i}$. Writing $f=f_1/f_2$ and $g=g_1/g_2$ with $f_i,g_i\in\mathbb{F}_q[X]$, we see that $\deg(g_1)+\deg(g_2)\leqslant S(\boldsymbol{k},\boldsymbol{r})(\deg(f_1)+\deg(f_2))\leqslant S(\boldsymbol{k},\boldsymbol{r})\operatorname{cond}(\mathcal{F}_q)$. By Theorem 2.5 and Remark 2.9 applied to the Kummer sheaf $\mathcal{L}_{\chi(g)}$, it follows that

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\chi(g(x))=\delta_{g\text{ is a }d-\text{power}}+O(S(\boldsymbol{k},\boldsymbol{r})c^2q^{-1/2}).$$

Observe that $\mathrm{mult}_1(\mathrm{Std}^{\otimes k_i}\otimes D(\mathrm{Std})^{\otimes r_i})=\delta_{d|k_i-r_i}$, so that the claim is clear if $f=X$. Otherwise, the compatibility assumption shows that[3] there exists a zero x of f such that $f(x+a)\neq 0$ for all $a\in I$. Indeed, otherwise, for any zero x of f and any integer $d_f\geqslant 0$, there would exist $a_1,\dots,a_{d_f}\in\overline{\mathbb{F}}_q$ with $x+a_1,\dots,x+\sum_{i=1}^{d_f}a_i$ distinct zeros of f, which is impossible. This implies that g cannot be a d-power if $d\nmid k_i-r_i$ for some i. □

4.2.2. *Conclusion.* The asymptotic accuracy of the model then follows from Proposition 4.2 applied to (16), recalling that $\sum_{k_1+\cdots+k_H=k,\ k_i\geqslant 0}\binom{k}{k_1\dots k_H}=H^k$:

Proposition 4.3. *Under the hypotheses of Theorem 2.14, for all integers $k,r\geqslant 0$ and $I_q\subset\mathbb{F}_q$ of size H, we have*

$$M_q(k,r;I_q)=M_{\mathrm{prob}}(k,r;H)+O\left(c^{3(k+r)}q^{-1/2}H^{k+r}\right)$$

with $c=\max_q\operatorname{cond}(\mathcal{F}_q)$.

We make the normalizations

$$\tilde{S}(t_q,I_q+x)=S(t_q,I_q+x)/|I_q|^{1/2}\text{ and }\tilde{S}(H)=S(H)/H^{1/2},$$

and for $k,r\geqslant 0$ we denote by $\tilde{M}_q(k,r;I_q)$, $\tilde{M}_{\mathrm{prob}}(k,r;H)$ the corresponding moments, so that Proposition 4.3 becomes:

$$\tilde{M}_q(k,r;I_q)=\tilde{M}_{\mathrm{prob}}(k,r;H)+O\left(c^{3(k+r)}q^{-1/2}H^{\frac{k+r}{2}}\right). \tag{19}$$

[3] This idea appears on page 9 of the published version of [LZ12].

4.3. **Central limit theorem.**

Proposition 4.4. *Under the hypotheses and notations of Theorem 2.14, the random variable $\tilde{S}(H)$ converges in law to the random variable $\mathcal{N}$ when $H \to \infty$. Moreover,*

$$\lim_{H\to\infty} \tilde{M}_{\mathrm{prob}}(k, r; H) = M_{\mathcal{N}}(k, r),$$

for all integers $k, r \geqslant 0$, where $M_{\mathcal{N}}(k, r)$ is the (k, r)-th moment of $\mathcal{N}$.

Proof. This follows from the two-dimensional central limit theorem and Lemma 3.5. To obtain the convergence of moments, it suffices to show that $\tilde{S}(H)$ is uniformly integrable (see e.g. [Gut05, Chapter 5.5]), which follows from [Gut05, Theorem 7.5.1]. □

By (19), this immediately implies:

Corollary 4.5 (Moments are asymptotically Gaussian)**.** *Under the hypotheses and notations of Theorem 2.14, we have for all integers $k, r \geqslant 0$ that*

$$\lim_{q,|I_q|\to\infty} \tilde{M}_q(k, r; I_q) = M_{\mathcal{N}}(k, r).$$

4.4. **Method of moments and proof of Theorem 2.14.** To conclude the proof of Theorem 2.14, it now suffices to apply the method of moments:

Proposition 4.6 (Method of moments for complex-valued random variables)**.** *Let $(X_n)_{n\geqslant 0}$ be a sequence of complex random variables with moments $M_{X_n}(k, r)$. If $\lim_{n\to\infty} M_{X_n}(k, r) = M_{X_0}(k, r)$ for all integers $k, r \geqslant 0$ and if*

$$\limsup_{k+r\to\infty} \frac{|M_{X_0}(k, r)|^{\frac{1}{k+r}}}{k + r} < \infty,$$

then X_n converges in law to X_0.

Proof. See for example [Gut05, Chapter 5.8.4]. □

Corollary 4.7 (Method of moments for normal convergence)**.** *Let $(X_n)_{n\geqslant 0}$ be a sequence of complex random variables. If for all integers $k, r \geqslant 0$, the moment $M_{X_n}(k, r)$ converges to the corresponding moment of a normal random variable $\mathcal{N}$ as $n \to \infty$, then X_n converges in law to $\mathcal{N}$.*

Hence, by Corollary 4.7, Theorem 2.14 follows directly from Corollary 4.5.

5. Quantitative version (Theorem 2.16)

5.1. **Review of Lamzouri's method.** We recall that the idea of [Lam13] is to remark that the random variable Z modeling the values of the Dirichlet characters has moments bounded by those of a Gaussian. In particular, this implies that if $S(H) = Z_1 + \cdots + Z_H$ with Z_i independent distributed like Z as above, we have

$$\mathbb{E}\left((\operatorname{Re} S(H))^{2k}(\operatorname{Im} S(H))^{2r}\right) \ll (k + r)!H^{k+r}$$

(see [Lam13, (3.5)]), which is a square-root cancellation over the trivial bound $H^{2(k+r)}(2k+2r)!$. This implies that one can:

(1) Approximate the characteristic function of $(S(\chi_p, x, H_p))_{x\in\mathbb{F}_p}$ asymptotically by that of the probabilistic model when $p, H_p \to \infty$ (see the proof of [Lam13, Theorem 3.1]).

Lamzouri then proceeds as follows:

(2) As in the classical proof of the central limit theorem, the characteristic function of the model is approximated by that of a Gaussian ([Lam13, Lemma 3.2]).
(3) Combining the last two points, this gives an asymptotic approximation of the characteristic function of $(S(\chi_p, x, H_p))_{x\in\mathbb{F}_p}$ by that of a Gaussian ([Lam13, Theorem 3.1]).
(4) Using a smooth approximation for the sign function involving characteristic functions, due to Selberg ([Lam13, (4.4)]), one gets an approximate expression of the joint distribution function from the characteristic function, which allows to conclude.

5.2. **Generalization to trace functions.** As we explained in the introduction, this can be generalized to coherent families of trace functions thanks to Proposition 2.18. We will however proceed a bit differently than Lamzouri, skipping steps (2)–(3) above and:

(1) Directly use step (4) to approximate the joint distribution function of the random variable (1) by that of the model.
(2) Apply a generalization to higher dimensions of the Berry-Esseen theorem appearing in [BRR86], to obtain an approximation of the joint distribution function of the model.

5.3. **Characteristic function of a Gaussian.** Let us recall that if Z is a normal random variable in $\mathbb{R}$ with mean 0 and variance σ^2, the moments are

$$\mathbb{E}(Z^k) = \begin{cases} 0 & \text{if } k \geqslant 1 \text{ is odd} \\ \sigma^k (k-1)!! & \text{if } k \geqslant 0 \text{ is even} \end{cases}$$

and its characteristic function is $u \mapsto \mathbb{E}(e^{iuZ}) = e^{-\frac{1}{2}\sigma^2 u^2}$.

Hence, if Z is a normal random variable in $\mathbb{C} \cong \mathbb{R}^2$ with mean 0 and diagonal covariance matrix $\sigma^2 \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, then its characteristic function is

$$(u, v) \mapsto \tilde{\phi}(u, v) = \mathbb{E}\left(e^{i(u \operatorname{Re} Z + v \operatorname{Im} Z)}\right) = e^{-\frac{\sigma^2}{2}(u^2+v^2)}.$$

As we explained in Remark 3.4, we will continue to rather work with moments of the form $\mathbb{E}(Z^k\overline{Z^r})$ and characteristics functions of the form $(u, v) \mapsto \phi(u, v) = \mathbb{E}(e^{i(uZ+v\overline{Z})})$, which renders the computations easier and more natural in our setting. Note that

$$\begin{aligned} \phi(u, v) &= \tilde{\phi}(u + v, i(u - v)) \text{ and} \\ \tilde{\phi}(u, v) &= \phi\left(\frac{u - iv}{2}, \frac{u + iv}{2}\right) \end{aligned} \tag{20}$$

for all $u, v \in \mathbb{C}$. Hence, $\phi(u, v) = e^{-2\sigma^2 uv}$, so that $\mathbb{E}\big(Z^k\overline{Z^r}\big) = (2\sigma^2)^k k!\delta_{k=r}$.

5.4. **Approximation of characteristic functions through moments.**

Lemma 5.1. *Let X_1, X_2 be complex random variables with moments $M_j(k,r) = \mathbb{E}(X_j^k \overline{X_j^r})$ and characteristic functions $(u,v) \mapsto \phi_j(u,v) = \mathbb{E}(e^{i(uX_j + v\overline{X_j})})$ $(j=1,2)$ for $u,v \in \mathbb{C}$ and $k,r \geqslant 0$ integers. Assume that*

$$M_1(k,r) = M_2(k,r) + O(g(k,r))$$

for all $k,r \geqslant 0$ with some $g : \mathbb{N}^2 \to \mathbb{R}$. Then for any fixed even integer $N \geqslant 1$ and $u \in \mathbb{C}$, we have

$$\begin{aligned}\phi_1(u,\overline{u}) &= \phi_2(u,\overline{u}) + O\left(\frac{|u|^N}{N!}(|M_1(N/2,N/2)| + |M_2(N/2,N/2)|)\right)\\ &\quad + O\left(\sum_{n<N}\frac{|u|^n}{n!}\sum_{a=0}^{n}\binom{n}{a}|g(a,n-a)|\right).\end{aligned}$$

In particular, if $g(k,r) = h(k+r)$ for all $k,r \geqslant 0$ for some $h : \mathbb{N} \to \mathbb{R}$, we have

$$\begin{aligned}\phi_1(u,\overline{u}) &= \phi_2(u,\overline{u}) + O\left(\frac{|u|^N}{N!}(|M_1(N/2,N/2)| + |M_2(N/2,N/2)|)\right)\\ &\quad + O\left(\max_{n<N}|h(n)|(1+|u|^N)\right).\end{aligned}$$

If X_1, X_2 are random variables in $\mathbb{R}$, then a similar relation holds for $\phi_1(u,0)$ and $\phi_2(u,0)$ with $u \in \mathbb{R}$.

Proof. It suffices to use the expansion $e^{ix} = \sum_{n<N} i^n x^n/n! + O(|x|^N/N!)$ valid for $x \in \mathbb{R}$. □

5.5. **Bounding moments.** In order to apply Lemma 5.1, we will need bounds on the moments $M_{\mathrm{prob}}(N,N;H)$, provided by Proposition 2.18. Recall that by Proposition 3.3, we have

$$M_{\mathrm{prob}}(N,N;H) = N!^2 \sum_{\substack{k_1+\cdots+k_H=N\\ k_i\geqslant 0}} \sum_{\substack{r_1+\cdots+r_H=N\\ r_i\geqslant 0}} \prod_{i=1}^{H} \frac{\mathbb{E}(Z_i^{k_i}\overline{Z_i^{r_i}})}{k_i! r_i!}.$$

Note that if all Z_i were normal variables in $\mathbb{C}$ with mean 0 and covariance matrix $\sigma^2 \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ (resp. $\sigma^2 \left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$), then this would be equal to $(2\sigma^2)^N N! H^N$ (resp. $\sigma^{2N}(2N-1)!! H^N$).

Proposition 5.2 (Non-self-dual case)**.** *If the conclusions of Proposition 2.18 hold, then in the non-self-dual case, $M_{\mathrm{prob}}(N,N;H) \leqslant (N+H-1)^N H^N$.*

Proof. By the Cauchy-Schwarz inequality,

$$M_{\mathrm{prob}}(N,N;H) \leqslant \left(\sum_{\substack{k_1+\cdots+k_H=N\\ k_i\geqslant 0}} \frac{N!}{\sqrt{k_1!\dots k_H!}}\right)^2 \leqslant H^N \frac{(N+H-1)!}{(H-1)!},$$

since the number of weak H-compositions[4] of N is equal to $\binom{N+H-1}{H-1}$. Finally, we use that $\frac{(N+H-1)!}{(H-1)!} \leqslant (N+H-1)^N$. □

Remark 5.3. In Remarks 2.17 and 2.19, we explained that the reason for the restriction on the range in Theorem 2.16 for the non-self-dual case came from the fact that X_i may have infinitely many nonzero nondiagonal moments. If (14) in Theorem 2.16 held for all distinct $k, r \geqslant 0$, then we would get the bound H^N instead of $H^N(N+H-1)^N$. We will see later how this additional exponential in H modifies the aforementioned range.

For Dirichlet characters, we can achieve the following better bound:

Proposition 5.4 (Non-self-dual case, Kummer sheaves)**.** *In the case of Kummer sheaves, we have* $M_{\mathrm{prob}}(N, N; H) \leqslant N!H^N$.

Proof. If Z is a random variable uniformly distributed in $\mu_d(\mathbb{C})$, then

$$\mathbb{E}(Z^k\overline{Z^r}) = \frac{1}{d}\sum_{i=0}^{d-1} \zeta_d^{i(k-r)} = \delta_{k=r}, \text{ so}$$

$$M_{\mathrm{prob}}(N, N; H) \leqslant N! \sum_{\substack{k_1+\cdots+k_H=N \\ k_i\geqslant 0}} \frac{N!}{(k_1!\dots k_H!)^2} \leqslant N!H^N.$$

□

Remark 5.5. Actually, Lamzouri [Lam13] models Z as a random vector uniformly distributed on the unit circle S^1. This is equivalent since the moments are then

$$\mathbb{E}(Z^k\overline{Z^r}) = \frac{1}{2\pi}\int_0^{2\pi} e^{i\theta(k-r)}d\theta = \delta_{k=r} \quad (k, r \geqslant 0).$$

Proposition 5.6 (Self-dual case)**.** *If the conclusions of Proposition 2.18 hold, then in the self-dual case,*

$$M_{\mathrm{prob}}(N, N; H) \leqslant (2N-1)!!H^N.$$

Proof. Since $(k-1)!! = \frac{k!}{2^{k/2}(k/2)!}$ for $k \geqslant 1$ odd,

$$\begin{aligned} M_{\mathrm{prob}}(N, N; H) &\leqslant \sum_{\substack{k_1+\cdots+k_H=2N \\ k_i\geqslant 0 \text{ even}}} \frac{(2N)!}{k_1!\dots k_H!}\prod_{i=1}^{H}\frac{k_i!}{2^{k_i/2}(k_i/2)!} \\ &= \frac{(2N)!}{N!2^N}\sum_{\substack{m_1+\cdots+m_H=N \\ m_i\geqslant 0}} \binom{N/2}{m_1\dots m_H} = (2N-1)!!H^N. \end{aligned}$$

□

[4]Recall that a *weak H-composition* of an integer N is a tuple of nonnegative integers $(k_1, \dots, k_H)$ such that $k_1 + \cdots + k_H = N$.

5.6. **Approximation of joint distribution functions through characteristic functions.** The following result appears in [Lam13], and follows from a smooth approximation of the sign function (and thus of the characteristic function of a rectangle in $\mathbb{R}^2$) by Selberg in [Sel92].

Proposition 5.7. *Let X be a complex random variable with characteristic function $\phi_X(u,v) = \mathbb{E}\left(e^{i(u\operatorname{Re}X + v\operatorname{Im}X)}\right)$ $(u,v \in \mathbb{R})$ and $A = [a,b]\times[c,d]$ be a rectangle in $\mathbb{R}^2 \cong \mathbb{C}$. Then, for any real number $t > 0$,*

$$\begin{aligned} P(X\in A) &= \frac{1}{2}\operatorname{Re}\int_0^t\int_0^t G(u/t)G(v/t)\Big(\phi_X(2\pi u,-2\pi v)f_{a,b}(u)\overline{f_{c,d}(v)} \\ &\qquad -\phi_X(2\pi u,2\pi v)f_{a,b}(u)f_{c,d}(v)\Big)\frac{du}{u}\frac{dv}{v} \\ &\quad + O\left(\frac{1}{t}\int_0^t(|\phi_X(2\pi u,0)| + |\phi_X(0,2\pi u)|)du\right) \end{aligned}$$

where $G(u) = 2u/\pi + 2(1-u)\cot(\pi u)$ for $u\in[0,1]$ and $f_{\alpha,\beta}(u) = (e(-\alpha u) - e(-\beta u))/2$ for $u\in\mathbb{C}$, $\alpha,\beta\in\mathbb{R}$.

Proof. See [Lam13, Section 4]. □

Corollary 5.8. *If X, Y are complex random variables such that there exists a nonnegative continuous function $g:\mathbb{R}^2\to\mathbb{R}_{\geqslant 0}$ with*

$$\phi_X(2\pi u,2\pi v) = \phi_Y(2\pi u,2\pi v) + O(g(|u|,|v|))$$

for all $u,v\in\mathbb{R}$, then we have, for any A,t as in Proposition 5.7,

$$\begin{aligned} P(X\in A) &= P(Y\in A) \\ &\quad + O\left(\int_0^t\int_0^t g(u,v)dudv + \frac{1}{t}\int_0^t(g(u,0)+g(0,u))du\right) \\ &\quad + O\left(\frac{1}{t}\int_0^t(|\phi_X(2\pi u,0)| + |\phi_X(0,2\pi u)|)du\right). \end{aligned}$$

5.7. **Central limit theorem and sums of quasi-normal random variables.**

Lemma 5.9. *For $H\geqslant 1$, let $X_1,\dots,X_H$ be independent identically distributed random variables and consider*

$$S(H) = \frac{X_1+\cdots+X_H}{\sqrt{H}}.$$

Assume that for $0\leqslant k,r\leqslant N$, the moments $M(k,r) = \mathbb{E}(X_1^k\overline{X_1^r})$ of X_1 correspond to the moments of a normal random variable in $\mathbb{C}$ with mean 0 and covariance matrix $\sigma^2\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, respectively $\left(\begin{smallmatrix}\sigma^2&0\\0&0\end{smallmatrix}\right)$. Then the characteristic function $\phi_H(u,v) = \mathbb{E}\left(e^{i(uS(H)+v\overline{S(H)})}\right)$ of $S(H)$ satisfies

$$\phi_H(u,\overline{u}) = e^{-2\sigma^2|u|^2}\left(1 + O\left(\frac{|u|^N}{H^{(N-1)/2}}\right)\right),$$

when $u \in \mathbb{C}$ *with* $|u| \leqslant H^{\frac{N-2}{2N}}$, *respectively*

$$\phi_H(u,0) = e^{-\frac{1}{2}\sigma^2 u^2}\left(1 + O\left(\frac{|u|^N}{H^{(N-1)/2}}\right)\right)$$

when $u \in \mathbb{R}$ *with* $|u| \leqslant H^{\frac{N-2}{2N}}$.

Proof. By independence of the X_i, we have $\phi_H(u,v) = \phi(u/\sqrt{H}, v/\sqrt{H})^H$ where $\phi(u,v) = \mathbb{E}\left(e^{i(uX_1+v\overline{X_1})}\right)$ is the characteristic function of X_1. Then

$$\begin{aligned}\phi_H(u,\overline{u}) &= \left(e^{-2\sigma^2|u|^2/H} + O\left(\frac{|u|^N}{H^{(N+1)/2}}\right)\right)^H \\ &= e^{-2\sigma^2|u|^2}\left(1 + O\left(\frac{|u|^N}{H^{(N-1)/2}}\right)\right)\end{aligned}$$

in the first case, since $(e^a + O(a^2))^H = e^{aH}(1 + O(a^2H))$ if $a^2H \leqslant 1$. The second case is similar. □

5.8. **Normal approximation.** Below, we give a particular case of the generalization of the Berry-Esseen Theorem in higher dimensions appearing in [BRR86].

Proposition 5.10. *Let* $X_1, \ldots, X_H$ *be independent and identically distributed random vectors in* $\mathbb{R}^2$, *satisfying*

$$\mathbb{E}(X_1) = 0, \text{ and } \mathbb{E}(||X_1||^4) < \infty,$$

and let $S(H) = (X_1 + \cdots + X_H)/\sqrt{H}$. *Then for any* $A \subset \mathbb{R}^2$ *Borel-measurable,*

$$P(S(H) \in A) = P(\mathcal{N} \in A) + O(\mu(A)H^{-1/2}),$$

where $\mathcal{N}$ *is a normal random vector in* $\mathbb{R}^2$ *with mean* 0 *and covariance* $\mathrm{Cov}(X_1)$.

Proof. This follows from [BRR86, Theorem 13.2] taking $d = 2$ and $f = 1_A$. Note that, under the notations of the latter,

$$\delta_H \ll \frac{H\log H}{e^{CH}} \text{ and } \omega_f^*(2^{7/2}\pi^{-1/3}2^{4/3}\rho_3 H^{-1/2} : \Phi) \ll \frac{\mu(A)}{\sqrt{H}}$$

for some absolute constant $C > 0$. Thus, for Φ the density function of $\mathcal{N}$,

$$\begin{aligned}\left|\int_A d(S(H) - \Phi)\right| &\ll \omega_f(\mathbb{R}^2)\left(\frac{1}{\sqrt{H}} + \frac{\log H}{H} + \frac{1}{H\sqrt{\log H}} + \frac{1}{e^{CH}\sqrt{H\log H}}\right) \\ &\quad + \omega_f^*(2^{7/2}\pi^{-1/3}2^{4/3}\rho_3 H^{-1/2} : \Phi) \\ &\ll \mu(A)H^{-1/2}.\end{aligned}$$

□

5.9. **Proof of Theorem 2.16.** Combining the above results, we can finally prove Theorem 2.16, conditionally on Proposition 2.18. Let us consider the characteristic functions

$$\phi_{q,I}(u,v) = \mathbb{E}\left(e^{i(u\tilde{S}(t_q,I+x)+v\overline{\tilde{S}(t_q,I+x)})}\right) \ (u,v\in\mathbb{C})$$

of the normalized complex-valued random variable $(\tilde{S}(t_q, I+x))_{x\in\mathbb{F}_q}$ and

$$\phi_H(u,v) = \mathbb{E}\left(e^{i(uS(H)+v\overline{S(H)})}\right) \ (u,v\in\mathbb{C})$$

of the random model

$$S(H) = \frac{X_1+\cdots+X_H}{\sqrt{H}},$$

where $H = |I|$. Recall that by (19), we have for all integers $k, r \geqslant 0$

$$\tilde{M}_q(k,r;I) = \tilde{M}_{\mathrm{prob}}(k,r;H) + O\left(c^{3(k+r)}q^{-1/2}H^{\frac{k+r}{2}}\right).$$

Let us fix $0<\varepsilon<1/2$ and let

$$N = 2M \leqslant \varepsilon\frac{\log q}{\log(c^6H)} \tag{21}$$

be an even integer, so that in particular $c^{6M}q^{-1/2}H^M \leqslant q^{-1/2+\varepsilon}$ and

$$\tilde{M}_q(M,M;I) = \tilde{M}_{\mathrm{prob}}(M,M;H) + O(q^{-1/2+\varepsilon}).$$

By Lemma 5.1, we find the following relation between the characteristic functions:

$$\begin{aligned}\phi_{q,I}(u,\overline{u}) &= \phi_H(u,\overline{u})\\ &\quad +O\left(\frac{|u|^N}{N!}|\tilde{M}_{\mathrm{prob}}(M,M;H)| + q^{-1/2+\varepsilon}(1+|u|^N)\right).\end{aligned}$$

Let $t = M^\alpha/(2\pi)$ for some $\alpha>0$ to be determined later. We apply Corollary 5.8 after making a change of variable with (20) to consider characteristic functions arising from $(u,v)\mapsto u\operatorname{Re}X + v\operatorname{Im}X$ $(u,v\in\mathbb{R})$ instead of $(u,v)\mapsto uX+v\overline{X}$ $(u,v\in\mathbb{C})$. For all $u,v\in\mathbb{R}$, we then have by Hölder's inequality

$$\begin{aligned}P(\tilde{S}(t_q,I+x)\in A) &= P(S(H)\in A)\\ &\quad +O\left(\frac{1}{t}\int_0^t(|\phi_H(\pi u,\pi u)|+|\phi_H(i\pi u,-i\pi u)|)du\right)\\ &\quad +O\left(\int_0^t\int_0^t g(u,v)dudv\right)\\ &\quad +O\left(\frac{1}{t}\int_0^t(g(u,0)+g(0,u))du\right)\end{aligned} \tag{22}$$

where

$$g(x,y) = (2\pi)^N\left[\frac{x^N+y^N}{N!}|\tilde{M}_{\mathrm{prob}}(M,M;H)| + q^{-1/2+\varepsilon}(1+x^N+y^N)\right].$$

Let us bound the three error terms in (22) one after another:

(1) For the first one, note that

$$\frac{1}{t}\int_0^t |\phi_H(2\pi u, 2\pi u)|du \leqslant \frac{1}{t}\int_{\mathbb{R}} |\phi_H(2\pi u, 2\pi u)|du.$$

Using Lemma 5.9 and the assumptions on the moments, we have

$$\phi_H(u,u) = e^{-u^2/2}\left(1 + O\left(\frac{|u|^R}{H^{(R-1)/2}}\right)\right)$$

for $|u| \leqslant H^{\frac{R-1}{2R}}$. Since $\int_{\mathbb{R}} e^{-u^2/2} < \infty$, the error term becomes $O(1/t) = O\left(M^{-\alpha}\right)$ under the condition

$$2\pi t \leqslant H^{\frac{R-1}{2R}}, \text{ i.e. } M \leqslant H^{\frac{R-1}{2R\alpha}}. \tag{23}$$

(2) The second term $\int_0^t\int_0^t g(u,v)dudv$ is bounded (up to a constant) by

$$\frac{\tilde{M}_{\mathrm{prob}}(M,M;H)}{(2M)!}\frac{(2\pi t)^{2M+2}}{M} + q^{-1/2+\varepsilon}\left((2\pi t)^2 + \frac{(2\pi t)^{2M+1}}{M}\right). \tag{24}$$

By Propositions 5.2 (non-self-dual case), 5.4 (Kummer case) and 5.6 (self-dual case),

$$\tilde{M}_{\mathrm{prob}}(M,M;H) \leqslant \begin{cases} (M+H-1)^M & \text{non-self-dual case} \\ M! & \text{Kummer case} \\ (2M-1)!! & \text{self-dual case.} \end{cases}$$

By Stirling's approximation, the first summand of (24) is bounded (up to a constant) by:

- In the Kummer case: $M^{M(2\alpha-1)+2\alpha-1}$.
- In the self-dual case: $M^{2\alpha-\frac{3}{2}+M\left(2\alpha-1+\frac{\log(e/2)}{\log M}\right)}$.
- In the non-self-dual case:

$$M^{2\alpha-\frac{3}{2}}\left(\frac{e^4}{4}\left(M^{2\alpha-1}+HM^{2\alpha-2}-M^{2\alpha-2}\right)\right)^M \ll M^{2\alpha-\frac{3}{2}} \tag{25}$$

if $\alpha < 1/2$ and under the additional condition $M \gg H^{\frac{1}{2-2\alpha}}$. With (21), this imposes the more restrictive range

$$H = o\left((\log q)^{\frac{2-2\alpha}{1+\varepsilon(2-2\alpha)}}\right)$$

and the condition

$$\frac{1}{2-2\alpha} \leqslant \frac{R-1}{2R\alpha}, \text{ i.e. } \alpha \leqslant \frac{R-1}{2R-1} \tag{26}$$

because of (23).

By (23), the second summand of (24) is $O\left(q^{-1/2+2\varepsilon}\right)$ if $\log H/\log q \leqslant \varepsilon$ since

$$\begin{aligned} (2\pi t)^2 &\leqslant H^{\frac{R-1}{R}} = q^{\frac{\log H}{\log q}\frac{R-1}{R}} \text{ and} \\ (2\pi t)^{2M+1} &\leqslant H^{3M\frac{R-1}{2R}} \leqslant q^{\frac{3(R-1)}{4R}\varepsilon}. \end{aligned}$$

(3) Under the same conditions, the last error term $\frac{1}{t}\int_0^t (g(u,0)+g(0,u))du$ of (22) is bounded by the first one.

Hence, the error term in (22) is:

– In the self-dual and Kummer cases

$$O\left(M^{-\alpha}+M^{2\alpha-1+M\left(2\alpha-1+\frac{\log(e/2)}{\log M}\right)}+q^{-\frac{1}{2}+2\varepsilon}\right).$$

We optimize by taking $\alpha=\dfrac{M\left(1-\frac{\log(e/2)}{\log M}\right)+1}{2M+3}$, which leads to an error term of $O\left(M^{-1/2+\varepsilon}+q^{-1/2+2\varepsilon}\right)$.

– In the non-self-dual case, $O\left(M^{-\alpha}+q^{-1/2+2\varepsilon}\right)$ (since $2\alpha-3/2\leqslant-\alpha$ when $\alpha\leqslant 1/2$). By (26), we optimize by taking $\alpha=\frac{R-1}{2R-1}$ and we obtain the error term $O\left(M^{-\frac{R-1}{2R-1}}+q^{-1/2+2\varepsilon}\right)$ for the range

$$H=o\left((\log q)^{\frac{2R}{(2R-1)(1+2\varepsilon)}}\right).$$

Finally, after letting

$$M=\left\lceil \min\left(H^{\frac{R-1}{2R\alpha}},\frac{\varepsilon}{2}\frac{\log q}{\log(c^6H)}\right)\right\rceil\to+\infty,$$

we can apply Proposition 5.10 to $S(H)$, and combining with (22) gives Theorem 2.16.

6. Traces of random matrices in classical groups

In this section, we prove Proposition 2.18, which will conclude the proof of Theorem 2.16. In comparison to earlier works, recall that it is important for us to obtain bounds on moments of high order with respect to the rank.

6.1. **Special linear case.**

Proposition 6.1. *Let $N\geqslant 2$ and let $X=\operatorname{tr}\theta$, where θ is a random variable uniformly distributed in $\mathrm{SU}_N(\mathbb{C})$ with respect to the Haar measure. For $k,r\geqslant 0$ integers, let us consider the moment $M(k,r)=\mathbb{E}(X^k\overline{X^r})$. Then:*

(1) We have

$$M(k,r)=\delta_{N|k-r}\sum_{\substack{\lambda\vdash k\\ l(\lambda)\leqslant N,\,\lambda_N\geqslant -a}}\dim S_\lambda\dim S_{\lambda+(a^N)}$$

where $a=(k-r)/N$ and S_λ, respectively $S_{\lambda+a}$, is the Specht $\mathfrak{S}_k$-module (resp. $\mathfrak{S}_r$-module) associated to the partition λ, respectively $\lambda+(a^N)=\lambda+(a,\dots,a)$.

(2) $M(k,r)\leqslant\sqrt{k!r!}$.

(3) $M(k,k)=k!$ if $k\leqslant N$.

(4) $M(k,r)=0$ if $k,r<N$ and $k\neq r$.

Proof. We use the same technique as in [DS94], but we also need to handle the case $k,r\geqslant N$.

Let Std be the standard representation of $\mathrm{SU}_N(\mathbb{C})$ in $\mathrm{GL}_N(\mathbb{C})$. Recall that the irreducible representations of $\mathrm{SL}_N(\mathbb{C})$ (and hence of its maximal

compact subgroup $\mathrm{SU}_N(\mathbb{C})$) are the Schur-Weyl modules $S_\lambda(\mathrm{Std})$ indexed by partitions λ of length $l(\lambda) \leqslant N$ (see [FH91, 15.3]). Moreover, the character of $S_\lambda(\mathrm{Std})$ is given by the Schur polynomial s_λ evaluated on the eigenvalues (see [Mac95, I.3] or [FH91, 6.1]). For $\lambda = (\lambda_1, \dots, \lambda_l)$, recall the *power symmetric polynomials*

$$p_\lambda = p_{\lambda_1} \dots p_{\lambda_l} \text{ where } p_m = x_1^m + \dots + x_N^m \text{ for any } m \in \mathbb{N}.$$

By the representation theory of the symmetric group and the theory of symmetric polynomials (see [Mac95, I.7.8]), we have the decomposition of p_λ into the basis of Schur polynomials: for any partition λ of length $\leqslant k$,

$$p_\lambda = \sum_{\mu \vdash k} \chi_\mu(\lambda) s_\mu,$$

where $\chi_\mu(\lambda)$ is the character of the irreducible Specht $\mathfrak{S}_k$-module S_μ corresponding to λ, evaluated on the conjugacy class corresponding to λ. In particular,

$$(x_1 + \dots + x_N)^k = \sum_{\substack{\mu \vdash k \\ l(\mu) \leqslant N}} \dim S_\mu s_\mu(x_1, \dots, x_N).$$

Since $(x_1 + \dots + x_N)^k$ (resp. $s_\mu(x_1, \dots, x_N)$) is the character of $\mathrm{Std}^{\otimes k}$ (resp. of the irreducible representation $S_\mu(\mathrm{Std})$) evaluated at a matrix whose eigenvalues are $x_1, \dots, x_N$, we get by orthogonality that $M(k, r)$ is equal to

$$\int_{\mathrm{SU}_N(\mathbb{C})} \mathrm{tr}(g)^k \overline{\mathrm{tr}(g)^r} dg = \sum_{\substack{\mu_1 \vdash k \\ l(\mu_1) \leqslant N}} \sum_{\substack{\mu_2 \vdash r \\ l(\mu_2) \leqslant N}} \dim S_{\mu_1} \dim S_{\mu_2} \delta_{S_{\mu_1}(\mathrm{Std}) \cong S_{\mu_2}(\mathrm{Std})}. \tag{27}$$

The Cauchy-Schwarz inequality yields

$$M(k, r)^2 \leqslant \sum_{\substack{\mu_1 \vdash k \\ l(\mu_1) \leqslant N}} (\dim S_{\mu_1})^2 \sum_{\substack{\mu_2 \vdash r \\ l(\mu_2) \leqslant N}} (\dim S_{\mu_2})^2 \leqslant k! r! \tag{28}$$

since the Specht modules S_μ ($\mu \vdash k$) give the irreducible representations of the symmetric group $\mathfrak{S}_k$ (see [Mac95, I.7]). Hence we obtain (2).

Next, note that $S_{\mu_1}(\mathrm{Std}) \cong S_{\mu_2}(\mathrm{Std})$ if and only if $\mu_2 = \mu_1 + (a^N)$ for some $a \in \mathbb{Z}$ (see [FH91, p. 223]). If the latter holds, we have $N \mid k - r$, $a = (k - r)/N$, $l(\mu_1) \leqslant N$ and $(\mu_1)_N \geqslant -a$. Thus (27) becomes

$$M(k, r) = \sum_{\substack{\lambda \vdash k \\ l(\lambda) \leqslant N,\, \lambda_N \geqslant -a}} \dim S_\lambda \dim S_{\lambda + (a^N)}$$

if $N \mid k - r$ and 0 otherwise. This gives (1).

Let us now assume that $k \leqslant N$. We then automatically have $l(\lambda) \leqslant k \leqslant N$ for every partition λ of k. If moreover $k = r$, then $a = 0$ and

$$M(k, k) = \sum_{\lambda \vdash k} (\dim S_\lambda)^2 = k!,$$

which is (3). Finally, if $0 \leqslant k, r < N$ are distinct, then $N \nmid k - r$ and $M(k, r) = 0$, which is (4). □

Remark 6.2. (see also Remarks 2.17 and 2.19). The second bound we have given in (28) is not asymptotically tight for $k \neq r$. However, replacing it by a better asymptotic would not improve the results (or in particular recover the range $\log H = o(\log q)$ in the non-self-dual case of Theorem 2.16). Indeed, Regev [Reg81, Corollary 4.4] used the hook-length formula to show that as $k \to \infty$, we have

$$\sum_{\substack{\lambda \vdash k \\ l(\lambda) \leqslant N}} (\dim S_\lambda)^2 \sim C(N) \frac{N^{2k}}{k^{(N^2-1)/2}},$$

where $C(N) = N^{N^2/2} (2\pi)^{(1-N)/2} 2^{(1-N^2)/2} \prod_{n=1}^{N-1} n!$. The bound (25) becomes

$$((1+\varepsilon)C(R+1))^H M^{2\alpha-\frac{3}{2}} \left(HM^{2\alpha-2}(R+1)^2\right)^M$$

for any $\varepsilon > 0$, for which we still need the restricted range $M > H^{\frac{1}{2-2\alpha}}$.

6.2. **Symplectic case.**

Proposition 6.3. *Let $N \geqslant 1$ and $X = \operatorname{tr}\theta$, where θ is a random variable uniformly distributed in $\mathrm{USp}_{2N}(\mathbb{C}) = \mathrm{Sp}_{2N}(\mathbb{C}) \cap U_{2N}(\mathbb{C})$ with respect to the Haar measure. For $k \geqslant 0$ an integer, let us consider the moment $M(k) = \mathbb{E}(X^k)$. Then*

(1) $M(k) = 0$ if k is odd.
(2) $M(k) \leqslant (k-1)!!$ if k is even, with equality if $k \leqslant N$.

Proof. Let Std be the standard representation of $\mathrm{Sp}_{2N}(\mathbb{C})$. As in the simple linear case, recall that the irreducible representations of $\mathrm{Sp}_{2N}(\mathbb{C})$ (and hence of $\mathrm{USp}_{2N}(\mathbb{C})$) are given by the Weyl modules $S_{\langle\mu\rangle}(\mathrm{Std})$ indexed by partitions μ with $l(\mu) \leqslant N$ ([FH91, 17.3]). By Peter-Weyl, $M(k) = \mathrm{mult}_1(\mathrm{Std}^{\otimes k})$. By [Sun86, Theorem 6.15], we have the decomposition

$$\mathrm{Std}^{\otimes k} = \bigoplus_{\substack{\mu \\ l(\mu) \leqslant N}} f_\mu^k(N) S_{\langle\mu\rangle}(\mathrm{Std}),$$

where $f_\mu^k(N)$ is the number of sequences of partitions $(\varnothing = \mu_0, \dots, \mu_k = \mu)$ such that

(a) two consecutive partitions differ by exactly one box in their Young diagrams, and
(b) $l(\mu_i) \leqslant N$ for all i.

Hence, $M(k) = f_0^k(N)$, so that (1) is clear. By [Sun86, Lemma 8.3], when k is even, the number f_μ^k of sequences of partitions $(\varnothing = \mu_0, \dots, \mu_k = \mu)$ verifying (a) satisfies $f_0^k = (k-1)!!$, whence (2) since $f_0^{2k}(N) \leqslant f_0^{2k}$, with equality if $k \leqslant N$ since then $l(\mu_i) \leqslant i \leqslant k$. □

Remark 6.4. When $k \leqslant N$, this is proven in [DS94, Theorem 6] by using the analogue for Sp of the Schur-Weyl duality, through the Brauer algebra $D_f(-2N)$, following results of Wenzl and Ram (see in particular [Ram95, Theorem 4.4 (c), Corollary 4.5 (c)]). However, this cannot be exploited when $k > N$ since $D_f(-2N)$ is not semisimple in that case.

6.3. **Special orthogonal case.**

Proposition 6.5. *Let $N \geqslant 2$ and $X = \operatorname{tr}\theta$, where θ is a random variable uniformly distributed in $\mathrm{SO}_N(\mathbb{R})$ with respect to the Haar measure. Let us consider the moment $M(k) = \mathbb{E}(X^k)$ for $k \geqslant 0$ an integer. Then:*

(1) $M(k) = 0$ if k is odd.
(2) $M(k) \leqslant (k-1)!!$ if k is even, with equality if $k \leqslant \lfloor N/2 \rfloor$.

Proof. This is similar to the symplectic case. Let Std be the standard representation of $\mathrm{SO}_N(\mathbb{R})$.

(1) (Case $N = 2N'+1$ odd). By [Sun90, Theorem 4.2], we have the decomposition

$$\mathrm{Std}^{\otimes k} = \bigoplus_{\substack{\mu \\ l(\mu)\leqslant N'}} F_\mu^k(N') S_{[\mu]}(\mathrm{Std}),$$

where $S_{[\mu]}(\mathrm{Std})$ is the irreducible representation of $\mathrm{SO}_{2N'+1}(\mathbb{R})$ associated to the partition μ (obtained from the Weyl module, see [FH91, 19.5]) and $F_\mu^k(N')$ is the number of sequences of partitions $(\varnothing = \mu_0, \dots, \mu_k = \mu)$ such that:
   (a) two consecutive partitions either differ by exactly one box in their Young diagrams, or are equal of length N', and
   (b) $l(\mu_i) \leqslant N'$ for all i.
Hence, $M(k) = F_0^k(N')$. Clearly, $F_0^k(N') \leqslant f_0^k(N') \leqslant f_0^k$ with equality if $k \leqslant N'$, where $f_0^k(N')$ and f_0^k are as in the proof of Proposition 6.3. The result follows then from the latter.

(2) (Case $N = 2N'$ even). By [Pro90, Corollary 4], we have for $\mathrm{SO}_{2N'}(\mathbb{R})$ the decomposition

$$\mathrm{Std}^{\otimes k} = \bigoplus_{\substack{\mu \\ l(\mu)\leqslant N'}} G_\mu^k(N') S_{[\mu]}(\mathrm{Std}),$$

where $G_\mu^k(N')$ is the number of sequences of partitions $(\varnothing = \mu_0, \dots, \mu_k = \mu)$ such that:
   (a) two consecutive partitions differ by exactly one box in their Young diagrams, and
   (b) for every $0 \leqslant i \leqslant k$, the sum of the length of the first two columns in the Young diagram of μ_i is $\leqslant N'$.
Thus, we have again $G_\mu^k(N') \leqslant f_0^k(N') \leqslant f_0^k$ with equality if $k \leqslant N'$, since the Young diagram of μ_i contains at most $i \leqslant k$ boxes.

□

Remark 6.6. As for the symplectic case (see Remark 6.4), this is proved when $k \leqslant N$ in [DS94, Theorem 4], by using [Ram95, Theorem 4.4 (b), Corollary 4.5 (b)], but again this method cannot be applied when $k > N$.

The idea of Sundaram in [Sun86] and [Sun90] is to define tableaux generalizing the Robinson-Schensted-Knuth correspondence and to prove a generalized insertion scheme. The symplectic case actually goes back to Berele, and the odd-dimensional orthogonal case is an extension of the latter. For

orthogonal groups, there are also generalized tableaux by King-Welsh, Koike-Terada and Fulmek-Krattenhalter, but these do not have at first an easy combinatorial description.

7. Examples: coherent families

In this final section, we give examples of coherent families arising from the examples of Section 1.3.1, so that Theorems 2.14 and 2.16 apply.

The construction of the sheaves and the computation of their monodromy groups come from Katz's works [Kat88, KS91]. It usually remains to argue that the conductor is bounded independently from q, show the independence of shifts and to show that the arithmetic and geometric monodromy groups coincide (eventually up to twisting, see Section 2.5). We start by two technical sections with tools to do so, before treating the examples successively.

7.1. Independence of shifts.

Showing that a geometric isomorphism of the form (8) does not exist can usually be done by looking at the ramification on both sides.

Lemma 7.1. *Let $\mathcal{F}$ be a nontrivial ℓ-adic sheaf over $\mathbb{F}_q$ and let $a \in \mathbb{G}_m(\mathbb{F}_q)$ such that there exists a geometric isomorphism of the form (8). Then*

(1) $\mathrm{Sing}(\mathcal{F})\Delta(\mathrm{Sing}(\mathcal{F})-a) \subset \mathrm{Sing}(\mathcal{L}) \subset \mathrm{Sing}(\mathcal{F}) \cup (\mathrm{Sing}(\mathcal{F})-a)$, *where Δ denotes the symmetric difference.*

(2) If $\mathrm{Sing}(\mathcal{F}) \cap \mathbb{A}^1(\mathbb{F}_q) \neq \varnothing$, $\mathbb{A}^1(\mathbb{F}_q)$, *there exists* $x \in \mathrm{Sing}(\mathcal{F}) \cap \mathbb{A}^1(\mathbb{F}_q)$ *such that* $\mathcal{F}^{I_x} = 0$.

(3) If $\mathrm{Sing}(\mathcal{F}) \neq \varnothing, \{\infty\}$, *the sheaf $\mathcal{L}$ is not geometrically trivial.*

(4) If $\mathcal{L}$ is not geometrically trivial,

$$|\mathrm{Sing}(\mathcal{L})| + \sum_{x \in \mathrm{Sing}(\mathcal{L})} \mathrm{Swan}_x(\mathcal{L}) \geqslant 2. \tag{29}$$

(5) If $\mathcal{F}$ has unique break $t \in \mathbb{R}_{\geqslant 0}$ at $x \in \mathbb{P}^1(\mathbb{F}_q)$, then the break decomposition of $\mathcal{F} \otimes \mathcal{L}$ at x is

$$\mathcal{F} \otimes \mathcal{L} = \begin{cases} (\mathcal{F} \otimes \mathcal{L})(\mathrm{Swan}_\infty(\mathcal{L})) & \text{if } t < \mathrm{Swan}_\infty(\mathcal{L}) \\ (\mathcal{F} \otimes \mathcal{L})(t) & \text{if } t > \mathrm{Swan}_\infty(\mathcal{L}) \\ \sum_{z \leqslant t} (\mathcal{F} \otimes \mathcal{L})(z) & \text{if } t = \mathrm{Swan}_\infty(\mathcal{L}). \end{cases} \tag{30}$$

(6) If $\mathcal{F}$ has unique break $t \in \mathbb{R}_{\geqslant 0}$ at ∞, then $\mathrm{Swan}_\infty(\mathcal{L}) \leqslant t$. *If t is not an integer, then* $\mathrm{Swan}_\infty(\mathcal{L}) \leqslant \lfloor t \rfloor$.

Proof. (1) This is clear.

(2) If $x \in \mathrm{Sing}(\mathcal{L}) - \mathrm{Sing}(\mathcal{F})$, then

$$\mathcal{F}^{I_{x+a}} \cong ([+a]^*\mathcal{F})^{I_x} \cong (\mathcal{F} \otimes \mathcal{L})^{I_x} = \mathcal{F} \otimes \mathcal{L}^{I_x} = 0.$$

In particular, by (1), if $y \in \mathrm{Sing}(\mathcal{F})$ but $y - a \notin \mathrm{Sing}(\mathcal{F})$, then $\mathcal{F}^{I_y} = 0$. If $x \in \mathrm{Sing}(\mathcal{F}) \cap \mathbb{A}^1(\mathbb{F}_q)$ and $\mathbb{A}^1(\mathbb{F}_q) \not\subset \mathrm{Sing}(\mathcal{F})$, there exists an integer $m \geqslant 1$ such that $y = x - (m-1)a \in \mathrm{Sing}(\mathcal{F})$ but $x - ma \notin \mathrm{Sing}(\mathcal{F})$, whence the conclusion.

(3) By (1), $\mathcal{L}$ is not lisse under the assumptions.

(4) The Euler-Poincaré formula of Grothendieck-Ogg-Safarevich gives that the left-hand side of (29) is equal to

$$2 + \dim H_c^1(U_{\mathcal{L}} \times \overline{\mathbb{F}}_q, \mathcal{L}) \geqslant 2$$

if $\mathcal{L}$ is nontrivial.

(5) This follows from [Kat88, Lemma 1.3].

(6) By (30), we have

$$\mathrm{Swan}_\infty(\mathcal{F} \otimes \mathcal{L}) = \begin{cases} \mathrm{rank}(\mathcal{F})\,\mathrm{Swan}_\infty(\mathcal{L}) & \text{if } t < \mathrm{Swan}_\infty(\mathcal{L}) \\ \mathrm{rank}(\mathcal{F})t & \text{if } t > \mathrm{Swan}_\infty(\mathcal{L}). \end{cases}$$

On the other hand, by (8),

$$\mathrm{Swan}_\infty(\mathcal{F} \otimes \mathcal{L}) = \mathrm{Swan}_\infty([+a]^*\mathcal{F}) = \mathrm{Swan}_\infty(\mathcal{F}) = t\,\mathrm{rank}(\mathcal{F}),$$

which implies that the case $t < \mathrm{Swan}_\infty(\mathcal{L})$ cannot hold. The last statement follows from the fact that the Swan conductor is an integer. □

The following classification result will also be useful:

Lemma 7.2. *Let $\mathcal{F}$ be a geometrically irreducible ℓ-adic sheaf over $\mathbb{F}_q$.*

(1) If $\mathrm{Sing}(\mathcal{F}) = \varnothing$, then $\mathcal{F}$ is geometrically trivial.

(2) If $|\mathrm{Sing}(\mathcal{F})| = 1$ and $\mathcal{F}$ is tamely ramified, then $\mathcal{F}$ is geometrically trivial.

(3) If $\mathrm{Sing}(\mathcal{F}) = \{x, y\}$ for $x, y \in \mathbb{P}^1(\mathbb{F}_q)$ distinct and $\mathcal{F}$ is tamely ramified, then there exists a multiplicative character $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ and a geometric isomorphism

$$\mathcal{F} \cong \mathcal{L}_{\chi((X-y)/(X-y))}.$$

(4) If $\mathrm{Sing}(\mathcal{F}) = \{x\}$ and $\mathrm{Swan}_x(\mathcal{F}) \leqslant 1$, there exists an additive character $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ and a geometric isomorphism

$$\mathcal{F} \cong \begin{cases} \mathcal{L}_\psi & \text{if } x = \infty \\ \mathcal{L}_{\psi(1/(X-x))} & \text{if } x \neq \infty. \end{cases}$$

Proof. See [FKM14a, Proposition 4.4.6]. □

7.1.1. *Arguments with unipotent blocks.*

Lemma 7.3. *Let $\mathcal{G}$ an ℓ-adic sheaf over $\mathbb{F}_q$ such that $\mathrm{Sing}(\mathcal{G}) \cap \mathbb{A}^1(\mathbb{F}_q) \neq \varnothing$, $\mathbb{A}^1(\mathbb{F}_q)$. For every $s \in \mathrm{Sing}(\mathcal{G}) \cap \mathbb{A}^1(\mathbb{F}_q)$, we consider the tame part of the break decomposition of $\mathcal{G}$ at s,*

$$\mathcal{G}(s)^{\mathrm{tame}} = \bigoplus_\chi \left(\mathrm{Unip.} \otimes \mathcal{L}_{\chi(X+s)}\right), \tag{31}$$

and we assume that either the trivial multiplicative character $\chi = 1$ appears, or that at least two distinct characters χ_1, χ_2 appear. Then there is no isomorphism of the form (8) with $a \neq 0$.

Proof. Let us assume that there is an isomorphism of the form (8) for $\mathcal{G}$ with $a \neq 0$. If the break decomposition of $\mathcal{G}$ at some $s \in \mathrm{Sing}(\mathcal{G}) \cap \mathbb{A}^1(\mathbb{F}_q)$ does not contain a summand $\mathrm{Unip.} \otimes \mathcal{L}_{\chi(X+s)}$ with χ trivial, we replace $\mathcal{G}$

by $\mathcal{G}\otimes\mathcal{L}_{\overline{\chi}_1(X+s)}$, where χ_1 is a character appearing in (31). This new sheaf still satisfies the same hypotheses as $\mathcal{G}$, with the same a in (8) (but with a different $\mathcal{L}$), and with a unipotent block in the break decomposition at s.

Recursively, we can hence assume that the tame part of $\mathcal{G}$ at any $s\in \mathrm{Sing}(\mathcal{G})\cap\mathbb{A}^1(\mathbb{F}_q)$ contains a unipotent block.

By Lemma 7.1 (2), there exists $s\in\mathrm{Sing}(\mathcal{G})\cap\mathbb{A}^1(\mathbb{F}_q)$ such that $\mathcal{G}^{I_s}=0$, a contradiction. □

Lemma 7.4. *Let $\psi:\mathbb{F}_q\to\mathbb{C}^\times$ be a nontrivial additive character and let $\mathcal{G}=\mathrm{FT}_\psi(\mathcal{F})$ be the ℓ-adic Fourier transform of a Fourier sheaf $\mathcal{F}$ over $\mathbb{F}_q$, with $\mathrm{rank}(\mathcal{F})<q-1$. For all $s\in\mathbb{A}^1(\mathbb{F}_q)$, we consider the break decomposition of $\mathcal{F}^{(s)}=\mathcal{F}\otimes\mathcal{L}_{\psi(sX)}$ at ∞:*

$$\begin{aligned}\mathcal{F}^{(s)} &= \bigoplus_{t\in\mathbb{R}_{\geqslant 0}}\mathcal{F}^{(s)}(t)=\mathcal{F}^{(s),\mathrm{tame}}\oplus\mathcal{F}^{(s),\mathrm{wild}}\\ &= \left(\bigoplus_{\chi}\left(\mathrm{Unip}(\chi,s)\otimes\mathcal{L}_{\chi(X+s)}\right)\right)\oplus\left(\bigoplus_{t>0}\mathcal{F}^{(s)}(t)\right).\end{aligned}\tag{32}$$

We assume that:

- *The decomposition (32) at $s=0$ contains at least one break $t\in[0,1]$.*
- *For all $s\in\mathbb{A}^1(\mathbb{F}_q)$ such that the decomposition (32) contains a break $t\in[0,1)$, either the trivial multiplicative character appears in the tame part, or the latter contains at least two distinct characters.*

Then there is no isomorphism of the form (8) for $\mathcal{G}$ with $a\neq 0$.

Proof. By [Kat88, Corollary 8.5.8] (see also [Kat90, Corollary 7.4.5]), the first assumption and the condition on the rank of $\mathcal{F}$ imply that $\mathrm{Sing}(\mathcal{G})\cap\mathbb{A}^1(\mathbb{F}_q)\neq\varnothing,\ \mathbb{A}^1(\mathbb{F}_q)$. Moreover, $s\in\mathrm{Sing}(\mathcal{G})\cap\mathbb{A}^1(\mathbb{F}_q)$ if and only if the decomposition (32) contains a break $t\in[0,1)$. By [Kat90, 7.4.4(3)], the tame part of the break decomposition of $\mathcal{G}$ at s is in this case

$$\bigoplus_{\chi}\left(\mathrm{Unip}(\chi,s)\otimes\mathcal{L}_{\overline{\chi}(X+s)}\right)$$

(with the same unipotent blocks). It suffices to apply Lemma 7.3 to conclude. □

7.2. **Equality of arithmetic and geometric monodromy groups.** In [Kat90], often only the geometric monodromy group $G_{\mathrm{geom}}=G_{\mathrm{geom}}(\mathcal{F})$ of an ℓ-adic sheaf $\mathcal{F}$ over $\mathbb{F}_q$, or its connected component

$$G^0_{\mathrm{geom}}\leqslant G_{\mathrm{geom}}\leqslant G_{\mathrm{arith}}=G_{\mathrm{arith}}(\mathcal{F}),$$

are directly given. As is explained in [Kat90, 7.11–7.14] and [Mic98], it is usually possible to get

$$G^0_{\mathrm{geom}}=G_{\mathrm{geom}}=G_{\mathrm{arith}},$$

up to twisting $\mathcal{F}$ by a rank 1 sheaf, or even, ideally, a constant:

- (Symplectic case) This is the simplest case. Proving that $G^0_{\mathrm{geom}}=\mathrm{Sp}_n(\mathbb{C})$ with the techniques in [Kat90, Chapter 7] actually shows that the sheaf is itself symplectically self-dual (see [Kat90, 7.13, p. 244]),

as for Kloosterman sheaves (see [Kat88, 4.1.11]). Hence $G_{\mathrm{arith}} \subset \mathrm{Sp}_n(\mathbb{C})$ and thus $G_{\mathrm{geom}} = G_{\mathrm{arith}} = \mathrm{Sp}_n(\mathbb{C})$.

– (Special orthogonal case) Similarly, proving that $G^0_{\mathrm{geom}} = \mathrm{SO}_n(\mathbb{C})$ (or $\mathrm{O}_n(\mathbb{C})$) with the techniques of [Kat90, Chapter 7] actually shows that $G_{\mathrm{arith}} \subset \mathrm{O}_n(\mathbb{C})$ (see [Kat90, 7.14, O-Example(2)]). Hence, there exists $\alpha \in \{\pm 1\}$ such that $\mathcal{F}' = \alpha^{1/n} \otimes \mathcal{F}$ has $G_{\mathrm{geom}}(\mathcal{F}') = G_{\mathrm{arith}}(\mathcal{F}') = \mathrm{SO}_n(\mathbb{C})$.

– (Special linear case) This is the hardest case. Assume that $G^0_{\mathrm{geom}} = G^{0,\mathrm{der}}_{\mathrm{geom}} = \mathrm{SL}_n(\mathbb{C})$. We can determine the geometric determinant $\det(\mathcal{F})$ and twist it by a rank one sheaf $\mathcal{L}$ to make it geometrically trivial, hence arithmetically isomorphic to $\alpha \otimes \overline{\mathbb{Q}}_\ell$, for a Weil number α of weight 0 (which may be difficult to determine explicitly). If we let $\mathcal{F}' = \alpha^{-1/n} \otimes \mathcal{L} \otimes \mathcal{F}$, we have $G_{\mathrm{arith}}(\mathcal{F}') \subset \mathrm{SL}_n(\mathbb{C})$ and $\mathrm{SL}_n(\mathbb{C}) = G^0_{\mathrm{geom}} \subset G^0_{\mathrm{geom}}(\mathcal{F}')$ since G^0_{geom} is equal to its derived subgroup and $\mathcal{L}$ has rank one. This gives

$$G_{\mathrm{geom}}(\mathcal{F}') = G_{\mathrm{arith}}(\mathcal{F}') = \mathrm{SL}_n(\mathbb{C}).$$

Moreover, it happens in some cases that $\mathcal{L}$ is arithmetically constant, so that $\mathcal{F}' = \alpha^{-1/n} \otimes \mathcal{F}$ is simply a renormalization of $\mathcal{F}$.

7.3. **Kummer sheaves: multiplicative characters.**

Proposition 7.5. *A family $(\mathcal{F})_q$ of Kummer sheaves $\mathcal{L}_{\chi(f)}$, where $\deg(f)$ is bounded independently from q and f has no zero or pole of order divisible by $\mathrm{ord}(\chi)$, is coherent.*

Proof. For the construction of the Kummer sheaf, see [Del77, Exposé 6, Section 1] or [Kat88, Section 4.3]. We have $\mathrm{cond}(\mathcal{L}_{\chi(f)}) = 1 + \deg(f_1) + \deg(f_2)$ where $f = f_1/f_2$ with $f_1, f_2 \in \mathbb{F}_q[X]$, $(f_1, f_2) = 1$. □

7.4. **Kloosterman sheaves.**

Theorem 7.6 (Deligne, Katz)**.** *For $n \geqslant 2$ an integer, there exists a* Kloosterman ℓ-adic sheaf $\mathcal{K}l_n$ *over $\mathbb{F}_q$, of rank n, with trace function equal to the Kloosterman sum (3). The family $(\mathcal{K}l_{n,q})_{q \text{ odd}}$ is coherent, with monodromy group equal to*

$$\begin{cases} \mathrm{SL}_n(\mathbb{C}) & \text{if } n \text{ odd} \\ \mathrm{Sp}_n(\mathbb{C}) & \text{if } n \text{ even.} \end{cases}$$

Proof. For the construction and computation of monodromy groups, see [Kat88]. We have $\mathrm{cond}(\mathcal{K}l_n) = n + 3$. Finally, the independence of shifts follows from Lemma 7.4, which can be applied thanks to [Kat88, 7.4.1]. □

7.5. **Hypergeometric sheaves.**

Proposition 7.7 (Katz)**.** *Let $n \geqslant m \geqslant 0$ be integers with $r = m + n \geqslant 1$, $\boldsymbol{\chi}_q = (\chi_{i,q})_{1 \leqslant i \leqslant n}$, $\boldsymbol{\rho}_q = (\rho_{j,q})_{1 \leqslant j \leqslant m}$ tuples of pairwise distinct characters of $\mathbb{F}_q^\times$. There exists a* hypergeometric sheaf $\mathcal{H}(\boldsymbol{\chi}_q, \boldsymbol{\rho}_q)$ *over $\mathbb{F}_q$ of rank n, with*

trace function equal to the hypergeometric sum $\mathrm{Hyp}(\boldsymbol{\chi}_q, \boldsymbol{\rho}_q) : \mathbb{F}_q \to \mathbb{C}$ *defined by*

$$t \mapsto \frac{(-1)^{r-1}}{q^{(r-1)/2}} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n, \boldsymbol{y}\in\mathbb{F}_q^m \\ N(\boldsymbol{x})=tN(\boldsymbol{y})}} \left(\prod_{i=1}^{n} \chi_{i,q}(x_i) \prod_{j=1}^{m} \overline{\rho_{j,q}(y_j)}\right) e\left(\frac{\mathrm{tr}(T(\boldsymbol{x}) - T(\boldsymbol{y}))}{p}\right),$$

where $N : \mathbb{F}_q^n \to \mathbb{F}_q$ *is the norm (product of components) and* $T : \mathbb{F}_q^n \to \mathbb{F}_q$ *the trace (sum of components). We assume that* $\Lambda_q = \prod_i \chi_{i,q} = 1$ *and either:*

(1) $n = m$ *is odd and* $\Gamma_q = \prod_j \rho_{j,q} = 1$ *is constant, or*

(2) $n - m \geqslant 3$ *is odd.*

Then the family $(\mathcal{H}(\boldsymbol{\chi}_q, \boldsymbol{\rho}_q))_q$ *is coherent with monodromy group* $\mathrm{SL}_n(\mathbb{C})$.

Proof. The construction can be found in [Kat90, Theorem 8.4.2]. We find that $\mathrm{cond}(\mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho})) = n + 3$.

The connected component at the identity G^0_{geom} is computed in [Kat90, Theorems 8.11.2, 8.11.3], and can be $\mathrm{SL}_n(\mathbb{C})$, $\mathrm{Sp}_n(\mathbb{C})$, $\mathrm{SO}_n(\mathbb{C})$, plus some exceptional cases in low rank. Moreover, $G^0_{\mathrm{geom}} = G^{0,\mathrm{der}}_{\mathrm{geom}}$. The distinction between the possible cases is not straightforward (see [Kat90, p. 291]), but $G^0_{\mathrm{geom}} = G^{0,\mathrm{der}}_{\mathrm{geom}} = \mathrm{SL}_n(\mathbb{C})$ if either:

(1) $n = m$ is odd and $\Lambda_q = 1$, or

(2) $n - m \geqslant 3$ is odd.

To make the arithmetic and geometric monodromy group coincide, we use the strategy of Section 7.2. By the computation of the arithmetic determinant in [Kat90, 8.12], there is an explicit Weil number $\alpha = \alpha(\boldsymbol{\chi}, \boldsymbol{\rho}) \in \overline{\mathbb{Q}}_\ell$ of weight 0 such that $\det \mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho}) \cong \alpha \otimes \mathcal{L}$ with

$$\mathcal{L} = \begin{cases} \mathcal{L}_\Lambda \otimes [x \mapsto 1 - x]^* \mathcal{L}_{\Gamma/\Lambda} & \text{if } n = m, \\ \mathcal{L}_\psi \otimes \mathcal{L}_\Lambda & \text{if } n - m = 1, \\ \mathcal{L}_\Lambda & \text{if } n - m \geqslant 2. \end{cases}$$

Under the assumptions of the proposition, $\mathcal{L}$ is arithmetically trivial and $\alpha = 1$.

The break decomposition of the hypergeometric sheaf is determined recursively in [Kat90, Theorem 8.4.2(6)], and the independence of shifts is then a consequence of Lemma 7.4. □

Example 7.8. Thus, families of hypergeometric sums of the form

$$\frac{(-1)^{r-1}}{q^{(r-1)/2}} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n, \boldsymbol{y}\in\mathbb{F}_q^n \\ N(\boldsymbol{x})=tN(\boldsymbol{y})}} \left(\prod_{i=1}^{n-1} \chi_i(x_i x_n^{-1}) \overline{\rho_i(y_i y_n^{-1})}\right) e\left(\frac{\mathrm{tr}(T(\boldsymbol{x}) - T(\boldsymbol{y}))}{p}\right) \quad (t \in \mathbb{F}_q)$$

with n odd or

$$\frac{(-1)^{r-1}}{q^{(r-1)/2}} \sum_{\substack{\boldsymbol{x}\in\mathbb{F}_q^n, \boldsymbol{y}\in\mathbb{F}_q^m \\ N(\boldsymbol{x})=tN(\boldsymbol{y})}} \left(\prod_{i=1}^{n} \chi_i(x_i x_n^{-1}) \prod_{j=1}^{m} \overline{\rho_j(y_j)}\right) e\left(\frac{\mathrm{tr}(T(\boldsymbol{x}) - T(\boldsymbol{y}))}{p}\right) \quad (t \in \mathbb{F}_q)$$

with $n - m \geqslant 3$ odd, are coherent.

For $m = 0$ and $\boldsymbol{\chi} = (1)_{1\leqslant i\leqslant n}$, we recover the Kloosterman sheaf $\mathcal{K}l_n$.

7.6. **General exponential sums of the form (4).**

Proposition 7.9. *Let $f, g, h \in \mathbb{Q}(X)$. If q is large enough to consider $f, g, h \in \mathbb{F}_q(X)$ and g (resp. h) has no pole or zero (resp. no pole) of order divisible by p, we consider the sheaves*

$$\mathcal{F}_1 = \mathcal{L}_{\psi(h)} \otimes \mathcal{L}_{\chi(g)}, \ \mathcal{F}_2 = f_*\mathcal{F}_1,$$

for $\psi : \mathbb{F}_q \to \mathbb{C}$ (resp. $\chi : \mathbb{F}_q^\times \to \mathbb{C}$) an additive (resp. multiplicative) character. If $\mathcal{F}_2$ is a Fourier sheaf, then there exists a sheaf $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F}_2)$ (the ℓ-adic Fourier transform of $\mathcal{F}_2$) with trace function given by (4). Moreover, $\mathrm{cond}(\mathcal{G})$ is bounded above independently from q.

Proof. The construction of the ℓ-adic Fourier transform can be found in [Kat88, Chapters 5, 8]. The uniform bound on the conductor follows from the general bound on conductors of Fourier transforms [FKM15a, Proposition 8.2], obtained from Laumon's analysis of the ramification of ℓ-adic Fourier transforms [Kat90, 7.3–7.5]. □

We can distinguish the following cases:

(i) $h = 0$ and $\chi = 1$, so that $\mathcal{F}_1$ is the trivial sheaf. These are sums of the form (6), studied in [Kat90, 7.10] and by Fouvry-Michel in [Mic98], [FM02] and [FM03].

(ii) $\mathcal{F}_1$ is nontrivial and $f = X$. More particularly, we consider the case $\chi = 1$ and h a polynomial of degree $n \geqslant 2$, which includes Birch sums (5). These are studied in [Kat90, 7.12] and [Kat87].

(iii) $\mathcal{F}_1$ is nontrivial and $f \neq X$. More particularly, we will consider the case studied in [Kat90, 7.7, 7.13, 7.14] where h is odd with a pole of order $\geqslant 1$ at ∞, $f \neq 0$ is an odd polynomial, and there exists an even or odd rational function L with $g(x)g(-x) = L(x)^{\mathrm{ord}(\chi)}$.

7.6.1. *Independence of shifts.* The following criterion generalizes the argument of [FKM15b] for Birch sums to sheaves of the general form of Proposition 7.9 and allows to reduce to the case of $\mathcal{L}$ being an Artin-Schreier sheaf in a geometric isomorphism of the form (8).

Lemma 7.10. *In the setting of Proposition 7.9, let us assume that $\mathcal{F}_2$ is a Fourier sheaf, f a polynomial of degree $d \geqslant 1$, $n = \mathrm{Swan}_\infty(\mathcal{F}_1) > d$, and $(n, d) = (d, p) = 1$. If there is a geometric isomorphism of the form (8) with $a \neq 0$ for $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F}_2)$, then*

$$\mathrm{Swan}_\infty(\mathcal{L}) \in \left\{0, 1, \dots, \left\lfloor \frac{n}{n-d} \right\rfloor\right\}.$$

If $n > 2d$, there exists an additive character $\psi_1 : \mathbb{F}_q \to \mathbb{C}^\times$ such that $\mathcal{L} \cong \mathcal{L}_{\psi_1}$.

Proof. By [Kat90, 7.7], $\mathcal{F}_2$ has unique break n/d at ∞, thus

$$\mathrm{Swan}_\infty(\mathcal{F}_2) = (n/d)\,\mathrm{rank}(\mathcal{F}_2) = n.$$

Moreover, $\mathcal{G}$ is lisse on $\mathbb{A}^1$. By Lemma 7.1 (1), $\mathrm{Sing}(\mathcal{L}) \subset \{\infty\}$. We may assume that $\mathcal{L}$ is not geometrically trivial, the conclusions being clear otherwise. By Lemma 7.1 (4), it follows that $\mathrm{Sing}(\mathcal{L}) = \{\infty\}$ and $\mathrm{Swan}_\infty(\mathcal{L}) \geqslant 1$.

By [Kat90, 7.4.1(1)], $\mathcal{G}$ has unique break $\frac{n}{n-d}$ at ∞, with multiplicity

$$\frac{n-d}{n}\operatorname{Swan}_\infty(\mathcal{F}_2) = n-d.$$

The break $\frac{n}{n-d}$ is not an integer since we assume that $(n,d)=1$, and the first conclusion follows from Lemma 7.1 (6). For the second one, note that $\frac{n}{n-d} < 2$ if $n > 2d$ and use Lemma 7.2 (4). □

The next lemma consequently considers isomorphisms of the form (8) when $\mathcal{L}$ is an Artin-Schreier sheaf.

Lemma 7.11. *In the setting of Proposition 7.9, let us assume that $\mathcal{F}_2$ is a Fourier sheaf and that there is an isomorphism of the form (8) for $\mathcal{G}$ with $a \in \mathbb{F}_q^\times$ and $\mathcal{L} = \mathcal{L}_{\psi_1}$ for some additive character $\psi_1 : \mathbb{F}_q \to \mathbb{C}^\times$. Then*

(1) $\operatorname{Sing}(\mathcal{F}_2) = \{\infty\}$ *or* $\mathbb{A}^1(\mathbb{F}_q) \subset \operatorname{Sing}(\mathcal{F}_2)$.

(2) If $f = X$, then either $\chi \neq 1$ and g is constant, or $\chi = 1$ and h is a polynomial of degree at most 2.

Remark 7.12. Since we consider families of sheaves whose conductors are bounded uniformly from q, the condition $\mathbb{A}^1(\mathbb{F}_q) \subset \operatorname{Sing}(\mathcal{F}_2)$ is clearly exceptional.

Proof. Let $b \in \mathbb{F}_q$ such that $\psi_1(x) = \psi(bx)$ $(x \in \mathbb{F}_q)$ and let us assume that we have a geometric isomorphism

$$[+a]^*\mathcal{G} \cong \mathcal{G} \otimes \mathcal{L}_{\psi(bX)}$$

with $a \in \mathbb{F}_q^\times$. Taking Fourier transform on both sides of the isomorphism and using that

$$\begin{aligned} [+a]^* \operatorname{FT}_\psi(\mathcal{F}) &\cong \operatorname{FT}_\psi(\mathcal{F} \otimes \mathcal{L}_{\psi(aX)}) \\ \operatorname{FT}_\psi(\operatorname{FT}_\psi(\mathcal{F}) \otimes \mathcal{L}_{\psi(bX)}) &\cong [x \mapsto -b-x]^*\mathcal{F} \end{aligned}$$

for any Fourier sheaf $\mathcal{F}$, we get a geometric isomorphism

$$\mathcal{F}_2 \otimes \mathcal{L}_{\psi(aX)} \cong [+(-b)]^*\mathcal{F}_2. \tag{33}$$

Then:

- If $b = 0$, taking determinants shows that $a = 0$.
- Since the Artin-Schreier sheaf is ramified at most at ∞, we have $\operatorname{Sing}(\mathcal{F}_2) \cap \mathbb{A}^1(\mathbb{F}_q) = (\operatorname{Sing}(\mathcal{F}_2) \cap \mathbb{A}^1(\mathbb{F}_q)) + b$. If $b \neq 0$, this yields
$$\operatorname{Sing}(\mathcal{F}_2) = \varnothing,\ \{\infty\},\ \text{or } \mathbb{A}^1(\mathbb{F}_q) \subset \operatorname{Sing}(\mathcal{F}_2)$$
because for any $y \in \mathbb{F}_q$, $b \in \mathbb{F}_q^\times$, the map $\mathbb{F}_q \to \mathbb{F}_q$, $x \mapsto y + xb$, is a bijection. By Lemma 7.2, $\operatorname{Sing}(\mathcal{F}_2) \neq \varnothing$ because we assume that $\mathcal{F}_2$ is geometrically irreducible and not geometrically trivial.

If $f = X$ and $b \neq 0$, the geometric isomorphism (33) becomes

$$\mathcal{L}_{\psi(h(X)-h(X-b)+aX)} \cong \mathcal{L}_{\chi(g(X-b)/g(X))}.$$

Since the Kummer sheaf is tame while the Artin-Schreier sheaf is not, we must have $\chi = 1$ or $x \mapsto g(x-b)/g(x)$ constant on $\mathbb{F}_q$. If $\chi = 1$, then

$$x \mapsto h(x) - h(x-b) + ax \text{ is constant on } \mathbb{F}_q,$$

i.e. $h(x) = -ab^{-1}x^2/2 + ax/2 + \text{constant}$. On the other hand, if $x \mapsto g(x-b)/g(x)$ is constant, then g is constant.

The case with a geometric isomorphism $[+a]^*\mathcal{G} \cong D(\mathcal{G})\otimes\mathcal{L}_{\psi(bX)}$ is similar. □

7.6.2. *Sums of the form* (6).

Proposition 7.13. *Let $f \in \mathbb{Q}(X)$ and let $Z_{f'}$ be the set of zeros of f' in $\mathbb{C}$. We assume that either*

- *(H): $k_f = |Z_{f'}|$ is even, $\beta = \sum_{z\in Z_{f'}} f(z) = 0$, and if $s_1 - s_2 = s_3 - s_4$ with $s_i \in f(Z_{f'})$, then $s_1 = s_3, s_2 = s_4$ or $s_1 = s_2, s_3 = s_4$.*
- *(H'): f is odd, and if $s_1 - s_2 = s_3 - s_4$ with $s_i \in f(Z_{f'})$, then $s_1 = s_3, s_2 = s_4$ or $s_1 = s_2, s_3 = s_4$ or $s_1 = -s_4, s_2 = -s_3$.*

For q large enough, there exists an ℓ-adic sheaf $\mathcal{G}_{f,q}$ over $\mathbb{F}_q$ with trace function

$$x \mapsto \frac{-1}{\sqrt{q}} \sum_{y\in\mathbb{F}_q} e\left(\frac{\mathrm{tr}(xf(y))}{p}\right) \quad (x \in \mathbb{F}_q).$$

Moreover, there exist Weil numbers $\alpha_q \in \overline{\mathbb{Q}}_\ell$ of weight 0 such that the family of ℓ-adic sheaves $(\alpha_q \otimes \mathcal{G}_{f,q})_q$ is coherent, with monodromy group $\mathrm{SL}_{k_f}(\mathbb{C})$ if (H) holds, and Sp_{k_f} if (H') holds (in which case $\alpha_q = 1$).

Proof. The construction of $\mathcal{G}_{f,q}$ is done in [Kat90, Theorem 7.9.4, Lemmas 7.10.2.1, 7.10.2.3] and the computation of monodromy groups in [Kat90, 7.9.6, 7.9.7, 7.10].

By Section 7.2, we get $G_{\mathrm{geom}} = G_{\mathrm{arith}} = \mathrm{Sp}_{k_f}(\mathbb{C})$ in the (H') case. In the (H) case, we use the determination (geometrically) of the determinant of $\mathcal{G}_{f,q}$ from [Kat90, 7.10.4]: there is a geometric isomorphism

$$\det(\mathcal{G}_{f,q}) \cong \mathcal{L}_{\psi(-\beta X)} \otimes \mathcal{L}_\chi,$$

where $\chi = \chi_2^{k_f}$ for χ_2 the character of order 2 of $\overline{\mathbb{F}}_q^\times$ and β is viewed in $\overline{\mathbb{F}}_q$. Under (H) or (H'), this sheaf is geometrically trivial, and it suffices to apply [FKM14a, Proposition 3.2.3].

It remains to show the independence of shifts. We consider the case of a geometric isomorphism

$$[+a]^*\mathcal{G}_{f,q} \cong \mathcal{G}_{f,q} \otimes \mathcal{L} \tag{34}$$

for $\mathcal{L}$ a rank 1 sheaf and $a \in \mathbb{F}_q$, the argument with $D(\mathcal{G}_{f,q})$ being similar. We adapt the multiplicative case treated in the proof of [Mic98, Théorème 2.3]. By Lemma 7.1 (1), since $\mathcal{G}_{f,q}$ is lisse on $\mathbb{G}_m$, we must have $\mathrm{Sing}(\mathcal{L}) = \{0, -a, \infty\}$ or $\{0, -a\}$. Moreover, by [Kat90, 7.5.4(5)], the ramification of $\mathcal{L}$ at 0 and $-a$ is tame. By [Kat90, 7.9.4], $\mathcal{G}_{f,q}$ as I_∞-representation is

$$\mathcal{G}_{f,q}(\infty) \cong \bigoplus_{z\in Z_{f'}} \left(\mathcal{L}_{\psi(f(z)X)} \otimes \mathcal{L}_{\overline{\chi}_z(X)}\right)$$

where χ_z is a multiplicative character, and we view $Z_{f'}$ in $\overline{\mathbb{F}}_q$. Hence, by [Kat88, Lemma 1.3] all the breaks are at 1 and as representations of the wild

inertia group P_∞, we have

$$\mathcal{G}_{f,q}(\infty) \cong \bigoplus_{z\in Z_{f'}} \mathcal{L}_{\psi(f(z)X)}.$$

We distinguish two cases:

– If $\infty \notin \mathrm{Sing}(\mathcal{L})$, then Lemma 7.2 (3) implies that there is a multiplicative character χ_1 such that

$$\mathcal{L} \cong \mathcal{L}_{\chi_1((X+a)/X)}.$$

Hence, there exists some $\beta \in \mathbb{C}$ of unit norm such that

$$\beta \sum_{y\in\mathbb{F}_q} e\left(\frac{\mathrm{tr}((x+a)f(y))}{p}\right) = \sum_{y\in\mathbb{F}_q} e\left(\frac{\mathrm{tr}(xf(y))}{p}\right)\chi_1\left(\frac{x+a}{x}\right)$$

for all $x \in \mathbb{F}_q^\times$. If $a \neq 0$, taking $x = -a$ gives $\beta q = 0$, a contradiction.

– Assume that $\infty \in \mathrm{Sing}(\mathcal{L})$. By [Kat88, Lemma 1.3], $\mathrm{Swan}_\infty(\mathcal{L}) \in \{0, 1\}$ because all the breaks of $\mathcal{G}_{f,q}$ at ∞ are at 1. If $\mathrm{Swan}_\infty(\mathcal{L}) = 1$, the break-depression lemma [Kat88, 8.5.7] implies that $\mathcal{L} \cong (\text{tame at } \infty)\otimes \mathcal{L}_{\psi(bX)}$ for some $b \in \mathbb{F}_q^\times$. On the other hand, $\mathcal{L}$ is by definition tame at ∞ if $\mathrm{Swan}_\infty(\mathcal{L}) = 0$. In both cases, the restriction of the isomorphism (34) to P_∞ gives

$$\bigoplus_{z\in Z_{f'}} \mathcal{L}_{\psi(f(z)(X+a))} \cong \bigoplus_{z\in Z_{f'}} \mathcal{L}_{\psi((f(z)+b)X)}$$

for some $b \in \mathbb{F}_q$. Thus the sets $\{f(z)(X + a) : z \in Z_{f'}\}$ and $\{(f(z) + b)X : z \in Z_{f'}\}$ are equal, which implies that $a = 0$ (and $b = 0$).

□

Remark 7.14. Lemma 7.10 does not apply here because $\mathcal{F}_1$ is trivial.

Examples 7.15. The following examples are given in [Mic98, p. 229], [FM03, p. 7] and [Kat90, 7.10]:

(1) The polynomial $f = aX^{r+1} + bX$ with $a, b, r \in \mathbb{Z}$ and $ab \neq 0$ verifies $k_f = |r|$ and

$$\begin{cases} (H) & \text{if } |r| \geqslant 3 \text{ odd,} \\ (H') & \text{if } r \neq 0 \text{ even.} \end{cases}$$

(2) Let $g \in \mathbb{Z}[X]$ be monic of degree r with full Galois group $\mathfrak{S}_r$ (a "generic" condition by [vdW34]), and let $f \in \mathbb{Q}[X]$ be the unique primitive of g with $\sum_{i=1}^r f(\alpha_i) = 0$, where $\alpha_1, \dots, \alpha_r$ are the zeros of f. Assuming that $r \geqslant 6$ is even, we have that (H) holds for f and $k_f = n$.

(3) For $n \geqslant 3$ and $a \in \mathbb{Z}$ nonzero, the polynomial $f = X^n - naX$ satisfies (H'), and $k_f = n - 1$.

7.6.3. *Sums of the form* (4) *with* $f = X$, $\chi = 1$, h *polynomial.*

Proposition 7.16. *Let $h = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ be a polynomial of degree $n \geqslant 3$. For p large enough (depending on h), there exists an ℓ-adic sheaf $\mathcal{G}_{h,q}$ over $\mathbb{F}_q$ of rank $n-1$ corresponding to the trace function*

$$x \mapsto \frac{-1}{\sqrt{q}} \sum_{y \in \mathbb{F}_q} e\left(\frac{\mathrm{tr}(xy + h(y))}{p}\right) \ (x \in \mathbb{F}_q).$$

If $a_{n-1} = 0$ and $n \notin \{7, 9\}$, there exist Weil numbers $\alpha_q \in \overline{\mathbb{Q}}_\ell$ of weight 0 such that the family $(\alpha_q \otimes \mathcal{G}_{h,q})_q$ is coherent, with monodromy group:

(1) $\mathrm{SL}_{n-1}(\mathbb{C})$ *if $n-1$ is odd,*
(2) If n is odd:
- $\mathrm{Sp}_{n-1}(\mathbb{C})$ *if h has no monomial of even positive degree,*
- $\mathrm{SL}_{n-1}(\mathbb{C})$ *otherwise.*

Moreover, $\alpha_q = 1$ in the symplectic case.

Proof. The construction of $\mathcal{G}_{h,q}$ and the computation of its geometric monodromy group can be found in [Kat90, Section 7.12] and [Kat87]. In the symplectic case, Section 7.2 gives that $G_{\mathrm{geom}} = G_{\mathrm{arith}} = \mathrm{Sp}_{n-1}(\mathbb{C})$. In the special linear case, the hypothesis $a_{n-1} = 0$ implies that the geometric determinant of $\mathcal{G}$ is trivial by [Kat90, Section 7.12], and the statement follows from Section 7.2.

The independence of shifts follows directly from Lemmas 7.10 and 7.11, similarly to Kloosterman sheaves. □

Example 7.17. For the Birch sums (5), we have $h = X^3$ and the corresponding monodromy group is $\mathrm{Sp}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})$.

7.6.4. *Sums of the form (4) with f polynomial, $\chi \neq 1$.*

Proposition 7.18. *Let*
- *$h \in \mathbb{Q}(X)$ with a pole of order $n \geqslant 1$ at ∞.*
- *$f \in \mathbb{Z}[X]$ nonzero of degree d with $(d, n) = 1$.*
- *$g \in \mathbb{Q}(X)$ nonzero.*
- *χ a character of $\mathbb{F}_q^\times$ of order $r \geqslant 2$, with the order of any zero or pole of g not divisible by r.*

For p large enough (depending on f, g, h), there exists an ℓ-adic sheaf $\mathcal{G}_q$ over $\mathbb{F}_q$ corresponding to the trace function (4). Assuming that $n > 2d$, that f, h are odd and that

(1) there exists $L \in \mathbb{Q}(X)$ even or odd with $L(x)^r = g(x)g(-x)$,
(2) either g is nonconstant or $h \notin \mathbb{Z}[X]$,
(3) either $N = \mathrm{rank}(\mathcal{G}) \neq 7, 8$ or $n - d \neq 6$,

then there exist $\alpha_q \in \{\pm 1\}$ such that the family $(\alpha_q \otimes \mathcal{G}_q)_q$ is coherent, with monodromy group $\mathrm{Sp}_N(\mathbb{C})$ if L is odd (in which case $\alpha_q = 1$) and $\mathrm{SO}_N(\mathbb{C})$ if L is even.

Proof. The construction and the computation of the geometric monodromy group of $\mathcal{G}_q$ can be found in [Kat90, 7.7, 7.13 (Sp-example(2)) and 7.14 (O-example(2))]. Section 7.2 show the existence of $\alpha_q \in \{\pm 1\}$ so that $G_{\mathrm{geom}}(\alpha_q \otimes \mathcal{G}_q) = G_{\mathrm{arith}}(\alpha_q \otimes \mathcal{G}_q)$ is as stated.

We show the independence of shifts. Let us assume that there is a geometric isomorphism of the form (8) for $\mathcal{G}$ with $a \neq 0$. By Lemmas 7.10 and 7.11, we have $\mathrm{Sing}(\mathcal{F}_2) = \{\infty\}$ or $\mathbb{A}^1(\mathbb{F}_q) \subset \mathrm{Sing}(\mathcal{F}_2)$. Since $\mathrm{cond}(\mathcal{F}_2)$ is bounded independently from q, the last possibility is excluded for q large enough. Let us then assume that $\mathrm{Sing}(\mathcal{F}_2) = \{\infty\}$. Because f is a polynomial, we have $\mathrm{Sing}(\mathcal{F}_1) \subset \{\infty\}$. Since the Kummer sheaf is tamely ramified everywhere while the Artin-Schreier sheaf is totally wild at all ramified points, this implies that $h \in \mathbb{Z}[X]$ and that g is constant. □

7.7. **Families of hyperelliptic curves.**

Proposition 7.19. *Let $f \in \mathbb{Z}[X]$ be a squarefree polynomial of degree $2g \geqslant 2$. For q large enough, we consider the family of smooth projective models of the affine hyperelliptic curves over $\mathbb{F}_q$ of genus g given by*

$$X_z : y^2 = f(x)(x - z),$$

parametrized by $z \in \mathbb{F}_q$, which are nonsingular when $z \notin Z_{f,q}$, for $Z_{f,q} \subset \overline{\mathbb{F}}_q$ the set of zeros of f in $\mathbb{F}_q$. There exists a geometrically irreducible ℓ-adic sheaf $\mathcal{F}_{f,q}$ over $\mathbb{F}_q$ of rank $2g$, with trace function

$$t_{\mathcal{F}}(z) = \frac{q + 1 - |X_z(\mathbb{F}_q)|}{q^{1/2}} \quad (z \notin Z_{f,q}).$$

The family $(\mathcal{F}_{f,q})_q$ is coherent with monodromy group $\mathrm{Sp}_{2g}(\mathbb{C})$.

Proof. For the construction, see [KS91, Section 10.1] or [Hal08, Section 4] (using middle-convolutions). Here, we moreover normalize with a Tate twist to get a sheaf of weight 0. We have $\mathrm{Sing}(\mathcal{F}_{f,q}) = \{\infty\} \cup Z_f$ and $\mathcal{F}_{f,q}$ is everywhere tame. In particular, $\mathrm{cond}(\mathcal{F}_{f,q}) = 2g + |Z_{f,q}|$.

By [KS91, Theorem 10.1.16], the geometric monodromy group is symplectic. Since we normalized, [KS91, Lemma 10.1.9] shows that the arithmetic monodromy group preserves the sames pairing (without normalization, it is a symplectic similitude with multiplicator q).

It remains to show the independence of shifts. By [KS91, 10.1.13], at any $z \in Z_{f,q}$ the quotient V/V^{I_z} is the trivial (one-dimensional) I_z–representation, for $V = (\mathcal{F}_{f,q})_{\overline{\eta}}$. Let us assume that there exists an isomorphism of the form (8) for $\mathcal{F}_{f,q}$. By Lemma 7.1 (2), if q is large enough, there exists $x \in \mathrm{Sing}(\mathcal{F}) \cap \mathbb{A}^1(\mathbb{F}_q)$ such that $V^{I_x} = 0$, a contradiction. □

References

[BRR86] Rabi N. Bhattacharya and Ramaswamy Ranga Rao. *Normal approximation and asymptotic expansions*. Robert E. Krieger Publishing Co., 1986. Reprint of the 1976 original.

[DE52] Harold Davenport and Paul Erdős. The distribution of quadratic and higher residues. *Publ. Math. Debrecen*, 2:252–265, 1952.

[Del77] Pierre Deligne. *Cohomologie étale, séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$*, volume 569 of *Lecture notes in Mathematics*. Springer, 1977.

[Del80] Pierre Deligne. La conjecture de Weil. II. *Publ. Math. Inst. Hautes Études Sci.*, 52(1):137–252, 1980.

[DS94] Persi Diaconis and Mehrdad Shahshahani. On the eigenvalues of random matrices. *J. Appl. Probab.*, 31:49–62, 1994.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate texts in Mathematics*. Springer, 1991.

[FKM14a] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Trace functions over finite fields and applications. https://people.math.ethz.ch/~kowalski/elements.pdf, December 2014.

[FKM14b] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Trace functions over finite fields and their applications. In *Colloquium De Giorgi 2013 and 2014*, volume 5 of *Colloquia*, pages 7–35. Ed. Norm., Pisa, 2014.

[FKM15a] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. Algebraic twists of modular forms and Hecke orbits. *Geom. Funct. Anal.*, 25(2):580–657, 2015.

[FKM15b] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. A study in sums of products. *Philos. Trans. A*, 373(2040), 2015.

[FM02] Étienne Fouvry and Philippe Michel. A la recherche de petites sommes d'exponentielles. *Ann. Inst. Fourier (Grenoble)*, 52(1):47–80, 2002.

[FM03] Étienne Fouvry and Philippe Michel. Sommes de modules de sommes d'exponentielles. *Pacific J. Math.*, 209(2), 2003.

[Gut05] Allan Gut. *Probability: a graduate course*. Springer texts in statistics. Springer, 2005.

[Hal08] Chris Hall. Big symplectic or orthogonal monodromy modulo ℓ. *Duke Math. J.*, 141(1):179–203, 2008.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*. Colloquium Publications. American Mathematical Society, 2004.

[Kat87] Nicholas M. Katz. On the monodromy groups attached to certain families of exponential sums. *Duke Math. J.*, 54(1), 1987.

[Kat88] Nicholas M. Katz. *Gauss sums, Kloosterman sums, and monodromy Groups*, volume 116 of *Annals of Mathematical Studies*. Princeton University Press, 1988.

[Kat90] Nicholas M. Katz. *Exponential sums and differential equations*, volume 124 of *Annals of Mathematical Studies*. Princeton University Press, 1990.

[KS91] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues and monodromy*, volume 45 of *Colloquium Publications*. American Mathematical Society, 1991.

[KS14] Emmanuel Kowalski and William F. Sawin. Kloosterman paths and the shape of exponential sums. *Compos. Math.*, 2014. To appear.

[Lam13] Youness Lamzouri. The distribution of short character sums. *Math. Proc. Cambridge Philos. Soc.*, 155(2):207–218, 2013.

[Lar90] Michael Larsen. The normal distribution as a limit of generalized Sato-Tate measures. Unpublished note, http://mlarsen.math.indiana.edu/~larsen/papers/gauss.pdf, 1990.

[LZ12] Youness Lamzouri and Alexandru Zaharescu. Randomness of character sums modulo m. *J. Number Theory*, 132(12):2779–2792, 2012.

[Mac95] Ian Macdonald. *Symmetric functions and Hall polynomials*. Oxford Mathematical Monographs. Oxford University Press, second edition, 1995.

[Mic98] Philippe Michel. Minorations de sommes d'exponentielles. *Duke Math. J.*, 95(2), 1998.

[MZ11] Kit-Ho Mak and Alexandru Zaharescu. The distribution of values of short hybrid exponential sums on curves over finite fields. *Math. Res. Lett.*, 18(1):155–174, 2011.

[PG16] Corentin Perret-Gentil. *Probabilistic aspects of short sums of trace functions over finite fields*. PhD thesis, ETH Zürich, 2016.

[Pol14] D.H.J. Polymath. New equidistribution estimates of Zhang type. *Algebra Number Theory*, 8(9), 2014.

[Pro90] Robert A. Proctor. A Schensted algorithm which models tensor representations of the orthogonal group. *Canad. J. Math.*, 42(1):28–49, 1990.

[PV04] Luc Pastur and Vladimir Vasilchuk. On the moments of traces of matrices of classical groups. *Comm. Math. Phys.*, 252, 2004.

[Ram95] Arun Ram. Characters of Brauer's centralizer algebras. *Pacific J. Math.*, 169(1), 1995.

[Reg81] Amitai Regev. Asymptotic values for degrees associated with strips of Young diagrams. *Adv. Math.*, 41(2):115–136, 1981.

[Sag15] SageMath. *The Sage Mathematics Software System (Version 6.10)*, 2015. http://www.sagemath.org.

[Sel92] Atle Selberg. Old and new conjectures and results about a class of Dirichlet series. *Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989) University of Salerno*, pages 367–385, 1992.

[Ser89] Jean-Pierre Serre. *Abelian ℓ-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. Addison-Wesley, 1989.

[Sun86] Sheila Sundaram. *On the combinatorics of representations of* $\mathrm{Sp}(2n, \mathbb{C})$. PhD thesis, Massachusetts Institute of Technology, 1986.

[Sun90] Sheila Sundaram. Orthogonal tableaux and an insertion algorithm for $\mathrm{SO}(2n+1)$. *J. Combin. Theory Ser. A*, 53(2):239–256, 1990.

[vdW34] Bartel Leendert van der Waerden. Die Seltenheit der Gleichungen mit Affekt. *Math. Ann.*, 109:13–16, 1934.

ETH Zürich, Department of Mathematics
E-mail address: corentin.perretgentil@{math.ethz.ch,gmail.com}