Diss. ETH No. 23625

Probabilistic aspects of short sums of trace functions over finite fields

A thesis submitted to attain the degree of
Doctor of Sciences of ETH Zürich

Presented by
Corentin Perret-Gentil-dit-Maillard

MSc in Mathematics
(Ecole polytechnique fédérale de Lausanne)

Updated version
December 2017

Accepted on the recommendation of
Prof. Emmanuel Kowalski Examiner
Prof. Philippe Michel Co-examiner

2016

Summary

This thesis investigates probabilistic questions concerning ℓ-adic trace functions over finite fields and sums thereof, under the framework of Deligne, Katz and others. These functions notably include characters of finite fields, hyper-Kloosterman sums, general exponential sums, and functions counting points on families of curves. Additionally, we consider these functions reduced modulo a prime ideal of the cyclotomic integers in which they lie.

To do so, a probabilistic model based on random walks in monodromy groups is introduced, inspired by Deligne's equidistribution theorem and recent works of Lamzouri for Dirichlet characters. Under rather generic conditions on the trace functions, we show that this model is accurate by applying Deligne's generalization of the Riemann hypothesis over finite fields.

Using the works of Katz, in particular computations of monodromy groups, it is shown that these generic conditions hold for the examples mentioned above. To compute the finite monodromy groups of hyper-Kloosterman sheaves, we extend Katz's arguments by using the theory of finite groups of Lie type, improving a result of Gabber and Nori.

Through this model, we show that short sums of trace functions over finite fields follow asymptotically a normal distribution with mean 0 when the origin varies, generalizing results of Erdős-Davenport, Mak-Zaharescu and Lamzouri. By computing and bounding moments of traces of random matrices in monodromy groups, a quantitative version can be given.

Concerning trace functions reduced modulo prime ideals in cyclotomic fields, we give an equidistribution result for values and/or shifted sums, a generalization of a result of Lamzouri-Zaharescu concerning the distribution of families of reduced sums of the Legendre symbol, and zero-density estimates for arguments where trace functions take values in certain algebraic subsets.

Résumé

Cette thèse investigue des questions probabilistes concernant les fonctions trace ℓ-adiques sur les corps finis et les sommes de celles-ci, dans le cadre des travaux de Deligne, Katz et autres. Ces fonctions incluent notamment les caractères des corps finis, les sommes de Kloosterman généralisées, des sommes exponentielles générales, et des fonctions comptant le nombre de points sur des familles de courbes. De plus, nous considérons ces fonctions réduites modulo un idéal premier des entiers cyclotomiques dans lesquels elles prennent valeurs.

Pour ce faire, un modèle probabiliste basé sur des marches aléatoires dans les groupes de monodromie est introduit, inspiré par le théorème d'équidistribution de Deligne et des travaux récents de Lamzouri pour les caractères de Dirichlet. Sous des conditions assez génériques sur les fonctions traces, nous montrons que ce modèle est précis en appliquant la généralisation par Deligne de l'hypothèse de Riemann sur les corps finis.

En utilisant les travaux de Katz, en particulier les calculs de groupes de monodromie, nous montrons que ces conditions génériques sont vérifiées pour les exemples mentionnés ci-dessus. Pour calculer les groupes finis de monodromie des faisceaux de Kloosterman généralisés, nous étendons les arguments de Katz par la théorie des groupes finis de type Lie, améliorant un résultat de Gabber et Nori.

Au travers de ce modèle, nous montrons que les sommes courtes de fonctions traces sur les corps finis suivent asymptotiquement une distribution normale avec espérance nulle quand l'origine varie, généralisant des résultats d'Erdős-Davenport, Mak-Zaharescu et Lamzouri. En calculant et bornant les moments des traces de matrices aléatoires dans les groupes de monodromie, une version quantitative peut être donnée.

Concernant les fonctions trace réduites modulo des idéaux premiers dans des entiers cyclotomiques, nous donnons un résultat d'équidistribution pour les valeurs et/ou sommes décalées, une généralisation d'un résultat de Lamzouri-Zaharescu concernant la distribution de sommes réduites du symbole de Legendre, et des estimations de zéro-densité pour les arguments où des fonctions trace prennent valeurs dans certains sous-ensembles algébriques.

Acknowledgements

I would like to express my gratitude to my doctoral advisor, Prof. Emmanuel Kowalski, for his supervision, encouragement, and for providing ideal working and learning conditions.

It is my pleasure to thank Prof. Philippe Michel for accepting to co-examine this work and for guiding my first steps in analytic number theory.

I have benefited from the pleasant and interesting atmosphere at the department of Mathematics of ETH Zürich, and I more particularly acknowledge the interactions with the members of the number theory group and its visitors. On the topics of this thesis, discussions with Dante Bonolis, Javier Fresán, Benny Löffel, Paul Nelson and Richard Pink have been helpful.

This thesis builds on the work of many others that I greatly enjoyed to study, and I wish to express my appreciation to the authors listed in the bibliography hereafter.

This work was partially supported by DFG-SNF lead agency program grant 200021L_153647.

The computations present in this document have been performed with SageMath [Sag15], including the GAP and PARI/GP systems.

Finally, I thank my friends and family for their continued and invaluable support.

Table of contents

Notations

Unless otherwise stated, the letters p and ℓ will denote distinct prime numbers and the letter q a power of p. Similarly, the letter λ will stand for an ℓ-adic valuation on a number field, while $\mathbb{F}_\lambda$ will denote a finite field of characteristic ℓ.

In the table below, we give the notations that are not recalled in the text.

$[a \dots b]$	The integer interval $[a, b] \cap \mathbb{Z}$
$e(x)$	$\exp(2\pi i x)$, for $x \in \mathbb{C}$
$\mathrm{ch}(K)$	Characteristic of a field
K^{sep}	A separable closure of a field
$\zeta_n, \mu_n(K)$	A primitive nth root of unity, resp. the group of nth roots of unity in a field K
	Finite fields
$\mathbb{F}_q$	A finite field with q elements
tr	The trace map $\mathrm{tr} : \mathbb{F}_q \to \mathbb{F}_p$
Frob_q	The geometric Frobenius in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, i.e. the inverse of the arithmetic Frobenius $a \mapsto a^q$
ψ	Unless otherwise mentioned, the standard character $\psi : \mathbb{F}_q \to \mathbb{C}$ defined by $\psi(x) = e(\mathrm{tr}(x)/p)$
	Asymptotic notations
$f = O(g)$, $f \ll g$	There exists an *implicit constant* $C > 0$ such that $\lvert f(x)\rvert \leqslant C\lvert g(x)\rvert$ for all x (or eventually asymptotically). If C depends on some parameter α, we may also write $f = O_\alpha(g)$ and $f \ll_\alpha g$
$f = \Theta(g)$	$f = O(g)$ and $g = O(f)$
$f = o(g)$, $f \sim g$	$f/g \to 0$, resp. $f/g \to 1$
	Probability theory
P	Probability of an event in a probability space
$P(\varphi(x))$	The probability $P(\{x : \varphi(x)\})$ if $\varphi(x)$ is a formula with one free variable
$(f(x))_{x \in X}$	The random variable $x \mapsto f(x)$ on the probability space X
$\mathbb{E}$, Var	Expected value (resp. variance) of a random variable
	Group theory/Representation theory
$A.B$	A group such that there is a short exact sequence $1 \to A \to A.B \to B \to 1$
$\mathfrak{S}_n$, $\mathrm{Alt}(n)$	The symmetric (resp. alternating) group on n elements
Aut, Out, Inn	Automorphism group. Outer (resp. inner) automorphism group
Stab	Stabilizer
$G^\sharp$	Set of conjugacy classes
$Z(G)$, G^{der}	Center, derived subgroup
G^0	Connected component of the identity of a topological group
$\widehat{G}$	Set of characters of irreducible representations
$D(\cdot)$	Dual of a representation
Std	Standard representation of a subgroup of GL_n
mult_1	Multiplicity of the trivial representation in a group representation

Chapter 1

Introduction

We start by reviewing the importance of sums over finite fields in analytic number theory and the questions related to them, in particular of probabilistic flavour. We then present the relevant concept of trace functions over finite fields that arose from Deligne's proof of the Weil conjectures. Finally, we introduce the problems that are treated in this thesis.

1.1. Sums over finite fields

By definition, analytic number theory uses *continuous* methods to study various *discrete* objects arising in number theory, with the recurring objective to *count* them precisely. It is then natural that sums of the form

$$S(f,E)=\sum_{x\in E} f(x), \tag{1.1}$$

for E a finite set and $f : E \to \mathbb{C}$ an "arithmetic" function, are a fundamental tool and a matter of great interest.

1.1.1. Examples. To give only a few examples:

(1) By the orthogonality relations, sums of additive or multiplicative characters of $\mathbb{F}_p$ can be used to detect congruence classes modulo p.

(2) The quadratic reciprocity law can be proved via the Gauss sums $\sum_{x\in\mathbb{F}_p^\times} \psi(x)\chi(x)$, where $\psi : \mathbb{F}_p \to \mathbb{C}^\times$ and $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ are characters.

(3) Sums of Dirichlet characters modulo p over small subsets of $\mathbb{F}_p$ provide information about the least quadratic nonresidue modulo p and subconvexity bounds for Dirichlet L-functions.

(4) The Weyl equidistribution criterion asserts (in particular) that a sequence $(a_x)_{x\in\mathbb{F}_q}$ in a compact group K, indexed by the elements of a finite field, becomes equidistributed with respect to the Haar measure as $q \to +\infty$ if and only if $\sum_{x\in\mathbb{F}_q} \chi(a_x) = o(q)$ for every nontrivial irreducible character $\chi : K \to \mathbb{C}$.

(5) The sum

$$a_p(E)=\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right)$$

of the Legendre symbol composed with a cubic polynomial is related to the number of $\mathbb{F}_p$-points of the elliptic curve $E : y^2 = x^3 + ax + b$, for $a, b \in \mathbb{F}_p$. Indeed, we have $a_p(E) = p + 1 - |E(\mathbb{F}_p)|$.

(6) Hyper-Kloosterman sums

$$\mathrm{Kl}_{n,q}(a) = \frac{(-1)^{n-1}}{q^{(n-1)/2}} \sum_{\substack{x_1,\dots,x_n\in\mathbb{F}_q^\times \\ x_1\dots x_n=a}} e\left(\frac{\mathrm{tr}(x_1+\cdots+x_n)}{p}\right) \quad (a\in\mathbb{F}_q^\times) \tag{1.2}$$

were used by Kloosterman when $n = 2$ to study the number of representations of an integer by an integral positive-definite quarternary quadratic form, and admit deep links with the spectral theory of automorphic forms.

As is apparent in these examples, the set of summation E is often a subset of the points of a variety over a finite field, either because finite fields are naturally part of the question (as in Example (5)), or because the problem can be reduced to the consideration of congruences modulo p, and $\mathbb{Z}/p \cong \mathbb{F}_p$ (as for Kloosterman's work[1] in Example (6)). As we will see, this allows the use of powerful techniques from algebraic geometry, and this is the setting we are going to consider from now on.

1.1.2. Bounds. Sums of the form (1.1) often exhibit cancellation due to oscillations, and as a general phenomenon we can expect *square-root cancellation* with respect to the size of the summation set, i.e.

$$\sum_{x\in E} f(x) \ll |E|^{1/2}. \tag{1.3}$$

As is the case for the last four examples above, a major goal is often to find sharp asymptotic bounds.

Examples. For example, we have the famous *Weil bound*

$$|\mathrm{Kl}_{2,p}(a)| \leqslant 2\sqrt{p} \quad (a\in\mathbb{F}_p) \tag{1.4}$$

for Kloosterman sums and the *Hasse bound*

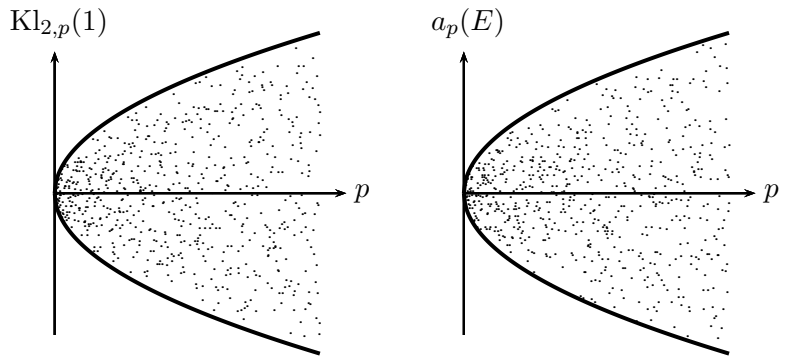
$$\big|a_p(E)\big| \leqslant 2\sqrt{p} \tag{1.5}$$

for the number of $\mathbb{F}_p$-points of an elliptic curve E over the finite field $\mathbb{F}_p$. The weaker bound $|\mathrm{Kl}_{2,p}(a)| \leqslant 2p^{3/4}$ led Kloosterman to his result on quarternary quadratic forms, while the Hasse bound provides an asymptotic expression for the number of rational points of E.

The Weil conjectures. The two estimates above follow from the *Riemann hypothesis for curves over finite fields*, conjectured by Artin and solved by Weil. This is a special case of the Weil conjectures.

Complete and incomplete sums. As we have seen in the examples above, we are often interested in "incomplete" sums, namely sums over (small) subsets of a variety over a finite field. Since techniques from algebraic geometry only allow to estimate "complete" sums (i.e. over the whole variety), the estimate of the former is often reduced to that of the latter by techniques such as completion (as in the Pólya-Vinogradov inequality).

[1] More precisely, Kloosterman needs to bound sums of the form $\sum_{x\in(\mathbb{Z}/n)^\times} e((x+x^{-1})/n)$. This can be reduced to the case of n being a prime power, and explicit evaluations are available when n is a nonprime prime power.



(a) The Weil bound (b) The Hasse bound

FIGURE 1.1: Bounds on exponential sums: the Weil bound for the (real-valued) Kloosterman sum $\mathrm{Kl}_{2,p}(1)$ and the Hasse bound for the elliptic curve $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_p$, for $p < 5 \cdot 10^3$. In bold, the graph of $y = 2\sqrt{p}$.

1.1.3. Distribution of families. More generally than bounding them, we may want to understand the distribution of the values of sums of the form (1.1) in families.

When f or the sum itself is bounded, we may normalize and study the distribution in a compact set.

Angles of exponential sums. For families of complete sums, this question was studied by authors such as Kummer, Hasse, Heath-Brown and Patterson (cubic Gauss sums), Deligne (Gauss sums), Katz (Kloosterman sums) or Duke, Friedlander and Iwaniec (Salié sums).

For example, by the Weil bound (1.4) and the Hasse bound (1.5), there exist angles $\theta_{a,p}, \theta_{E,p} \in [0, \pi]$ such that

$$\begin{aligned} \mathrm{Kl}_{2,p}(a) &= 2\sqrt{p}\cos\theta_{a,p} \quad (a \in \mathbb{F}_p) \\ p + 1 - |E(\mathbb{F}_p)| &= 2\sqrt{p}\cos\theta_{E,p}, \end{aligned}$$

and the study of the distribution of

$$\{\theta_{1,p} : p \text{ prime}\} \text{ or } \{\theta_{a,p} : a \in \mathbb{F}_p\}, \quad \text{resp. } \{\theta_{E,p} : p \text{ prime}\}$$

in $[0, \pi]$ is the *Sato-Tate conjecture* for Kloosterman sums, respectively for the elliptic curve E.

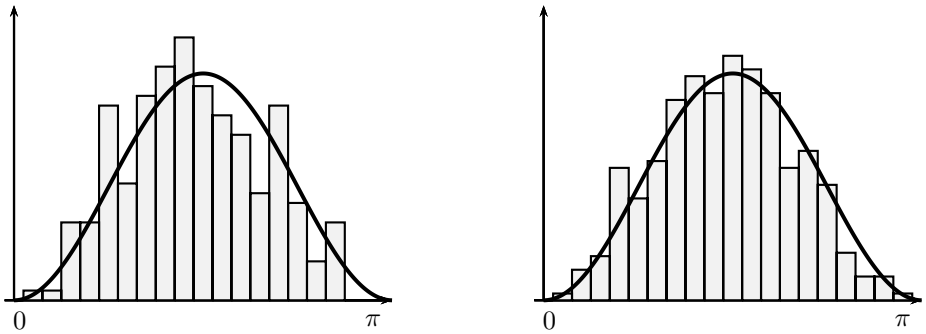
Distribution of short sums. Let $\chi_p : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a multiplicative character and for integers $x, H \in [0 \dots p)$, consider the sum

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

of length H starting at x.

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

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



(a) Kloosterman sum (b) Elliptic curve

FIGURE 1.2: Distribution of exponential sums: histograms of the angles $(\theta_{x,p})_{x\in\mathbb{F}_p}$ of the Kloosterman sums $\mathrm{Kl}_{2,p}$ for $p = 104743$, and of the angles $(\theta_p)_{p\leqslant 5000}$ of the elliptic curve $E : y^2 = x^3 + x + 1$, against the Sato-Tate distribution in bold.

(with respect to the uniform measure on $\mathbb{F}_p$) converges in law to a normal distribution with mean 0 and unit variance when

$$p, H \to \infty \text{ with } \log H = o(\log p). \tag{1.6}$$

This was generalized by Mak-Zaharescu [MZ11] and Lamzouri [Lam13] to all Dirichlet characters: if χ_p is a non-real Dirichlet character, the random variable $(S(\chi_p, x, H)/\sqrt{H/2})_{x\in\mathbb{F}_p}$ 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 $p, H \to \infty$ under the same condition (1.6).

These interesting results belong to the realm of probabilistic number theory. In particular, Lamzouri uses a *probabilistic model* where the values of a multiplicative character of order d are modeled as independent random variables uniformly distributed on the unit circle or in the set of dth roots of unity. This model is shown to be accurate (in the sense of convergence in law) by bounding an exponential sum through the use of Weil's Riemann hypothesis for curves over finite fields.

1.2. Trace functions over finite fields

1.2.1. Deligne's proof of the Weil conjectures. Using the machinery of ℓ-adic cohomology developed by Grothendieck, Deligne [Del74] proved the general Weil conjectures for smooth projective algebraic varieties over a finite field, allowing to estimate the number of rational points on the latter (see [Del74, Section 8]).

As a (nontrivial) application [Del69], he notably obtained the Ramanujan-Petersson conjecture for holomorphic modular forms of weight $\geqslant 2$.

1.2.2. Generalization and applications to sums of trace functions. The subsequent paper [Del80] gives a deep generalization of the Weil conjectures, providing in particular a way to estimate sums of the form (1.1) when E is an algebraic variety over $\mathbb{F}_q$ and $f : E \to \mathbb{C}$ is the *trace function of a "normalized" ℓ-adic sheaf on E* (this appears in [Del77, Exposé 6]).

We will define precisely the latter in the next chapter, but we mention for now that they notably cover:

(1) Additive and multiplicative characters of a finite field.

(2) The sum, product and complex conjugate of other trace functions.

(3) The sum of a trace function over the solutions of a polynomial equation.

(4) The polynomial change of variable of a trace function.

(5) Most interestingly, the Fourier transform of another trace function (under some technical conditions), by deep works of Grothendieck, Deligne and Laumon.

In particular, this includes all the examples of the first section.

Sums of trace functions. If f is a trace function on E associated to a geometrically irreducible normalized sheaf, Deligne's work shows that the sum (1.1) is

$$S(f, E) = Cq^d + O\left(q^{d-1/2}\right),$$

where $d = \dim(E)$, and $C = 1$ if the sheaf is geometrically trivial (in which case f is constant), $C = 0$ otherwise. The implicit constant in the error term is a sum of Betti numbers for the corresponding étale cohomology groups, which often does *not* depend on q in applications.

In this case, square-root cancellation (1.3) amounts to $C = 0$ and the vanishing of the cohomology groups for $i > d$.

When E is a projective curve, which is the setting we will mainly consider, the above becomes

$$S(f, E) = Cq + O(\sqrt{q}),$$

and the implicit constant is bounded by the "conductor" of the sheaf, which again often does not depend on q. Square-root cancellation then amounts to $C = 0$.

1.2.3. Applications to analytic number theory. The above "ℓ-adic formalism" provides a very general and flexible setting to control exponential sums over finite fields.

Deligne's applications. For example, Deligne obtained the bound

$$\mathrm{Kl}_{n,q}(a) \ll nq^{\frac{n-1}{2}} \quad (a \in \mathbb{F}_q)$$

for hyper-Kloosterman sums (1.2), generalizing the Weil bound (1.5), after realizing the former as trace functions by means of a powerful *ℓ-adic Fourier transform*. By the Weyl criterion, this implies that the angles of Gauss sums of primitive characters modulo p are equidistributed in $[0, \pi]$ as $p \to +\infty$ (see [IK04, Theorem 21.6]).

Distribution and monodromy groups. By computing the *monodromy groups* of Kloosterman sheaves, Katz [Kat88] proved the *vertical Sato-Tate law for Kloosterman sums*, i.e. that the set of angles $\{\theta_{a,p} : a \in \mathbb{F}_p\}$ becomes equidistributed in $[0, \pi]$ according to the Sato-Tate measure $\frac{2}{\pi}\sin^2\theta d\theta$ as $p \to +\infty$.

We will soon see that monodromy groups of ℓ-adic sheaves are a fundamental tool to understand the distribution of the values of trace functions. In particular, *Deligne's equidistribution theorem* states that a "natural" family of ℓ-adic sheaves on a variety always satisfies an equidistribution result with respect to the Haar measure of a maximal compact subgroup of the monodromy group.

Bounds on exponential sums. The papers of Friedlander-Iwaniec [FI85] and Conrey-Iwaniec [CI00] show the strength of these techniques to handle complex exponential sums appearing in analytic number theory. In particular, the second one treats exponential sums over a variety of dimension 2.

Katz, Laumon and Fouvry have also obtained very general results about the size of "generic" exponential sums over algebraic varieties (see [FK01]).

More generally, we refer to [IK04, Chapter 11] for a survey of applications of Deligne's work in analytic number theory.

The works of Fouvry-Kowalski-Michel and others. New applications in number theory have recently been developed by Fouvry, Kowalski, Michel and collaborators, and some of them are surveyed in [FKM14b].

For example, the results of [FKM15a] allow to estimate "correlation sums" which appeared in works of Friedlander-Iwaniec, Iwaniec, Pitt and Munshi.

Most recently, Polymath8 [Pol14] showed how to use Deligne's formalism to significantly improve Type III estimates in Zhang's work on bounded gaps between primes, in connection with the work of Friedlander-Iwaniec mentioned above.

A new feature of these is the full use of the ℓ-adic formalism, with the authors not settling for merely using the examples of applications from algebraic geometers.

1.2.4. Probabilistic questions for families of trace functions. In this thesis, we will be interested in *probabilistic aspects of (short) sums of trace functions over finite fields in "coherent families"*. In particular, we will develop and use a probabilistic model inspired by Deligne's equidistribution theorem and the articles [Lam13], [LZ12] mentioned above.

We will make the notion of "coherent families" precise in due time. Mostly, they are families indexed by finite fields $\mathbb{F}_q$ such that:

(1) The "conductor", measuring the complexity of the underlying sheaf, is bounded independently from q.

(2) The arithmetic and geometric monodromy groups coincide, have fixed type (e.g. in the sense of the classification of semisimple Lie groups/algebras), and are "large".

(3) There is a property of independence of additive shifts.

These conditions are rather generic (but the determination of the monodromy groups may be difficult). These families include for example:

(1) Dirichlet characters composed with the reduction of rational polynomials.

(2) Hyper-Kloosterman sums (1.2) and hypergeometric sums of fixed rank.

(3) General exponential sums of the form

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

for $f, g, h \in \mathbb{Q}(X)$ rational functions and χ a multiplicative character on $\mathbb{F}_q^\times$, such as Birch sums or sums considered by Fouvry-Michel.

(4) Functions counting points on families of curves over $\mathbb{F}_q$ parametrized by varieties over $\mathbb{F}_q$.

To show that our model is accurate (in the sense of convergence in law), we will use techniques similar to those surveyed in [FKM15b] to estimate *sums of products* of trace functions.

In the next two sections, we survey our results.

1.3. Distribution of sums of trace functions

The first part of this thesis generalizes to trace functions the results of Erdős-Davenport, Mak-Zaharescu and Lamzouri presented above. More precisely, we show:

Theorem. *Let $(t_q : \mathbb{F}_q \to \mathbb{C})_q$ be a coherent family of trace functions and for $I_q \subset \mathbb{F}_q$, $x \in \mathbb{F}_q$, let*

$$S(t_q, x, I_q) = S(t_q, I_q + x),$$

where $I_q + x = \{y + x : y \in \mathbb{F}_q\}$ is the translate of I_q by x. If $\mathcal{F}_q$ is I_q-compatible for all q, the random variable

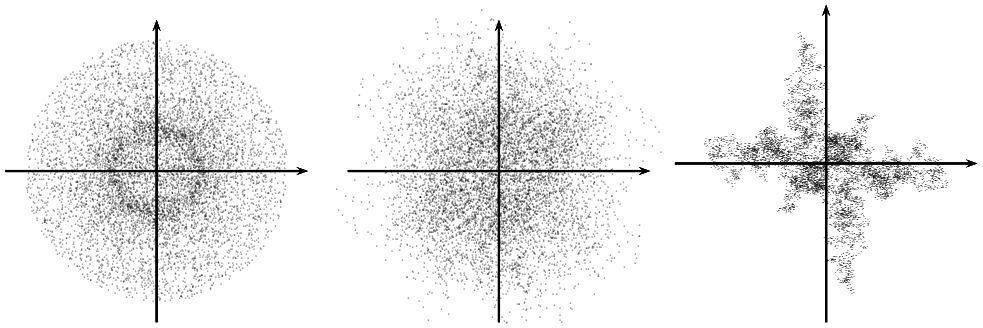
$$\left(\frac{S(t_q, x, I_q)}{\sqrt{|I_q|}}\right)_{x\in\mathbb{F}_q}$$

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

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

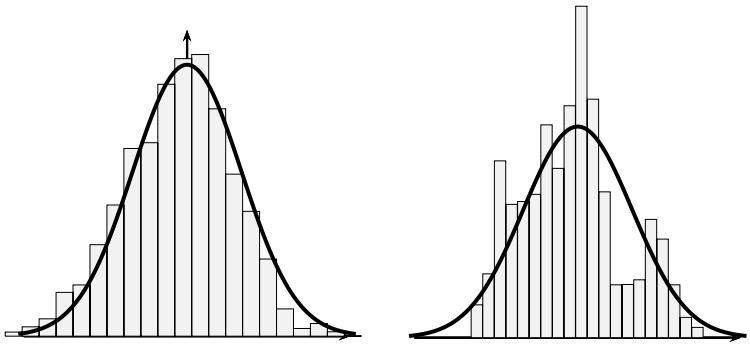
when $q, |I_q| \to +\infty$ with $\log|I_q| = o(\log q)$.

Note that we do not require that I_q is an interval, but it can rather be *any* small subset.



(a) $H = 3$ (b) $H = 50$ (c) $H = 1000$

FIGURE 1.3: Distribution of sums of trace functions for a Dirichlet character modulo $p = 7927$ of order $p - 1$.



(a) $H = 100$ (b) $H = 1300$

FIGURE 1.4: 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.

1.3.1. Probabilistic model. To prove this theorem, we extend and adapt the method of [Lam13]. The values of the trace functions are modeled by independent random variables distributed like traces of random matrices uniform in maximal compact subgroups of the monodromy groups (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.

1.3.2. Examples. By the examples of coherent families above, this holds in particular for multiplicative characters (the classical case), hyper-Kloosterman and hypergeometric sums, rather general exponential sums, and functions counting points on families of curves.

1.3.3. 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 $(S(\chi_p, x, H))_{x\in\mathbb{F}_p}$ asymptotically, and in turn, this 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 the moments of traces of random matrices in classical groups are also Gaussian as the rank tends to infinity, as already remarked and exploited for example by Larsen [Lar90] and Diaconis-Shahshahani [DS94]. More precisely, we moreover need bounds on high order moments with respect to the rank. We also improve the method of Lamzouri, which is necessary in the non-real-valued case, by using a generalization of the Berry-Esseen inequality from [BRR86].

Theorem. *Under the notations and hypotheses of the above theorem, for any $\varepsilon \in (0, 1/2)$ and 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*

$$P\left(\frac{S(t_q, x, I)}{\sqrt{|I|}} \in A\right) = \frac{|\{x \in \mathbb{F}_q : S(t_q, x, I)/|I|^{1/2} \in A\}|}{q}$$

is given by

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

when q, $|I| \to \infty$ with under the range $\log|I| = o(\log q)$ if t_q is real-valued and $|I| = o\left((\log q)^{\frac{3}{2(1+\varepsilon)}}\right)$ otherwise, where $\mathcal{N}$ is a normal random variable in $\mathbb{C}$ with mean 0 and covariance matrix as in the previous theorem. As the rank of the monodromy group grows (or in the real-valued case), the exponents $2/5$ and $3/2$ can be replaced by $1/2$ and 1.

1.4. Trace functions with values in the cyclotomic integers

In the second part of this thesis, we operate a shift in paradigm in the way we consider trace functions, which opens new questions about the distribution of their values, from infinite compact groups to finite groups.

1.4.1. Trace functions in cyclotomic fields, integers, and residue fields.

Cyclotomic fields. Until that point, we will have considered trace functions $f : E \to \mathbb{C}$ as functions with values in the complex numbers, arising from ℓ-adic sheaves of $\overline{\mathbb{Q}}_\ell$-modules on curves over a finite field (recall that $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ as fields).

However, exponential sums actually take values in *cyclotomic fields*. For example, a multiplicative character of $\mathbb{F}_p$ of order d has image in $\mathbb{Q}(\zeta_d) \subset \mathbb{Q}(\zeta_{p-1})$ for $\zeta_d \in \mathbb{C}^\times$ a primitive dth root of unity, while an additive character has image in $\mathbb{Q}(\zeta_p)$.

More generally, the functions we can form from additive and multiplicative characters of a finite field $\mathbb{F}_q$ of characteristic p by taking sums, products, and Fourier transforms, will take values in

$$\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_{p-1}) = \mathbb{Q}(\zeta_{p(p-1)}).$$

Correspondingly, most of the trace functions that we can naturally form with the corresponding operations on the level of sheaves take values in cyclotomic fields.

Fisher [Fis95] extended Katz's vertical Sato-Tate law for Kloosterman sums (see above) to this point of view by studying their distribution as elements of $K = \mathbb{Q}(\zeta_p)$ via the Minkowski embedding $\mathbb{Q}(\zeta_p) \to \mathbb{R}^{p-1}$, with the hope of getting results on their distinctness. His equidistribution result with respect to the product of the Sato-Tate measure amounts to showing that it is possible to (explicitly) construct for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ an ℓ-adic sheaf whose trace function corresponds to the σ-conjugate of the Kloosterman sum.

Cyclotomic integers and residue fields. A step further is to consider exponential sums/trace functions as having values in *cyclotomic integers*, say $\mathcal{O} = \mathbb{Z}[\zeta_d]$ for some $d \geqslant 1$. This is clearly the case for all the examples we have mentioned so far, up to the normalization. Wan [Wan95] took such a point of view and studied the minimal polynomial of Kloosterman sums, improving some of Fisher's results.

By reducing modulo a prime ideal $\mathfrak{q} \trianglelefteq \mathcal{O}$, we can study the distribution of their values in the finite residue field $\mathcal{O}/\mathfrak{q}$.

1.4.2. Translation in the ℓ-adic formalism. We will be able to continue using the techniques of Deligne and Katz to handle this setting because the sheaves considered happen to be themselves definable as *sheaves of $\mathcal{O}_\lambda$-modules*, where λ is the ℓ-adic valuation corresponding to a prime ideal $\mathfrak{q} \trianglelefteq \mathcal{O}$ above ℓ. Indeed, this is the case for additive and multiplicative characters, and sums, products, and even Fourier transforms can be defined on the level of $\mathcal{O}_\lambda$-modules. The reduction of the trace function modulo $\mathfrak{q}$ then corresponds to the trace function of the reduced sheaf of $\mathcal{O}_\lambda/\mathfrak{q}\mathcal{O}_\lambda \cong \mathbb{F}_\lambda$-modules.

For simplicity, we will focus in this introduction on multiplicative characters and Kloosterman sums, but the same results will hold for all coherent families of sheaves of $\mathbb{F}_\lambda$-modules.

1.4.3. Probabilistic model. As in the first part, we can set up a probabilistic model for the values of reduced trace functions $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ as independent random variables distributed like traces of random matrices in monodromy groups, which are now subgroups of $\mathrm{GL}_n(\mathbb{F}_\lambda)$.

Using Deligne's analogue of the Riemann hypothesis over finite fields, we can again show that this model is accurate (in terms in convergence in law), with an explicit error term for the densities.

Determinations of monodromy groups. As a preliminary step, we determine the $\mathbb{F}_\lambda$-monodromy groups of Kloosterman sheaves for ℓ large enough depending only on the rank:

Theorem. *Let $n \geqslant 2$ be an integer coprime with p. If $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$ and λ is an ℓ-adic valuation on*[2] *$\mathcal{O} = \mathbb{Z}[\zeta_{4p}]$ with $(n, [\mathbb{F}_\lambda : \mathbb{F}_\ell]) = 1$, then the*

[2] We consider normalized Kloosterman sheaves, so we must ensure that $q^{(n-1)/2}$ belongs to the ring of definition. By the evaluation of quadratic Gauss sums, $\mathbb{Z}[\zeta_p, \sqrt{p}] \leqslant \mathbb{Z}[\zeta_{4p}]$.

monodromy of the Kloosterman sheaf $\mathcal{K}l_n$ of $\mathcal{O}_\lambda$-modules is

$$G_{\mathrm{geom}}(\mathcal{K}l_n) = G_{\mathrm{arith}}(\mathcal{K}l_n) = \begin{cases} \mathrm{SL}_n(\mathcal{O}_\lambda) & : n \text{ odd} \\ \mathrm{Sp}_n(\mathcal{O}_\lambda) & : n \text{ even.} \end{cases}$$

In particular, the result holds for a set of valuations λ of density 1 depending only on n.

This was already known by results of Gabber, Larsen and Nori, but for $\mathbb{F}_\lambda = \mathbb{F}_\ell$ with ℓ large enough depending on q and with an ineffective constant, which would have been unusable for our applications.

To prove this theorem, we use the theory of finite groups of Lie type to extend Katz's proof for the continuous monodromy. Specifically, we appeal to the classification of maximal subgroups of finite classical groups, a theorem on Larsen-Pink on finite subgroups of algebraic groups, and results on representations of finite groups of Lie type in various characteristics. This allows to reduce to the descent of a classification of subgroups of classical groups over algebraically closed fields containing regular unipotent elements. Actually, we will see that Katz's theorem can also be deduced from the latter.

Computations in the model. The next task is to study random walks in the monodromy groups we consider, which we do by using results of D.S. Kim (for classical groups) and of Heath-Brown, Konyagin, Bourgain and others about sums of additive characters over multiplicative subgroups of finite fields.

1.4.4. Equidistribution of values of trace functions and shifted short sums thereof. The first outcome is an equidistribution result for (in particular) Kloosterman sums reduced modulo an ideal of $\mathbb{Z}[\zeta_{4p}]$ and shifted sums of multiplicative characters of order d reduced modulo an ideal of $\mathbb{Z}[\zeta_d]$.

Proposition (Kloosterman sums)**.** *For $n \geqslant 2$, and $\mathfrak{q} \trianglelefteq \mathbb{Z}[\zeta_{4p}]$ a prime ideal above a prime $\ell \gg_n 1$ distinct from p with $\ell \equiv 1 \pmod 4$, let*

$$\mathrm{Kl}_{n,q} : \mathbb{F}_q \to \mathbb{Z}[\zeta_{4p}]_{\mathfrak{q}} \to \mathbb{Z}[\zeta_{4p}]_{\mathfrak{q}}/\mathfrak{q} \cong \mathbb{F}_\lambda$$

be the reduction modulo $\mathfrak{q}$ of the (normalized) Kloosterman sum over $\mathbb{F}_q$. For any $I \subset \mathbb{F}_q$ of size L, the probability

$$P\Big(S(\mathrm{Kl}_{n,q}, I + x) \equiv a\Big)$$

is given by

$$\frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O_n\left(|\mathbb{F}_\lambda|^{-L^{\frac{n^2-1}{2}}} + |\mathbb{F}_\lambda|^{L^{\frac{n^2+n-2}{2}}+n(n-1)-1} q^{-\frac{1}{2}}\right) & \text{if } n \text{ odd} \\ O_n\left(|\mathbb{F}_\lambda|^{-L^{\frac{n(n+2)}{8}}} + |\mathbb{F}_\lambda|^{L^{\frac{n(n+2)}{4}}+\frac{n^2-2}{2}} q^{-\frac{1}{2}}\right) & \text{if } n \text{ even} \end{cases}$$

uniformly for all $a \in \mathbb{F}_\lambda$. In particular, for $L = 1$, this gives an asymptotic expression (under appropriate ranges) for the probability $P\left(\mathrm{Kl}_{n,q}(x) \equiv a\right)$.

Proposition (Multiplicative characters). *Let $d \geqslant 2$ be an integer, $\mathfrak{q} \trianglelefteq \mathbb{Z}[\zeta_d]$ be a prime ideal,*

$$\chi : \mathbb{F}_q^\times \to \mathbb{Z}[\zeta_d] \to \mathbb{Z}[\zeta_d]/\mathfrak{q} \cong \mathbb{F}_\lambda$$

be the reduction modulo $\mathfrak{q}$ of a multiplicative character of order d, and $f \in \mathbb{Q}(X)$ whose poles and zeros have order not divisible by d. Let $\delta \in (0,1)$ be such that[3]

$$\frac{d}{(d, |F^\times|)} \geqslant |\mathbb{F}_\lambda|^\delta$$

for every subfield $F \not\leqslant \mathbb{F}_\lambda$ with $\log_\ell |F| \mid \log_\ell |\mathbb{F}_\lambda|$.

Let $I \subset \mathbb{F}_q$. If $f \neq X$, we assume moreover that $|I| = 1$ or $I \subset [1 \dots p/\deg(f))^e \subset \mathbb{F}_p^e \cong \mathbb{F}_q$. Then there exists $\alpha = \alpha(\delta) > 0$ such that

$$P\Big(S(\chi \circ f, I + x) \equiv a\Big) = \frac{1}{|\mathbb{F}_\lambda|} + O_f\left(\frac{1}{|\mathbb{F}_\lambda|^{L\alpha}} + \frac{Ld^{L+1}}{q^{1/2}|\mathbb{F}_\lambda|^{\min(L\alpha,1)}}\right)$$

uniformly for all $a \in \mathbb{F}_\lambda$. In particular,

$$P\Big(\chi(f(x)) \equiv a\Big) \ll_f \frac{1}{|\mathbb{F}_\lambda|^\alpha}\left(1 + \frac{d^2}{q^{1/2}}\right).$$

If $\delta > 1/2$, we can choose $\alpha(\delta) = \delta - 1/2$. If $\mathbb{F}_\lambda = \mathbb{F}_\ell$, we can choose

$$\alpha(\delta) = \begin{cases} \frac{3\delta-1}{8} & \text{if } \delta \in (1/3, 1/2] \\ \frac{5\delta-2}{8} & \text{if } \delta \in (1/2, 2/3] \\ \delta - \frac{2}{3} & \text{if } \delta \in (2/3, 1]. \end{cases}$$

The choice of the various parameters will be carefully studied in due time. The condition on I if $f \neq X$ is for example satisfied if $I = \{1, \dots, L\}$ with $L < p/\deg(f)$.

Moreover, this also applies to point-counting functions on families of hyperelliptic curves.

1.4.5. Distribution of families of reduced short sums. In [LZ12], Lamzouri and Zaharescu studied the distribution of a family of short sums of the Legendre symbol $\chi_p : \mathbb{F}_p \to \{\pm 1\} \cong \mathbb{Z}[\zeta_2]$ reduced modulo an integer $\ell \geqslant 2$. Specifically, they show that

$$\frac{|\{1 \leqslant k \leqslant p : S(\chi_p, [1 \dots k]) \equiv a \pmod{\ell}\}|}{p} = \frac{1}{\ell} + O\left(\left(\frac{\ell}{\log p}\right)^{\frac{1}{2}}\right)$$

uniformly with respect to $a \in \mathbb{Z}/\ell$. As in [Lam13], a probabilistic model is used (with sums of independent random variables uniformly distributed in $\{\pm 1\}$), whose accuracy is proved through a bound derived from the Riemann hypothesis for curves over finite fields.

We generalize this result to the distribution of short families of multiplicative characters of any order and of Kloosterman sums, reduced modulo a prime ideal as above.

The first example concerns shifts of small subsets as in the complex-valued case. The Gaussian distribution becomes uniform in $\mathbb{F}_\lambda$:

[3] If $\mathbb{F}_\lambda = \mathbb{F}_\ell$, if d is prime, or if $\delta > 1/2$, the condition is simply $d \geqslant |\mathbb{F}_\lambda|^\delta$.

Proposition (Shifts of small subsets)**.** *Let $\varepsilon \in (0, 1/4)$ and let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be either:*

- *$t = \mathrm{Kl}_{n,q}$ the Kloosterman sum of rank $n \geqslant 2$ reduced modulo a prime ideal of $\mathbb{Z}[\zeta_{4p}]$ above a prime $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$.*
- *$t = \chi \circ f$ as in the previous proposition.*

Let $E \subset \mathbb{F}_q$ be a "small"[4] subset. Then

$$\frac{|\{x \in \mathbb{F}_q : S(t, E + x) \equiv a\}|}{q} = \frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O_{\varepsilon,n}\left(\frac{1}{q^{1/4-\varepsilon}} + \left(\frac{|E|\log|\mathbb{F}_\lambda|}{\log q}\right)^{\frac{1}{2}}\right) \\ O_{\varepsilon,f}\left(\frac{1}{q^{1/4-\varepsilon}} + \left(\frac{|E|\log d}{\log q}\right)^{\frac{1}{2}}\right) \end{cases}$$

for Kloosterman sums, respectively multiplicative characters, uniformly for all $a \in \mathbb{F}_\lambda$.

The second example generalizes the result of [LZ12] to all multiplicative characters:

Proposition (Partial intervals)**.** *Let $\varepsilon \in (0, 1/4)$ and let $t = \chi \circ f : \mathbb{F}_p \to \mathbb{F}_\lambda$ be as above. Then*

$$\frac{|\{1 \leqslant k \leqslant p : S(\chi_p \circ f, [1 \dots k]) \equiv a\}|}{p} = \frac{1}{|\mathbb{F}_\lambda|} + O_{\varepsilon,f}\left(\frac{1}{p^{1/4-\varepsilon}} + \left(\frac{\log d}{\log p}\right)^{\frac{1}{2}}\right)$$

uniformly for all $a \in \mathbb{F}_\lambda$.

The method does not allow this to be generalized to Kloosterman sums, but we can nonetheless do the following:

Proposition (Partial intervals with shifts of small subsets)**.** *We consider the situation of the first proposition above with $\mathbb{F}_q = \mathbb{F}_{p^e} \cong \mathbb{F}_p^e$ and we let $E_2, \dots, E_e \subset \mathbb{F}_p$ be "small" subsets. Then the density*

$$\frac{|\{(x_1, \dots, x_e) \in \mathbb{F}_p^e \cong [1 \dots p]^e : S(t, [1 \dots x_1] \times \prod_{i=2}^e (E_i + x_i)) \equiv a\}|}{q}$$

(with respect to any $\mathbb{F}_p$-basis of $\mathbb{F}_q$) is equal to

$$\frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O_{\varepsilon,n}\left(\frac{1}{q^{1/4-\varepsilon}} + \left(\frac{|E|\log|\mathbb{F}_\lambda|}{\log q}\right)^{\frac{1}{2}}\right) \\ O_{\varepsilon,f}\left(\frac{1}{q^{1/4-\varepsilon}} + \left(\frac{|E|\log d}{\log q}\right)^{\frac{1}{2}}\right) \end{cases}$$

for Kloosterman sums, respectively multiplicative characters, uniformly for all $a \in \mathbb{F}_\lambda$.

Again, these examples also apply to functions counting points on families of hyperelliptic curves.

[4] This will be made more precise later on.

1.4.6. Application of the large sieve. As a last application of our computation of the $\mathbb{F}_\lambda$-monodromy groups of Kloosterman sheaves, we get zero-density estimates for arguments of hyper-Kloosterman sums with values in some algebraic subset of the cyclotomic integers. The case of point-counting functions on families of hyperelliptic curve was the subject of [Kow06a] and [Kow08].

Proposition. *Let $n \geqslant 2$ be an integer and let $\varepsilon > 0$. For $m \geqslant 2$ coprime to p, we have*

$$P\Big(\mathrm{Kl}_{n,q}(x) \in \mathbb{Q}(\zeta_{4p})^m\Big) \ll_{m,\varepsilon} \frac{p^\varepsilon \log q}{B_n q^{1/(2B_n)}} \to 0,$$

when $q = p^e \to +\infty$ with $e \geqslant 16B_n$, where $B_n = \frac{2n^2+n-1}{2}$ if n is odd and $B_n = \frac{2n^2+3n+4}{4}$ if n is even, and $\mathbb{Q}(\zeta_{4p})^m$ is the set of mth powers in $\mathbb{Q}(\zeta_{4p})$.

More generally:

Proposition. *Let $n \geqslant 2$ be an integer and let $\varepsilon > 0$. For almost all $f \in \mathbb{Z}[X]$ of fixed degree, we have*

$$P\Big(\mathrm{Kl}_{n,q}(x) \in f(\mathbb{Q}(\zeta_{4p}))\Big) \ll_{\varphi,\varepsilon} \frac{p^\varepsilon \log q}{B_n q^{1/(2B_n)}} \to 0$$

when $q = p^e \to +\infty$ with $e \geqslant 16B_n$, for B_n as above.

This can further be extended to definable subsets of $\mathbb{Q}(\zeta_{4p})$ (i.e. defined by a first-order formula in the language of rings), under some technical conditions.

1.5. Structure

This thesis is structured as follows:

- In the first preliminary chapter, we define precisely ℓ-adic trace functions over finite fields and survey their properties. In particular, we recall the application of Deligne's generalization of the Riemann hypothesis over finite fields to the estimation of sums of trace functions. After a presentation of the ℓ-adic Fourier transform, we give the examples of trace functions we will consider and their properties.

- In the second chapter, we recall the definition and use of monodromy groups, notably through Deligne's equidistribution theorem. We survey Katz's computation of the monodromy of ℓ-adic Fourier transforms such as Kloosterman sheaves ([Kat88], [Kat90]). Finally, we consider $\mathbb{F}_\lambda$-monodromy groups and prove our result about the finite monodromy groups of hyper-Kloosterman sheaves.

- In the third chapter, we set up probabilistic models for trace functions, reduced modulo an ideal of a cyclotomic field or not, inspired by Deligne's equidistribution theorem and the articles of Lamzouri [Lam13] and Lamzouri-Zaharescu [LZ12]. In order to be able to prove their accuracy in the next chapters, we survey the methods for estimating sums of products in the ℓ-adic formalism, following [FKM15b]. We review the Goursat-Kolchin-Ribet criterion of Katz for complex Lie groups of positive dimension and give an analogue for finite quasisimple groups. We can then define the "coherent

families" we will consider from that point. Finally, we state general criteria on the ramification of sheaves so that the latter are part of a coherent family. Altogether, we try to give a presentation which is as unified as possible between the complex and finite cases.

– The fourth chapter is dedicated to proving our results generalizing the works of Erdős-Davenport and Lamzouri. We start by showing that the probabilistic model is accurate and we compute moments in the model before concluding for the qualitative version. We finally prove the quantitative version by adapting the arguments of Lamzouri. In particular, we need to estimate moments of traces of random matrices in classical groups.

– In the fifth and final chapter, we prove the results mentioned above about trace functions reduced modulo an ideal of a cyclotomic field. Again, we first prove the accuracy of the probabilistic model, before carrying out computations in the latter. The three applications (equidistribution, distribution of families of short sums, and use of the large sieve) are then treated in the subsequent sections.

As a general principle, we try to give a self-contained exposition (excluding Chapter 2). We give references for the proofs of non-original results, unless a sketch is particularly enlightening for the remainder of the discussion.

Chapter 2

Trace functions over finite fields

In this preliminary chapter, we first define precisely the concept of *ℓ-adic trace function over a finite field* that we will study, following the recent works of Fouvry-Kowalski-Michel, after Grothendieck, Deligne, Katz and others. Then, we recall how Deligne's work on the Weil conjectures can be used to estimate sums of trace functions. Finally, we give the examples we will consider throughout, along with their main properties.

This chapter is mainly based on [Kat88, Chapters 1–2, 5–7], [Kat90, 7.2–7.5], [Kat80, Chapter 4] and [FKM14a]. The references [Pol14, Section 6] and [FKM14b] are also good surveys on the subject toward applications in number theory. The notes [KR15] contain more in depth information and further references about ℓ-adic sheaves and étale cohomology. All of the latter are based on [Del80] and [Del77].

2.1. Definitions and first properties

2.1.1. Middle-extension ℓ-adic sheaves on curves.

Definition 2.1. An *ℓ-adic coefficient ring* is either:

- the finite field $\mathbb{F}_\lambda$,
- the field E_λ,
- the ring $\mathcal{O}_\lambda$,
- the field $\overline{\mathbb{Q}}_\ell$,

where E is a number field with ring of integers $\mathcal{O}$ and λ an ℓ-adic valuation on $\mathcal{O}$ corresponding to an prime ideal over the prime ℓ with residue field $\mathbb{F}_\lambda$. When A has characteristic 0, we supposed fixed an embedding[1] $\iota : A \to \mathbb{C}$.

Definition 2.2. Let A be an ℓ-adic coefficient ring and let X be a proper smooth geometrically connected algebraic curve over $\mathbb{F}_q$. We call *middle-extension sheaf of A-modules on X* a constructible sheaf $\mathcal{F}$ of A-modules on X (with respect to the étale topology) such that for every nonempty open $j : U \to X$ on which $j^*\mathcal{F}$ is lisse, we have $\mathcal{F} \cong j_* j^* \mathcal{F}$.

For the remaining of this section, we let X, A and $\mathcal{F}$ be as in Definition 2.2.

Definition 2.3. We write $\mathrm{Sing}(\mathcal{F}) = X(\overline{\mathbb{F}}_q) - U_{\mathcal{F}}(\overline{\mathbb{F}}_q)$ for the set of *singularities* (or *ramified points*) of $\mathcal{F}$, where $U_{\mathcal{F}}$ is the maximal open set of lissity[2] of $\mathcal{F}$.

2.1.2. Correspondence with ℓ-adic representations.

There is an alternative point of view for middle-extension ℓ-adic sheaves that can be very convenient in

[1] We recall that $\overline{\mathbb{Q}}_\ell$ and $\mathbb{C}$ are isomorphic as fields, but not as topological spaces (with the usual topologies).

[2] 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].

practice, through ℓ-adic representations of étale fundamental groups. As we shall see, both perspectives complement each other.

Étale fundamental groups.

DEFINITION 2.4. We denote by $\pi_1(X,\overline{\eta})$ the *arithmetic étale fundamental group* of X with respect to a geometric generic point $\overline{\eta}$. The *geometric étale fundamental group* is $\pi_1^{\mathrm{geom}}(X,\overline{\eta}) = \pi_1(X\times\overline{\mathbb{F}}_q,\overline{\eta})$.

In what follows, we let K be the function field of X, K^{sep} be the separable closure of K corresponding to $\overline{\eta}$, and U be a nonempty open of X.

DEFINITION 2.5. For $\mathbb{F}_{q'}/\mathbb{F}_q$ a finite extension and $x\in U(\mathbb{F}_{q'})$, we let

(1) $I_x \trianglelefteq D_x \leqslant \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the *inertia (resp. decomposition) group* at the valuation corresponding to x, defined up to conjugation. Moreover, we write P_x for the p-Sylow of I_x, the *wild inertia group*.

(2) $\mathrm{Frob}_{x,q'}\in D_x/I_x \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q'})$ be the *geometric Frobenius at* x, a class mapping to the geometric Frobenius $\mathrm{Frob}_{q'}$. This is again defined up to conjugation.

Proposition 2.6. *The étale fundamental group $\pi_1(U,\overline{\eta})$, resp. $\pi_1^{\mathrm{geom}}(U,\overline{\eta})$, is isomorphic to the quotient of*

$$\pi_1(K,\overline{\eta}) = \mathrm{Gal}(K^{\mathrm{sep}}/K), \quad \textit{resp. } \pi_1^{\mathrm{geom}}(K,\overline{\eta}) = \mathrm{Gal}(K^{\mathrm{sep}}/\overline{\mathbb{F}}_q K), \tag{2.1}$$

by the smallest closed normal subgroup containing all the inertia groups I_x for $x\in U(\overline{\mathbb{F}}_q)$.

Proof. See [KR15, Example 6.6(b)] and [Sza09, Chapter 4]. □

NOTATION 2.7. We will write $\pi_{1,q}$ (resp. $\pi_{1,q}^{\mathrm{geom}}$) for the groups (2.1) when $K=\mathbb{F}_q(T)$ (e.g. when $X=\mathbb{P}^1\times\mathbb{F}_q$), with respect to a fixed algebraic closure of $\mathbb{F}_q$.

Sheaves and ℓ-adic representations.

Proposition 2.8. *There is an equivalence of categories between:*

(1) Middle-extension sheaves $\mathcal{F}$ of A-modules on X.

(2) Continuous ℓ-adic representations

$$\rho_{\mathcal{F}} : \pi_1(K,\overline{\eta}) \to \mathrm{GL}(\mathcal{F}_{\overline{\eta}}) \cong \mathrm{GL}_n(A).$$

Moreover, $\mathcal{F}$ is lisse at $x\in X(\overline{\mathbb{F}}_q)$ if and only if I_x acts trivially on A^n.

Proof. See [KR15, Theorem 7.13]. □

Galois actions.

NOTATION 2.9. For any $G \leqslant \mathrm{GL}(\mathcal{F}_{\overline{\eta}}) = \mathrm{GL}(V)$, we will write $\mathcal{F}^G$ (resp. $\mathcal{F}_G$) for the space of G-invariants V^G (resp. the space of G-coinvariants V_G).

By the above, we see that:

– For any $x \in X(\mathbb{F}_q)$, the geometric Frobenius $\mathrm{Frob}_{x,q}$ acts continuously on $\mathcal{F}^{I_x}$ and on $\mathcal{F}_{I_x}$.

– Since $\pi_1(K,\overline{\eta})/\pi_1^{\mathrm{geom}}(K,\overline{\eta}) \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, the absolute Galois group of $\mathbb{F}_q$ acts continuously on $\mathcal{F}^{\pi_1^{\mathrm{geom}}(K,\overline{\eta})}$ and on $\mathcal{F}_{\pi_1^{\mathrm{geom}}(K,\overline{\eta})}$.

2.1.3. Rank, geometric isomorphism, irreducibility.

DEFINITION 2.10. (1) The *rank* or *dimension* of $\mathcal{F}$ is the dimension of $\rho_{\mathcal{F}}$, i.e. the dimension of the generic fiber $\mathcal{F}_{\overline{\eta}}$.

(2) We say that $\mathcal{F}$ is *arithmetically (resp. geometrically) irreducible* if $\rho_{\mathcal{F}}$ (resp. the restriction of $\rho_{\mathcal{F}}$ to $\pi_1^{\mathrm{geom}}(K,\overline{\eta})$) is irreducible.

(3) We say that $\mathcal{F}$ is *arithmetically (resp. geometrically) isotypic* if $\rho_{\mathcal{F}}$ (resp. the restriction of $\rho_{\mathcal{F}}$ to $\pi_1^{\mathrm{geom}}(K,\overline{\eta})$) is a sum of isomorphic irreducible representations.

(4) We say that two middle-extension A-sheaves on X are *geometrically isomorphic* if the corresponding representations of $\pi_1^{\mathrm{geom}}(K,\overline{\eta})$ are isomorphic.

2.1.4. Purity.

DEFINITION 2.11. An element $\alpha \in \overline{\mathbb{Q}}_\ell$ is a *q-Weil number of weight $i \geqslant 0$* if for any embedding $\jmath : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ we have $|\jmath(\alpha)| = q^{i/2}$.

DEFINITION 2.12. If A has characteristic 0, we say that $\mathcal{F}$ is *pointwise pure of weight $i \geqslant 0$* if, for any finite extension $\mathbb{F}_{q'}/\mathbb{F}_q$ and any $x \in U_{\mathcal{F}}(\mathbb{F}_{q'})$, the eigenvalues of $\rho_{\mathcal{F}}(\mathrm{Frob}_{x,q'})$ are q'-Weil numbers of weight i.

CONVENTION 2.13. From now on, "*sheaf of A-modules on X (resp. over $\mathbb{F}_q$)*" will be synonymous for "middle-extension sheaf of A-modules on X (resp. on $\mathbb{P}^1 \times \mathbb{F}_q$)". We will assume that $\mathrm{Sing}(\mathcal{F}) \subset X(\mathbb{F}_q)$ and that if A has characteristic 0, then $\mathcal{F}$ is pointwise pure of weight 0. We may replace "sheaf of A-modules" by "ℓ-adic sheaf" when the coefficient ring is either clear or left free to choose.

As we shall see, the purity assumption amounts to asking all sheaves to be normalized, but its validity may depend on deep consequences of the Riemann hypothesis over finite fields.

2.1.5. Trace functions.

DEFINITION 2.14. The *trace function* of $\mathcal{F}$ is the map

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

If A has characteristic 0, we may also view $t_{\mathcal{F}} : X(\mathbb{F}_q) \to \iota(A) \subset \mathbb{C}$ through the embedding ι. If $\mathbb{F}_{q'}/\mathbb{F}_q$ is any finite extension, we may also consider $t_{\mathcal{F}} : X(\mathbb{F}_{q'}) \to A$, $t_{\mathcal{F}}(x) = \mathrm{tr}(\rho_{\mathcal{F}}(\mathrm{Frob}_{x,q'}) \mid V^{I_x})$.

Proposition 2.15. *If A has characteristic 0, then*

$$||t_{\mathcal{F}}||_\infty \leqslant \mathrm{rank}(\mathcal{F}).$$

Proof. If $x \notin \mathrm{Sing}(\mathcal{F})$, then $|t_{\mathcal{F}}(x)| \leqslant \mathrm{rank}(\mathcal{F})$ by the purity assumption. On the other hand, if $x \in \mathrm{Sing}(\mathcal{F})$, [Del80, (1.8.9)] shows that the eigenvalues of $\rho_{\mathcal{F}}(\mathrm{Frob}_x)$ on V^{I_x} are still Weil numbers of weight 0. □

Proposition 2.16. *If $\mathcal{F}$ and $\mathcal{G}$ are two geometrically isomorphic sheaves of $\overline{\mathbb{Q}}_\ell$-modules on X, there exists $\alpha \in A^\times$ such that $t_{\mathcal{F}} = \alpha \cdot t_{\mathcal{G}}$. If $\mathcal{F}$ and $\mathcal{G}$ are pure of weight 0, then α is a q-Weil number of weight 0.*

Proof. This follows from the fact that $\pi_1(K, \overline{\eta})/\pi_1^{\mathrm{geom}}(K, \overline{\eta}) \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and Clifford theory, see [FKM14a, Proposition 3.2.3]. □

NOTATION 2.17. As in Convention 2.13, if $X = \mathbb{P}^1 \times \mathbb{F}_q$, we will call $t_{\mathcal{F}}$ an *ℓ-adic trace function over $\mathbb{F}_q$*. Note that in general there exists more than one sheaf with a given trace function.

2.1.6. Ramification.

As we shall see, a precise study of the behavior of a sheaf at singularities will be fundamental, in particular for the determination of monodromy groups. We present below some of the tools we will need. These are surveyed in [Kat88, Chapter 1 and Section 7.0] and detailed proofs can be found in [KR15, Sections 3–4]. Let again $\mathcal{F}$ be as in Definition 2.2 corresponding to a representation $\rho_{\mathcal{F}} : \pi_1(K, \overline{\eta}) \to \mathrm{GL}(V)$.

Break decomposition. Let $x \in X(\mathbb{F}_q)$. There exists a uniquely defined decomposition of I_x-modules

$$V = V^{\mathrm{tame}} \oplus V^{\mathrm{wild}} = V(0) \bigoplus \left(\bigoplus_{t \in \mathbb{R}_{>0}} V(t) \right)$$

with $V^{\mathrm{tame}} = V(0) = V^{P_x}$, called the *break decomposition* of $\mathcal{F}$ at x. Note that if $x \notin \mathrm{Sing}(\mathcal{F})$, then $V = V(0)$. The finitely many $t \geqslant 0$ such that $V(t) \neq 0$ are called the *breaks* of $\mathcal{F}$ at x. If $V = V(0)$, we say that $\mathcal{F}$ is *tamely ramified* at x.

Remark 2.18. If $\mathcal{F}$ is a sheaf of $\mathcal{O}_\lambda$-modules (for $\mathcal{O}_\lambda$ as in Definition 2.1), then, by [Kat88, Remark 1.10], its break decomposition as sheaf of $\overline{\mathbb{Q}}_\ell$-modules (by extension of scalars) is simply obtained by extension of scalars from its break decomposition as sheaf of $\mathcal{O}_\lambda$-modules. Similarly, if $\mathfrak{m}_\lambda$ is the maximal ideal of $\mathcal{O}_\lambda$, the break-decomposition of the sheaf $\mathcal{F}/\mathfrak{m}_\lambda\mathcal{F}$ of $\mathbb{F}_\lambda = \mathcal{O}_\lambda/\mathfrak{m}\mathcal{O}_\lambda$-modules is obtained by reducing the break decomposition of $\mathcal{F}$.

Since the tame inertia group I_x/P_x is topologically cyclic, we can also decompose the tame part with respect to the Jordan decomposition of a generator,

$$V^{\mathrm{tame}} = \bigoplus_{\chi} V^{\chi-\mathrm{unip.}} = \bigoplus_{\chi} (\mathrm{Unip.} \otimes \mathcal{L}_\chi(X + x)) \tag{2.2}$$

where χ runs over characters of I_x of finite order prime to p (see [Kat88, Section 1.0, Section 7.0]) and $\mathcal{L}_\chi$ is a Kummer sheaf (see below).

Swan conductors.

Definition 2.19. The *Swan conductor* of $\mathcal{F}$ at $x \in \mathrm{Sing}(\mathcal{F})$ is

$$\mathrm{Swan}_x(\mathcal{F}) = \sum_{t \geqslant 0} t \dim V(t),$$

where $V = \bigoplus_{t \geqslant 0} V(t)$ is the break decomposition of $\mathcal{F}$ at x.

Note that $\mathcal{F}$ is tamely ramified at x if and only if $\mathrm{Swan}_x(\mathcal{F}) = 0$.

Proposition 2.20. *The Swan conductor is a nonnegative integer.*

Proof. See [KR15, Section 4.4.2]. □

Remark 2.21. By Remark 2.18, we see that the Swan conductor does not change if we view a sheaf of $\mathcal{O}_\lambda$-modules $\mathcal{F}$ as a sheaf of $\overline{\mathbb{Q}}_\ell$-modules or as a sheaf of $\mathbb{F}_\lambda$-modules, namely

$$\mathrm{Swan}_x(\mathcal{F}) = \mathrm{Swan}_x(\mathcal{F}/\mathfrak{m}_\lambda \mathcal{F}) = \mathrm{Swan}_x(\mathcal{F} \otimes \overline{\mathbb{Q}}_\ell)$$

for all $x \in \mathrm{Sing}(\mathcal{F})$.

Conductor. The following quantity was introduced by Fouvry-Kowalski-Michel [FKM15a], and combines three invariants of the sheaf to measure its "complexity" (with respect to dimension and ramification).

Definition 2.22. The *conductor* of $\mathcal{F}$ is the positive integer

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

The error term in Deligne's theorem on estimates of sums of trace functions will depend on the dimension, number of singularities and Swan conductors of the sheaf, and the conductor is simply the most natural bound for the former.

2.1.7. Operations. In this section, we let $\mathcal{F}_1$, $\mathcal{F}_2$ be sheaves of A-modules on X as in Definition 2.2 and Convention 2.13, corresponding to representations $\rho_i : \pi_1(K, \overline{\eta}) \to \mathrm{GL}(V_i)$ and trace functions $t_i : X(\mathbb{F}_q) \to A$ $(i = 1, 2)$. For the proofs, we refer the reader to [FKM14a, Chapter 3] (and [Kat88, Lemma 1.3] for the break decomposition of products).

Sum, product, conjugation.

Proposition 2.23.

(1) The sheaf $\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_2$ of A-modules on X corresponding to the representation $\rho_1 \oplus \rho_2$ has trace function $t_1 + t_2$. Moreover, for all $x \in X(\mathbb{F}_q)$,

$$\begin{aligned} \mathrm{Sing}(\mathcal{F}) &= \mathrm{Sing}(\mathcal{F}_1) \cup \mathrm{Sing}(\mathcal{F}_2) \\ \mathrm{Swan}_x(\mathcal{F}) &= \mathrm{Swan}_x(\mathcal{F}_1) + \mathrm{Swan}_x(\mathcal{F}_2) \\ \mathrm{cond}(\mathcal{F}_1 \oplus \mathcal{F}_2) &= \mathrm{cond}(\mathcal{F}_1) + \mathrm{cond}(\mathcal{F}_2) \end{aligned}$$

(2) The sheaf $\mathcal{F} = \mathcal{F}_1 \otimes \mathcal{F}_2$ of A-modules on X corresponding to the representation $\rho_1 \otimes \rho_2$ has trace function equal to $t_1 \cdot t_2$ on $X(\mathbb{F}_q) - (\mathrm{Sing}(\mathcal{F}_1) \cap \mathrm{Sing}(\mathcal{F}_2))$. Moreover, for all $x \in X(\mathbb{F}_q)$,

$$V_1(t_1) \otimes V_2(t_2) \subset \begin{cases} (V_1 \otimes V_2)(\max(t_1, t_2)) & : t_1 \neq t_2 \\ \bigoplus_{u \leqslant t_1} (V_1 \otimes V_2)(u) & : t_1 = t_2 \end{cases}$$

if $V_i = \bigoplus_{t \geqslant 0} V_i(t)$ (resp. $V_1 \otimes V_2 = \bigoplus_{t \geqslant 0} (V_1 \otimes V_2)(t)$) is the break decomposition at x of $\mathcal{F}_i$ (resp. of $\mathcal{F}$), and

$$\begin{aligned} \mathrm{Sing}(\mathcal{F}) &\subset \mathrm{Sing}(\mathcal{F}_1) \cup \mathrm{Sing}(\mathcal{F}_2) \\ \mathrm{Swan}_x(\mathcal{F}) &\leqslant \mathrm{rank}(\mathcal{F}_1 \otimes \mathcal{F}_2)(\mathrm{Swan}_x(\mathcal{F}_1) + \mathrm{Swan}_x(\mathcal{F}_2)) \\ \mathrm{cond}(\mathcal{F}) &\ll \mathrm{cond}(\mathcal{F}_1)^2 \, \mathrm{cond}(\mathcal{F}_2)^2. \end{aligned}$$

(3) The sheaf $D(\mathcal{F}_1)$ of A-modules on X corresponding to the dual representation $D(\rho_1)$ has same singularities, Swan conductors, and conductor than $\mathcal{F}_1$. If A has characteristic 0, then the complex-valued trace function of $D(\mathcal{F}_1)$ is $\overline{t_1}$.

In particular, by Convention 2.13, we assert that these sheaves are still pointwise pure of weight 0.

Change of variable.

Proposition 2.24. *If $f : X \to X$ is a nonconstant morphism defined over $\mathbb{F}_q$, the inverse image sheaf $f^*\mathcal{F}_1$ has trace function equal to $t_1 \circ f$ on $X(\mathbb{F}_q) - f^{-1}(\mathrm{Sing}(\mathcal{F}_1))$. Moreover,*

$$\begin{aligned} \mathrm{Sing}(f^*\mathcal{F}_1) &\subset f^{-1}(\mathrm{Sing}(\mathcal{F}_1)) \\ \mathrm{cond}(f^*\mathcal{F}_1) &\ll \deg(f) \, \mathrm{cond}(\mathcal{F}_1)^2 \end{aligned}$$

If f is an isomorphism, the conductors are equal and $\mathcal{F}_1$ is irreducible (resp. geometrically irreducible) if and only if $\mathcal{F}_1$ is.

NOTATION 2.25. For $a \in \mathbb{A}^1(\mathbb{F}_q)$, we will write $[+a]^*$ (resp. $[\times a]^*$) for the inverse image through the map $x \mapsto x + a$ (resp. $x \mapsto ax$).

Sum over solutions.

Proposition 2.26. *If $f : X \to X$ is a nonconstant morphism defined over $\mathbb{F}_q$, the direct image sheaf $f_*\mathcal{F}_1$ has trace function equal to $f_*t_1 : X(\mathbb{F}_q) \to A$, for*

$$f_*t_1(x) = \sum_{\substack{y\in X(\mathbb{F}_q)\\ f(y)=x}} t_1(y) \quad (x \in X(\mathbb{F}_q)).$$

Moreover, for S_f the set of ramified points of f over $\mathbb{F}_q$ and $x \in X(\mathbb{F}_q)$,

$$\begin{aligned} \mathrm{Sing}(f_*\mathcal{F}_1) &\subset f(\mathrm{Sing}(\mathcal{F}_1)) \cup S_f \\ \mathrm{Swan}_x(f_*\mathcal{F}_1) &= \sum_{y\in\mathbb{P}^1(\mathbb{F}_q)\,:\,f(y)=x} \mathrm{Swan}_y(\mathcal{F}_1) \\ \mathrm{cond}(f_*\mathcal{F}_1) &\ll \deg(f)^2\,\mathrm{cond}(\mathcal{F}_1)^2. \end{aligned}$$

2.1.8. Decompositions.

Proposition 2.27. *(1) There exists a family $(\mathcal{F}_i)_{1\leqslant i\leqslant n}$ of arithmetically irreducible and geometrically isotypic sheaves of A-modules on X such that $t_{\mathcal{F}} = \sum_{i=1}^n t_{\mathcal{F}_i}$.*

(2) The representation $\rho_{\mathcal{F}}\,|_{\pi_1^{\mathrm{geom}}(K,\overline{\eta})}$ is semisimple.

Proof. See [FKM14a, Propositions 3.3.6, 3.5.3] and [Del80, Théorème 3.4.1(iii)]. For the second assertion, we use the assumption that $\mathcal{F}$ is pointwise pure of weight 0. □

2.2. Sums of trace functions

We can finally state Deligne's analogue of the Riemann hypothesis over finite fields and its application to the estimation of sums of trace functions.

We refer the reader to [Del77, Exposé 6], [FKM14a, Chapter 4], [Kat88, Chapter 2] and [FKM15a, Section 9] for other versions of this statement.

Theorem 2.28. *Let A be an ℓ-adic coefficient ring of characteristic 0. For $\mathcal{F}$ an sheaf of A-modules over $\mathbb{F}_q$ as in Convention 2.13, we have*

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

$$E(\mathcal{F}) = \mathrm{rank}(\mathcal{F})\left[|\,\mathrm{Sing}(\mathcal{F})| - 1 + \sum_{x\in\mathrm{Sing}(\mathcal{F})} \mathrm{Swan}_x(\mathcal{F})\right] \ll \mathrm{cond}(\mathcal{F})^2.$$

This will be the foundation of the remaining of our work.

Remark 2.29. In the works of Fouvry-Kowalski-Michel and others, the error term is usually only given in terms of the conductor (i.e. $\mathrm{cond}(\mathcal{F})^2\sqrt{q}$). We are more precise above to be able to discuss cases where the conductor will be growing (see Section 4.2).

Remark 2.30. By Schur's Lemma and Proposition 2.27 (2), $\dim(\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}})$ is equal to the number of trivial geometrically irreducible components of $\mathcal{F}$.

It follows that geometrically irreducible ℓ-adic trace functions over $\mathbb{F}_q$ are "almost orthogonal":

Corollary 2.31. *Let A be an ℓ-adic coefficient ring of characteristic 0. If $\mathcal{F}$, $\mathcal{G}$ are geometrically irreducible sheaves of A-modules over $\mathbb{F}_q$, then*

$$\sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x)\overline{t_{\mathcal{G}}(x)} = C(\mathcal{F},\mathcal{G})q + O(\mathrm{cond}(\mathcal{F})^2\,\mathrm{cond}(\mathcal{G})^2\sqrt{q})$$

with $C(\mathcal{F},\mathcal{F}) = 1$ and $C(\mathcal{F},\mathcal{G}) = 0$ if $\mathcal{F}$ and $\mathcal{G}$ are not geometrically isomorphic.

Remark 2.32. By Proposition 2.27 (1), we may theoretically always reduce to this case.

2.2.1. Proof of Theorem 2.28 and Corollary 2.31. For the rest of this section, we let $\mathcal{F}$ be a sheaf of $\overline{\mathbb{Q}}_\ell$-modules on a curve X as in Convention 2.13, and we assume moreover that $\mathcal{F}$ is lisse on a nonempty open U of X.

Cohomological interpretation. The cohomological interpretation of sums of trace functions is given by the following:

Theorem 2.33 (Grothendieck-Lefschetz trace formula)**.** *We have*

$$\sum_{x\in U(\mathbb{F}_q)} t_{\mathcal{F}}(x) = \sum_{i=0}^{2}(-1)^i\,\mathrm{tr}\left(\mathrm{Frob}_q \mid H_c^i(U\times\overline{\mathbb{F}}_q,\mathcal{F})\right),$$

where H_c^i are the étale cohomology group with compact support, on which $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ acts.

This is a deep link between the *local* Frobenius acting on the stalks of the sheaf and the *global* Frobenius acting on the étale cohomology groups (see e.g. [KR15, Section 8] and [Del77, Rapport, Section 3 and Exposé 4, Section 3]).

Structure of extremal cohomology groups.

Theorem 2.34. *If U is affine, then*

$$\begin{aligned} H_c^0(U\times\overline{\mathbb{F}}_q,\mathcal{F}) &= 0,\\ H_c^2(U\times\overline{\mathbb{F}}_q,\mathcal{F}) &\cong \mathcal{F}_{\pi_1^{\mathrm{geom}}(K,\overline{\eta})}(-1),\end{aligned}$$

where the last expression denotes a Tate twist (see [KR15, 7.1.9]).

This follows from Poincaré duality (see e.g. [KR15, Theorem 8.4]).

Deligne's analogue of the Riemann hypothesis over finite fields. By purity, we have the following fundamental estimate:

Theorem 2.35 ([Del80, Theorem 3.3.1])**.** *For every $i \geqslant 0$, the eigenvalues of Frob_q acting on $H_c^i(U\times\overline{\mathbb{F}}_q,\mathcal{F})$ are q-Weil numbers of weight at most i.*

By Theorems 2.33, 2.34 and 2.35, we get that

$$\sum_{x\in U(\mathbb{F}_q)} t_{\mathcal{F}}(x) = q\cdot \operatorname{tr}\left(\mathrm{Frob}_q \mid \mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}(U,\overline{\eta})}\right) + O\left(q^{1/2}\dim H_c^1(U\times\overline{\mathbb{F}}_q,\mathcal{F})\right)$$

with an absolute implicit constant.

Remark 2.36. Up to this point, the same arguments would apply if X were replaced by a smooth geometrically connected (quasi-projective) *variety* over $\mathbb{F}_q$ of dimension d with geometric generic point $\overline{\eta}$ (and $\mathcal{F}$ is not supposed middle-extension anymore). Then, if U is affine,

$$\sum_{x\in U(\mathbb{F}_q)} t_{\mathcal{F}}(x) = q^d\cdot \operatorname{tr}\left(\mathrm{Frob}_q \mid \mathcal{F}_{\pi_1^{\mathrm{geom}}(U,\overline{\eta})}\right) + O\left(\sum_{i=0}^{2d-1} q^{i/2}\dim H_c^i(U\times\overline{\mathbb{F}}_q,\mathcal{F})\right)$$

for $\rho_{\mathcal{F}}:\pi_1(U,\overline{\eta})\to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ the representation corresponding to $\mathcal{F}$. If q varies, but the sum of Betti numbers in the error term does not depend on q, which is often the case in applications (see for example the survey in [IK04, pp. 307–308, 311–312]), then

$$\sum_{x\in U(\mathbb{F}_q)} t_{\mathcal{F}}(x) = q^d\cdot \operatorname{tr}\left(\mathrm{Frob}_q \mid \mathcal{F}_{\pi_1^{\mathrm{geom}}(U,\overline{\eta})}\right) + O\left(q^{d-1/2}\right)$$

with an absolute implicit constant. A greater saving in the error term would be implied by the vanishing of further cohomology groups. For example, we have square-root cancellation if $H_c^i(U\times\overline{\mathbb{F}}_q,\mathcal{F})=0$ for all $i>d$.

Bound on $\dim H_c^1(U\times\overline{\mathbb{F}}_q,\mathcal{F})$.

Theorem 2.37 (Euler-Poincaré formula/Grothendieck-Ogg-Safarevich)**.** *If X has genus g, then*

$$\begin{aligned}\sum_{i=0}^{2}(-1)^i\dim H_c^i(U\times\overline{\mathbb{F}}_q,\mathcal{F}) &= \operatorname{rank}(\mathcal{F})\Big(2-2g-|(X-U)(\overline{\mathbb{F}}_q)|\Big)\\ &\quad - \sum_{x\in(X-U)(\overline{\mathbb{F}}_q)}\operatorname{Swan}_x(\mathcal{F}).\end{aligned}$$

(See e.g. [KR15, Section 9]).

Conclusion. Therefore, if $X=\mathbb{P}^1\times\mathbb{F}_q$ and $U_{\mathcal{F}}$ is affine (e.g. $U_{\mathcal{F}}\neq X$), Theorems 2.37 and 2.34 show that

$$\dim H_c^1(U_{\mathcal{F}}\times\overline{\mathbb{F}}_q,\mathcal{F}) \leqslant \operatorname{rank}(\mathcal{F})(|\operatorname{Sing}(\mathcal{F})|-1) + \sum_{x\in\operatorname{Sing}(\mathcal{F})}\operatorname{Swan}_x(\mathcal{F}).$$

Theorem 2.28 now follows from the fact that

$$\sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x) = \sum_{x\in U_{\mathcal{F}}(\mathbb{F}_q)} t_{\mathcal{F}}(x) + O\left(|\operatorname{Sing}(\mathcal{F})|\operatorname{rank}(\mathcal{F})\right)$$

by Proposition 2.15. Corollary 2.31 is then a consequence of Schur's Lemma and Proposition 2.16.

2.3. The ℓ-adic Fourier transform

Discrete Fourier transform.

Definition 2.38. For $f : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{C}$ any function, we define its (normalized) *Fourier transform* $\mathrm{FT}_\psi(f) : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{C}$ with respect to a nontrivial additive character $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ by

$$\mathrm{FT}_\psi(f)(x) = \frac{-1}{\sqrt{q}} \sum_{y \in \mathbb{F}_q} f(y)\psi(xy) \qquad (x \in \mathbb{F}_q)$$

and $\mathrm{FT}_\psi(f)(\infty) = -f(0)/\sqrt{q}$.

Proposition 2.39. *Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be an additive character. Then:*

(1) We have $\mathrm{FT}_\psi \circ \mathrm{FT}_\psi = [\times(-1)]^*$.

(2) FT_ψ is a unitary operator on the space of functions $\mathbb{P}^1(\mathbb{F}_q) \to \mathbb{C}$ with respect to the inner product

$$\langle f_1, f_2 \rangle = \frac{1}{q} \sum_{x \in \mathbb{F}_q} f_1(x)\overline{f_2(x)} \quad (f_1, f_2 : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{C}).$$

The ℓ-adic Fourier transform. The following deep result of Deligne shows that it is possible to perform Fourier transform on the level of ℓ-adic sheaves:

Definition 2.40. A sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ is a *Fourier sheaf* if it does not contain an Artin-Schreier sheaf $\mathcal{L}_\psi$ (for $\psi : \mathbb{F}_q \to \mathbb{C}$ an additive character) in its geometric Jordan-Hölder decomposition (see Proposition 2.27).

Theorem 2.41 (Deligne, Laumon, Brylinski)**.** *Let $\psi : \mathbb{F}_q \to \mathbb{C}$ be a nontrivial character. If $\mathcal{F}$ is an ℓ-adic Fourier sheaf over $\mathbb{F}_q$, there exists an ℓ-adic sheaf $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F})$ over $\mathbb{F}_q$ with trace function*

$$t_{\mathcal{G}} = \mathrm{FT}_\psi(t_{\mathcal{F}}).$$

Moreover:

(1) $\mathcal{G}$ is a Fourier sheaf.

(2) $\mathcal{G}$ is geometrically irreducible if and only if $\mathcal{F}$ is.

(3) There is an isomorphism $\mathrm{FT}_\psi(\mathcal{G}) \cong [\times(-1)]^*\mathcal{F}$.

(4) If E is a number field with ring of integers $\mathcal{O}$ such that $\sqrt{p} \in \mathcal{O}$ and λ is an ℓ-adic valuation on $\mathcal{O}$, then $\mathcal{G}$ can be defined as a sheaf of $\mathcal{O}_\lambda$-modules if $\mathcal{F}$ can.

Proof. See for example [Kat88, Chapters 5, 8]. For the last point, note that the condition $\sqrt{p} \in \mathcal{O}$ implies that $\sqrt{p} \in \mathcal{O}_\lambda^\times$ since $\ell \neq p$. □

The ramification properties of an ℓ-adic Fourier transform have been studied in details by Laumon, see [Kat90, Sections 7.3–7.5] and [Kat88, Chapters 7–8]. It follows that the conductor of the Fourier transform can be polynomially bounded in terms of that of the base sheaf:

Proposition 2.42 ([FKM15a, Proposition 8.2]). *If $\mathcal{F}$ is a Fourier sheaf and $\psi : \mathbb{F}_q \to \mathbb{C}$ a nontrivial character, we have*

$$\operatorname{cond}(\mathrm{FT}_\psi(\mathcal{F})) \ll \operatorname{cond}(\mathcal{F})^2.$$

Remark 2.43. According to Convention 2.13, the statement of Theorem 2.41 includes the fact that the Fourier transform is pure of weight 0, so by Proposition 2.15,

$$||\,\mathrm{FT}_\psi(t_\mathcal{F})||_\infty \leqslant \operatorname{rank}(\mathcal{G}) \leqslant \operatorname{cond}(\mathrm{FT}_\psi(\mathcal{F})) \ll \operatorname{cond}(\mathcal{F})^2,$$

which is usually bounded independently from q. Such a bound is of fundamental importance in applications (see e.g. [FKM+16]). Note that this would also follow by applying Theorem 2.28; actually, the proof of Theorem 2.41 relies on Deligne's Theorem 2.35.

2.4. Examples

In this section, we give the examples of trace functions we will consider later on. In prevision of Chapter 6, we duly take note of the definition on discrete ℓ-adic coefficient rings in some cases.

2.4.1. Characters. For this section, we refer the reader to [Del77, Exposé 6, Section 1], [KR15, Examples 7.16–17] and [Kat88, Section 4.3]. An explicit construction as ℓ-adic Galois representations can be found in [FKM14a, Sections 2.3–2.4].

Artin-Schreier sheaves.

Proposition 2.44. *Let $\psi : \mathbb{F}_q \to \mathbb{Z}[\zeta_p]$ be a nontrivial additive character, λ be an ℓ-adic valuation on $\mathbb{Z}[\zeta_p]$ corresponding to a prime ideal $\mathfrak{q}$ above ℓ with all poles of order $< p$, and $f = f_1/f_2 \in \mathbb{F}_q(X)$. There exists a sheaf $\mathcal{L}_{\psi(f)}$ of $\mathbb{Z}[\zeta_p]_\lambda$-modules on $\mathbb{F}_q$ with:*

(1) trace function $\psi \circ f$ (under the convention that $\psi(\infty) = 0$).

(2) singularities at the poles of f, with Swan conductor equal to the order of the pole.

(3) $\operatorname{cond}(\mathcal{L}_{\psi(f)}) \leqslant 1 + 2\deg(f_2)$.

By reduction modulo $\mathfrak{q}$, this gives a sheaf of $\mathbb{F}_\lambda \cong \mathbb{Z}[\zeta_p]_\lambda/\mathfrak{q}\mathbb{Z}[\zeta_p]_\lambda$-modules with the same properties and trace function $\psi \circ f \pmod{\mathfrak{q}}$.

Kummer sheaves.

Proposition 2.45. *Let $\chi : \mathbb{F}_q^\times \to \mathbb{Z}[\zeta_d]$ be a nontrivial multiplicative character of order $d \geqslant 2$, λ be an ℓ-adic valuation on $\mathbb{Z}[\zeta_d]$ corresponding to a prime ideal $\mathfrak{q}$ above ℓ, and $f = f_1/f_2 \in \mathbb{F}_q(X)$ that is not a d-power. We assume that f has no zero or pole of order divisible by d. There exists a sheaf $\mathcal{L}_{\chi(f)}$ of $\mathbb{Z}[\zeta_d]_\lambda$-modules on $\mathbb{F}_q$ with:*

(1) trace function $\chi \circ f$ (under the convention that $\chi(0) = \chi(\infty) = 0$).

(2) tame singularities at the zeros and poles of f.

(3) $\mathrm{cond}(\mathcal{L}_{\chi(f)}) = 1 + \deg(f_1) + \deg(f_2)$.

By reduction modulo $\mathfrak{q}$, this gives a sheaf of $\mathbb{F}_\lambda \cong \mathbb{Z}[\zeta_d]_\lambda/\mathfrak{q}\mathbb{Z}[\zeta_d]_\lambda$-modules with the same properties and trace function $\chi \circ f \pmod{\mathfrak{q}}$.

2.4.2. Hyper-Kloosterman and hypergeometric sheaves.

Kloosterman sheaves.

Proposition 2.46 (Deligne)**.** *Let $n \geqslant 2$ be an integer.*

(1) There exists a Kloosterman sheaf *$\mathcal{K}l_n$ of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$, of rank n, with trace function equal to the Kloosterman sum*

$$x \mapsto \mathrm{Kl}_{n,q}(x) = \frac{(-1)^{n-1}}{q^{\frac{n-1}{2}}} \sum_{\substack{x_1,\dots,x_n \in \mathbb{F}_q^\times \\ x_1 \dots x_n = x}} e\left(\frac{\mathrm{tr}(x_1 + \cdots + x_n)}{p}\right) \quad (x \in \mathbb{F}_q^\times),$$

and $\mathrm{Kl}_{n,q}(0) = (-1)^{n-1} q^{-(n-1)/2}$. Moreover, $\mathcal{K}l_n$ is geometrically irreducible, lisse on $\mathbb{G}_m \times \mathbb{F}_q$, $\mathrm{Swan}_\infty(\mathcal{K}l_n) = 1$, $\mathrm{Swan}_0(\mathcal{K}l_n) = 0$, and $\mathrm{cond}(\mathcal{K}l_n) = n + 3$.

(2) Let λ be an ℓ-adic valuation on $\mathbb{Z}[\zeta_{4p}]$ corresponding to a prime ideal $\mathfrak{q}$ above ℓ. The sheaf $\mathcal{K}l_n$ can then be defined as a sheaf of $\mathbb{Z}[\zeta_{4p}]_\lambda$-modules and we note that $\mathrm{Kl}_{n,q}(x) \in \mathbb{Z}[\zeta_{4p}]_{q^{(n-1)/2}} \leqslant \mathbb{Z}[\zeta_{4p}]_\mathfrak{q}$ for all $x \in \mathbb{F}_q$.

(3) By reduction modulo $\mathfrak{q}$, this gives a sheaf of $\mathbb{F}_\lambda \cong \mathbb{Z}[\zeta_{4p}]_\lambda/\mathfrak{q}\mathbb{Z}[\zeta_{4p}]_\lambda$-modules over $\mathbb{F}_q$ with the same properties and trace function $\mathrm{Kl}_{n,q} \pmod{\mathfrak{q}}$.

Proof. By letting $\mathrm{Kl}_1 = \psi : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{C}$ with $\psi(\infty) = 0$, we get that the Kloosterman sum $\mathrm{Kl}_n : \mathbb{F}_q^\times \to \mathbb{C}$ of rank $n \geqslant 2$ satisfies

$$\mathrm{Kl}_n = \mathrm{FT}_\psi([x \mapsto x^{-1}]^* \mathrm{Kl}_{n-1}).$$

Thus, we can recursively construct the Kloosterman sheaf with Theorem 2.41 by setting $\mathcal{K}l_1 = \mathcal{L}_\psi$ (the Artin-Schreier sheaf) and $\mathcal{K}l_n = \mathrm{FT}_\psi([x \mapsto x^{-1}]^* \mathcal{K}l_{n-1})$. For the remaining properties, see [Kat88, Theorem 4.1.1] or [Del77, Exposé 6, Théorème 7.8]. Concerning (2) and (3), recall that

$$\varepsilon_p \sqrt{p} \in \mathbb{Z}[\zeta_p] \text{ with } \varepsilon_p = \begin{cases} 1 & : p \equiv 1 \pmod 4 \\ i & : p \equiv 3 \pmod 4 \end{cases}$$

by the evaluation of quadratic Gauss sums, so $\sqrt{p} \in \mathbb{Z}[\zeta_p, \zeta_4] \leqslant \mathbb{Z}[\zeta_{4p}]$ and $\sqrt{p} \in \mathbb{Z}[\zeta_{4p}]_\mathfrak{q}^\times$ since $\ell \neq p$. □

Remark 2.47. Recall that $|\mathbb{F}_\lambda| = \ell^f$, where $f \geqslant 1$ is minimal subject to the condition $\ell^f \equiv 1 \pmod{4p}$, by the ramification theory of cyclotomic fields (see [Was97, Theorem 2.13]).

Remark 2.48. If $p \equiv 1 \pmod 4$ or if n is odd, we can replace $\mathbb{Z}[\zeta_{4p}]$ by $\mathbb{Z}[\zeta_p]$ (in the second case by using an untwisted ℓ-adic Fourier transform before applying a Tate twist of order $\frac{n-1}{2} \in \mathbb{N}$)

As a consequence of Propositions 2.46 and 2.15, we get Deligne's bound for Hyper-Kloosterman sums, generalizing Weil's Bound (1.4):

Corollary 2.49. *We have* $|\mathrm{Kl}_{n,q}(x)| \leqslant n$ *for all* $x \in \mathbb{F}_q$.

Hypergeometric sheaves.

Proposition 2.50 (Katz)**.** *Let* $n \geqslant m \geqslant 0$ *be integers with* $r = m + n \geqslant 1$, $\boldsymbol{\chi} = (\chi_i)_{1\leqslant i\leqslant n}$, $\boldsymbol{\rho} = (\rho_j)_{1\leqslant j\leqslant m}$ *tuples of pairwise distinct characters of* $\mathbb{F}_q^\times$. *There exists a geometrically irreducible* hypergeometric sheaf $\mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho})$ *over* $\mathbb{F}_q$ *of rank* n, *with trace function equal to the hypergeometric sum* $\mathrm{Hyp}(\boldsymbol{\chi}, \boldsymbol{\rho}) : \mathbb{F}_q \to \mathbb{C}$ *defined by*

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

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). Moreover,* $\mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho})$ *is*

- *lisse on* $\mathbb{G}_m \times \mathbb{F}_q$, *tame at* 0, *and* $\mathrm{Swan}_\infty(\mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho})) = 1$, *if* $m \neq n$,
- *lisse on* $\mathbb{G}_m \times \mathbb{F}_q - \{1\}$ *and tame everywhere, if* $m = n$.

Hence, $\mathrm{cond}(\mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho})) = n + 3$.

Proof. See [Kat90, Theorem 8.4.2]. □

Example 2.51. For $m = 0$ and $\boldsymbol{\chi} = (1)_{1\leqslant i\leqslant n}$, we get the Kloosterman sheaf $\mathcal{K}l_n$.

2.4.3. Exponential sums. Next, we consider general exponential sums of the form

$$\frac{-1}{\sqrt{q}} \sum_{y\in\mathbb{F}_q} e\left(\frac{\mathrm{tr}(xf(y) + h(y))}{p}\right) \chi(g(y)) \quad (x \in \mathbb{F}_q), \tag{2.3}$$

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

$$\mathrm{Bi}(x, q) = \frac{-1}{\sqrt{q}} \sum_{y\in\mathbb{F}_q} e\left(\frac{\mathrm{tr}(xy + y^3)}{p}\right) \quad (x \in \mathbb{F}_q), \tag{2.4}$$

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

$$\frac{-1}{\sqrt{q}} \sum_{y\in\mathbb{F}_q} e\left(\frac{\mathrm{tr}(xf(y))}{p}\right) \quad (x \in \mathbb{F}_q) \tag{2.5}$$

for $f \in \mathbb{Q}(X)$, studied by Katz and Fouvry-Michel.

Proposition 2.52. *Assume that* p *is large enough to consider* $f, g, h \in \mathbb{F}_q(X)$ *and assume that* g *(resp.* h*) has no pole or zero (resp. no pole) of order divisible by* p. *Let*

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

If the sheaf $\mathcal{F}_2$ *is a Fourier sheaf, then there is an* ℓ*-adic sheaf* $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F}_2)$ *over* $\mathbb{F}_q$ *with trace function given by* (2.3). *Moreover,*

(1) $\mathcal{G}$ *is geometrically irreducible if* $\mathcal{F}_2$ *is.*

(2) The singularities of $\mathcal{F}_1$ *are contained in the union of the set of poles of* g, h *with the set of zeros of* g*. At any* $x \in \mathbb{P}^1(\mathbb{F}_q)$*, we have*

$$\mathrm{Swan}_x(\mathcal{F}_1) = \begin{cases} \mathrm{ord}_x(h) & \text{if } x \text{ is a pole of } h \\ 0 & \text{otherwise.} \end{cases}$$

(3) For $\mathcal{F}_2$*, we have* $\mathrm{Sing}(\mathcal{F}_2) = f(\mathrm{Sing}(\mathcal{F}_1)) \cup S_f$*, where* S_f *is the set of ramified points of* f *as a morphism of* $\mathbb{P}^1$*. Moreover,*

$$\mathrm{Swan}_\infty(\mathcal{F}_2) = \sum_{y \in \mathbb{P}^1(\mathbb{F}_q) \,:\, f(y)=\infty} \mathrm{Swan}_y(\mathcal{F}_1).$$

In particular, if f *is a nonconstant polynomial,* $\mathrm{Swan}_\infty(\mathcal{F}_2) = \mathrm{Swan}_\infty(\mathcal{F}_1)$*.*

(4) We have the bound

$$\mathrm{cond}(\mathcal{G}) \ll \deg(f)^4 \deg(h_2)^8 (1 + \deg(g_1) + \deg(g_2))^8$$

where $\deg(f)$ *is the degree of* f *as a morphism of* $\mathbb{P}^1$ *and* $g = g_1/g_2$*,* $h = h_1/h_2$ *for* $g_i, h_i \in \mathbb{F}_q[X]$*.*

Proof. This follows directly from Section 2.1.7, Theorem 2.41 and Proposition 2.42 since the sum (2.3) is given by the discrete Fourier transform $\mathrm{FT}_\psi(f_*(\psi(h)\chi(g)))$. See also [Kat90, Chapter 7] and [Del77, Exposé 6] . □

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 (2.5), studied in [Kat90, 7.10].

(ii) $\mathcal{F}_1$ is nontrivial and $f = X$. Of course, $\mathcal{F}_2 = \mathcal{F}_1$ in this case.
More particularly, we will consider the case $\chi = 1$ and h is a polynomial of degree $n \geqslant 2$, which includes Birch sums (2.4). These are studied in [Kat90, 7.12] and [Kat87].

(iii) $\mathcal{F}_1$ is nontrivial and $f \neq X$.
The ramification of $\mathcal{F}_2$ and $\mathcal{G}$ is studied in [Kat90, 7.7].
More particularly, we will consider the case 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 $g(x)g(-x) = L(x)^{\mathrm{ord}(\chi)}$.

We review these situations in the next sections.

Supermorse functions and sums of the form (2.5). Exponential sums of the form (2.5) have been studied by Fouvry and Michel in [Mic98], [FM02] and [FM03], using their construction as trace functions and the determination of their monodromy groups by Katz.

Proposition 2.53. *Let* $f \in \mathbb{F}_q(X)$ *with degree* $\deg(f)$ *as a morphism of* $\mathbb{P}^1$*. Then:*

(1) If $p > \deg(f)$*, the sheaf* $f_*\overline{\mathbb{Q}}_\ell$ *is Fourier.*

(2) *If the zeros of f' in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ are simple and f separates the zeros of f' (we say that f is* supermorse*), then the sheaf $f_*\overline{\mathbb{Q}}_\ell$ is geometrically irreducible.*

Thus, if the above conditions hold, there exists a geometrically irreducible ℓ-adic sheaf $\mathcal{G}_f$ over $\mathbb{F}_q$ of rank $\deg(f)-1$, lisse on $\mathbb{G}_m \times \mathbb{F}_q$, and with trace function given by (2.5).

Proof. This follows from [Kat90, Theorem 7.9.4, Lemmas 7.10.2.1, 7.10.2.3] and Proposition 2.52. □

Sums of the form (2.3) with $f = X$, $\chi = 1$, h polynomial..

Proposition 2.54. *Let $h \in \mathbb{Z}[X]$ be a polynomial of degree $n \geqslant 2$. For p large enough (depending on h), there exists a geometrically irreducible ℓ-adic sheaf $\mathcal{G}_h$ over $\mathbb{F}_q$ of rank $n-1$ corresponding to the trace function*

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

Proof. Clearly, $\mathcal{L}_{\psi(h)}$ is an irreducible Fourier sheaf, so the first part of the statement follows from Proposition 2.52. The computation of the rank can be found in [Kat90, 7.12.4.2] (see also [Kat87]). □

Sums of the form (2.3) with f polynomial, $\chi \neq 1$.

Proposition 2.55. *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, and 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 a geometrically irreducible ℓ-adic sheaf $\mathcal{G}$ over $\mathbb{F}_q$ corresponding to the trace function (2.3), with rank*

$$N = \max(d,n) - 1 + |S| + |T| + \sum_{x \in S} \mathrm{ord}_x(h),$$

where S is the set of poles of h in $\mathbb{A}^1(\overline{\mathbb{F}}_q)$ and $T = \{x \notin S : g(x) = 0\}$.

Proof. By [Kat90, 7.7, 7.13 (Sp-example(2)) and 7.14 (O-example(2))], the sheaf $f_*(\mathcal{L}_{\psi(h)} \otimes \mathcal{L}_{\chi(g)})$ is an irreducible Fourier sheaf, so the conclusion follows from Proposition 2.52. The same reference contains the computation of the rank. □

2.4.4. Zeta functions of families curves.

Zeta functions of curves. Recall that the *zeta function* of a variety X over $\mathbb{F}_q$ is defined as

$$Z(X,T) = \exp\left(\sum_{n \geqslant 1} |X(\mathbb{F}_{q^n})| \frac{T^n}{n}\right) \in \mathbb{Z}[[T]].$$

If X has dimension d, the Grothendieck-Lefschetz trace formula (Theorem 2.33) gives that

$$\begin{aligned} |X(\mathbb{F}_{q^n})| &= \sum_{i=0}^{2d}(-1)^i \operatorname{tr}(\mathrm{Frob}_q^n \mid H_c^i(X \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)), \text{ thus} \\ Z(X,T) &= \prod_{i=0}^{2d} \det(1 - T\,\mathrm{Frob}_q \mid H_c^i(X \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell))^{(-1)^{i+1}}. \end{aligned}$$

Remark 2.56. This gives the rationality part of the Weil conjectures, and the Riemann hypothesis is contained in Theorem 2.35.

When X is a curve, Theorem 2.34 implies that

$$Z(X,T) = \frac{\det(1 - T\,\mathrm{Frob}_q \mid H_c^1(X \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell))}{(1-T)(1-qT)}, \text{ so} \tag{2.6}$$

$$a_{q^n}(X) := q^n + 1 - |X(\mathbb{F}_{q^n})| = \operatorname{tr}(\mathrm{Frob}_{q^n} \mid H_c^1(X \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)).$$

Families of curves. Let U be a smooth geometrically connected projective variety over $\mathbb{F}_q$, with geometric generic point η, and let $\pi : \mathcal{C} \to U$ be a proper smooth morphism whose geometric fibers are smooth connected projective curves over $\mathbb{F}_q$ (i.e. a family of curves parametrized by U). One can construct a sheaf $\mathcal{F}$ of $\mathbb{Z}_\ell$-modules on U, corresponding to an ℓ-adic representation $\rho : \pi_1(U, \overline{\eta}) \to \mathrm{GL}(V)$ such that

$$Z(\mathcal{C}_x, T) = \frac{\det(1 - T\rho(\mathrm{Frob}_x))}{(1-T)(1-qT)} \quad (x \in U(\mathbb{F}_q)).$$

In particular, the corresponding trace function is

$$t_{\mathcal{F}}(x) = a_q(\mathcal{C}_x) = q + 1 - |\mathcal{C}_x(\mathbb{F}_q)| \ \ (x \in U(\mathbb{F}_q)).$$

This is surveyed in [KS99, Chapter 10] (using the higher direct image $R^1\pi_!\mathbb{Z}_\ell$ of the morphism π); see also [Kat09] for examples over function fields.

Families of hyperelliptic curves. We will focus on the following example (because the monodromy groups have been precisely determined):

Proposition 2.57. *For $f \in \mathbb{F}_q[X]$ a squarefree polynomial of degree $2g \geqslant 2$, such that its set of zeros Z_f is contained[3] in $\mathbb{F}_q$, 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 $z \notin Z_f$.

(1) There exists a geometrically irreducible sheaf of $\mathbb{Z}_\ell$-modules $\mathcal{F}$ over $\mathbb{F}_q$ of rank $2g$, pointwise pure of weight 1, corresponding to a representation

$$\rho : \pi_{1,q} \to \mathrm{GL}(V) = \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$$

[3] This is for convenience, to agree with Convention 2.13.

such that for all $z \notin Z_f$,

$$\begin{aligned} Z(X_z, T) &= \frac{\det(1 - T\rho(\mathrm{Frob}_z))}{(1-T)(1-qT)}, \\ t_{\mathcal{F}}(z) &= a(X_z) = q + 1 - |X_z(\mathbb{F}_q)| \in \mathbb{Z}. \end{aligned}$$

Moreover:

a) $\mathrm{Sing}(\mathcal{F}) = \{\infty\} \cup Z_f$ *and* $\mathcal{F}$ *is everywhere tame. In particular,* $\mathrm{cond}(\mathcal{F}) = 2g + |Z_f|$.

b) At any $z \in Z_f$, *the quotient* V/V^{I_z} *is the trivial (one-dimensional)* I_z*–representation.*

(2) By reduction modulo ℓ, *this gives a sheaf* $\widehat{\mathcal{F}}$ *of* $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell \cong \mathbb{F}_\ell$*-modules over* $\mathbb{F}_q$ *with the same properties and trace function* $t_{\mathcal{F}} \pmod{\ell}$.

(3) Up to changing the above relations to

$$Z(X_z, T) = \frac{\det(1 - q^{1/2}T\rho(\mathrm{Frob}_z))}{(1-T)(1-qT)} \text{ and } t_{\mathcal{F}}(z) = a(X_z)q^{-1/2},$$

we may assume that $\mathcal{F}$ *is pointwise pure of weight* 0 *by either:*

- *assuming that* $\sqrt{q} \in \mathbb{Z}_\ell^\times$ *(i.e.* $\left(\frac{\ell}{p}\right) = 1$ *by Hensel's Lemma),*
- *considering it as a sheaf of* $\overline{\mathbb{Q}}_\ell$*-modules,*
- *considering it as a sheaf of* $\mathbb{Z}[\zeta_{4p}]_\lambda$*-modules, for* λ *an* ℓ*-adic valuation.*

Proof. See [KS99, Section 10.1] or [Hal08, Section 4] (using middle-convolutions). For (3), it suffices to normalize with a Tate twist. □

Chapter 3

Monodromy

In this chapter, we introduce monodromy groups of sheaves of A-modules over $\mathbb{F}_q$, for A any ℓ-adic coefficient ring (hence giving algebraic, compact, and finite groups).

We first consider monodromy groups over $\mathbb{C}$, review results about their structure, and state Deligne's equidistribution Theorem as a motivation for the use of monodromy groups to study distribution questions.

Then, we pass to integral and finite monodromy groups and present our strategy to compute the latter by using the classification of maximal subgroup of classical groups.

We review the local monodromy of Kloosterman sheaves, both as $\overline{\mathbb{Q}}_\ell$ and $\mathbb{F}_\lambda$-modules, along with the explicit computation of some conjugacy classes.

The computation of the monodromy groups of Kloosterman sheaves over $\mathbb{C}$ is recalled, as a prelude to the proof of our result on their finite monodromy groups.

In the last section, we give further examples of the computation by Katz of monodromy groups of sheaves from Section 2.4, with techniques to make algebraic and geometric monodromy groups coincide.

3.1. Monodromy groups over $\mathbb{C}$

Definition 3.1. Let $\mathcal{F}$ be a sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$, corresponding to a representation $\rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$. The *geometric (resp. arithmetic) monodromy group* of $\mathcal{F}$ is the algebraic group in $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ defined by

$$G_{\mathrm{geom}}(\mathcal{F}) = \overline{\rho_{\mathcal{F}}\left(\pi_{1,q}^{\mathrm{geom}}\right)} \quad \leqslant \quad G_{\mathrm{arith}}(\mathcal{F}) = \overline{\rho_{\mathcal{F}}\left(\pi_{1,q}\right)} \qquad \leqslant \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell),$$

where $\overline{\cdot}$ denotes Zariski closure. Through the fixed isomorphism of fields $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ (continuous for the Zariski topology), we may also view these as complex algebraic subgroups of $\mathrm{GL}_n(\mathbb{C})$.

3.1.1. Structure. The reason to take Zariski closure is twofold:

- It gives a more rigid structure to the groups, making them *algebraic groups*.
- It allows to pass without issues from the situation over $\overline{\mathbb{Q}}_\ell$ (where the sheaves are defined) to the situation over $\mathbb{C}$ (in which we want to consider our trace functions).

The two following results support these ideas:

Proposition 3.2 (Deligne)**.** *Let $\mathcal{F}$ be a sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$. Then $G^0_{\mathrm{geom}}(\mathcal{F})$ is semisimple.*

Proof. The geometric monodromy group $G_{\mathrm{geom}}(\mathcal{F})$ is reductive by Proposition 2.27 (2) (recall that in our convention, $\mathcal{F}$ is pure of weight 0) and the semisimplicity follows from a result of Deligne ([Del80, 1.3.9], see [KS99, 9.0.12]). □

Corollary 3.3. *Let $\mathcal{F}$ be a sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ and $G = G_{\mathrm{geom}}(\mathcal{F})$. There is an equivalence of categories between:*

- *The complex representations of G as a complex algebraic group,*
- *The $\overline{\mathbb{Q}}_\ell$-representations of G as an algebraic group over $\overline{\mathbb{Q}}_\ell$,*
- *The complex representations of $G(\mathbb{C})$ as a complex Lie group,*
- *The complex representations of a maximal compact subgroup of $G(\mathbb{C})$,*

where all the representations are assumed to be finite-dimensional.

Proof. See [Kat88, 3.2], [KS99, 9.2.4], and more particularly [Mil13, Remark III.2.11]. The equivalence between the last two categories is Weyl's unitary trick. □

3.1.2. Reformulation of Theorem 2.28. It is often desirable to have equal arithmetic and geometric monodromy groups, so that the Frobenius conjugacy classes lie in the geometric monodromy group, giving for example the following proposition. As we will see in Section 3.5.7, this is often achievable up to twisting by a sheaf of rank one.

Proposition 3.4. *For $\mathcal{F}$ a sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ with monodromy groups $G = G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F})$, we have*

$$\sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x) = q\dim(\mathcal{F}_G) + O\left(\mathrm{cond}(\mathcal{F})^2\sqrt{q}\right),$$

In particular, if $\mathcal{F}$ is irreducible, then $\dim(\mathcal{F}_G) = 1$ if $\mathcal{F}$ is trivial and 0 otherwise.

Proof. Since the coinvariants are defined by an algebraic relation, we have $\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}} = \mathcal{F}_G$. Since $\mathrm{Frob}_q \in G_{\mathrm{arith}}(\mathcal{F}) = G_{\mathrm{geom}}(\mathcal{F})$, the Frobenius acts trivially on $\mathcal{F}_G$ and the result follows from Theorem 2.28. The last claim follows from Schur's lemma. □

3.1.3. Deligne's equidistribution theorem. The following theorem of Deligne shows that for a "natural" family of ℓ-adic sheaves, there is always an equidistribution result in a compact group.

Let $\mathcal{F}$ be an ℓ-adic trace function over $\mathbb{F}_q$, corresponding to a representation $\rho : \pi_{1,q} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$. Again, we assume that

$$G = G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F}) \leqslant \mathrm{GL}_n(\mathbb{C})$$

and we let K be a maximal compact subgroup of the complex Lie group $G(\mathbb{C})$. For any $x \in U_{\mathcal{F}}(\mathbb{F}_q)$, let

$$\iota(\rho(\mathrm{Frob}_x))^{\mathrm{ss}}$$

be the semisimple part of the Jordan-Chevalley decomposition in G, defined up to conjugation in G. Since all its eigenvalues lie in the unit circle ($\mathcal{F}$ is pure of weight 0), any element of this conjugacy class belongs to a maximal compact subgroup of $G(\mathbb{C})$, and is thus conjugate to an element θ_x of K.

Lemma 3.5. *The conjugacy class $\theta_x \in K^\sharp$ is well-defined, and $t_{\mathcal{F}}(x) = \mathrm{tr}(\theta_x)$.*

Proof. This follows from Corollary 3.3 and the Peter-Weyl Theorem, see [KS99, 9.2.4] or [Kat88, 3.3]. □

Theorem 3.6 (Deligne's equidistribution theorem)**.** *Let $(\mathcal{F}_q)_q$ be a family of ℓ-adic sheaves over $\mathbb{F}_q$, corresponding to representations*

$$\rho_q : \pi_{1,q} \to \mathrm{GL}_n(\overline{\mathbb{Q}_\ell}).$$

We assume that there is an algebraic group $G \leqslant \mathrm{GL}_n(\mathbb{C})$ such that

(1) The arithmetic and geometric monodromy groups of $\mathcal{F}_q$ are conjugate to G in $\mathrm{GL}_n(\mathbb{C})$ for all q.

(2) $\mathrm{cond}(\mathcal{F}_q)$ is uniformly bounded (i.e. independently of q).

Let K be a maximal compact subgroup of $G(\mathbb{C})$ and for all q, $x \in U_{\mathcal{F}}(\mathbb{F}_q)$, let $\theta_{x,q} \in K^\sharp$ be the conjugacy class given by Lemma 3.5. When $q \to \infty$, the set

$$\{\theta_{x,q} : x \in U_{\mathcal{F}}(F_q)\}$$

becomes equidistributed in $K^\sharp$ with respect to the pushforward μ of the normalized Haar measure of K. In other words, for any $f \in C(K^\sharp)$, we have

$$\lim_{q\to\infty} \frac{1}{q} \sum_{x\in U_{\mathcal{F}}(F_q)} f(\theta_{x,q}) = \int_{K^\sharp} f d\mu.$$

Proof. By Weyl's criterion, it suffices to show that for any nontrivial irreducible representation $\eta : K \to \mathrm{GL}_m(\mathbb{C})$ we have

$$\frac{1}{q} \sum_{x\in U_{\mathcal{F}}(F_q)} (\mathrm{tr}\circ\eta)(\theta_{x,q}) = o(q) \ (q \to +\infty).$$

By Corollary 3.3, there exist $\hat{\eta}$ (resp. $\tilde{\eta}$) a complex representation of G (resp. a $\overline{\mathbb{Q}}_\ell$-representation of the algebraic group $\iota^{-1}(G)$ over $\overline{\mathbb{Q}}_\ell$) such that the diagram

$$\begin{array}{ccc} \iota^{-1}(G) & \xrightarrow{\tilde{\eta}} & \mathrm{GL}_m(\overline{\mathbb{Q}}_\ell) \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ G & \xrightarrow{\hat{\eta}} & \mathrm{GL}_m(\mathbb{C}) \\ \uparrow & \nearrow_{\eta} & \\ K & & \end{array}$$

commutes. Let $\mathcal{G}_q$ be the sheaf corresponding to the ℓ-adic representation

$$\tilde{\eta} \circ \rho_q : \pi_{1,q} \to \iota^{-1}(G) \to \mathrm{GL}_m(\overline{\mathbb{Q}}_\ell).$$

Note that $\mathcal{G}_q$ is irreducible, and has arithmetic and geometric monodromy group equal to $\hat{\eta}(G)$. Moreover, for all $x \in U_{\mathcal{F}}(\mathbb{F}_q)$,

$$\begin{aligned} t_{\mathcal{G}_q}(x) &= \mathrm{tr}\left((\eta\circ\iota\circ\rho_q)(\mathrm{Frob}_{x,q})\right) = \mathrm{tr}\left((\eta\circ\iota\circ\rho_q)(\mathrm{Frob}_{x,q})^{\mathrm{ss}}\right) \\ &= \mathrm{tr}\left(\eta\big(\iota(\rho_q(\mathrm{Frob}_{x,q}))^{\mathrm{ss}}\big)\right) = \mathrm{tr}(\eta(\theta_{x,q})). \end{aligned}$$

By Proposition 3.4,

$$\frac{1}{q}\sum_{x\in U_{\mathcal{F}}(F_q)}(\mathrm{tr}\circ\eta)(\theta_{x,q}) = \frac{1}{q}\sum_{x\in U_{\mathcal{F}}(\mathbb{F}_q)} t_{\mathcal{G}_q}(x) \ll \mathrm{cond}(\mathcal{G}_q)^2 q^{-1/2}.$$

By definition, $x \notin \mathrm{Sing}(\mathcal{G}_q)$ if and only if $\tilde{\eta}(\rho(I_x)) = 1$. In particular, $\mathrm{Sing}(\mathcal{G}_q) \subset \mathrm{Sing}(\mathcal{F}_q)$. Moreover, $\mathrm{Swan}_x(\mathcal{G}_q) \leqslant \dim \eta\, \mathrm{Swan}_x(\mathcal{F}_q)$ for all $x \in \mathbb{P}^1(\mathbb{F}_q)$ by [Kat88, 3.6.2]. It follows that $\mathrm{cond}(\mathcal{G}_q) \leqslant m\,\mathrm{cond}(\mathcal{F}_q) \ll 1$ by hypothesis, whence the conclusion. □

Remark 3.7. See also [KS99, Theorem 9.2.6, Theorem 9.6.10] for other variants.

Example 3.8 (Kloosterman sums, [Kat88, 13.5.3]). Let $\mathcal{K}l_2$ be the Kloosterman sheaf over $\mathbb{F}_q$ from Section 2.4.2, with trace function equal to the classical Kloosterman sum $\mathrm{Kl}_{2,q}$. By Proposition 2.46, the conductor is bounded independently from q. As we shall soon see, the geometric monodromy group is $\mathrm{SL}_2(\mathbb{C})$, with maximal compact subgroup $K = \mathrm{SU}_2(\mathbb{C})$, and coincides with the arithmetic monodromy group. The map $\arccos(\frac{1}{2}\,\mathrm{tr}) : K^\sharp \to [0,\pi]$ is a bijection, so that we can write for all $x \in \mathbb{F}_q^\times$

$$\mathrm{Kl}_{2,q}(x) = 2\cos(\theta_{x,q}(x))$$

with $\theta_{x,q} \in [0,\pi]$ uniquely determined. Therefore the set

$$\{\theta_{x,q} : x \in \mathbb{F}_q^\times\}$$

becomes equidistributed in $[0,\pi]$ as $q \to \infty$ with respect to the measure $\frac{2}{\pi}\sin^2\theta d\theta$. This is the vertical Sato-Tate law for Kloosterman sums, and this answers one of the questions of Section 1.1.3.

3.1.4. Real-valued trace functions and monodromy groups. Finally, we note the following relationship, that will be useful in Chapter 5, between the range of the trace function and the monodromy group:

Proposition 3.9. *Let $\mathcal{F}$ be a geometrically irreducible ℓ-adic sheaf over $\mathbb{F}_q$, 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) $\mathrm{mult}_1(\mathrm{Std}^{\otimes 2}) = \mathrm{mult}_1(\mathrm{Std}\otimes D(\mathrm{Std})) = 1$.

Proof. Let K be a maximal compact subgroup of $G(\mathbb{C})$. By Corollary 3.3, it does not matter whether we consider 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 $\iota(\mathrm{tr}(\rho_{\mathcal{F}}(\pi_{1,q}))) \subset \mathbb{R}$ for all q, which in turn holds if and only if $\mathrm{tr}(G) \subset \mathbb{R}$. Hence, (1) is equivalent to (2) by character theory of $G(\mathbb{C})$. If (2) holds, then

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

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 Lemma 3.5. □

Example 3.10. Recall that the standard representations of $\mathrm{Sp}_{2n}(\mathbb{C})$ and $\mathrm{SO}_n(\mathbb{C})$ are self-dual, but not that of $\mathrm{SL}_n(\mathbb{C})$ for $n \geqslant 3$. Thus, the fact that Kloosterman sums of even rank are real-valued agrees with the fact that the monodromy group is symplectic (Theorem 3.23 below).

3.1.5. Determining monodromy groups. As we will see in the remaining of this chapter, one successful general strategy to determine the monodromy groups of an ℓ-adic sheaf corresponding to a representation

$$\rho : \pi_{1,q} \to \mathrm{GL}_n(A)$$

is to study the images of the inertia groups at singularities, which lie in G_{geom}. For example, the tame part of the break decomposition gives unipotent elements with prescribed Jordan form (see e.g. Proposition 3.19 below), while the Swan conductor can rule out the existence of certain morphisms (see e.g. [Kat88, Lemma 1.19]).

Assume that we want to show that G_{geom} is equal to some complex algebraic group H. The idea exploited in [Kat88], [Kat90] is:

(1) Show that $G_{\mathrm{geom}} \leqslant H$, often for symmetry reasons.

(2) By using the information provided by the ramification, apply classification theorems to the Lie algebra of G^0_{geom} (which is semisimple by Proposition 3.2) to show that $G^0_{\mathrm{geom}} = H$.

It would then follows that $G_{\mathrm{geom}} = G^0_{\mathrm{geom}} = H$.

3.2. Integral and finite monodromy groups

3.2.1. Integral monodromy groups.

Definition 3.11. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_\lambda$-modules over $\mathbb{F}_q$, corresponding to a representation $\rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}_n(\mathcal{O}_\lambda)$, for $\mathcal{O}$ the ring of integer of a number field and λ an ℓ-adic valuation on $\mathcal{O}$. The *integral arithmetic (resp. geometric) monodromy group* of $\mathcal{F}$ is the group

$$G_{\mathrm{arith}}(\mathcal{F}) = \rho_{\mathcal{F}}(\pi_{1,q}), \quad \text{resp. } G_{\mathrm{geom}}(\mathcal{F}) = \rho_{\mathcal{F}}\big(\pi_{1,q}^{\mathrm{geom}}\big) \quad \leqslant \mathrm{GL}_n(\mathcal{O}_\lambda).$$

3.2.2. Finite monodromy groups.

Definition 3.12. Let $\mathcal{F}$ be a sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$, corresponding to a representation $\rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\lambda)$, for $\mathbb{F}_\lambda$ a finite field of characteristic ℓ. The *arithmetic (resp. geometric) finite monodromy group* of $\mathcal{F}$ is the finite group

$$G_{\mathrm{arith}}(\mathcal{F}) = \rho_{\mathcal{F}}(\pi_{1,q}), \quad \text{resp. } G_{\mathrm{geom}}(\mathcal{F}) = \rho_{\mathcal{F}}\big(\pi_{1,q}^{\mathrm{geom}}\big) \quad \leqslant \mathrm{GL}_n(\mathbb{F}_\lambda).$$

3.2.3. Determining monodromy groups. The determination of the integral and finite monodromy groups is usually much more difficult than that of the monodromy groups over $\mathbb{C}$, since we consider simply subgroups of $\mathrm{GL}_n(A)$ for A an ℓ-adic coefficient ring, instead of algebraic subgroups G of $\mathrm{GL}_n(\mathbb{C})$ with G^0 semisimple as before, and the structure of such groups and their subgroups is much more complicated.

Here, we will focus on $\mathbb{F}_\lambda$-monodromy groups, since this is the case of interest for our applications. We will nonetheless survey some results and techniques for integral monodromy groups later on. The two are closely related.

Using the classification of maximal subgroups of classical groups. Suppose that $\mathcal{F}$ is a sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$ such that $G_{\mathrm{geom}}(\mathcal{F})$ is contained in some *classical group* $G \leqslant \mathrm{GL}_n(\mathbb{F}_\lambda)$, and we want to show that $G_{\mathrm{geom}}(\mathcal{F}) = G$. If this is not the case, there exists a maximal subgroup H of G such that

$$G_{\mathrm{geom}}(\mathcal{F}) \lneq H \lneq G.$$

We may be able to exclude this possibility by using the classification of maximal subgroups of classical groups. This can be achieved for Kloosterman sheaves, as we will show.

In the remaining of this section, we survey this classification in a way adapted to our needs.

Theorem 3.13 ([Asc84], [LS98])**.** *Let $\mathbb{F}_\lambda$ be a finite field of odd characteristic ℓ and for $n \geqslant 2$, let $G = \mathrm{SL}_n(\mathbb{F}_\lambda)$ or $G = \mathrm{Sp}_n(\mathbb{F}_\lambda)$ (n even). We denote by $\pi : \mathrm{GL}_n(\overline{\mathbb{F}}_\lambda) \to \mathrm{PGL}_n(\overline{\mathbb{F}}_\lambda)$ the projection. If H is a maximal (proper) subgroup of G, then either:*

(1) H belongs to one of the classes $\mathcal{C}_1, \dots, \mathcal{C}_7$ described below, or

(2) $\pi(H)$ is almost simple*: there exists a simple group S such that*

$$S \cong \mathrm{Inn}(S) \trianglelefteq \pi(H) \leqslant \mathrm{Aut}(S).$$

Moreover, H admits a unique normal subgroup T such that $\pi(T) = S$, and the action of $T \trianglelefteq H \leqslant \mathrm{SL}_n(\mathbb{F}_\lambda)$ on $\overline{\mathbb{F}}_\lambda^n$ is absolutely irreducible. If $G = \mathrm{SL}_n(\mathbb{F}_\lambda)$, then T preserves no nondegenerate bilinear or unitary form on $\mathbb{F}_\lambda^n$.

Proof. This is a combination of Theorems 1 and 2 from [LS98]. □

This classification originated from the work of Aschbacher [Asc84], and was then expanded by Kleidman-Liebeck [KL90b]. Another proof was given by Liebeck-Seitz [LS98] by proving an analogous result over an algebraically closed field and using descent[1] (as in the treatment of finite groups of Lie type with Steinberg

[1]The following comments in the introduction of [LS98] are particularly enlightening: "*Aschbacher's result is an analogous reduction theorem for subgroups of finite classical groups. We obtain this as a relatively easy consequence of our main result by taking fixed points under the action of a Frobenius morphism, using a standard process involving Lang's theorem. [...] Various complications which arise in the finite group setting in [Asc84] become much more straightforward in the algebraic group setting; in particular, questions involving extension fields do not occur, and issues of conjugacy are easily settled.*"

isomorphisms). A good exposition of these results can be found in [MT11, II.18.1, III.27–28].

We now recall the definition of the classes $\mathcal{C}_1, \dots, \mathcal{C}_7$, along with some useful properties we will use.

Let $V = \mathbb{F}_\lambda^n$, $\boldsymbol{V} = \overline{\mathbb{F}}_\lambda^n$, and $\mathrm{Frob} \in \mathrm{Gal}(\overline{\mathbb{F}}_\lambda/\mathbb{F}_\lambda)$ be the *arithmetic* Frobenius $x \mapsto x^{|\mathbb{F}_\lambda|}$. We will write $\boldsymbol{G} = \mathrm{SL}_n(\overline{\mathbb{F}}_\lambda)$ (resp. $\mathrm{Sp}_n(\overline{\mathbb{F}}_\lambda)$). Let β be the zero bilinear form on V if $G = \mathrm{SL}_n(\mathbb{F}_\lambda)$ or the symplectic form associated to G if $G = \mathrm{Sp}_n(\mathbb{F}_\lambda)$. The classes appearing in (1) of Theorem 3.13 are the following:

– Class $\mathcal{C}_1$ (subspace stabilizers):

$$H = \mathrm{Stab}_G(W)$$

with $0 \neq W \lneq V$ totally singular or nondegenerate with respect to β. Note that $W \leqslant V$ is a submodule, so this case does not arise if H acts on V irreducibly.

– Class $\mathcal{C}_2$ (stabilizers of orthogonal decompositions):

$$\begin{aligned} \boldsymbol{V} &= \boldsymbol{V}_1 \perp \cdots \perp \boldsymbol{V}_t \\ &\quad (t \geqslant 2,\ \text{all the } \boldsymbol{V}_i \text{ isometric},\ n = \dim(\boldsymbol{V}_1)t), \\ \boldsymbol{M} &= \mathrm{Stab}_{\boldsymbol{G}}(\boldsymbol{V}_1 \perp \cdots \perp \boldsymbol{V}_t), \\ H &\leqslant \boldsymbol{M}^{\mathrm{Frob}}. \end{aligned}$$

In other words, the elements of $\boldsymbol{M}$ are the $g \in \boldsymbol{G}$ such that there exists a permutation $\sigma \in \mathfrak{S}_t$ with $g\boldsymbol{V}_i = \boldsymbol{V}_{\sigma(i)}$ for all $1 \leqslant i \leqslant t$.

– Class $\mathcal{C}_3$ (stabilizers of totally singular decompositions): if $G = \mathrm{Sp}_n(\mathbb{F}_\lambda)$,

$$\begin{aligned} \boldsymbol{V} &= \boldsymbol{V}_1 \oplus \boldsymbol{V}_2 \quad (\boldsymbol{V}_i \text{ maximal totally isotropic: } \beta|_{\boldsymbol{V}_i} = 0), \\ \boldsymbol{M} &= \mathrm{Stab}_{\boldsymbol{G}}(\boldsymbol{V}_1 \oplus \boldsymbol{V}_2), \\ H &\leqslant \boldsymbol{M}^{\mathrm{Frob}}. \end{aligned}$$

In other words, the elements of M are the $g \in \boldsymbol{G}$ such that there exists a permutation $\sigma \in \mathfrak{S}_2$ with $g\boldsymbol{V}_i = \boldsymbol{V}_{\sigma(i)}$ for $i = 1, 2$. In particular, $\dim(\boldsymbol{V}_1) = \dim(\boldsymbol{V}_2) = n/2$.

– Class $\mathcal{C}_4$ (stabilizers of tensor product decompositions):

$$\begin{aligned} \boldsymbol{V} &= \boldsymbol{V}_1 \otimes \cdots \otimes \boldsymbol{V}_t \quad (\dim \boldsymbol{V}_i \geqslant 2,\ t \geqslant 2), \\ \boldsymbol{L} &= \boldsymbol{G}(\boldsymbol{V}_1) \times \cdots \times \boldsymbol{G}(\boldsymbol{V}_t), \text{ acting on } \boldsymbol{V} \text{ by tensor product}, \\ \boldsymbol{M} &= N_{\mathrm{GL}_n(\overline{\mathbb{F}}_\lambda)}(\boldsymbol{L}) \cap \boldsymbol{G}, \\ H &\leqslant \boldsymbol{M}^{\mathrm{Frob}}, \end{aligned}$$

with $t = 2$ if the $\boldsymbol{V}_i$ are not mutually isomorphic, where we write $\boldsymbol{G}(\boldsymbol{V}_i)$ for the classical group of type $\boldsymbol{G}$ on the vector space $\boldsymbol{V}_i$. Note that $n = \dim(\boldsymbol{V}_1) \dots \dim(\boldsymbol{V}_t)$, and $n = \dim(\boldsymbol{V}_1)^t$ if the $\boldsymbol{V}_i$ are mutually isomorphic. We have

$$\pi\left(N_{\mathrm{GL}_n(\overline{\mathbb{F}}_\lambda)}(\boldsymbol{L}) \cap \boldsymbol{G}\right) \leqslant N_{\mathrm{PGL}_n(\overline{\mathbb{F}}_\lambda)}(\pi(\boldsymbol{L})) \cap \pi(\boldsymbol{G}) = \boldsymbol{N}.$$

Since $\pi(\boldsymbol{G})$ has trivial center, there is a morphism from $\boldsymbol{N}$ to

$$\begin{aligned}\mathrm{Aut}(\pi(\boldsymbol{L})) &= \mathrm{Aut}\left(\pi(\boldsymbol{G}(\boldsymbol{V}_1)) \times \cdots \times \pi(\boldsymbol{G}(\boldsymbol{V}_t))\right) \\ &\cong \begin{cases} \mathrm{Aut}\left(\pi(\boldsymbol{G}(\boldsymbol{V}_1))\right) \times \mathrm{Aut}\left(\pi(\boldsymbol{G}(\boldsymbol{V}_2))\right) & : t = 2 \\ \mathrm{Aut}\left(\pi(\boldsymbol{G}(\boldsymbol{V}_1))\right) \wr \mathfrak{S}_t & : t > 2 \end{cases} \\ &\to \begin{cases} \mathrm{Out}\left(\pi(\boldsymbol{G}(\boldsymbol{V}_1))\right) \times \mathrm{Out}\left(\pi(\boldsymbol{G}(\boldsymbol{V}_2))\right) & : t = 2 \\ \mathrm{Out}\left(\pi(\boldsymbol{G}(\boldsymbol{V}_1))\right) \wr \mathfrak{S}_t & : t > 2, \end{cases}\end{aligned}$$

with kernel isomorphic to $\pi(\boldsymbol{L}) \cap \pi(\boldsymbol{G})$. The isomorphism on the second line follows from:

Lemma 3.14. *Let $G_1, \ldots, G_t$ be nonabelian simple groups and let $G = G_1 \times \cdots \times G_t$. Then $\mathrm{Aut}(G_1 \times \cdots \times G_t)$ is isomorphic to*

$$\mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_t)$$

if there is no isomorphism among the G_i, respectively

$$\mathrm{Aut}(G_1) \wr \mathfrak{S}_t$$

if the G_i are mutually isomorphic.

Proof. Proceed as in the second paragraph of the proof of [Rob96, 3.3.20]. □

– Class $\mathcal{C}_5$ (symplectic-type r-subgroups):

$$\pi(H) \cong \begin{cases} \mathbb{Z}/r^{2m}.\,\mathrm{Sp}_{2m}(\mathbb{F}_r) & : G = \mathrm{SL}_n(\mathbb{F}_{r^m}) \\ \mathbb{Z}/2^{2m}.\,\mathrm{GO}^-_{2m}(\mathbb{F}_2) & : G = \mathrm{Sp}_n(\mathbb{F}_{2^m}) \end{cases}$$

with $n = r^m$, $r \neq \ell$ prime, $\ell \equiv 1 \pmod{r(2,r)}$. Here, we only give the classification of the subgroups that arise in the class; for more details about the latter, see [KL90b, Section 4.6].

– Class $\mathcal{C}_6$ (normalizers of classical groups): For $G = \mathrm{SL}_n(\mathbb{F}_\lambda)$ with n odd (since $\ell \neq 2$, this class does not arise in the symplectic case) and $\mathbb{F}' \leqslant \mathbb{F}_\lambda$ a subfield such that $|\mathbb{F}'| = |\mathbb{F}_\lambda|^{1/2}$,

$$H = N_G(\mathrm{SO}_n(\mathbb{F}_\lambda)) \text{ or } N_G(\mathrm{SU}_n(\mathbb{F}')).$$

– Class $\mathcal{C}_7$ (subfield subgroups): For $\mathbb{F}' \leqslant \mathbb{F}_\lambda$ of prime index,

$$H = N_G(G(\mathbb{F}')).$$

Note that the unitary cases of classes $\mathcal{C}_6$ and $\mathcal{C}_7$ do not arise if $\mathbb{F}_\lambda = \mathbb{F}_\ell$.

Remark 3.15. Similar results hold for other classical groups and the description of the classes $\mathcal{C}_i$ can be made more explicit (see [LS98]).

Review on automorphisms groups. We now recall results about automorphisms of Lie algebras/Lie groups/finite groups of Lie type that will be useful several times in this chapter and the next one, in particular to handle class $\mathcal{C}_4$ and case (2) of Theorem 3.13.

Proposition 3.16. *If G is a simple Lie algebra (resp. a simply connected simple Lie group) over an algebraically closed field, there is an isomorphism between* $\mathrm{Out}(G)$ *and the group of graph automorphisms of the corresponding Dynkin diagram.*

Proof. This can be found in [Hum80, Chapter 16.5] and [FH91, Proposition D.40]. □

In the finite case, this becomes:

Proposition 3.17. *If G is a finite simple group of Lie type defined over a finite field k, every automorphism can be written as the product of an inner, graph, diagonal, and field automorphism. More precisely,*

$$\mathrm{Out}(G) \cong (\mathrm{Diag}(G)\,\mathrm{Aut}(k))\,.\mathrm{Graph}(G),$$

where $\mathrm{Diag}(G)$ *(resp.* $\mathrm{Graph}(G)$*) is the group of diagonal automorphisms (resp. the group of graph automorphisms of the corresponding Dynkin diagram).*

Proof. See [Gor82, 4.237] and [Car72, Theorem 12.5.1]. □

Proposition 3.18. *The automorphism group of a Dynkin diagram is*

$$\begin{cases} \mathbb{Z}/2 & \text{for } A_n,\ D_n\ (n>1),\ \text{and } E_6, \\ \mathfrak{S}_3 & \text{for } D_4, \\ \text{trivial} & \text{otherwise.} \end{cases}$$

3.3. Local monodromy of Kloosterman sheaves

In this section, we summarize the properties of Kloosterman sheaves (see Section 2.4.2) that will be useful to recall Katz's [Kat88] computation of the monodromy over $\mathbb{C}$ and to prove our version over $\mathbb{F}_\lambda$. According to Katz, all were already known to Deligne but the last one.

Proposition 3.19. *Let $n \geqslant 2$ and let $\mathcal{K}l_n$ be the Kloosterman sheaf of A-modules over $\mathbb{F}_q$ from Proposition 2.46, corresponding to a representation $\rho : \pi_{1,q} \to \mathrm{GL}_n(A)$, for A equal to $\overline{\mathbb{Q}}_\ell$, or $\mathbb{F}_\lambda$. Then*

(1) $\mathcal{K}l_n$ is unipotent as I_0-representation, with a single Jordan block.

(2) $\mathcal{K}l_n$ is totally wild at ∞, with $\mathrm{Swan}_\infty(\mathcal{K}l_n) = 1$. In particular:

  a) $\rho(I_\infty)$ acts irreducibly on A^n and admits no faithful A-linear representation of dimension $< n$.

  b) Any character $\rho(I_\infty) \to A^\times$ is trivial on $\rho(P_\infty)$.

(3) $\det \mathcal{K}l_n$ is trivial.

(4) *If n is even, there exists an alternating perfect pairing $\mathcal{K}l_n \otimes \mathcal{K}l_n \to A$ of lisse sheaves.*

(5) *If n is odd, then $\mathcal{K}l_n \otimes \mathcal{K}l_n$ is totally wild at ∞, with all breaks at $1/n$. In particular, there is no nonzero P_∞-equivariant bilinear form $\mathcal{K}l_n \otimes \mathcal{K}l_n \to A$.*

Proof. (1) See [Kat88, 7.4.1]. By [Kat88, 12.3.3], $\mathcal{K}l_n$ as a sheaf of $\mathbb{F}_\lambda$-modules still has a single Jordan block.

(2) This is [Kat88, 1.11, 1.18] with the fact that $\mathrm{Swan}_\infty(\mathcal{K}l_n) = 1$.

(3) See [Kat88, 7.4.3].

(4) See [Kat88, 4.1.11] (existence) and [Kat88, 4.2.1] (sign).

(5) For the first assertion, see [Kat88, 10.4.4]. For the second, proceed as in [Kat88, 4.1.7].

In the finite case, see also [Kat88, 12.3]. □

3.3.1. Explicit local monodromy. We now compute explicit conjugacy classes in the monodromy groups that will serve as heuristics and to exclude subfield subgroups in the computation of finite monodromy groups.

Local monodromy at ∞. The local monodromy at ∞ of $\mathcal{K}l_n$ is determined explicitly in [Kat88] (as P_∞-representation) and [KMS16] (more precisely as I_∞-representation), and more generally for hypergeometric sheaves in [Fu10, Proposition 0.7]. We make this even more concrete for Kloosterman sheaves by finding a matrix form of the representation.

Proposition 3.20. *Assume that $n \geqslant 2$ is coprime with p and that $k = \mathbb{F}_q$ contains a primitive $2n$th root of unity ζ_{2n}. Let $Z \in \overline{k(T)}$ be a solution to $Z^{2n} = T$ and $W \in \overline{k(Z)} = \overline{k(T)}$ be a solution to*

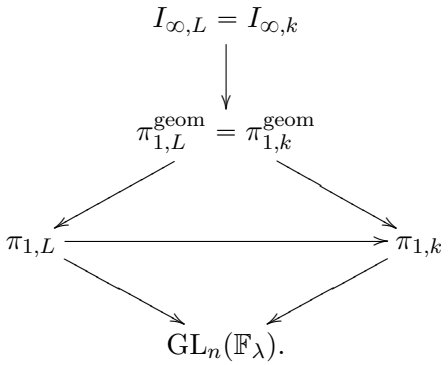
$$W^{|k|} - W = -Z^2.$$

Then the restriction $I_\infty \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ of the representation associated to the sheaf $\mathcal{K}l_n$ over k is isomorphic to

$$\sigma \mapsto \left((-1)^{(n+1)\left(\frac{j-i+i_0}{n}\right)} e\left(\frac{n \operatorname{tr}_{k/\mathbb{F}_p}(a_0\zeta_n^i)}{p}\right) \delta_{i-j\equiv i_0 \pmod n} \right)_{1\leqslant i,j\leqslant n,}$$

where $i_0 \in \mathbb{Z}/2n$ and $a_0 \in k$ are such that $\sigma(Z) = \zeta_{2n}^{i_0} Z$ and $\sigma(W) = \zeta_{2n}^{2i_0}(W + a_0)$.

Remark 3.21. Assuming that k contains a nth root of unity is not a restriction for our purpose. Indeed, if L/k is a finite extension, we have a commutative diagram



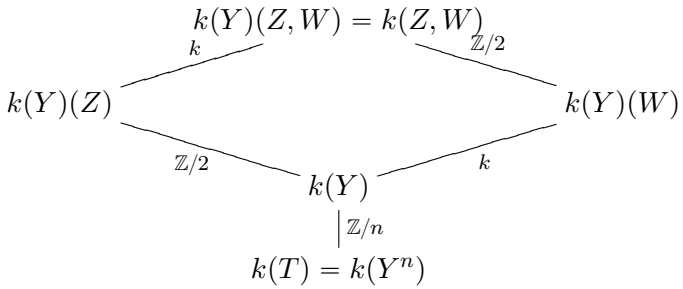
Proof. By [Kat88, 10.4.5] and [KMS16, Lemma 4.8][2], the representation of I_∞ corresponding to $\mathcal{K}l_n$ is isomorphic to

$$[x \mapsto x^n]_* \left(\mathcal{L}_{\chi_2}^{n+1} \otimes \mathcal{L}_{\psi(xn)}\right),$$

where χ_2 is the character of order 2 of $\overline{\mathbb{F}}_p^\times$ and $\psi(x) = e(\mathrm{tr}(x)/p)$. In other words, it is isomorphic to

$$\mathrm{Ind}_{I_{\infty,n}}^{I_\infty} \left(\mathcal{L}_{\chi_2}^{n+1} \otimes \mathcal{L}_{\psi(xn)}\right),$$

where $I_{\infty,n}$ is the unique subgroup of index n in I_∞ (see [Kat88, 1.13]).



The extension $k(Z,W)/k(T)$ is Galois, and we have a split exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k & \longrightarrow & G & \longrightarrow & \mathbb{Z}/2n & \longrightarrow & 0 \\ & & \wr\| & & \| & & \wr\| & & \\ & & \mathrm{Gal}(k(Z,W)/k(Z)) & & \mathrm{Gal}\left(k(Z,W)/k(T)\right) & & \mathrm{Gal}(k(Y)(Z)/k(T)), & & \end{array}$$

so an isomorphism

$$\begin{array}{rcl} k \rtimes \mathbb{Z}/2n & \to & G = \mathrm{Gal}\left(k(Z,W)/k(T)\right) \\ (a,i) & \mapsto & \sigma(a,i) \end{array}$$

where $\sigma(a,i)$ is such that $W \mapsto \zeta_{2n}^{2i}(W+a)$ and $Z \mapsto \zeta_{2n}^i Z$. For every $(a,i) \in G$, there exists an element of $I_{\infty,n}$ extending $\sigma(a,i)$, that we will again denote by $\sigma(a,i)$.

We have

$$I_{\infty,n} = I_\infty \cap \pi_{1,q}^{(n)},$$

[2]The factor $1/k$ in $\hat{\psi}$ therein should be replaced by k.

where $\pi_{1,q}^{(n)} = \mathrm{Gal}(\overline{K(T)}/K(Y))$ is the subgroup of index n in $\pi_{1,q}$. Indeed,

$$\begin{aligned} I_\infty/(I_\infty \cap \pi_{1,q}^{(n)}) &= I_\infty \pi_{1,q}^{(n)}/\pi_{1,q}^{(n)} = \pi_{1,q}/\pi_{1,q}^{(n)} \\ &\cong \mathrm{Gal}(k(Y)/k(T)) \cong \mu_n(k) \cong \mathbb{Z}/n. \end{aligned}$$

Note that $(\sigma_i)_{1\leqslant i\leqslant n}$ is a complete reduced system of representatives of $I_\infty/I_{\infty,n}$, where we abbreviate $\sigma_i = \sigma(0,i)$.

By definition (or properties) of induced representations, a matrix form of the representation $I_\infty \to \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ evaluated at $\sigma = \sigma(a_0,i_0) \in I_\infty$ is then

$$\left(\left(\mathcal{L}_{\chi_2}^{n+1} \otimes \mathcal{L}_{\psi(xn)}\right)(\sigma_{i,j}(\sigma))\delta_{\sigma_{i,j}(\sigma)\in I_{\infty,n}} \right)_{1\leqslant i,j\leqslant n,}$$

where $\sigma_{i,j}(\sigma) = \sigma_i^{-1}\sigma\sigma_j$. It remains to note that $\sigma_{i,j}(\sigma) \in I_{\infty,n}$ if and only if $2(i-j) \equiv 2i_0 \pmod{2n}$, in which case:

– By definition of the Artin-Schreier representation,

$$\mathcal{L}_{\psi(xn)}(\sigma_{i,j}(\sigma)) = \psi((\sigma_{i,j}(\sigma)(W) - W)n),$$

and $\sigma_{i,j}(\sigma)(W) - W = \zeta_n^{2(j+i_0)}a_0$.

– By definition of the Kummer representation, if n is even,

$$\mathcal{L}_{\chi_2}^{n+1}(\sigma_{i,j}(\sigma)) = \zeta_n^{\frac{j-i+i_0}{2}} = (-1)^{\frac{j-i+i_0}{n}}.$$

□

In particular, we see that the image of the representation of I_∞ contains an element conjugate to the (permutation, up to signs) matrix

$$m = \begin{pmatrix} 0 & 0 & \dots & 0 & (-1)^{n+1} \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & & & 1 & 0 \end{pmatrix}.$$

Note that m has order n (resp. $2n$) if n is odd (resp. even).

Local monodromy at 0. By Proposition 3.19 (1), the geometric monodromy group contains an element conjugate to the Jordan block

$$u = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & 1 & \ddots & \\ & & & \ddots & 1 \\ & & & & 1 \end{pmatrix}.$$

Note that for $\mathbb{F}_\lambda$ a finite field of characteristic ℓ, the element $u \in \mathrm{SL}_n(\mathbb{F}_\lambda)$ satisfies $(u^k)_{ij} = \delta_{i\leqslant j\leqslant k}\binom{k}{j-i}$ for $1 \leqslant i,j \leqslant n$, so it has order $\ell^{\lceil \log_\ell n \rceil}$ by Lucas' theorem. In particular, u has order ℓ if $\ell \gg_n 1$.

3.3.2. Fields generated by traces. The following will be useful to deal with subfield subgroups; it shows that we still recover arithmetic information (the subfield generated by the traces of the Frobenius) in the geometric monodromy group.

Proposition 3.22. *Let $n \geqslant 2$, λ be an ℓ-adic valuation on*

$$\mathcal{O} = \begin{cases} \mathbb{Z}[\zeta_p] & n \text{ odd or } p \equiv 1 \pmod 4 \\ \mathbb{Z}[\zeta_{4p}] & \text{otherwise,} \end{cases}$$

and let $\rho_n : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\lambda)$ be the representation corresponding to the Kloosterman sheaf $\mathcal{K}l_n$ of $\mathcal{O}_\lambda$-modules over $\mathbb{P}^1/\mathbb{F}_q$. Then

$$\mathbb{F}_\ell\left(\mathrm{Kl}_{n,q}(a) : a \in \mathbb{F}_q^\times\right) = \mathbb{F}_\ell\left(\operatorname{tr} \rho_n(I_\infty)\right),$$

with index (f, n) in $\mathbb{F}_\lambda$.

Proof. Under the hypotheses, $\mathbb{F}_\lambda = \mathbb{F}_\ell(\zeta_p)$ (since $\zeta_4 \in \mathbb{F}_\ell$ if $\ell \equiv 1 \pmod 4$) and $f := [\mathbb{F}_\lambda : \mathbb{F}_\ell] = \mathrm{ord}(\ell \in \mathbb{F}_p^\times)$. Fisher [Fis95, Proposition 2.8] showed that for $\mathbb{Q}(\zeta_p)$-valued Kloosterman sums,

$$\mathbb{Q}(\mathrm{Kl}_{n,q}(a) : a \in \mathbb{F}_q) = \mathbb{Q}(\zeta_p)^{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})[n]}.$$

We proceed similarly to show that for $G = \mathrm{Gal}(\mathbb{F}_\ell(\zeta_p)/\mathbb{F}_\ell)$,

$$\left.\begin{array}{l} L_1 := \mathbb{F}_\ell\left(\mathrm{Kl}_{n,q}(a) : a \in \mathbb{F}_q^\times\right) \\ L_2 := \mathbb{F}_\ell\left(\operatorname{tr} \rho_n(I_\infty)\right) \end{array}\right\} = \mathbb{F}_\ell(\zeta_p)^{G[n]}.$$

For $\sigma \in G$, let $u_\sigma \in \mathbb{F}_p^\times$ be such that $\sigma(\zeta_p) = \zeta_p^{u_\sigma}$, and note that for $a \in \mathbb{F}_q^\times$,

$$\begin{aligned} \sigma(\mathrm{Kl}_{n,q}(a)) &= \mathrm{Kl}_{n,q}(a u_\sigma^n) \\ \sigma\left(\operatorname{tr} \rho(\sigma(a,0))\right) &= \operatorname{tr} \rho(\sigma(a u_\sigma, 0)) = \sum_{i=1}^{n} e\left(\frac{n \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a u_\sigma \zeta_n^i)}{p}\right), \end{aligned}$$

where $\sigma(a,0)$ is as defined in the proof of Proposition 3.20. Hence, $G[n] \leqslant \mathrm{Gal}(\mathbb{F}_\ell(\zeta_p)/L_i)$ for $i = 1, 2$.

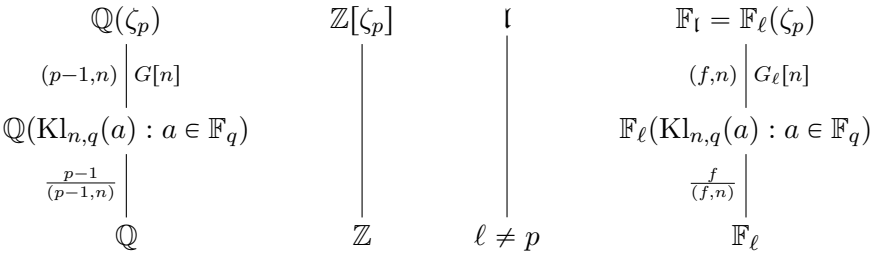
On the other hand, let us assume that $\sigma \in \mathrm{Gal}(\mathbb{F}_\ell(\zeta_p)/L_2)$. For every character $\Lambda : \mathbb{F}_q^\times \to \overline{\mathbb{F}}_\ell$, we define

$$\begin{aligned} S_2(\Lambda) &= \sum_{a \in \mathbb{F}_q^\times} \operatorname{tr} \rho(\sigma(a,0)) \Lambda(a) \\ &= \sum_{i=1}^{n} \overline{\Lambda}(\zeta_n^i) G_n(\Lambda) = n \delta_{\Lambda|_{\mu_n}=1} G_n(\Lambda), \end{aligned}$$

where $G_n(\Lambda) := \sum_{a \in \mathbb{F}_q^\times} e\left(\frac{n \operatorname{tr}_{\mathbb{F}_q/\mathbb{F}_p}(a)}{p}\right) \Lambda(a) \neq 0$ since $G_n(\Lambda) G_{-n}(\overline{\Lambda}) = q \in \mathbb{F}_\ell^\times$. Then, since $\sigma\,|_{L_2} = 1$, we have $S_2(\Lambda) = \overline{\Lambda}(u_\sigma) S_2(\Lambda)$, which yields that $\Lambda(u_\sigma) = 1$ whenever $\Lambda\,|_{\mu_n} = 1$. Thus, $\sum_{\Lambda \in \mathbb{F}_q^\times/\mu_n} \Lambda(u_\sigma) = (q-1)/n$, so that $u_\sigma \in \mu_n$, i.e. $\sigma \in G[n]$.

Similarly, $\mathrm{Gal}(\mathbb{F}_\ell(\zeta_p)/L_1) \leqslant G[n]$ by considering $S_1(\Lambda) = \sum_{a \in \mathbb{F}_q^\times} \mathrm{Kl}_{n,q}(a) \Lambda(a)$ (as in [Fis95, Proposition 2.8] over number fields).

The claim on the index follows from $|G[n]| = |(\mathbb{Z}/f)[n]| = (n, f)$. □



3.4. Monodromy groups of Kloosterman sheaves

For $n \geqslant 2$, we study in this section the monodromy groups of the Kloosterman sheaves $\mathcal{K}l_n$, as sheaves of $\overline{\mathbb{Q}}_\ell$, $\mathbb{Z}[\zeta_{4p}]_\lambda$, and $\mathbb{F}_\lambda$-modules. Most of it is dedicated to proving our result on the finite monodromy.

3.4.1. Monodromy over $\mathbb{C}$. By (3) and (4) of Proposition 3.19, the monodromy groups of the Kloosterman sheaf $\mathcal{K}l_n$ of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ satisfy

$$G_{\mathrm{geom}}(\mathcal{K}l_n) \leqslant G_{\mathrm{arith}}(\mathcal{K}l_n) \leqslant \begin{cases} \mathrm{SL}_n(\mathbb{C}) & : n \geqslant 2 \\ \mathrm{Sp}_n(\mathbb{C}) & : n \geqslant 2 \text{ even.} \end{cases}$$

One of the main results of Katz [Kat88] is that the two groups coincide and are as large as possible:

Theorem 3.23 ([Kat88, Chapter 11])**.** *In the above setting, assuming that $\mathbb{F}_q$ has odd*[3] *characteristic,*

$$G_{\mathrm{geom}}(\mathcal{K}l_n) = G_{\mathrm{arith}}(\mathcal{K}l_n) = \begin{cases} \mathrm{SL}_n(\mathbb{C}) & : n \text{ odd} \\ \mathrm{Sp}_n(\mathbb{C}) & : n \text{ even.} \end{cases} \tag{3.1}$$

The proof follows the strategy described in Section 3.1.5:

Katz's classification theorem. By Proposition 3.2, $G^0_{\mathrm{geom}}(\mathcal{K}l_n) \leqslant \mathrm{SL}_n(\mathbb{C})$ is semisimple and acts irreducibly on $\mathbb{C}^n$ (since the sheaf is geometrically irreducible). Thus, the Lie algebra $\mathcal{G}$ of $G^0_{\mathrm{geom}}(\mathcal{K}l_n)$ is semisimple and has a faithful irreducible representation into $\mathfrak{sl}_n(\mathbb{C})$. By using the existence of a unipotent element with a single Jordan block (Proposition 3.19 (1)), Katz shows that $\mathcal{G}$ is even simple ([Kat88, 11.5.2.3]).

Hence, the proof of Theorem 3.23 is reduced to the following classification theorem. Indeed, cases other than $\mathfrak{sl}_n(\mathbb{C})$ (n odd) or $\mathfrak{sp}_n(\mathbb{C})$ (n even) in the conclusion of Theorem 3.24 are excluded by properties (2) and (5) of Proposition 3.19. This determines $G^0_{\mathrm{geom}}(\mathcal{K}l_n)$ and then $G_{\mathrm{geom}}(\mathcal{K}l_n)$ (see [Kat88, 11.7]).

Theorem 3.24 ([Kat88, Classification Theorem 11.6])**.** *Let $n \geqslant 2$ an integer and $\mathcal{G}$ a simple Lie algebra over $\mathbb{C}$ given with a faithful irreducible representation*

$$\rho : \mathcal{G} \hookrightarrow \mathfrak{sl}_n(\mathbb{C}).$$

[3] The characteristic 2 case is also handled by Katz, but we omit it here for the sake of simplicity.

Suppose that there exists a nilpotent element $N \in \mathcal{G}$ such that $\rho(N)$ has a single Jordan block. Then the pair $(\mathcal{G}, \rho)$ is isomorphic to one of the following:

(1) $\mathcal{G} = \mathfrak{sl}_n(\mathbb{C})$ $(n \geqslant 2)$, $\mathfrak{sp}_n(\mathbb{C})$ $(n \geqslant 4$ even$)$ or $\mathfrak{so}_n(\mathbb{C})$ $(n \geqslant 5$ odd$)$, with the standard n-dimensional representation.

(2) $\mathcal{G} = \mathfrak{g}_2(\mathbb{C})$ with its unique 7-dimensional irreducible representation.

Remark 3.25. Theorem 3.24 also follows from a classification of Suprunenko [Sup95, Theorem (1.9)], which is valid over an algebraically closed field of arbitrary characteristic, and that we will use in the next section after descent.

3.4.2. Integral monodromy. We now consider the Kloosterman sheaf $\mathcal{K}l_n$ of $\mathbb{Z}[\zeta_{4p}]_\lambda$-modules over $\mathbb{F}_q$ (see Section 2.4.2). By (3) and (4) of Proposition 3.19, we still have

$$G_{\mathrm{geom}}(\mathcal{K}l_n) \leqslant G_{\mathrm{arith}}(\mathcal{K}l_n) \leqslant \begin{cases} \mathrm{SL}_n(\mathbb{Z}[\zeta_{4p}]_\lambda) & : n \text{ odd} \\ \mathrm{Sp}_n(\mathbb{Z}[\zeta_{4p}]_\lambda) & : n \text{ even.} \end{cases}$$

As Katz notes in the introduction of [Kat88], it is an interesting question to ask whether these integral monodromy groups are still equal and as big as possible, i.e. is it true that

$$G_{\mathrm{geom}}(\mathcal{K}l_n) = G_{\mathrm{arith}}(\mathcal{K}l_n) = \begin{cases} \mathrm{SL}_n(\mathbb{Z}[\zeta_{4p}]_\lambda) & : n \text{ odd} \\ \mathrm{Sp}_n(\mathbb{Z}[\zeta_{4p}]_\lambda) & : n \text{ even,} \end{cases} \tag{3.2}$$

knowing that their Zariski closure in $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ is $\mathrm{SL}_n(\overline{\mathbb{Q}}_\ell)$ (resp. $\mathrm{Sp}_n(\overline{\mathbb{Q}}_\ell)$) by Theorem 3.23 ?

In [Kat88, Chapter 12], Katz presents the proof of the following result of Gabber:

Theorem 3.26 (Gabber)**.** *If $\mathbb{Z}[\zeta_{4p}]_\lambda = \mathbb{Z}_\ell$ (e.g. if ℓ is completely split in $\mathbb{Z}[\zeta_{4p}]$), then there exists an integer $D = D(n,p)$ such that (3.2) holds if $\ell > D(n,p)$.*

Unfortunately, the constant $D(n,p)$ in the proof is ineffective, and nothing shows that it should be independent from p. A similar result is shown by Nori [Nor87], with the same limitations.

For the applications in analytic number theory that we consider, however, we require that (3.2) holds for all ℓ large enough, independently of p.

3.4.3. Finite monodromy. Finally, we consider the Kloosterman sheaf $\mathcal{K}l_n$ of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$ (i.e. the reduction modulo the ideal corresponding to λ of the sheaf of $\mathbb{Z}[\zeta_{4p}]_\lambda$-modules from the last section).

Again, we can wonder whether the finite monodromy groups

$$G_{\mathrm{geom}}(\mathcal{K}l_n) \leqslant G_{\mathrm{arith}}(\mathcal{K}l_n) \leqslant \begin{cases} \mathrm{SL}_n(\mathbb{F}_\lambda) & : n \text{ odd} \\ \mathrm{Sp}_n(\mathbb{F}_\lambda) & : n \text{ even} \end{cases}$$

are equal and as big as possible when $\ell \gg_n 1$. We will show that this is indeed the case:

Theorem 3.27. *Assume that n is coprime with p. For $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$ and $(n, [\mathbb{F}_\lambda : \mathbb{F}_\ell]) = 1$, the monodromy groups of the Kloosterman sheaf of $\mathbb{F}_\lambda$-modules $\mathcal{K}l_n$ over $\mathbb{F}_q$ are*

$$G_{\mathrm{geom}}(\mathcal{K}l_n) = G_{\mathrm{arith}}(\mathcal{K}l_n) = \begin{cases} \mathrm{SL}_n(\mathbb{F}_\lambda) & : n \text{ odd} \\ \mathrm{Sp}_n(\mathbb{F}_\lambda) & : n \text{ even.} \end{cases} \tag{3.3}$$

The same results hold true without restriction on $\ell \pmod 4$ if $p \equiv 1 \pmod 4$ or n is odd, with $\mathcal{O} = \mathbb{Z}[\zeta_p]$.

Remark 3.28. In any case, this holds for a set of valuations λ of natural density 1, since

$$\begin{aligned} \{\lambda \trianglelefteq \mathbb{Z}[\zeta_{4p}] : \ell \equiv 1 \pmod 4\} &\supset \{\lambda \trianglelefteq \mathbb{Z}[\zeta_{4p}] : \ell \equiv 1 \pmod{4p}\} \\ &= \{\lambda \trianglelefteq \mathbb{Z}[\zeta_{4p}] \text{ degree } 1\}. \end{aligned}$$

Consequence on integral monodromy groups. Of course, (3.2) would imply (3.3) for all ℓ by surjectivity of the reduction $\mathrm{SL}_n(R) \to \mathrm{SL}_n(R/\mathfrak{a})$ for any discrete valuation ring R and $\mathfrak{a} \trianglelefteq R$ (since $\mathrm{SL}_n(R)$ is generated by elementary matrices in this case). Conversely, an argument of Serre [Ser89, IV-23, 27-28] actually implies:

Corollary 3.29. *For $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$, the monodromy groups of the Kloosterman sheaf of $Z[\zeta_{4p}]_\lambda$-modules $\mathcal{K}l_n$ over $\mathbb{F}_q$ are as given by (3.2).*

See also [Kat90, 8.13.3] for a result valid for general closed subgroups of $\mathrm{GL}_n(\mathcal{O}_\lambda)$.

3.4.4. Further existing results and heuristics.

The results of Larsen-Pink. By results of Larsen and Pink (see [Lar95, Theorem 3.17] and the applications in [Kat12, Section 7], [Kow08, pp. 155–156], [Kow06a, p. 29] and [Kow06c, p. 7]), the monodromy result of Katz over $\mathbb{C}$ (Theorem 3.23) implies that for all p, there exists a set $\Lambda(n, p)$ of primes of Dirichlet density 1 such that for all $\ell \in \Lambda(n, p)$, the result (3.3) holds, because Kloosterman sheaves form a compatible system (see [Kat88, 8.9]).

However, as for the results of Gabber and Nori, the way $\Lambda(n, p)$ is constructed is highly dependent on p. This is not a problem for the applications of Kowalski mentioned above, but issues arise if we need to take $\ell, p \to \infty$ with some restrictions on the range as in [Kow06b].

Note incidentally that [Lar95] uses in particular the classification of finite simple groups.

(Invariant) generation of $\mathrm{SL}_n(\mathbb{F}_\ell)$. As an indication that the monodromy group for n odd should be $\mathrm{SL}_n(\mathbb{F}_\lambda)$, we have the following

Proposition 3.30. *For n odd, the elements u and m from Section 3.3.1 generate $\mathrm{SL}_n(\mathbb{F}_\ell)$.*

Proof. Proceed in a similar way to Gow-Tamburini [GT92], considering $w = m^2u(mum)^{-1}$ and using induction on n. □

However, we do not know whether these elements are *invariant generators*, namely whether any two conjugates are still generators. Without that, we may not conclude anything for our problem. For ℓ small, the answer is negative, but one may wonder if that holds for $\ell \gg_n 1$.

Example 3.31. The pair $(h^{-1}uh, m)$ does not generate $\mathrm{SL}_3(\mathbb{F}_3)$ for $h = \left(\begin{smallmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 2 & 0 \end{smallmatrix}\right)$. More precisely, this pair generates the group for about 61% of the elements $h \in \mathrm{GL}_3(\mathbb{F}_3)$. This proportion increases to about 93% for $\mathrm{SL}_3(\mathbb{F}_5)$.

There are many results on *probabilistic* invariant generation of classical groups, for example by Guralnick, Malle, Kantor, Lubotzky, Saxl or Weigel, but we consider here two specific elements.

The case $n = 2$ and $\mathbb{F}_\lambda = \mathbb{F}_\ell$ by the work of Yu and Hall. Hall [Hal08] proved the following classification theorem, which generalizes a theorem on Yu on the $\mathbb{F}_\ell$-monodromy of hyperelliptic curves, and also applies to show big monodromy results for families of twists of elliptic curves, as needed in [Kow06b].

Theorem 3.32 ([Hal08, Theorem 1.1])**.** *Let V be a $\mathbb{F}_\ell$-vector space with a perfect pairing $V \times V \to \mathbb{F}_\ell$, and let $H \leqslant \mathrm{GL}(V)$ be an irreducible primitive subgroup that preserves the pairing.*

(1) If the pairing is symmetric, H contains a reflection and an isotropic shear, and $\ell \geqslant 5$, then H is one of the following:

   a) the full orthogonal group $O(V)$,

   b) the kernel of the spinor norm,

   c) the kernel of the product of the spinor norm and the determinant.

(2) If the pairing is alternating, H contains a transvection and $\ell \geqslant 3$, then $H = \mathrm{Sp}(V)$.

See also the more general version [Hal08, Theorem 3.1]. In the alternating case, this is a relatively direct application of a classification of linear groups generated by transvections by Zalesski and Serezkin, which is a well-known result of Dickson for $n = 2$.

We can apply this to the sheaf $\mathcal{K}l_2$ as follows:

Proposition 3.33. *Let $\ell \geqslant 5$ be a prime with $\ell \equiv 1 \pmod{p}$, so that $\mathbb{F}_\lambda = \mathbb{F}_\ell$ (see Remark 2.47). Then (3.3) holds for the Kloosterman sheaf $\mathcal{K}l_2$ of $\mathbb{F}_\ell$-modules over $\mathbb{F}_q$: the arithmetic and geometric monodromy groups are equal to $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof. A unipotent element of drop 1 is an element whose Jordan decomposition has exactly one Jordan block of size 2 and all other blocks trivial. Moreover, a transvection is an element of drop 1 and determinant 1. The result then follows from Proposition 3.19 (1) and Theorem 3.32 (2) (or the corresponding result of Dickson). □

However, this argument does not generalize to $n \geqslant 3$, since the image of the inertia at 0 in $\mathcal{K}l_n$ contains a transvection only when $n = 2$. Moreover, we cannot

handle the case $\mathbb{F}_\lambda \neq \mathbb{F}_\ell$, since Hall considers only reduction of sheaves of $\mathbb{Z}_\ell$-modules (and not $\mathbb{Z}[\zeta_{4p}]_\lambda$-modules as for Kloosterman sheaves).

3.4.5. Classification theorem over $\mathbb{F}_\lambda$. We will prove Theorem 3.27 by first proving the following classification theorem. This is to be compared with how Katz's Classification Theorem 3.24 (for complex algebraic groups) was used to prove his Theorem 3.23.

Theorem 3.34 (Classification theorem over $\mathbb{F}_\lambda$)**.** *Let $n \geqslant 2$, let $\mathbb{F}_\lambda$ be a field of characteristic ℓ and let*

$$H \leqslant \begin{cases} \mathrm{SL}_n(\mathbb{F}_\lambda) & : n \text{ odd} \\ \mathrm{Sp}_n(\mathbb{F}_\lambda) & : n \text{ even} \end{cases}$$

be a maximal (proper) subgroup such that:

(1) The action of H on $\mathbb{F}_\lambda^n$ is irreducible.

(2) H contains a unipotent element with a single Jordan block.

Then, for $\ell \gg_n 1$, we have either:

(1) $H = N_{\mathrm{SL}_n(\mathbb{F}_\lambda)}(\mathrm{SO}_n(\mathbb{F}_\lambda))$ for $n \geqslant 3$ odd.

(2) $H = N_{\mathrm{SL}_n(\mathbb{F}_\lambda)}(\mathrm{SL}_n(\mathbb{F}'))$ for $n \geqslant 3$ odd or $H = N_{\mathrm{Sp}_n(\mathbb{F}_\lambda)}(\mathrm{Sp}_n(\mathbb{F}'))$ for n even, if $\mathbb{F}' \leqslant \mathbb{F}_\lambda$ is a subfield of prime degree.

(3) $H = N_{\mathrm{SL}_n(\mathbb{F}_\lambda)}(\mathrm{SU}_n(\mathbb{F}'))$ for $n \geqslant 3$ odd, if $\mathbb{F}' \leqslant \mathbb{F}_\lambda$ is a subfield such that $|\mathbb{F}'| = |\mathbb{F}_\lambda|^{1/2}$.

Remark 3.35. We recall that for n odd, there is only one type of orthogonal group over a finite field up to isomorphism (see e.g. [KL90b, Section 2.5]), so we do not need to specify the quadratic form.

Proof of Theorem 3.27 from Theorem 3.34. Assume that there exists a maximal subgroup $G_{\mathrm{geom}}(\mathcal{K}l_n) \leqslant H \leqslant \mathrm{SL}_n(\mathbb{F}_\lambda)$ if n is odd (resp. $\mathrm{Sp}_n(\mathbb{F}_\lambda)$ if n is even) be a maximal (proper) subgroup. By Proposition 3.19, H satisfies the hypotheses of Theorem 3.34.

It remains to show that the four cases of the conclusion of the latter are excluded:

(1) For n odd and $T = \mathrm{SO}_n(\mathbb{F}_\lambda)$, we proceed as in [Kat88, 11.5.2]. We have

$$H = N_{\mathrm{SL}_n(\mathbb{F}_\lambda)}(T) \cong T \times \mu_n(\mathbb{F}_\lambda).$$

Over $\mathbb{C}$, this follows from the fact that T contains no nontrivial scalars and that all automorphisms are inner by Propositions 3.16 and 3.18. In the finite case, we must take into account diagonal and field automorphisms by Proposition 3.17: the result is given in [KL90b, (2.6.2), Cor. 2.10.4, Prop. 2.10.6] (and is also true for[4] $T = G_2(\mathbb{F}_\lambda) \leqslant \mathrm{SO}_7(\mathbb{F}_\lambda)$ because there are no diagonal automorphisms).

[4] This is the realization of G_2 as the automorphism group of imaginary octonions, see [Wil09, 4.3].

Let $\rho : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\lambda)$ the representation corresponding to $\mathcal{K}l_n$. By (2)b of Proposition 3.19, considering the character $\rho(I_\infty) \to H \to \mu_n(\mathbb{F}_\lambda)$, we must have $\rho(P_\infty) \leqslant T$, which contradicts (5) of the same proposition. Indeed, T preserves a nonsingular symmetric bilinear form.

For (2) and (3), where subfields appear, we use Proposition 3.22: under the hypothesis $([\mathbb{F}_\lambda : \mathbb{F}_\ell], n) = 1$, we have

$$\mathbb{F}_\lambda = \mathbb{F}_\ell(\operatorname{tr} \rho_n(I_\infty)) \leqslant \mathbb{F}_\ell(\operatorname{tr}(G_{\mathrm{geom}})). \tag{3.4}$$

Lemma 3.36. *For L/k an extension of finite fields and $G \in \{\mathrm{SL}_n, \mathrm{Sp}_n\}$,*

$$[n]\,\mathrm{N}_{G(L)}(G(k)) \leqslant G(k),$$

where $[n] : G(L) \to G(L)$ is defined by $g \mapsto g^n$.

Proof. Let $\sigma \in \mathrm{Aut}_k(L)$ be the Frobenius. If $g \in \mathrm{N}_{G(L)}(G(k))$, we have $ghg \in G(k)$ for all $h \in G(k)$, i.e. $\sigma(ghg^{-1}) = ghg^{-1}$ (applying σ entry-wise), so $\sigma(g)h\sigma(g)^{-1} = ghg^{-1}$, which shows that $\sigma(g)g^{-1} \in C_{G(L)}(G(k))$. Recall that $\mathrm{SL}_n(k)$ is generated by elementary matrices $e_{i,j}$ $(i \neq j)$ and that $\mathrm{Sp}_n(k)$ (with the usual form) contains the elementary matrices $e_{i,\sigma(i)}$ where $\sigma(i) = i + n - 1 \pmod{2n}$. This yields $C_{G(L)}(G(k)) \leqslant Z(G(L))$. Therefore, $\sigma(g) = \lambda_g g$ with $\lambda_g \in \mu_n(L)$. Since $\sigma(g^n) = \sigma(g)^n = g^n$, we get that $g^n \in G(k)$. See also [KL90b, 4.5.3–4]. □

(2) If $H = N_{G(\mathbb{F}_\lambda)}(G(\mathbb{F}'))$ with $G \in \{\mathrm{SL}_n, \mathrm{Sp}_n\}$, then Lemma 3.36 shows that

$$\operatorname{tr} \rho(\sigma(an, 0)) \in \mathbb{F}'$$

for every $a \in \mathbb{F}_q$. Since $(n, p) = 1$, it follows that $\operatorname{tr} \rho(I_\infty) \subset \mathbb{F}'$, which contradicts (3.4) since $\mathbb{F}'$ is a proper subfield of $\mathbb{F}_\lambda$.

(3) Finally, we use a combination of the techniques used in (1)–(2) to handle the case of $H = N_{\mathrm{SL}_n(\mathbb{F}_\lambda)}(\mathrm{SU}_n(\mathbb{F}'))$. By [KL90b, Proposition 4.8.5],

$$\begin{aligned} H = \mu_n(\mathbb{F}_\lambda)\,\mathrm{SU}_n(\mathbb{F}') &\cong \frac{\mathrm{SU}_n(\mathbb{F}') \times \mu_n(\mathbb{F}_\lambda)}{\mathrm{SU}_n(\mathbb{F}') \cap \mu_n(\mathbb{F}_\lambda)} \\ &= \frac{\mathrm{SU}_n(\mathbb{F}') \times \mu_n(\mathbb{F}_\lambda)}{\mu_{(n,1+|\mathbb{F}'|)}(\mathbb{F}_\lambda)}. \end{aligned}$$

By Proposition 3.19 (2)b applied to the representation

$$H \to \mu_{n/(n,1+|\mathbb{F}'|)}(\mathbb{F}_\lambda)$$

restricted to $\rho(I_\infty)$, we have $\rho(P_\infty) \leqslant \mathrm{SU}_n(\mathbb{F}')$. In other words, P_∞ leaves invariant the sesquilinear form on $(\mathbb{F}_\lambda)^n$ associated to the involution $\sigma \in \mathrm{Aut}(\mathbb{F}_\lambda)$, $x \mapsto x^{|\mathbb{F}'|}$.

As in (5) of Proposition 3.19 (and its proof in [Kat88, 4.1.5–4.1.8]), this yields an isomorphism of P_∞-representations between ρ and $\sigma(D(\rho))$. Equivalently, there exists $A \in \mathrm{GL}_n(\mathbb{F}_\lambda)$ such that

$$A\rho(g)A^{-1} = \sigma\left(\rho(g^{-1})^t\right) \text{ for all } g \in P_\infty,$$

so $A\rho(P_\infty)A^{-1} \leqslant \mathrm{GL}_n(\mathbb{F}')$, which contradicts again (3.4).

□

Remarks 3.37. The conditions $p \nmid n$ and $([\mathbb{F}_\lambda : \mathbb{F}_\ell], n) = 1$ in Theorem 3.27 are required to exclude subfield subgroups. In particular:

- If $p \mid n$, the elements produced with Proposition 3.20 are all trivial.
- If $e = ([\mathbb{F}_\lambda : \mathbb{F}_\ell], n) > 1$, Proposition 3.22 shows that we cannot exclude that G_{geom} lies in $N_{G(\mathbb{F}_\lambda)}(G(\mathbb{F}'))$, for $\mathbb{F}' < \mathbb{F}_\lambda$ a proper subfield of index e (where $G = \mathrm{SL}_n$ if n is odd, Sp_n otherwise).

Moreover, in the case $p \equiv 3 \pmod 4$ and $\ell \equiv 2 \pmod 3$, we cannot exclude that G_{geom} is defined over $\mathbb{F}_\ell(\zeta_p) < \mathbb{F}_\ell(\zeta_{4p}) = \mathbb{F}_\lambda$. Indeed, $\zeta_4 \in \mathbb{F}_\lambda$ because of the Tate twist, which is trivial on the geometric fundamental group.

In [Hal08] (and applications in [Kow06a] and [Kow08]), subfield subgroups do not enter the picture because only sheaves of $\mathbb{Z}_\ell$-modules are considered, as opposed to reductions of sheaves of $\mathbb{Z}[\zeta_{4p}]_\lambda$-modules for Kloosterman sheaves.

The remaining of this section is dedicated to the proof of Theorem 3.34.

3.4.6. Strategy for the proof of Theorem 3.34. The latter will be proven by using the classification of maximal subgroups of classical groups (Theorem 3.13) presented in Section 3.2.3. The strategy is the following:

First, we exclude elements of classes $\mathcal{C}_1, \dots, \mathcal{C}_5$ by using that H contains a unipotent element u with a single Jordan block. Classes $\mathcal{C}_6$ and $\mathcal{C}_7$ remain in the conclusion of Theorem 3.34.

Remark 3.38. This also appears in [SS97, Proposition 2.1] to classify subgroups of algebraic groups *over an algebraically closed field* containing a regular unipotent element (i.e. a unipotent element with a single Jordan block in the case of SL_n), where the authors use the generalization we mentioned in Section 3.2.3 of Aschbacher's result to algebraically closed fields by Liebeck-Seitz [LS98]. We will comment further on this later on.

On the other hand, if H satisfies (2) of Theorem 3.13, there exists a nonabelian simple group S such that

$$S = \pi(T) \trianglelefteq \tilde{H} = \pi(H) \leqslant \mathrm{Aut}(S)$$

with $T \trianglelefteq H \leqslant \mathrm{SL}_n(\mathbb{F}_\lambda)$ and T acting irreducibly on $\overline{\mathbb{F}}_\lambda^n$, for $\pi : \mathrm{SL}_n \to \mathrm{PSL}_n$ the projection.

Since $u \in H$ has order ℓ (and is not scalar), we have $|H|, |\tilde{H}| \geqslant \ell$. Hence, when $\ell \gg_n 1$, the following result allows to reduce to the case where S is a group of Lie type in characteristic ℓ.

Theorem 3.39. *Let $S \leqslant \mathrm{PGL}_n(\mathbb{F}_\lambda)$ be a simple group. Then either $|S| \ll_n 1$, or S is a group of Lie type in characteristic ℓ.*

Our first proof used the classification of finite simple groups, but this is also a particular case of a powerful theorem of Larsen-Pink, independent from the clas-

sification.

Let us then assume that S is a finite group of Lie type in characteristic ℓ. We first show that the degree of the field of definition must be small, according to results of Liebeck on the minimal dimension of faithful irreducible modular representations of simple groups of Lie type. This implies that the group of outer automorphisms is small, and then that S must contain the regular unipotent element of $\tilde{H}$ for $\ell \gg_n 1$. Over an algebraically closed field, the irreducible representations of a semisimple algebraic group with central kernel whose image contains an element with a single Jordan block are classified by a result of Suprunenko. The absolute irreducibility of the action of T allows to descend to finite groups of Lie type by a result of Seitz-Testerman, and this gives Theorem 3.34.

Remark 3.40. The strategy to exclude alternating groups and groups of Lie type in cross-characteristic in the almost simple case of the characterization is quite standard (see e.g. [MT11, Chapter 28]). The results of Liebeck mentioned are notably used in [KL90a] to determine the probability that two random elements of $\mathrm{PSL}_n(\mathbb{F}_\ell)$ are generators, in the case $\ell \leqslant 9$.

Remark 3.41. According to [Lie85], building on Theorem 3.13 and the classification of finite simple groups, a maximal subgroup H of a classical group over a finite field $\mathbb{F}_\lambda$ of characteristic ℓ satisfies one of the following:

- H belongs to one of the families $\mathcal{C}_1, \dots, \mathcal{C}_7$.
- H is $\mathrm{Alt}(c)$ or $\mathfrak{S}_c$ with $c \in \{n+1, n+2\}$, and $H \to \mathrm{GL}_n(\mathbb{F}_\lambda)$ is the representation of minimal dimension.
- $|H| < |\mathbb{F}_\lambda|^{3n}$.

As we just mentioned, it is relatively easy to exclude the first two families by using the presence of a regular unipotent element or the growth of H when $\ell \to \infty$. Since $|\mathrm{SL}_n(\mathbb{F}_\lambda)| = \Theta_n(|\mathbb{F}_\lambda|^{n^2-1})$ and $|\mathrm{Sp}_n(\mathbb{F}_\lambda)| = \Theta_n(|\mathbb{F}_\lambda|^{n(2n+1)})$, the result of Liebeck shows that in the remaining cases H is quite small. In other words, we only need to show that the monodromy group is "moderately big" to show that it is the full classical group expected.

3.4.7. Excluding members of classes $\mathcal{C}_1, \dots, \mathcal{C}_5$. Let us consider a group $H \in \bigcup_{i=1}^5 \mathcal{C}_i$ acting irreducibly on V and containing a unipotent element u with a single Jordan block. We use the notations of Section 3.2.3. We assume throughout $\ell \gg_n 1$ so that u has order ℓ.

Lemma 3.42. *Let K be a field and $u \in \mathrm{SL}_n(K)$ be a Jordan block of size n. There are $n+1$ subspaces which are u-invariant, given by 0, $\mathrm{span}(e_1)$, $\mathrm{span}(e_1, e_2)$, $\dots$, $V = \mathrm{span}(e_1, \dots, e_n)$, where (e_i) is the canonical basis of K^n.*

Proof. As a $K[u]$-module, V is isomorphic to $K[X]/(X-1)^n$ and the claim is then clear since $K[X]$ is a principal ideal domain. □

Class $\mathcal{C}_1$. The first class is excluded by the assumption that H acts irreducibly on V.

Class $\mathcal{C}_2$. By assumption, there exists a permutation $\sigma \in \mathfrak{S}_t$ such that $u\boldsymbol{V}_i = \boldsymbol{V}_{\sigma(i)}$ for all i. Note that there is at most one $\boldsymbol{V}_i$ which is u-stable, since the $\boldsymbol{V}_i$ are disjoint with equal dimension, and u has exactly only invariant subspace of each dimension $0 \leqslant d \leqslant n$, by Lemma 3.42. In particular, σ has at most one fixed point. Write $\sigma = \sigma_1 \dots \sigma_k$ where $\sigma_1, \dots, \sigma_k$ are disjoint cycles, with σ_j of length $2 \leqslant s_j \leqslant n$. Since u has order ℓ, we have

$$\boldsymbol{V}_i = u^\ell \boldsymbol{V}_i = \boldsymbol{V}_{\sigma^\ell(i)},$$

so $\sigma^\ell = \mathrm{id}$ and either

- $\sigma = \mathrm{id}$, which implies that all $\boldsymbol{V}_i$ are u-stable, a contradiction.
- $\mathrm{ord}(\sigma) = \mathrm{lcm}(s_1, \dots, s_k) = \ell$. Hence $s_j = \ell$ for all j, thus $k\ell = n - |\operatorname{fix}(\sigma)|$, i.e. $\ell \mid n$ or $\ell \mid n-1$. This can be excluded if $\ell > n$.

Class $\mathcal{C}_3$. (for $G = \mathrm{Sp}_n(\mathbb{F}_\lambda)$). This is excluded in the same way as class $\mathcal{C}_2$.

Class $\mathcal{C}_4$. Consider the morphism

$$N_{\mathrm{PGL}(\overline{\mathbb{F}}_\lambda)}(\pi(\boldsymbol{L})) \cap \pi(\boldsymbol{G}) \to \begin{cases} \mathrm{Out}\,(\pi(\boldsymbol{G}(\boldsymbol{V}_1))) \times \mathrm{Out}\,(\pi(\boldsymbol{G}(\boldsymbol{V}_2))) & : t = 2 \\ \mathrm{Out}\,(\pi(\boldsymbol{G}(\boldsymbol{V}_1))) \wr \mathfrak{S}_t & : t > 2 \end{cases}$$

with kernel $\pi(\boldsymbol{L}) \cap \pi(\boldsymbol{G})$. If $\pi(u) \notin \pi(\boldsymbol{L})$, then the order of the image of $\pi(u)$ is

$$\ell \mid |\mathrm{Out}\,(\pi(\boldsymbol{G}(\boldsymbol{V}_i)))|^t \, t! = 2^t t!$$

for some $i \in \{1, 2\}$, by Propositions 3.16 and 3.18. Thus $\ell \ll_n 1$ since $t \leqslant n$. On the other hand, elements in $\pi(\boldsymbol{L})$ have at least two Jordan blocks[5], which also rules out the case $\pi(u) \in \pi(\boldsymbol{L})$. Indeed, if $g_1 \in \boldsymbol{G}(\boldsymbol{V}_1)$ and $g_2 \in \boldsymbol{G}(\boldsymbol{V}_2)$ are two Jordan blocks, then $g_1 \otimes g_2$ fixes the linearly independent vectors $v_{1,1} \otimes v_{2,1}$ and $v_{1,2} \otimes v_{2,1} - v_{1,1} \otimes v_{2,2}$, where $v_{i,1}, v_{i,2}$ are the first two elements of the standard basis of $\boldsymbol{V}_i$ $(i = 1, 2)$.

Remark 3.43. A finer analysis in [SS97, pp. 374–375] shows that taking $\ell \geqslant 5$ is sufficient.

Class $\mathcal{C}_5$. Consider the morphism

$$H \to \pi(H) \to \pi(H)/(\mathbb{Z}/r^m) \cong \mathrm{Sp}_{2m}(\mathbb{F}_r).$$

Since u has order $\ell \neq r$, the image of u in $\mathrm{Sp}_{2m}(\mathbb{F}_r)$ still has order ℓ, hence

$$\ell \mid |\mathrm{Sp}_{2m}(\mathbb{F}_r)| = r^{m^2}(r^2-1)(r^4-1)\dots(r^{2m}-1) \leqslant r^{m(2m+1)},$$

which implies that $\ell \ll_n 1$ because $n = r^m$.

[5] Since the center of $\mathrm{GL}_n(\overline{\mathbb{F}}_\lambda)$ is the group of scalar matrices, it makes sense to speak of the number of Jordan blocks of an element in $\mathrm{PGL}_n(\overline{\mathbb{F}}_\lambda)$.

3.4.8. Excluding almost simple groups. Let us now assume there exists a nonabelian simple group S such that

$$S = \pi(T) \trianglelefteq \pi(H) = \tilde{H} \leqslant \mathrm{Aut}(S),$$

with $T \trianglelefteq H \leqslant \mathrm{SL}_n(\mathbb{F}_\lambda)$ and T acting irreducibly on $\overline{\mathbb{F}}_\lambda^n$. We assume moreover (see the hypotheses of Theorem 3.34) that H contains a unipotent element u with a single Jordan block, so in particular $|H|,\ |\tilde{H}| \geqslant \ell$ as above.

Reduction to groups of Lie type in characteristic ℓ. Theorem 3.39 is a direct consequence of [LP11, Theorem 0.2] (see [LP11, Theorem 0.3]), exploiting the theory of algebraic groups.

Let us nonetheless show how it also follows from the classification of finite simple groups ([GLS94, no. 1, p. 6]). According to the latter, S can be:

(1) An alternating group $\mathrm{Alt}(m)$ of degree $m \geqslant 5$.

(2) A simple group of Lie type over a finite field $\mathbb{F}_r$:

   a) A classical group of type A_n ($n \geqslant 1$), B_n ($n \geqslant 2$), C_n ($n \geqslant 3$) or D_n ($n \geqslant 4$).

   b) A Chevalley/Steinberg group:

      – Exceptional type: E_6, E_7, E_8, F_4, G_2.
      – Twisted type: ${}^2A_n$ ($n \geqslant 2$),${}^2D_n$ ($n \geqslant 4$).
      – Exceptional twisted type: ${}^2E_6, {}^3D_4$.

   c) A Suzuki-Ree group: ${}^2B_2(2^{2n+1})$, ${}^2F_4(2^{2n+1})$ over $\mathbb{F}_{2^{2n+1}}$, or ${}^2G_2(3^{3n+1})$ over $\mathbb{F}_{3^{3n+1}}$.

(3) A sporadic group.

Thus, it suffices to prove:

Proposition 3.44. *If S is sporadic, alternating or of Lie type in characteristic coprime to ℓ, then $\ell \ll_n 1$.*

Proof. First note that we have $|\mathrm{Aut}(S)| \ll_n 1$:

– If S is sporadic, this is clear.

– If $S = \mathrm{Alt}(m)$ (with $m \geqslant 5$), then Wagner [Wag77, Theorem 1.1] showed that the dimension of a faithful modular representation of S is at most $n+2$. Since $S \leqslant \tilde{H} \leqslant \mathrm{PSL}_n(\mathbb{F}_\lambda)$, it follows that $m \leqslant n+2$, so $|\mathrm{Aut}(S)| \ll_n 1$.

– If S is of Lie type of rank l over a field $\mathbb{F}_r$ of characteristic distinct from ℓ, then the main theorem of Landazuri-Seitz [LS74] shows that $r, l \ll_n 1$, so that $|\mathrm{Aut}(S)| \ll_n 1$.

Hence $\ell \leqslant |\tilde{H}| \leqslant |\mathrm{Aut}(S)| \ll_n 1$. □

Groups of Lie type in characteristic ℓ. Assume now that S is a group of Lie type of rank l over $\mathbb{F}_r$, with $r = \ell^a$. The first difficulty to overcome is that we do not know a priori whether S itself contains a regular unipotent element. However, we can show:

Proposition 3.45. *If $\ell \gg_n 1$, then $\pi(u) \in S$ and T contains as well an element with a single Jordan block.*

We prove this proposition in the following paragraphs. Recall that we have an exact sequence

$$1 \to S \cong \mathrm{Inn}(S) \to \mathrm{Aut}(S) \to \mathrm{Out}(S) \to 1,$$

an inclusion $S \leqslant \tilde{H} \leqslant \mathrm{Aut}(S)$, and $\pi(u) \in \tilde{H}$ of order ℓ. If $\pi(u) \notin S$, then its image in $\mathrm{Out}(S)$ has order ℓ and so ℓ divides $|\mathrm{Out}(S)|$. Thus, it suffices to show that $|\mathrm{Out}(S)| \ll_n 1$ to rule out this possibility.

Lemma 3.46. *We have*

$$|\mathrm{Out}(S)| = Na$$

with $N \in \{1, 2, 6, 8, 12\}$ unless

- *$S = A_l(r)$ with $l \geqslant 3$ odd, where we have $|\mathrm{Out}(S)| = 2a(l+1, r-1)$, or*
- *$S = {}^2A_l(r)$ with $l \geqslant 3$ odd, where we have $|\mathrm{Out}(S)| = 2a(l+1, r+1)$.*

Proof. See Propositions 3.17, 3.18 and Table 3.2: there are a field automorphisms, $1, 2$ or 3 graph automorphisms, and less that 4 diagonal automorphisms, except for A_l and ${}^2A_l$ which have respectively $(l+1, r-1)$ and $(l+1, r+1)$ diagonal automorphisms. □

Letting $m(S)$ be the minimal dimension of a faithful irreducible projective representation of S over an algebraically closed field of characteristic ℓ, the following result lets us bound the rank of S and the degree of its defining field:

Lemma 3.47. *We have*

$$l \leqslant m(S) \leqslant n^{([\mathbb{F}_\lambda : \mathbb{F}_\ell], a)/a},$$

whence $l, a \ll_n 1$. In particular, for n fixed, there is only a finite number of possibilities for S.

Proof. The bounds follow from [Lie85, (2.1)–(2.2)] and the fact that $S \leqslant \tilde{H} \leqslant \mathrm{PSL}_n(\mathbb{F}_\lambda)$. Since $m(S) \geqslant 2$ (see Table 3.1), we have $a \leqslant \frac{\log n}{[\mathbb{F}_\lambda : \mathbb{F}_\ell] \log 2} \ll_n 1$, so that $l, a \ll_n 1$. □

Remark 3.48. This is to be compared with the fact that $\mathrm{SL}_n(\mathbb{C})$ has no nontrivial irreducible complex representation of dimension $< n$ (and no nontrivial finite-dimensional unitary representation).

Remark 3.49. By a result of Seitz [Sei88, Corollary 6], one could actually assume that $a = 1$.

S	$m(S)$
$A_l, {}^2A_l$	$l+1 \geqslant 2$
B_l	$2l+1 \geqslant 5$
C_l	$2l \geqslant 6$
$D_l, {}^2D_l$	$2l \geqslant 6$
${}^3D_4$	8
G_2	7
F_4	26
$E_6, {}^2E_6$	27
E_7	56
E_8	248

Table 3.1: Minimal dimension of a faithful irreducible projective representation of a simple group of Lie type over an algebraically closed field in the same characteristic $p > 3$, according to [Lie85, Table 2] or [KL90a, Table 1].

By Lemmas 3.46 and 3.47,

$$|\operatorname{Out}(S)| \leqslant 12a(l+1) \ll_n 1,$$

which concludes the proof of Proposition 3.45.

The next difficulty is that we do not know whether the action of T on $\mathbb{F}_\lambda^n$ is the action induced by $T \leqslant H \leqslant \mathrm{SL}_n(\mathbb{F}_\lambda)$, i.e. if the inclusion $T \to \mathrm{SL}_n(\mathbb{F}_\lambda)$ is the standard representation. However, thanks to Proposition 3.45 and the irreducibility of the action of T on $\boldsymbol{V}$, we can now apply the following:

Theorem 3.50. *Let $T \leqslant \mathrm{SL}_n(\mathbb{F}_\lambda)$ be a finite group of Lie type in characteristic $\ell \geqslant 5$, of simply connected type and acting absolutely irreducibly on $\mathbb{F}_\lambda^n$. Assume that T contains an element with a single Jordan block. Then either (up to conjugacy):*

(1) $T = \mathrm{SL}_n(\mathbb{F}_\lambda)$, $\mathrm{Spin}_n(\mathbb{F}_\lambda)$ for n odd or $\mathrm{Sp}_n(\mathbb{F}_\lambda)$ for n even, with the standard embedding in $\mathrm{SL}_n(\mathbb{F}_\lambda)$.

(2) $T = \mathrm{SU}_n(\mathbb{F}')$ with the standard embedding in $\mathrm{SL}_n(\mathbb{F}_\lambda)$, if $\mathbb{F}' \leqslant \mathbb{F}_\lambda$ is a subfield such that $|\mathbb{F}'| = |\mathbb{F}_\lambda|^{1/2}$.

(3) $T = G_2(\mathbb{F}_\lambda)$ and $n = 7$, with $T \leqslant \mathrm{SL}_7(\mathbb{F}_\lambda)$ the unique 7-dimensional irreducible representation.

This is a version of [Sup95, Theorem (1.9)] for finite groups of Lie type[6]. To prove this variant, we use the lifting theorem of Seitz and Testerman:

Theorem 3.51 ([ST90, Theorem 1, case $G = \mathrm{SL}_n$][7])**.** *Let $\boldsymbol{H}$ be a simple algebraic group over $\overline{\mathbb{F}}_\lambda$, with a Steinberg endomorphism $F : \boldsymbol{H} \to \boldsymbol{H}$, and $X = [\boldsymbol{H}^F, \boldsymbol{H}^F]$ perfect. If $\varphi : X \to \mathrm{SL}_n(\mathbb{F}_\lambda)$ is a morphism such that $\varphi(X)$ lies in no proper*

[6] Suprunenko remarked herself in the article that the results could be "*easily transferred to irreducible $\mathbb{F}_\ell$-representations of finite Chevalley groups over fields of characteristic ℓ.*" It seems however that we need to restrict to absolutely irreducible representations.

[7] See also [MT11, Section 29.2].

F-stable parabolic subgroup of $\mathrm{SL}_n(\overline{\mathbb{F}}_\lambda)$*, then* φ *can be extended to a morphism of algebraic groups* $\boldsymbol{\varphi} : \boldsymbol{H} \to \mathrm{SL}_n(\overline{\mathbb{F}}_\lambda)$ *with* $\boldsymbol{\varphi}\,|_X = \varphi$.

Proof of Theorem 3.50. By hypothesis, $T = \boldsymbol{T}^F$ for $\boldsymbol{T}$ a simple algebraic group over $\overline{\mathbb{F}}_\ell$ and $F : \boldsymbol{T} \to \boldsymbol{T}$ a Steinberg endomorphism. We consider the absolutely irreducible representation $\varphi : T \to \mathrm{SL}_n(\mathbb{F}_\lambda)$. By irreducibility, the image of T is not contained in a proper parabolic subgroup of $\mathrm{SL}_n(\mathbb{F}_\lambda)$. Theorem 3.51 thus shows the existence of a morphism $\boldsymbol{\varphi} : \boldsymbol{T} \to \mathrm{SL}_n(\overline{\mathbb{F}}_\ell)$ extending φ and which is still an irreducible representation. We can then apply [Sup95, Theorem (1.9)], and the classification of Steinberg endomorphisms [MT11, 22.1–22.2] gives the result. □

Remark 3.52. Again, compare Theorem 3.50 with the fact that the only non-trivial irreducible representations of $\mathrm{SL}_n(\mathbb{C})$ of dimension $\leqslant n$ are the standard representation and its dual.

If n is odd, the cases $T = \mathrm{Spin}_n(\mathbb{F}_\lambda)$, $G_2(\mathbb{F}_\lambda)$ and $\mathrm{SU}_n(\mathbb{F}')$ can be excluded by the hypothesis (2) of Theorem 3.13, since these fix a nondegenerate bilinear or unitary form on V (see the proof of Theorem 3.27 page 53; note that we use here that $T \to \mathrm{SL}_n(\mathbb{F}_\lambda)$ is the natural representation). If n is even, there are no other cases than $T = \mathrm{Sp}_n(\mathbb{F}_\lambda)$. This concludes the proof of Theorem 3.34.

3.4.9. Concluding remarks.

Katz's classification theorem. We note that Katz's Theorem 3.24, leading to the determination of monodromy groups over $\mathbb{C}$ of Kloosterman sheaves, follows from Suprunenko's result [Sup95, Theorem (1.9)].

Further classification theorems. Let K be an algebraically closed field of characteristic $\ell \geqslant 0$ and let G be a classical group over K (e.g. $G = \mathrm{SL}_n(K)$ or $G = \mathrm{Sp}_n(K)$) with associated vector space V.

Saxl and Seitz [SS97] classified maximal closed subgroups $H \leqslant G$ of positive dimension acting irreducibly on V and containing a regular unipotent element of G (see Remark 3.38). In particular, this generalizes [Sup95, Theorem (1.9)]. A simplified[8] version can be stated as follows:

Theorem 3.53 ([SS97, Theorem B])**.** *Let $H \leqslant G$ as above, and assume that $\ell = 0$ or $\ell \gg 1$. Then either:*

(1) H is imprimitive on V, $\ell > 0$, $G \neq \mathrm{SO}_{2n}(K)$ and

$$H = \mathrm{Stab}_G(V_1 \perp \cdots \perp V_t)$$

for an orthogonal decomposition $V = V_1 \perp \cdots \perp V_t$ with t a power of ℓ.

(2) H^0 is tensor indecomposable on V and $H \leqslant G$ is either

a) $\mathrm{SL}_2(K) \leqslant G$,

[8] In [SS97], H is actually assumed to be reductive, but not necessarily irreducible. By [MT11, Corollary 17.14] a maximal closed subgroup of positive dimension $H \leqslant G$ is either parabolic (which is excluded if it acts irreducibly on V), or H^0 is reductive. The condition $\ell \gg 1$ is not present in [SS97], but was added here to simplify the statement.

S	$\lvert\operatorname{Out}(S)\rvert$
$A_l(r)$	$\begin{cases} 2a & : l = 1 \\ 2a & : l \geqslant 2 \text{ even} \\ 2a(l+1, r-1) & : l \geqslant 3 \text{ odd} \end{cases}$
${}^2A_l(r)$	$\begin{cases} 2a & : l \text{ even} \\ 2a(l+1, r+1) & : l \text{ odd} \end{cases}$
$B_l(r), C_l(r)$	$2a$
$D_l(r)$	$\begin{cases} 12a & : l = 4 \\ 8a & : l > 4 \text{ even} \\ 8a & : l \geqslant 5 \text{ odd}, r \equiv 1 \pmod 4 \\ 4a & : l \geqslant 5 \text{ odd}, r \equiv 3 \pmod 4 \end{cases}$
${}^2D_l(r)$	$\begin{cases} 4a & : r \equiv 1 \pmod 4 \\ 8a & : r \equiv 3 \pmod 4,\ l \text{ odd} \\ 4a & : r \equiv 3 \pmod 4,\ l \text{ even} \end{cases}$
${}^3D_4(r)$	a
$E_6(r)$	$\begin{cases} 6a & : r \equiv 1 \pmod 3 \\ 2a & : r \equiv 2 \pmod 3 \end{cases}$
${}^2E_6(r)$	$\begin{cases} 2a & : r \equiv 1 \pmod 3 \\ 6a & : r \equiv 2 \pmod 3 \end{cases}$
$E_7(r)$	$2a$
$E_8(r)$	a
$F_4(r)$	a
$G_2(r)$	a

Table 3.2: Outer automorphism groups of finite simple groups of Lie type over $\mathbb{F}_r$, with $r = q^a$ odd, $q > 3$.

b) $\operatorname{Sp}(V) \leqslant \operatorname{SL}(V)$ *with* $\dim V$ *even,*

c) $\operatorname{SO}(V) \leqslant \operatorname{SL}(V)$ *with* $\dim V$ *odd,*

d) $\operatorname{Spin}_7(K) \leqslant \operatorname{SO}_8(K)$*, the smallest faithful irreducible representation of* $\operatorname{Spin}_7(K)$*.*

As we already mentioned, this also uses the classification of Liebeck-Seitz [LS98]. Because of the positive-dimensional assumption, one can actually assume that H is itself simple in the almost simple case of Theorem 3.13 (observe the sketch of the proof of Theorem 3.13 in [MT11, Theorem 18.6]). Since H is closed, it is a simple linear algebraic group, and the classification can be finished by using weight theory.

Remark 3.54. Our classification theorem 3.34 over $\mathbb{F}_\lambda$ cannot be simply deduced from Theorem 3.53 by descent, avoiding the use of the classification of finite simple groups. Indeed, taking a maximal (proper) subgroup $H \leqslant \operatorname{SL}_n(\mathbb{F}_\lambda)$ containing a regular unipotent element and acting irreducibly on $\overline{\mathbb{F}}_\lambda^n$, we do not know whether there exists a positive-dimensional closed subgroup $H' \leqslant \operatorname{SL}_n(\overline{\mathbb{F}}_\lambda)$. Showing this would actually be more or less equivalent to our proof of Theorem 3.34: note that if H is allowed to be 0-dimensional in Theorem 3.53, one has to consider almost

simple subgroups and not only simple ones, which is the additional difficulty we need to deal with in the proof of Theorem 3.34.

More generally, Testerman and Zalesski [TZ13, Theorem 1.2] show that connected reductive linear algebraic groups containing a unipotent element with a single Jordan block are irreducible. Combined with [SS97], this gives a classification of semisimple subgroups H of simple algebraic groups G containing a regular unipotent element of G ([TZ13, Theorem 1.4]).

3.5. Further monodromy groups

In the next sections, we give further monodromy groups of sheaves from Section 2.4, most of them determined by Katz in [Kat90] (see in particular [Kat90, Main ℓ-adic Theorem 7.2.7]).

Remark 3.55. Except for characters and functions counting points on families of curves, we will consider in the following only monodromy groups over $\mathbb{C}$. In further work, we hope to generalize our technique used for the finite monodromy groups of Kloosterman sheaves to hypergeometrics and sheaves associated to general exponential sums, but this would require to extend classification results of Kostant, Kostant-Zahrin, Gabber or Kazhdan-Margulis in positive characteristic, which seems difficult.

3.5.1. Characters.

Proposition 3.56. *(1) Let $\mathcal{L}_{\psi(f)}$ be an Artin-Schreier sheaf of A-modules as in Proposition 2.44. The arithmetic and geometric monodromy groups are equal to $\mu_p(A)$.*

(2) Let $\mathcal{L}_{\chi(f)}$ be a Kummer sheaf of A-modules as in Proposition 2.45, where χ has order d. The arithmetic and geometric monodromy groups are equal to $\mu_d(A)$.

3.5.2. Hypergeometric sheaves. The connected component at the identity G_{geom}^0 of the geometric monodromy group of the hypergeometric sheaf $\mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho})$ from Proposition 2.50 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, $G_{\mathrm{geom}}^0 = G_{\mathrm{geom}}^{0,\mathrm{der}}$.

The distinction between the possible cases is not straightforward (see [Kat90, p. 291]), and we will for simplicity only consider two situations where G_{geom}^0 is determined without ambiguity.

Proposition 3.57. *For the hypergeometric sheaf $\mathcal{H}(\boldsymbol{\chi}, \boldsymbol{\rho})$ of Proposition 2.50, we have $G_{\mathrm{geom}}^0 = G_{\mathrm{geom}}^{0,\mathrm{der}} = \mathrm{SL}(\mathbb{C})$ if either*

(1) $n = m$ is odd and $\Lambda = \prod_i \chi_i = 1$, or

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

Proof. This is [Kat90, Theorems 8.11.2, 8.11.3]. □

3.5.3. Supermorse functions and sums of the form (2.5).

Proposition 3.58 (Katz). *Let us consider the ℓ-adic sheaf $\mathcal{G}_f$ over $\mathbb{F}_q$ associated by Proposition 2.53 to a supermorse function $f \in \mathbb{F}_q(X)$. For $Z_{f'}$ the set of zeros of f' in $\mathbb{P}^1(\overline{\mathbb{F}}_p)$ and $k_f = |Z_{f'}|$, we assume that $p > 2k_f + 1$ and either:*

- *(H) 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 $s_1 = -s_4$, $s_2 = -s_3$.*

Then

$$G^0_{\mathrm{geom}}(\mathcal{G}_f) = G^{0,\mathrm{der}}_{\mathrm{geom}}(\mathcal{G}_f) = \begin{cases} \mathrm{SL}_{k_f}(\mathbb{C}) & \text{if } (H) \text{ holds,} \\ \mathrm{Sp}_{k_f}(\mathbb{C}) & \text{if } (H') \text{ holds.} \end{cases}$$

Proof. This is [Kat90, 7.9.6, 7.9.7, 7.10]. □

Remark 3.59. This makes sense in the symplectic case since (H') implies that k_f is even.

Examples 3.60. The following examples are given in [Mic98, p. 229], [FM03, p. 7] and [Kat90, 7.10], where more details can also be found. In all cases, since f arises from the reduction of a polynomial in $\mathbb{Z}[X]$, its degree as a morphism of $\mathbb{P}^1 \times \overline{\mathbb{F}}_q$ is bounded independently from q.

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

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

(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 $\alpha_1, \ldots, \alpha_r$ 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) or (H') with $k_f = n - 1$.

3.5.4. Sums of the form (2.3) with $f = X$, $\chi = 1$, h polynomial..

Proposition 3.61 (Katz). *Let $\mathcal{G}_h$ be the ℓ-adic sheaf over $\mathbb{F}_q$ of Proposition 2.54 associated to the polynomial $h = \sum_{i=1}^n a_i X^i$ of degree $n \geqslant 3$. We assume that $a_{n-1} = 0$. The geometric monodromy group $G_{\mathrm{geom}}(\mathcal{G}_h)$ is*

(1) $\mathrm{SL}_{n-1}(\mathbb{C})$ *if $n - 1$ is odd,*

(2) If $n - 1 \notin \{6, 8\}$ is even:

- $\mathrm{Sp}_{n-1}(\mathbb{C})$ *if $h(x) + h(-x)$ is constant (i.e. h has no monomial of even positive degree),*
- $\mathrm{SL}_{n-1}(\mathbb{C})$ *otherwise.*

Proof. See [Kat90, 7.12.4.2] (also [Kat87]). □

Example 3.62. For the Birch sums (2.4), we have $h = X^3$ and the corresponding monodromy group is $\mathrm{Sp}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})$.

3.5.5. Sums of the form (2.3) with f polynomial, $\chi \neq 1$.

Proposition 3.63 (Katz). *Let $\mathcal{G}$ be the ℓ-adic sheaf over $\mathbb{F}_q$ associated to f, g, h, χ from Proposition 2.55. We assume furthermore that h and f are odd and that there exists $L \in \mathbb{Q}(X)$ even or odd with $L(x)^r = g(x)g(-x)$. If either $N \neq 7, 8$ or $|n - d| \neq 6$, then $G_{\mathrm{geom}}(\mathcal{G})$ is given by*

(1) $\mathrm{Sp}_N(\mathbb{C})$ *if L is even,*

(2) $\mathrm{SO}_N(\mathbb{C})$ *if L is odd and $n > d$.*

Proof. See [Kat90, 7.13 (Sp-example(2)) and 7.14 (O-example(2))]. □

3.5.6. Families of hyperelliptic curves.

Proposition 3.64.

(1) Let $\mathcal{F}$ be the normalized sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ from Proposition 2.57 (3). We have $G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F}) = \mathrm{Sp}_{2g}(\mathbb{C})$

(2) Assume that $\sqrt{q} \in \mathbb{Z}_\ell$ and let $\widehat{\mathcal{F}}$ be the normalized sheaf of $\mathbb{F}_\ell$-modules over $\mathbb{F}_q$ from Proposition 2.57 (3). We have $G_{\mathrm{geom}}(\widehat{\mathcal{F}}) = G_{\mathrm{arith}}(\widehat{\mathcal{F}}) = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.

Proof. (1) By [KS99, Theorem 10.1.16], the geometric monodromy group is symplectic. Since we normalized, [KS99, Lemma 10.1.9] shows that the arithmetic monodromy group preserves the sames pairing (without normalization, it is a symplectic similitude with multiplicator q).

(2) This is a theorem of Yu, also proven in [Hal08] with Theorem 3.32: indeed, by Proposition 2.57 (1)b, the geometric monodromy group contains a transvection.

□

3.5.7. Arithmetic and geometric monodromy groups. In the previous sections, often only the geometric monodromy group $G_{\mathrm{geom}} = G_{\mathrm{geom}}(\mathcal{F})$ of a sheaf $\mathcal{F}$, or its connected component

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

were given. However, as we see in Proposition 3.4 and Deligne's equidistribution Theorem 3.6, we are interested in G_{geom}, and it is desirable to have $G_{\mathrm{geom}} = G_{\mathrm{arith}}$.

As it 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 Proposition 3.19 (4)). 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 $\mathcal{F}$.

We will apply this strategy to the sheaves studied above in Section 5.5.

Chapter 4

Probabilistic models

In this chapter, we develop the probabilistic models that will be used to study the distribution of values and sums of trace functions (in $\mathbb{C}$ or in residue fields of cyclotomic fields), inspired by Deligne's equidistribution Theorem 3.6 and [Lam13], [LZ12]. We then introduce the tools that we will use to show that they are accurate (in the sense of convergence in law).

In this chapter, we fix an ℓ-adic coefficient ring A and an isomorphism $\iota : A \to \mathbb{C}$ if $A = \overline{\mathbb{Q}}_\ell$, $\iota = \mathrm{id} : A \to A$ otherwise.

4.1. Probabilistic models

We consider an ℓ-adic sheaf of A-modules $\mathcal{F}$ over $\mathbb{F}_q$, lisse on a dense open U, corresponding to a representation

$$\rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}(V) = \mathrm{GL}_n(\iota(A)).$$

We are interested in the distribution of the images of the compositions

$$\rho_{\mathcal{F}} \circ \mathrm{Frob} : \qquad \begin{array}{ccc} U(\mathbb{F}_q) & \xrightarrow{\mathrm{Frob}} & G^\sharp_{\mathrm{arith}} \\ & \searrow^{t_{\mathcal{F}}} & \downarrow \mathrm{tr} \\ & & \iota(A), \end{array}$$

or in other words in the $G^\sharp_{\mathrm{arith}}$-valued (resp. $\iota(A)$-valued) random variable

$$\Big(\rho_{\mathcal{F}}(\mathrm{Frob}_x)\Big)_{x \in U(\mathbb{F}_q),} \tag{4.1}$$

$$\text{resp.} \qquad \Big(t_{\mathcal{F}}(x)\Big)_{x \in \mathbb{F}_q} \tag{4.2}$$

(with the uniform measure on $\mathbb{F}_q$).

Convention 4.1. Note that if $x \in \mathrm{Sing}(\mathcal{F})$, then $\rho_{\mathcal{F}}(\mathrm{Frob}_x)$ belongs to $\mathrm{GL}(V^{I_x})^\sharp$, and not $\mathrm{GL}(V)^\sharp$, which is why exclude the singularities in (4.1). To simplify the notations, we will only implicitly restrict all expressions containing local Frobenius to unramified points. For example, we will write $(\rho_{\mathcal{F}}(\mathrm{Frob}_x))_{x \in \mathbb{F}_q}$ for (4.1). This will have no impact since any estimate of a sum of trace functions starts by restricting to the set of lissity (see Section 2.2).

4.1.1. Model for (4.1). Deligne's equidistribution Theorem 3.6 suggests to model (4.1) as the random variable

$$Y = \pi(X),$$

where X is a random variable uniformly distributed in a maximal compact subgroup K of $G_{\mathrm{arith}}(\mathbb{C})$ with respect to the normalized Haar measure and $\pi : K \to K^\sharp$ is the projection.

Remark 4.2. When A is finite, note that $K = G_{\mathrm{arith}}$ with the counting measure.

Remark 4.3. In [Lam13], the values of Dirichlet characters of order d are modeled by random variables uniformly distributed in the unit circle, while in [LZ12] and in our model, uniform random variables in the roots of unity of order d are used. Since the moments are the same (see Remark 5.23), this will make no difference.

4.1.2. Model for (4.2). We shall then naturally model the random variable (4.2) by the $\iota(A)$-valued random variable $Z = \operatorname{tr} Y$.

In other words, the measure corresponding to Z is the pushforward of the normalized Haar measure through the map $\operatorname{tr} \circ \pi : K \to \iota(A)$.

4.1.3. Model for shifts. Similarly, for $I \subset \mathbb{F}_q$ of size $L \geqslant 1$, we will model the random vector

$$\Big((\rho_{\mathcal{F}}(\mathrm{Frob}_{x+a}))_{a\in I} \Big)_{x\in\mathbb{F}_q}$$

by the random vector $(Y_1, \dots, Y_L)$, for Y_i independent distributed like Y, and correspondingly the random vector

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

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

Therefore, the sum of shifts

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

will be modeled by the random walk $S(L) = Z_1 + \cdots + Z_L$, as in [Lam13] and [LZ12].

4.2. Sums of products

To show that the models defined above are accurate (in the sense of convergence in law), we will need to estimate precisely "sums of products" of the form

$$\sum_{x\in\mathbb{F}_q} \prod_{i=1}^{L} t_i(x), \tag{4.3}$$

where $t_1, \dots, t_L : \mathbb{F}_q \to \iota(A)$ are trace functions over $\mathbb{F}_q$. More precisely:

– In the case $A = \overline{\mathbb{Q}}_\ell$, the method of moments will lead to sums of the form

$$\sum_{x\in\mathbb{F}_q} \prod_{a\in I} t(x+a)^{k_a} \overline{t(x+a)}^{r_a} \tag{4.4}$$

for $t : \mathbb{F}_q \to \mathbb{C}$ a trace function, $I \subset \mathbb{F}_q$ and $k_a, r_a \geqslant 0$ integers.

– In the finite case (A is a residue field), we can directly work with density functions by using the second orthogonality relations, and this will lead to sums of the form
$$\sum_{x\in\mathbb{F}_q}\prod_{a\in I}\chi_a(\rho(\mathrm{Frob}_{x+a})) \tag{4.5}$$
for $\rho : \pi_{1,q} \to G_{\mathrm{arith}}$ the representation corresponding to a trace function over $\mathbb{F}_q$, with monodromy group G_{arith}, $I \subset \mathbb{F}_q$, and $\chi_a : G_{\mathrm{arith}} \to \mathbb{C}$ characters of irreducible representations. We will see that this can be reinterpreted as a sum of products of trace functions.

In the rest of this chapter, we present how to achieve such estimates through the ℓ-adic formalism, building upon [FKM15b] and [Kat88].

Note that we here critically need to keep track of the dependency of implicit constants with respect to conductors, because those will be unbounded as the parameters grow, which is not the case in [FKM15b].

4.2.1. General sums of products.

Proposition 4.4. *Let $(\mathcal{F}_i)_{1\leqslant i\leqslant L}$ be a tuple of sheaves of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$, with corresponding trace functions $(t_i : \mathbb{F}_q \to \iota(A))_{1\leqslant i\leqslant L}$. Then*
$$\sum_{x\in\mathbb{F}_q} t_1(x)\dots t_L(x) = q\cdot\mathrm{tr}\left(\mathrm{Frob}_q \mid \mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}}\right) + O(r^L Lc^2\sqrt{q})$$
for $\mathcal{F} = \otimes_{1\leqslant i\leqslant L}\mathcal{F}_i$, $c = \max_{1\leqslant i\leqslant L}\mathrm{cond}(\mathcal{F}_i)$, $r = \max_{1\leqslant i\leqslant L}\mathrm{rank}(\mathcal{F}_i)$, and an absolute implicit constant. In particular, the error term is $O(c^{3L}\sqrt{q})$, and $O(Lc^2\sqrt{q})$ if $r = 1$.

Proof. First, we pass from the product of trace functions to the trace function of the product of the corresponding sheaves. By Proposition 2.23 (2), we have
$$\begin{aligned}\sum_{x\in\mathbb{F}_q} t_1(x)\dots t_L(x) &= \sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x) + O\left(||t_1||_\infty\dots||t_L||_\infty|E|\right)\\ &= \sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x) + O\left(\mathrm{rank}(\mathcal{F})|E|\right)\end{aligned}$$
where $E = \{x\in\mathbb{F}_q : t_1(x)\dots t_L(x)\neq t_{\mathcal{F}}(x)\}$, the second equality following from Proposition 2.15. We have $E\subset S$, where $S = \bigcup_{i=1}^L(\mathrm{Sing}(\mathcal{F}_i)\cap\mathbb{A}^1(\mathbb{F}_q))$. Hence,
$$\sum_{x\in\mathbb{F}_q} t_1(x)\dots t_L(x) = \sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x) + O\left(\mathrm{rank}(\mathcal{F})|S|\right). \tag{4.6}$$
For $x\in\mathrm{Sing}(\mathcal{F})$, we have $\mathrm{Swan}_x(\mathcal{F})\leqslant\mathrm{rank}(\mathcal{F})\sum_{i=1}^L\mathrm{Swan}_x(\mathcal{F}_i)$ by Proposition 2.23. Thus, by Theorem 2.28,
$$\sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x) = q\cdot\dim\left(\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}}\right) + O\left(E(\mathcal{F})\sqrt{q}\right)$$
with
$$E(\mathcal{F}) = \mathrm{rank}(\mathcal{F})\left(|S| - 1 + \sum_{x\in S}\sum_{i=1}^L\mathrm{Swan}_x(\mathcal{F}_i)\right)\ll r^L Lc^2.$$
□

Remark 4.5. Note that the error term is exponential in L, with basis r. If we had used the bound $E(\mathcal{F}) \ll \operatorname{cond}(\mathcal{F})^2$, we would have gotten the error term $O(c^{4L}\sqrt{q})$, which is exponential even when $r = 1$. For other applications, it may be interesting to know whether one could do better, e.g. an error term polynomial in r, L, c. We investigate this question in Appendix A.

4.2.2. Sums of products arising from a single sheaf. As we see in (4.4) and (4.5), we will need to handle the case where the trace functions $t_1, \ldots, t_L$ in (4.3) are obtained from a single sheaf by additive change of variable, multiplication, conjugation, or composition with a representation of the monodromy group. To do so, we will use the following:

Lemma 4.6. *Let $(\mathcal{F}_i)_{1\leqslant i\leqslant L}$ be a family of sheaves of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$, corresponding to representations $(\rho_i : \pi_{1,q} \to \mathrm{GL}(V_i))_{1\leqslant i\leqslant L}$. Let $\mathcal{G} = \bigoplus_{1\leqslant i\leqslant L} \mathcal{F}_i$ be the direct sum, which corresponds to the representation*

$$\rho_{\mathcal{G}} = \bigoplus_i \rho_i : \pi_{1,q} \to \mathrm{GL}(\oplus_i V_i) = \prod_i \mathrm{GL}(V_i).$$

If Λ is a $\overline{\mathbb{Q}}_\ell$-representation of $G_{\mathrm{arith}}(\mathcal{G})$ as a $\overline{\mathbb{Q}}_\ell$-algebraic group then the composition

$$\Lambda \circ \rho_{\mathcal{G}} : \qquad \begin{array}{ccccccc} \pi_{1,q} & \longrightarrow & \rho_{\mathcal{G}}(\pi_{1,q}) & \longrightarrow & G_{\mathrm{arith}}(\mathcal{G}) & \longrightarrow & \prod_i \mathrm{GL}(V_i) \\ & \searrow & & & \downarrow{\scriptstyle \Lambda} & & \\ & & & & \mathrm{GL}(W) & & \end{array}$$

corresponds to an ℓ-adic sheaf $\mathcal{G}(\Lambda)$ over $\mathbb{F}_q$ of dimension $\dim\Lambda$ *such that*

$$\mathcal{G}(\Lambda)_{\pi_{1,q}} = \Lambda_{G_{\mathrm{arith}}(\mathcal{G})}, \ \mathcal{G}(\Lambda)_{\pi_{1,q}^{\mathrm{geom}}} = \Lambda_{G_{\mathrm{geom}}(\mathcal{G})}.$$

Proof. This is clear by Proposition 2.8. □

Remark 4.7. More precisely, by Tannakian duality, the map $\Lambda \mapsto \Lambda \circ \rho_{\mathcal{G}}$ yields an equivalence of Tannakian categories between the category of sheaves of A-modules over $\mathbb{F}_q$ generated by the $\mathcal{F}_i$ and the category of representations of $G_{\mathrm{arith}}(\mathcal{G})$ (see [Sza09, Theorem 6.5.3, Proposition 6.5.15] and [FKM15b, Proposition 2.5]).

4.2.3. Sums of products of the form (4.4).

Proposition 4.8. *Let $\mathcal{F}$ be a sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ with monodromy groups $G = G_{\mathrm{arith}}(\mathcal{F}) = G_{\mathrm{geom}}(\mathcal{F})$. For $L \geqslant 1$, let $a_1, \ldots, a_L \in \mathbb{F}_q$ be distinct. We assume that the arithmetic and geometric monodromy groups of*

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

coincide and are as big as possible, i.e. isomorphic to G^L. Then, for all $\boldsymbol{k}, \boldsymbol{r} \in \mathbb{N}^L$, the sheaf

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

satisfies

$$\operatorname{tr}\left(\mathrm{Frob}_q \mid (\mathcal{G}_{\boldsymbol{k},\boldsymbol{r}})_{\pi_{1,q}^{\mathrm{geom}}}\right) = \prod_{1\leqslant i\leqslant L} \operatorname{mult}_1\left(\mathrm{Std}^{\otimes k_i}\otimes D(\mathrm{Std})^{\otimes r_i}\right),$$

where Std *is the standard representation of* G *in* $\mathrm{GL}_n(\mathbb{C})$.

Remark 4.9. Recall that there is an equivalence of categories between the $\overline{\mathbb{Q}}_\ell$-representations of the monodromy groups as $\overline{\mathbb{Q}}_\ell$-algebraic group and their representations as complex algebraic groups (see Corollary 3.3). Thus, it does not matter if we view G as a an algebraic group over $\mathbb{C}$ or $\overline{\mathbb{Q}}_\ell$ in the statement of Proposition 4.8. By the same reference, the multiplicity can also be computed in a maximal compact subgroup.

Proof. We apply Lemma 4.6 with $\mathcal{F}_i = [+a_i]^*\mathcal{F}$, observing that $\mathcal{G}_{\boldsymbol{k},\boldsymbol{r}} = \mathcal{G}(\Lambda)$ for the representation

$$\Lambda = \boxtimes_{1\leqslant i\leqslant L}\left(\mathrm{Std}^{\otimes k_i}\otimes D(\mathrm{Std})^{\otimes r_i}\right).$$

Since we assume that $G_{\mathrm{geom}}(\mathcal{G}) = G_{\mathrm{arith}}(\mathcal{G}) = G^L$, we have as in Proposition 3.4

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

where the last equality holds by Schur's Lemma. □

By combining Proposition 4.4 with Proposition 4.8, we immediately get our desired estimates about sums of products of the form (4.4). It also applies to Kummer sheaves by multiplicativity (for which a bit more care is needed when the character is composed with a rational function).

Definition 4.10. 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 such a Kummer sheaf, it is always I-compatible.

Corollary 4.11. *Let $\mathcal{F}$ be a sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ with monodromy groups $G = G_{\mathrm{arith}}(\mathcal{F}) = G_{\mathrm{geom}}(\mathcal{F})$ and let $a_1, \dots, a_L \in \mathbb{F}_q$ be distinct. Assume that either:*

(1) $\mathcal{F}$ and the a_i verify the hypotheses of Proposition 4.8, or

(2) $\mathcal{F}$ is a $\{a_1, \dots, a_L\}$-compatible Kummer sheaf $\mathcal{L}_{\chi(f)}$.

Then, for all $\boldsymbol{k}, \boldsymbol{r} \in \mathbb{N}^L$, the sum of products

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{1\leqslant i\leqslant L} t_{\mathcal{F}}(x+a_i)^{k_i}\overline{t_{\mathcal{F}}(x+a_i)}^{r_i}$$

is equal to

$$\prod_{1\leqslant i\leqslant L} \mathrm{mult}_1(\mathrm{Std}^{\otimes k_i}\otimes D(\mathrm{Std})^{\otimes r_i}) + O(r^{S(\boldsymbol{k},\boldsymbol{r})}S(\boldsymbol{k},\boldsymbol{r})c^2q^{-1/2})$$

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

Proof. It remains to treat the case of a Kummer sheaf $\mathcal{L}_{\chi(f)}$ for $\chi:\mathbb{F}_q^\times\to\mathbb{C}$ of order d and $f\in\mathbb{F}_q(T)$. By multiplicativity, the sum is 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 $g(X)=\prod_{1\leqslant i\leqslant L}f(X+a_i)^{k_i-r_i}$. 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

$$\deg(g_1)+\deg(g_2)\leqslant S(\boldsymbol{k},\boldsymbol{r})(\deg(f_1)+\deg(f_2))\leqslant S(\boldsymbol{k},\boldsymbol{r})\,\mathrm{cond}(\mathcal{F}).$$

By Proposition 2.45 and Corollary 2.31, 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[1] 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 $d_f\geqslant 0$, 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. □

Example 4.12. A Kummer sheaf $\mathcal{L}_{\chi(f)}$ is I-compatible if:

- If $I\subset[1\dots p]\cong\mathbb{F}_p$ with $\max_{a\in I}a<p/\deg(f)$.
- More generally, if $I\subset[1\dots p]^e\cong\mathbb{F}_q$ with $\max_{a\in I}\pi_i(a)<p/\deg(f)$ for all $1\leqslant i\leqslant e$, where $\pi_i:\mathbb{F}_q\to[1\dots p]$ are the projections.

4.2.4. Sums of products of the form (4.5). Let now $\mathcal{F}$ be a sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$, corresponding to a representation $\rho:\pi_{1,q}\to\mathrm{GL}_n(\mathbb{F}_\lambda)$, and with monodromy groups $G=G_{\mathrm{geom}}(\mathcal{F})=G_{\mathrm{arith}}(\mathcal{F})\leqslant\mathrm{GL}_n(\mathbb{F}_\lambda)$. We want to handle sums of the form

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{a\in I}\chi_a(\rho(\mathrm{Frob}_{x+a})) \tag{4.7}$$

for $I\subset\mathbb{F}_q$ and $\chi_a:G\to\mathbb{C}$ characters of irreducible representations.

Definition 4.13. We fix an isomorphism of fields $\iota:\mathbb{C}\to\overline{\mathbb{Q}}_\ell$ and:

(1) For $\sigma\in\mathrm{Aut}(\mathbb{F}_\lambda)$, we let $\sigma(\mathcal{F})$ be the sheaf of $\mathbb{F}_\lambda$-modules corresponding to the representation $\sigma\circ\rho:\pi_{1,q}\to\mathrm{GL}_n(\mathbb{F}_\lambda)$.

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

(2) For $\eta : G \to \mathrm{GL}(V)$ a complex representation, we let $\mathcal{F}_\eta$ be the sheaf of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ corresponding to the representation

$$\iota \circ \eta \circ \rho : \pi_{1,q} \to G \to \mathrm{GL}(V) \to \mathrm{GL}(\iota(V)).$$

Remark 4.14. Since G is discrete, there are no issues with the continuity of the composition $\iota \circ \eta \circ \rho$, even if ι is not continuous.

Note that the trace function of $\mathcal{F}_\eta$ at unramified points is precisely $\chi \circ \rho \circ \mathrm{Frob}$, where χ is the character of η.

As for Proposition 4.8/Corollary 4.11, we obtain:

Proposition 4.15. *We consider $\mathcal{F}$ be as above. For $L \geqslant 1$, let $a_1, \dots, a_L \in \mathbb{F}_q$ be distinct, and let η_i be complex irreducible representations of G, not all trivial, with characters χ_i $(1 \leqslant i \leqslant L)$. We assume that either:*

(1) The arithmetic and geometric monodromy groups of

$$\bigoplus_{1 \leqslant i \leqslant L} [+a_i]^* \mathcal{F}_{\eta_i}$$

coincide and are as big as possible, i.e. isomorphic to $\prod_{1 \leqslant i \leqslant L} G/\ker \eta_i$, or

(2) $\mathcal{F}$ is a $\{a_1, \dots, a_L\}$-compatible Kummer sheaf $\mathcal{L}_{\chi(f)}$.

Then the sum of products (4.7) is

$$\ll q^{-1/2} \operatorname{cond}(\mathcal{F})^2 |G|^\delta \left(\prod_{i=1}^{L} \dim \eta_i \right) \sum_{i=1}^{L} \dim \eta_i$$

with $\delta = 0$ in case (1) and $\delta = 1$ otherwise.

Proof. (1) As in Theorem 3.6, note that $\dim(\mathcal{F}_\eta) = \dim \eta$, $\mathrm{Sing}(\mathcal{F}_\eta) \subset \mathrm{Sing}(\mathcal{F})$ and $\mathrm{Swan}_x(\mathcal{F}_\eta) \leqslant \dim \eta \, \mathrm{Swan}_x(\mathcal{F})$. By Proposition 4.4 (with the error term given in the proof) and Lemma 4.6 applied with $\mathcal{F}_i = [+a_i]^* \mathcal{F}_{\eta_i}$, the sum (4.7) is thus

$$\prod_{1 \leqslant i \leqslant L} \dim(\mathcal{F}_{\eta_i}^G) + O\left(q^{-1/2} \operatorname{cond}(\mathcal{F})^2 \left(\prod_{i=1}^{L} \dim \eta_i \right) \sum_{i=1}^{L} \dim \eta_i \right).$$

By Schur's Lemma, $\dim(\mathcal{F}_{\eta_i}^G) = \delta_{\eta_i \text{ trivial}}$.

(2) For every $i = 1, \dots, L$, there exists an integer $0 \leqslant b_i < d$ such that η_i is the one-dimensional representation $x \mapsto x^{b_i}$. By multiplicativity,

$$\frac{1}{q} \sum_{x \in \mathbb{F}_q} \prod_{i=1}^{L} \chi_i(\rho(\mathrm{Frob}_{x+a_i})) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} t_{\mathcal{G}}(x)$$

where $\mathcal{G} = \mathcal{F}_{\chi(g)}$ with $g(X) = \prod_{i=1}^{L} f(X + a_i)^{b_i}$. Since

$$\operatorname{cond}(\mathcal{G}) \leqslant 1 + \deg(g) \leqslant 1 + Ld \deg(f),$$

Corollary 2.31 gives

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q} t_{\mathcal{G}}(x) = \delta_{g \text{ is a } d-\text{power}} + O(Ld\deg(f)q^{-1/2})$$

and the conclusion follows as in the proof of Corollary 4.11.

□

4.3. Goursat-Kolchin-Ribet criteria

In this section, we investigate when the hypotheses of Propositions 4.8 and 4.15 hold, namely given an ℓ-adic sheaf $\mathcal{F}$ over $\mathbb{F}_q$ with monodromy group $G = G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F})$, an integer $L \geqslant 1$ and $a_1, \dots, a_L \in \mathbb{F}_q$ distinct, when do the arithmetic and geometric monodromy groups of

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

coincide and are as big as possible (i.e. isomorphic to G^L), where $\mathcal{F}_i = \mathcal{F}$ if $A = \overline{\mathbb{Q}}_\ell$ (resp. $\mathcal{F}_i = \mathcal{F}_{\eta_i}$ for some irreducible representation η_i of G if $A = \mathbb{F}_\lambda$).

In the case $A = \overline{\mathbb{Q}}_\ell$, this is handled by the Goursat-Kolchin-Ribet criterion of Katz. After reviewing the latter, we give an analogue for sheaves of $\mathbb{F}_\lambda$-modules.

4.3.1. Preliminaries. First, recall the classical Goursat Lemma:

Lemma 4.16 (Goursat). *Let G_1, G_2 be groups (resp. Lie algebras) and $H \leqslant G_1 \times G_2$ be a subgroup (resp. Lie subalgebra) such that the two projections $p_i : H \to G_i$ $(i = 1, 2)$ are surjective.*

$$\begin{array}{ccccc} & & G_1 & \longrightarrow & G_1/\ker p_2 \\ & & \uparrow{\scriptstyle p_1} & & \uparrow \\ H & \longrightarrow & G_1 \times G_2 & \longrightarrow & (G_1/\ker p_2) \times (G_2/\ker p_1) \\ & & \downarrow{\scriptstyle p_2} & & \downarrow \\ & & G_2 & \longrightarrow & G_2/\ker p_1 \end{array}$$

Then the image of H in $G_1/\ker p_2 \times G_2/\ker p_1$ is the graph of an isomorphism $G_1/\ker p_2 \cong G_2/\ker p_1$. In particular, if G_1, G_2 are simple, then either $H = G_1 \times G_2$, or H is the graph of an isomorphism $G_1 \cong G_2$.

Proof. See for example [Rib76, Lemma 5.2.1]. □

Lemma 4.17 ([Rib76, Lemma 5.2.2 and p. 791]). *Let $G_1, \dots, G_n$ be either*

(1) finite groups with no nontrivial abelian quotients, or

(2) simple finite-dimensional Lie algebras,

and let $G \leqslant G_1 \times \cdots \times G_n$ be such that every projection $G \to G_i \times G_j$ $(i \neq j)$ is surjective. Then $G = G_1 \times \cdots \times G_n$.

DEFINITION 4.18. Let k be a field. A pair $(G_i \to \mathrm{GL}(V_i))_{i=1,2}$ (or $(G_i \to \mathrm{PGL}(V_i))_{i=1,2}$) of faithful group representations over k is *Goursat-adapted* if every potential isomorphism $G_1 \cong G_2$ is of the form

$$\begin{cases} X \mapsto A\sigma(X)A^{-1} & \text{for an isomorphism } A : V_1 \to V_2 \text{ or} \\ X \mapsto A\sigma(X)^{-t}A^{-1} & \text{for an isomorphism } A : V_1^* \to V_2 \end{cases}$$

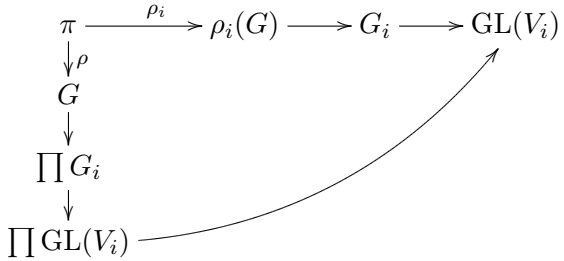
with $\sigma \in \mathrm{Aut}(k)$, $\sigma = \mathrm{id}$ unless k is finite.

Examples 4.19. (1) Let $G \in \{\mathrm{SL}_{n+1}(\mathbb{C}), \mathrm{Sp}_{2n}(\mathbb{C}), \mathrm{SO}_{n+1}(\mathbb{C})\} - \{\mathrm{SO}_8(\mathbb{C})\}$ for some $n \geqslant 1$, and assume that G_1, G_2 are conjugate to G. Then $(G_i, \mathrm{Std})_{i=1,2}$ is Goursat-adapted by Propositions 3.16 and 3.18. Indeed, $\mathrm{Out}(\mathfrak{sl}_n) \cong \mathbb{Z}/2$ (with the negative-transpose map) if $n > 2$, while $\mathrm{Out}(\mathfrak{sp}_n)$ and $\mathrm{Out}(\mathfrak{so}_{2n+1})$ are trivial. Similarly, $\mathrm{Out}(\mathfrak{so}_{2n}) \cong \mathbb{Z}/2$ (with conjugation by an orthogonal matrix) when $n \neq 4$ (but $\mathrm{Out}(\mathfrak{so}_8) \cong \mathfrak{S}_3$).

(2) Similarly, for k a finite field, $G \in \{\mathrm{PSL}_{n+1}(k), \mathrm{PSp}_{2n}(k)\}$ for $n \geqslant 1$, and G_1, G_2 are conjugate to G, the tuple $(G_i, \mathrm{Std})_{i=1,2}$ is Goursat-adapted by Propositions 3.17 and 3.18

4.3.2. Complex case. First we recall the Goursat-Kolchin-Ribet criterion of Katz for Lie groups of positive dimension:

Proposition 4.20 (Goursat-Kolchin-Ribet criterion, [Kat90, Chapter I.8])**.** *Let $\rho_i : \pi \to \mathrm{GL}(V_i)$ be finitely many complex irreducible representations of a topological group π, with monodromy groups $G_i = \overline{\rho_i(\pi)} \leqslant \mathrm{GL}(V_i)$ (where $\bar{\cdot}$ denotes Zariski closure). Consider the representation $\rho = \oplus \rho_i : \pi \to \mathrm{GL}(\oplus V_i) \cong \prod \mathrm{GL}(V_i)$ with monodromy group $G = \overline{\rho(\pi)}$.*



Assume that:

(1) $G_i^{0,\mathrm{der}}$ acts irreducibly on V_i and $\mathrm{Lie}(G_i^{0,\mathrm{der}})$ is simple.

(2) For every $i \neq j$, $\left(G_l^{0,\mathrm{der}} \to \mathrm{GL}(V_l)\right)_{l=i,j}$ is Goursat-adapted.

(3) For every $i \neq j$, there is no isomorphism

$$\rho_i \cong \chi \otimes \rho_j \text{ or } \rho_i \cong \chi \otimes D(\rho_j)$$

for χ a 1-dimensional representation of π.

Then $G^{0,\mathrm{der}}$ is as large as possible, i.e. $G^{0,\mathrm{der}} = \prod G_i^{0,\mathrm{der}}$.

Proof (idea). The group G is reductive, so $G^{0,\mathrm{der}}$ is semisimple (see e.g. [Mil12, Theorem 1.29]). Without loss of generality, we can assume $G = G^{0,\mathrm{der}}$ and $G_i = G_i^{0,\mathrm{der}}$ (the 1-dimensional representations in (3) arise through this reduction). By Lie theory, it is enough to prove that $\mathrm{Lie}(G^{0,\mathrm{der}}) = \prod \mathrm{Lie}(G_i^{0,\mathrm{der}})$. By Lemma 4.17, it is enough to treat the case $n = 2$. By Goursat's Lemma 4.16, either the conclusion holds or $\mathrm{Lie}(G^{0,\mathrm{der}})$ is the graph of an isomorphism $\mathrm{Lie}(G_1^{0,\mathrm{der}}) \cong \mathrm{Lie}(G_2^{0,\mathrm{der}})$. By Goursat-adaptedness, this gives an isomorphism as in (3). □

Example 4.21. By Example 4.19, this holds when there is

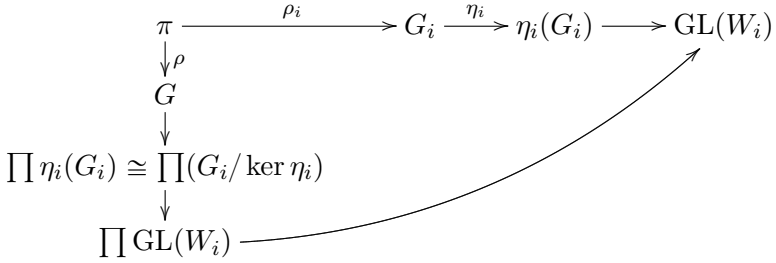
$$G \in \{\mathrm{SL}_{n+1}(\mathbb{C}), \mathrm{Sp}_{2n}(\mathbb{C}), \mathrm{SO}_{n+1}(\mathbb{C})\} - \{\mathrm{SO}_8(\mathbb{C})\}$$

for some $n \geqslant 1$ such that every G_i is conjugate to G.

4.3.3. Finite cases.

Goursat-Kolchin-Ribet for finite groups of Lie type. In the case of a finite monodromy group (i.e. a 0-dimensional Lie group), the Lie group is not connected and the Lie algebra is zero (thus not simple), so the above does not apply. We can however give a finite analogue, where quasisimplicity replaces semisimplicity.

Proposition 4.22 (Goursat-Kolchin-Ribet for quasisimple groups)**.** *Let $\rho_i : \pi \to \mathrm{GL}(V_i)$ be finitely many representations over a finite field k of a topological group π, with finite monodromy groups $G_i = \rho_i(\pi) \leqslant \mathrm{GL}(V_i)$, and let $\eta_i : G_i \to \mathrm{GL}(W_i)$ be nontrivial representations over a field F. Consider the representation $\rho = \oplus(\eta_i \circ \rho_i) : \pi \to \mathrm{GL}(\oplus W_i) \cong \prod \mathrm{GL}(W_i)$ with monodromy group $G = \rho(\pi)$.*



Assume that:

(1) The groups G_i are quasisimple, i.e. they are perfect ($G_i = G_i^{\mathrm{der}}$) and $G_i' = G_i/Z(G_i)$ is simple.

(2) For every $i \neq j$, $\left(G_l' \to \mathrm{PGL}(V_l)\right)_{l=i,j}$ is Goursat-adapted.

(3) For every $i \neq j$, there is no isomorphism

$$\rho_i \cong \chi \otimes \sigma(\rho_j) \text{ or } \rho_i \cong \chi \otimes D(\sigma(\rho_j))$$

for χ a 1-dimensional representation of π over k and $\sigma \in \mathrm{Aut}(k)$.

Then G is as large as possible, i.e. $G = \prod(G_i/\ker \eta_i)$.

Proof. Since G_i is quasisimple, note that we have either:

– $G_i = Z(G_i)\ker\eta_i$. By taking derived subgroups, this gives $G_i^{\mathrm{der}} = G_i \leqslant (\ker\eta_i)^{\mathrm{der}} \leqslant \ker\eta_i$, so $\ker\eta_i = G_i$ and η_i is trivial, which is excluded;

– $\ker\eta_i \leqslant Z(G_i)$.

For H any group, let us continue to denote $H' = H/Z(H)$. By perfectness, it is enough to show that $G' = \prod(G_i/\ker\eta_i)' \cong \prod G_i'$.

Since a quasisimple group has no nontrivial abelian quotient (the derived subgroup is the smallest normal subgroup with an abelian quotient), it is enough to treat the case $n = 2$ by Lemma 4.17.

By Goursat's Lemma 4.16 and the simplicity of G_i', either $G' = G_1' \times G_2'$, or G' is the graph of an isomorphism $G_1' \cong G_2'$. In the second case, since the center of GL is the group of scalar matrices, the isomorphism given by hypothesis (2) lifts to an isomorphism contradicting (3). □

Remark 4.23. The setting of Proposition 4.22 is more general than that of Proposition 4.20. This is to allow us to compute the monodromy group of sums of ℓ-adic representations composed with representations of the monodromy group, as in Section 4.2.4. Condition (3) is assumed on the original sheaves, and not also on the compositions.

Remark 4.24. In Proposition 4.20, the 1-dimensional representations appear when passing from G to $G^{0,\mathrm{der}}$, while in Proposition 4.22 they appear when passing from G to G'.

Example 4.25. Let k be a finite field and $n \geqslant 1$ be an integer. By [MT11, Theorem 24.17], $\mathrm{SL}_n(k)$ and $\mathrm{Sp}_{2n}(k)$ are quasisimple as soon as $|k| > 3$. Hence, by Example 4.19, conditions (1) and (2) of Proposition 4.22 hold if there exists $G \in \{\mathrm{PSL}_{n+1}(k), \mathrm{PSp}_{2n}(k)\}$ for some $n \geqslant 1$ such that every G_i is conjugate to G.

Goursat-Kolchin-Ribet for μ_d (d prime). Lastly, we give a version of the Goursat-Kolchin-Ribet criterion for cyclic groups of prime order.

Proposition 4.26. *Let $\rho_i : \pi \to k^\times$ be finitely many one-dimensional representations over a field k of a topological group π, with monodromy groups $G_i = \rho(\pi) \cong \mathbb{Z}/d$ (d prime), and let $\eta_i : G_i \to F^\times$ be nontrivial representations over a field F. Consider the representation $\rho = \oplus(\eta_i \circ \rho_i) : \pi \to \prod F^\times$ with monodromy group $G = \rho(\pi)$. If there is no isomorphism of the form*

$$\rho_i \cong \rho_j^{\otimes a} \quad \text{for } i \neq j,\ 1 \leqslant a < d,$$

then G is as large as possible, i.e. $G \cong \prod \mathbb{Z}/d$.

Proof. Since $\mathbb{Z}/d$ is simple, we can apply Lemma 4.17 to reduce to the case of two representations as before. By Goursat's Lemma 4.16, either G is as large as possible, or it is the graph of an isomorphism $G_1 \to G_2$. Since $\mathrm{Aut}(\mathbb{Z}/d) \cong (\mathbb{Z}/d)^\times$, this proves the statement. □

4.4. Coherent families

Being given Corollary 4.11 and Proposition 4.15 — that we will use to prove the accuracy of our models — and the criteria from Section 4.3 — which give

sufficient conditions to apply the former — we can now make precise the notion of good/natural families we mentioned in Section 1.2.4.

4.4.1. Definitions.

Definition 4.27 (Complex case). We fix a prime ℓ and an isomorphism of fields $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. A family $(\mathcal{F}_q)_q$ of geometrically irreducible sheaves of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$ (for q varying over powers of primes distinct from ℓ) is *coherent* if:

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

and either:

(2) *Kummer case*: For every q, $\mathcal{F}_q$ is a Kummer sheaf, and the associated characters are either all real-valued or all complex-valued.

(2′) *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

$$[+a]^*\mathcal{F}_q \cong \mathcal{F}_q \otimes \mathcal{L} \quad \text{or} \quad [+a]^*\mathcal{F}_q \cong D(\mathcal{F}_q) \otimes \mathcal{L} \tag{4.8}$$

for a sheaf $\mathcal{L}$ of rank 1 over $\mathbb{F}_q$ and $a \in \mathbb{G}_m(\mathbb{F}_q)$.

Definition 4.28 (Finite case). A family $(\mathcal{F})$ of irreducible sheaves of $\mathbb{F}_\lambda$-modules over finite fields $\mathbb{F}_q$ (with $\mathbb{F}_\lambda$ and $\mathbb{F}_q$ varying, of distinct characteristic) is *coherent* if:

(1) (Conductor) $\mathrm{cond}(\mathcal{F})$ is uniformly bounded for all $\mathcal{F}$ in the family,

and either:

(2) *Kummer case*: Every $\mathcal{F}$ in the family is a Kummer sheaf.

(2′) *Cyclic simple case*: For every sheaf $\mathcal{F}$ of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$ in the family:

a) (Monodromy groups) The geometric and arithmetic monodromy group of $\mathcal{F}$ coincide and are equal to $\mu_d(\mathbb{F}_\lambda)$ for some prime d.

b) (Independence of shifts) There is no geometric isomorphism of the form

$$[+a]^*\mathcal{F} \cong \mathcal{F}^{\otimes i} \ (1 \leqslant i < d,\ a \in \mathbb{F}_q^\times).$$

(2″) *Classical case*: There exists $G \in \{\mathrm{SL}_{n+1}, \mathrm{Sp}_{2n}\}$ for some $n \geqslant 1$ such that for every sheaf $\mathcal{F}$ of $\mathbb{F}_\lambda$-modules in the family:

a) (Monodromy groups) The geometric and arithmetic monodromy groups of $\mathcal{F}$ coincide and are conjugate to $G(\mathbb{F}_\lambda)$ in $\mathrm{GL}_n(\mathbb{F}_\lambda)$.

b) (Independence of shifts) There is no geometric isomorphism of the form

$$[+a]^*\mathcal{F} \cong \mathcal{L} \otimes \sigma(\mathcal{F}) \text{ or } [+a]^*\mathcal{F} \cong \mathcal{L} \otimes D(\sigma(\mathcal{F})) \tag{4.9}$$

for $a \in \mathbb{G}_m(\mathbb{F}_q)$, $\sigma \in \mathrm{Aut}(\mathbb{F}_\lambda)$ and $\mathcal{L}$ a rank 1 sheaf.

Remark 4.29. Note that we fix the structure of the monodromy group in the classical case (in particular the rank) but we let eventually the order of the character/monodromy group vary otherwise. By keeping track of the dependency of the conductor with respect to the rank we could also let the latter vary, but this is not a natural aspect in applications.

Remark 4.30. In the finite case, we let the coefficient ring vary to study the reductions of the trace function (whose image often does not depend on λ) modulo various ideals. See Chapter 6 for more details.

Remark 4.31. By Theorem 2.41 and Proposition 2.42, the geometric irreducibility and conductor conditions are stable by Fourier transform. As always, if the sheaf is not geometrically irreducible, one may decompose it by Proposition 2.27.

Remark 4.32. When the monodromy group is equal to $\mu_d(\mathbb{C})$ (resp. $\mu_d(\mathbb{F}_\lambda)$) with d nonprime, Proposition 4.20 (resp. Propositions 4.22 and 4.26) cannot be applied because the Lie algebra is not simple (resp. the group is not quasisimple). Thus, we assume that the sheaf is a Kummer sheaf to handle sums of products via multiplicativity instead.

4.4.2. Sums of products. Finally, we sum up the previous sections by showing how sums of products of the form (4.4) and (4.5) can be controlled for coherent families.

Complex case.

Proposition 4.33. *Let $(\mathcal{F}_q)_q$ be a coherent family of sheaves of $\overline{\mathbb{Q}}_\ell$-modules over $\mathbb{F}_q$, with monodromy group $G \leqslant \mathrm{GL}_n(\mathbb{C})$. Let $a_1, \dots, a_L \in \mathbb{F}_q$ be distinct. If $\mathcal{F}_q$ is $\{a_1, \dots, a_L\}$-compatible, then for all $\boldsymbol{k}, \boldsymbol{r} \in \mathbb{N}^L$,*

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

where the implicit constant does not depend on q, $S(\boldsymbol{k},\boldsymbol{r}) = \sum_{i=1}^L (k_i + r_i)$, and Std *is the standard representation of G.*

Proof. In the classical case, the Goursat-Kolchin-Ribet criterion (Proposition 4.20) and Example 4.21 show that the arithmetic and geometric monodromy groups of $\bigoplus_{1\leqslant i\leqslant L}[+a_i]^*\mathcal{F}_q$ coincide and are conjugate to G^L. Hence, we can apply Corollary 4.11. Under the compatibility assumption, the latter also applies to Kummer sheaves. □

Finite case.

Proposition 4.34. *Let $(\mathcal{F})$ be a coherent family of sheaves of $\mathbb{F}_\lambda$-modules over finite fields $\mathbb{F}_q$ (with $\mathbb{F}_q$ and $\mathbb{F}_\lambda$ varying, of distinct characteristic). Let $\mathcal{F}$ be a sheaf in the family, corresponding to a representation $\rho : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\lambda)$, and let $a_1, \dots, a_L \in \mathbb{F}_q$ be distinct. If $\mathcal{F}$ is $\{a_1, \dots, a_L\}$-compatible, then for all nontrivial*

irreducible complex characters $\chi_1, \dots, \chi_L$ *of the monodromy group* G *of* $\mathcal{F}$*,*

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{1\leqslant i\leqslant L}\chi_i(\rho(\mathrm{Frob}_{x+a_i})) \ll q^{-1/2}|G|^{\delta}\left(\prod_{i=1}^{L}\dim\eta_i\right)\sum_{i=1}^{L}\dim\eta_i,$$

where the implicit constant does not depend on q*, and* $\delta = 1$ *in the Kummer case,* $\delta = 0$ *otherwise.*

Proof. Let η_i be the representation corresponding to χ_i. We apply Proposition 4.15. In the classical and cyclic simple cases, it suffices to show that the geometric and arithmetic monodromy groups of the sheaf $\bigoplus_{i=1}^{L}[+a_i]^*\mathcal{F}_{\eta_i}$ coincide and are isomorphic to $\prod_{i=1}^{L} G/\ker\eta_i$. For the classical case, by Proposition 4.22 (see also Remark 4.23), it suffices to show that for $i \neq j$ there is no geometric isomorphism

$$[+a_i]^*\mathcal{F} \cong \mathcal{L}\otimes[+a_j]^*\sigma(\mathcal{F}) \text{ or } [+a_i]^*\mathcal{F} \cong \mathcal{L}\otimes[+a_j]^*\sigma(D(\mathcal{F}))$$

for some rank 1 sheaf $\mathcal{L}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_\lambda)$. This would give an isomorphism of the form (4.9) for some $a \in \mathbb{F}_q^\times$, which is excluded by the independence of shifts. For the cyclic simple case, proceed similarly with Proposition 4.26. The Kummer case is handled by the compatibility assumption. □

4.4.3. Examples. In Section 2.4 and Chapter 3, we already encountered families of sheaves with fixed large known monodromy groups and uniformly bounded conductors:

(1) Hyper-Kloosterman sheaves of fixed rank (Propositions 2.46 and Theorem 3.23), in the complex and finite cases.

(2) Families of additive or multiplicative characters, eventually with varying order, pre-composed with the reduction of a fixed rational polynomial in $\mathbb{Q}(X)$, in Sections 2.4.1 and 3.5.1, in the complex and finite cases.

(3) Hyper-geometric sums of fixed rank, in the complex case.

(4) The three families of general exponential sums of Sections 2.4.3 and 3.5, where the rational functions arise from the reduction of fixed rational polynomials in $\mathbb{Q}(X)$, in the complex case.

(5) The sheaves from Propositions 2.57 and 3.64, associated to zeta functions of hyperelliptic curves in a family, when f therein arises from the reduction of a fixed squarefree $f \in \mathbb{Z}[X]$.

Remark 4.35. According to Remark 3.55, we do not consider the finite cases for the last two families, even though one may be able to do so in the future.

To show that these are coherent families, it would remain to show the independence of shifts and the equality of the arithmetic and geometric monodromy groups. This study will be carried out in the next two chapters, respectively for the complex and finite cases.

We saw in Section 3.5.7 that the second condition could usually be achieved up to twisting the sheaf. In the next section, we will give criteria for the first condition.

4.5. Independence of shifts

Showing that a geometric isomorphism of the form (4.8) or (4.9) does not exist can usually be done by looking at the ramification on both sides. In this section, we give some general techniques that we will apply in the next chapter.

Lemma 4.36. *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 (4.8). 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,

$$|\,\mathrm{Sing}(\mathcal{L})| + \sum_{x \in \mathrm{Sing}(\mathcal{L})} \mathrm{Swan}_x(\mathcal{L}) \geqslant 2. \tag{4.10}$$

(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

$$\mathcal{F} \otimes \mathcal{L} = \begin{cases} (\mathcal{F} \otimes \mathcal{L})(\mathrm{Swan}_\infty(\mathcal{L})) & : t < \mathrm{Swan}_\infty(\mathcal{L}) \\ (\mathcal{F} \otimes \mathcal{L})(t) & : t > \mathrm{Swan}_\infty(\mathcal{L}) \\ \sum_{z \leqslant t} (\mathcal{F} \otimes \mathcal{L})(z) & : t = \mathrm{Swan}_\infty(\mathcal{L}). \end{cases} \tag{4.11}$$

(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 (Theorem 2.37) gives that the left-hand side of (4.10) is equal to

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

if $\mathcal{L}$ is nontrivial.

(5) This follows from Proposition 2.23.

(6) By (4.11), we have

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

On the other hand, by (4.8),

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

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 4.37. *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

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

Proof. This follows from Theorems 2.33, 2.34 and 2.37, and can be found in [FKM14a, Proposition 4.4.6]. □

Arguments with unipotent blocks.

Lemma 4.38. *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,*

$$\mathcal{G}(s)^{\mathrm{tame}} = \bigoplus_\chi \left(\mathrm{Unip.}\otimes\mathcal{L}_{\chi(X+s)}\right) \tag{4.12}$$

(see Section 2.1.6), 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 (4.8) with $a \neq 0$.

Proof. Let us assume that there is an isomorphism of the form (4.8) 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 (4.12). This new sheaf still satisfies the same

hypotheses as $\mathcal{G}$, with the same a in (4.8) (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 4.36 (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 4.39. *Let $\psi : \mathbb{F}_q \to \mathbb{C}^\times$ be a nontrivial additive character and let $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F})$ where $\mathcal{F}$ is an ℓ-adic Fourier sheaf 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 ∞:*

$$\begin{aligned} \mathcal{F}^{(s)} &= \bigoplus_{t \in \mathbb{R}_{\geqslant 0}} \mathcal{F}^{(s)}(t) = \mathcal{F}^{(s),\mathrm{tame}} \oplus \mathcal{F}^{(s),\mathrm{wild}} \\ &= \left(\bigoplus_{\chi} \left(\mathrm{Unip}(\chi, s) \otimes \mathcal{L}_{\chi(X+s)} \right) \right) \oplus \left(\bigoplus_{t>0} \mathcal{F}^{(s)}(t) \right) \end{aligned} \tag{4.13}$$

(see Section 2.1.6). We assume that

- *The decomposition (4.13) 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 (4.13) 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 (4.8) 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 (4.13) 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 4.38 to conclude. □

Arguments for sheaves of the form (2.3). In this section, we consider sheaves from Proposition 2.52, giving rise to general exponential sums of the form (2.3).

The following criterion generalizes the argument of [FKM15b] for Birch sums to sums of the general form (2.3) and allows to reduce to the case of $\mathcal{L}$ being an Artin-Schreier sheaf.

Lemma 4.40. *In the setting of Proposition 2.52, we assume that f is a polynomial of order $d \geqslant 1$, $n = \mathrm{Swan}_\infty(\mathcal{F}_1) > d$, and $(n,d) = (d,p) = 1$. If there is a geometric isomorphism of the form (4.8) for $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F}_2)$ with $a \neq 0$, 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 $\mathbb{A}^1 \times \mathbb{F}_q$. By Lemma 4.36 (1), $\mathrm{Sing}(\mathcal{L}) \subset \{\infty\}$. We may assume that $\mathcal{L}$ is not geometrically trivial, the conclusions being clear otherwise. By Lemma 4.36 (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

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

The break $\frac{n}{n-d}$ is not an integer since we assume that $(n, d) = 1$, and the first conclusion follows from Lemma 4.36 (6). For the second one, note that $\frac{n}{n-d} < 2$ if $n > 2d$ and use Lemma 4.37 (4). □

The next lemma consequently considers isomorphisms of the form (4.8) when $\mathcal{L}$ is an Artin-Schreier sheaf.

Lemma 4.41. *In the setting of Proposition 2.52, let us assume that there is an isomorphism of the form (4.8) 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) $\mathrm{Sing}(\mathcal{F}_2) = \{\infty\}$ *or* $\mathbb{A}^1(\mathbb{F}_q) \subset \mathrm{Sing}(\mathcal{F}_2)$.

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

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

for any Fourier sheaf $\mathcal{F}$ (see Theorem 2.41), we get a geometric isomorphism

$$\mathcal{F}_2 \otimes \mathcal{L}_{\psi(aX)} \cong [+(-b)]^*\mathcal{F}_2. \tag{4.14}$$

Then:

– If $b = 0$, taking determinants shows that $a = 0$.

– Since the Artin-Schreier sheaf is ramified at most at ∞, we have $\mathrm{Sing}(\mathcal{F}_2) \cap \mathbb{A}^1(\mathbb{F}_q) = (\mathrm{Sing}(\mathcal{F}_2) \cap \mathbb{A}^1(\mathbb{F}_q)) + b$. If $b \neq 0$, this yields

$$\mathrm{Sing}(\mathcal{F}_2) = \varnothing,\ \{\infty\},\ \text{or } \mathbb{A}^1(\mathbb{F}_q) \subset \mathrm{Sing}(\mathcal{F}_2)$$

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 4.37, $\mathrm{Sing}(\mathcal{F}_2) \neq \varnothing$ because we assume that $\mathcal{F}_2$ is geometrically irreducible and not geometrically trivial.

If $f = X$ and $b \neq 0$, the geometric isomorphism (4.14) 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. □

Chapter 5

Gaussian distribution of short sums of trace functions

In this chapter, we apply our probabilistic model to prove the results introduced in Section 1.3, extending works of Davenport-Erdős [DE52], Mak-Zaharescu [MZ11] and Lamzouri [Lam13].

Reminder on notations. For a function $t : \mathbb{F}_q \to \mathbb{C}$ and a subset $I \subset \mathbb{F}_q$, recall that

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

is the partial sum over I. For a family $(t_q : \mathbb{F}_q \to \mathbb{C})_q$ of functions, we are interested in the distribution of the complex random variable

$$\big(S(t_q, I + x)\big)_{x \in \mathbb{F}_q}$$

(with respect to the uniform measure on $\mathbb{F}_q$) as $q, |I| \to +\infty$, where $I + x = \{y + x : y \in I\}$ is the translate of I. We will write $S_q(x, I) := S(t_q, I + x)$.

Example 5.1. When $q = p$, the finite field $\mathbb{F}_p$ can be identified with the interval $[1 \dots p]$. For an interval $I_H = [1 \dots H] \subset [1 \dots p]$ and $1 \leqslant x \leqslant p$ an integer, we have the partial sum of length H starting at $x + 1$

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

This is the situation considered in the works mentioned above. More generally, when $q = p^e$, we can look at "boxes" in $\mathbb{F}_q \cong \mathbb{F}_p^e$.

5.1. Statement of the results

The general result is the following:

Theorem 5.2. *Let $(t_q : \mathbb{F}_q \to \mathbb{C})_q$ be a family of ℓ-adic trace functions, arising from a coherent family $(\mathcal{F}_q)_q$ of ℓ-adic sheaves over $\mathbb{F}_q$ (see Definition 4.27), with monodromy group $G \leqslant \mathrm{GL}_n(\mathbb{C})$, and denote by* Std *the standard representation of G in $\mathrm{GL}_n(\mathbb{C})$.*

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, with respect to the uniform measure on $\mathbb{F}_q$, the random variable

$$\left(\frac{S_q(I_q, x)}{\sqrt{|I_q|}}\right)_{x \in \mathbb{F}_q} \tag{5.1}$$

converges in law to a normal distribution in $\mathbb{C} \cong \mathbb{R}^2$ with mean 0 and covariance matrix

$$\Gamma = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ if Std is self-dual, and } \Gamma = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ otherwise,} \tag{5.2}$$

when

$$q, |I_q| \to \infty \text{ with } \log |I_q| = o(\log q). \tag{5.3}$$

Remark 5.3. In particular, the limit has independent real and imaginary parts.

Remark 5.4. The trace functions t_q in Theorem 5.2 can be complex- or real-valued (the latter occurring for example for hyper-Kloosterman sums of even rank and Birch sums). Let us write $\Gamma = \begin{pmatrix} \Gamma_{11} & \Gamma_{22} \\ \Gamma_{21} & \Gamma_{22} \end{pmatrix}$. Of course, if t_q is real valued, we expect that $\Gamma_{22} = 0$. Actually, we will see that $\Gamma_{22} = \frac{1}{2}(1 - \mathrm{mult}_1(\mathrm{Std}^{\otimes 2}))$, so t_q is indeed real-valued if and only if $\Gamma_{22} = 0$ by Proposition 3.9.

Remark 5.5. We recall that the I-coherence of $\mathcal{F}$ is a restriction only for Kummer sheaves $\mathcal{L}_{\chi(f)}$ with $f \neq X$, and holds if $I \subset [1 \dots p/\deg(f))^e \subset \mathbb{F}_q \cong \mathbb{F}_p^e$ by Example 4.12.

5.1.1. Quantitative version. As in [Lam13], we also get the following quantitative version, about the joint distribution function:

Theorem 5.6 (Quantitative version)**.** *In the notations and hypotheses of Theorem 5.2, fix $\varepsilon \in (0, 1/2)$ and let $R = \mathrm{rank}(G)$. 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*

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

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

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

where $\mathcal{N}$ is a normal random variable in $\mathbb{C}$ with mean 0 and covariance matrix Γ as in Theorem 5.2, and

$$\beta = \begin{cases} 1/2 - \varepsilon & : \textit{self-dual and Kummer cases} \\ \frac{R-1}{2R-1} & : \textit{otherwise.} \end{cases}$$

Remark 5.7. In the self-dual case, Theorem 5.6 recovers the bound and the range of [Lam13], with an improvement on the power of $|I|$ (from 1/4 to 1/2), thanks to a modification of the method.

Remark 5.8. 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 5.2 is valid. We will explain the reason for this later on.

5.1.2. Moments of traces of random matrices in classical groups. As we will see, an important ingredient in the proof of Theorem 5.6 is the following

result on moments[1] of traces of random matrices in maximal compacts[2] of classical groups with respect to the Haar measure:

Proposition 5.9. *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),*

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k}) = 0 \qquad (k \geqslant 0 \text{ odd}), \tag{5.4}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k}) = (k-1)!! \qquad (0 \leqslant k \leqslant R \text{ even}), \tag{5.5}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k}) \leqslant (k-1)!! \qquad (k \geqslant 1). \tag{5.6}$$

(2) Otherwise,

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k} \otimes D(\mathrm{Std}^{\otimes k})) = k! \qquad (0 \leqslant k \leqslant R), \tag{5.7}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k} \otimes D(\mathrm{Std}^{\otimes r})) = 0 \qquad (0 \leqslant k \neq r \leqslant R), \tag{5.8}$$

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes k} \otimes D(\mathrm{Std}^{\otimes r})) \leqslant \sqrt{k!r!} \qquad (k, r \geqslant 0), \tag{5.9}$$

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

In other words, these moments correspond to that of a Gaussian[3] in $\mathbb{R}^2 \cong \mathbb{C}$ if the order of the moment is small enough with respect to the rank. This has been known and exploited for example by Diaconis-Shahshahani [DS94], Pastur-Vasilchuk [PV04], as well as Larsen [Lar90] in the context of trace functions.

A new aspect is that we will moreover need the bounds (5.6) and (5.9) on the large order moments.

Remark 5.10. Recall that (see Section 5.3.3):

- 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 (see (5.12)).
- 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 nondiagonal terms. This is the reason for the restricted range in the non-self-dual case of Theorem 5.6 noted in Remark 5.8.

5.1.3. Examples. At the end of this chapter, we will finish to prove that the families of $\overline{\mathbb{Q}}_\ell$-sheaves of Section 4.4.3 are coherent, so that Theorems 5.2 and 5.6 apply to them.

Recall that these families include (as trace functions):

[1] For a complex-valued random variable X, we consider here the moments $\mathbb{E}(X^k\overline{X^r})$ (and *not* $\mathbb{E}((\mathrm{Re}\, X)^k(\mathrm{Im}\, X)^r)$); see Remark 5.12 below.

[2] Recall that by Corollary 3.3, the moments can be computed in G or in a maximal compact subgroup K of $G(\mathbb{C})$ (this is Weyl's unitary trick).

[3] Still in the sense of Footnote 1.

(1) Dirichlet characters pre-composed with a rational function f (this is the case of [Lam13] when $f = \mathrm{id}$ and $q = p$).
If $f \neq X$, we must assume that I has no zero-m-sum for $m \leqslant \deg(f)$, e.g. $I \subset [1 \dots p/\deg(f))^e \subset \mathbb{F}_q \cong \mathbb{F}_p^e$.

(2) Hyper-Kloosterman sums and hypergeometric sums.

(3) General exponential sums of the form (2.3), including Birch sums and Fouvry-Michel sums.

(4) Point counting on families of hyperelliptic curves.

Note that 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 Γ of Theorems 5.2 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 $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$.

5.2. Proof of Theorem 5.2

5.2.1. Strategy and comparison with other approaches. The idea of the proof of Theorem 5.2 is the following:

(1) By the method of moments, it suffices to show that the moments of the random variable (5.1) tend to that of the Gaussian $\mathcal{N}$.

(2) We show that the probabilistic model of Chapter 4 is accurate, in the sense that the moments of (5.1) 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 (5.1) 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 5.3.

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 of random matrices.

5.2.2. Moments of the model. Recall from Chapter 4 that we model (5.1) by the random variable

$$S(H) = Z_1 + \cdots + Z_H$$

where $H = |I|$ and Z_i are independent uniformly distributed like $\mathrm{tr}(\pi(X))$, for X uniformly distributed in a maximal compact subgroup K of $G(\mathbb{C})$ (with respect to the Haar measure) and $\pi : K \to K^\sharp$ the projection.

Proposition 5.11 (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

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

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

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

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 5.12. The covariance matrix (5.2) of Theorem 5.2 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 $\binom{Z}{\overline{Z}} = \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)\binom{\mathrm{Re}\,Z}{\mathrm{Im}\,Z}$ and consider as in Proposition 5.11 the moments $\mathbb{E}(Z^k\overline{Z^r})$ instead of $\mathbb{E}((\mathrm{Re}\,Z)^k(\mathrm{Im}\,Z)^r)$. The reason is that conjugation has the algebraic interpretation of dualization of representations, characters, and trace functions. In the self-dual case (i.e. when the trace function takes only real values, see Remark 5.4), there is no difference.

Lemma 5.13. *The covariance matrix of the random vector $Z = (\mathrm{Re}\,Z, \mathrm{Im}\,Z)$ is equal to the one given in (5.2), and $\mathbb{E}(Z) = 0$.*

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

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

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

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

Finally, again by Schur's Lemma,

$$\mathrm{mult}_1(\mathrm{Std}^{\otimes 2}) = \mathrm{mult}_1(\mathrm{Std} \otimes D(D(\mathrm{Std})) = \delta_{\mathrm{Std\ self\text{-}dual}}.$$

□

5.2.3. Accuracy of the model.

Proposition 5.14. *Under the hypotheses of Theorem 5.2, for all integers $k, r \geqslant 0$ and $I \subset \mathbb{F}_q$ of size H, the moment*

$$M_q(k, r; I) := \mathbb{E}\left(S_q(x, I)^k \overline{S_q(x, I)^r}\right)$$

satisfies

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

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

Proof. As in Proposition 5.11, the moment $M_q(k, r; I)$ equals

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

where $I = \{a_1, \dots, a_H\}$. By Proposition 4.33, this is equal to

$$\sum_{\substack{k_1+\cdots+k_H=k \\ k_i \geqslant 0}} \sum_{\substack{r_1+\cdots+r_H=r \\ r_i \geqslant 0}} \binom{k}{k_1 \dots k_H}\binom{r}{r_1 \dots r_H} \times \prod_{1 \leqslant i \leqslant H} \mathrm{mult}_1(\mathrm{Std}_i^{\otimes k_i} \otimes D(\mathrm{Std}_i)^{\otimes r_i}) + O\left(c^{3(k+r)} q^{-1/2} H^{k+r}\right)$$

for all integers $k, r \geqslant 0$, recalling that $\sum_{k_1+\cdots+k_H=k,\ k_i \geqslant 0} \binom{k}{k_1 \dots k_H} = H^k$. The conclusion follows from Proposition 5.11. □

We make the normalizations

$$\tilde{S}_q(x, I) = S_q(x, I)/\sqrt{|I|} \text{ and } \tilde{S}(H) = S(H)/\sqrt{H},$$

and for $k, r \geqslant 0$ we denote by $\tilde{M}_q(k, r; I)$, $\tilde{M}_{\mathrm{prob}}(k, r; H)$ the corresponding moments, so that Proposition 5.14 becomes:

$$\tilde{M}_q(k, r; I) = \tilde{M}_{\mathrm{prob}}(k, r; H) + O\left(c^{3(k+r)} q^{-1/2} H^{\frac{k+r}{2}}\right). \tag{5.10}$$

5.2.4. Central limit theorem.

Proposition 5.15. *Under the hypotheses and notations of Theorem 5.2, 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 5.13. 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 (5.10), this immediately implies:

Corollary 5.16 (Moments are asymptotically Gaussian)**.** *Under the hypotheses and notations of Theorem 5.2, we have for all integers $k, r \geqslant 0$ that*

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

5.2.5. Method of moments and proof of Theorem 5.2. To conclude the proof of Theorem 5.2, it now suffices to apply the method of moments:

Proposition 5.17 (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 5.18 (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 5.18, Theorem 5.2 follows directly from Corollary 5.16.

5.3. Quantitative version: proof of Theorem 5.6

5.3.1. Review of Lamzouri's method. An improvement of [Lam13] on previous results is the ability to give a bound on the error term for the joint distribution function:

Theorem ([Lam13, Theorem 1]). *If χ_p is a non-real Dirichlet character modulo p and $A \subset \mathbb{C}$ a rectangle with edges parallel to the axes, the probability*

$$\frac{1}{p}\left|\left\{ x \in \mathbb{F}_p : \frac{S(\chi_p, x, H)}{\sqrt{H/2}} \in A \right\}\right|$$

is given by

$$P(\mathcal{N} \in A) + O\left(\mu(A)\left(H^{-1/4} + \sqrt{\frac{\log H}{\log p}} + p^{-1/8}\right)\right)$$

when $\log H = o(\log p)$, for $\mathcal{N}$ a normal random variable in $\mathbb{C}$ with mean 0 and unit covariance matrix, and μ the Lebesgue measure.

The idea is to study more precisely the random variable Z modeling the values of the Dirichlet character and remark that its moments are 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 approximate the characteristic function of $(S(\chi_p, x, H))_{x\in\mathbb{F}_p}$ asymptotically by that of the probabilistic model when $p, H \to \infty$ (see the proof of [Lam13, Theorem 3.1]). Lamzouri then proceeds as follows:

(1) 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]).

(2) Combining these, this gives an asymptotic approximation of the characteristic function of $(S(\chi_p, x, H))_{x\in\mathbb{F}_p}$ by that of a Gaussian ([Lam13, Theorem 3.1]).

(3) 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.

5.3.2. Generalization to trace functions. It turns out that this can be generalized to trace functions because traces of random matrices in maximal compact subgroups of $\mathrm{SL}_n(\mathbb{C})$, $\mathrm{Sp}_{2n}(\mathbb{C})$ and $\mathrm{SO}_{n+1}(\mathbb{C})$ have Gaussian moments as the rank tends to infinity, and can be well bounded when the rank is fixed: this is Proposition 5.9.

One actually needs only bounds on the moments, but exploiting the fact that they become exactly Gaussian allows to improve the error terms as the rank tends to infinity.

Hence, we use 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".

We will however proceed a bit differently than Lamzouri, skipping steps (1)–(2) above and:

(1) Directly use step (3) to approximate the joint distribution function of the random variable (5.1) 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.

We first prove Theorem 5.6 conditionally on Proposition 5.9, before taking care of the latter.

5.3.3. 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, its 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 5.12, we will continue to rather work with moments of the form $\mathbb{E}(Z^k \overline{Z^r})$ and characteristics functions of the form

$$(u,v) \mapsto \phi(u,v) = \mathbb{E}\left(e^{i(uZ+v\overline{Z})}\right),$$

which renders the computations easier and more natural in our setting. Note that

$$\begin{aligned} \phi(u,v) &= \tilde{\phi}(u+v, i(u-v)) \text{ and} \\ \tilde{\phi}(u,v) &= \phi\left(\frac{u-iv}{2}, \frac{u+iv}{2}\right) \end{aligned} \tag{5.11}$$

for all $u, v \in \mathbb{C}$. Hence, $\phi(u,v) = e^{-2\sigma^2 uv}$, so that[4]

$$\mathbb{E}\big(Z^k \overline{Z^r}\big) = (2\sigma^2)^k k! \delta_{k=r}. \tag{5.12}$$

5.3.4. Approximation of characteristic functions through moments.

Lemma 5.19. *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 $(u,v) \mapsto \phi_j(u,v) = \mathbb{E}(e^{i(uX_j + v\overline{X_j})})$ for $u, v \in \mathbb{C}$ and $k, r \geqslant 0$ integers. Assume that*

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

[4]This is a nice combinatorial identity to prove directly, if one does not use characteristic functions.

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 $e^{ix} = \sum_{n<N}\frac{i^n x^n}{n!} + O\left(\frac{|x|^N}{N!}\right)$ valid for $x \in \mathbb{R}$. □

5.3.5. Bounding moments. In order to apply Lemma 5.19, we will need bounds on the moments $M_{\mathrm{prob}}(N,N;H)$, provided by Proposition 5.9. Recall that by Proposition 5.11, 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 5.20 (Non-self-dual case)**.** *If the conclusions of Proposition 5.9 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[5] of N is equal to $\binom{N+H-1}{H-1}$. Finally, we use that $\frac{(N+H-1)!}{(H-1)!} \leqslant (N+H-1)^N$. □

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

Remark 5.21. In Remarks 5.8 and 5.10, we explained that the reason for the restriction on the range in Theorem 5.6 for the non-self-dual case came from the fact that X_i may have infinitely many nonzero nondiagonal moments. If (5.8) in Theorem 5.6 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 5.22 (Non-self-dual case, Kummer sheaves)**.** *In the case of Kummer sheaves, we have*

$$M_{\text{prob}}(N, N; H) \leqslant N! H^N.$$

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

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

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

□

Remark 5.23. 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 5.24 (Self-dual case)**.** *If the conclusions of Proposition 5.9 hold, then in the self-dual case,*

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

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

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

□

5.3.6. 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 5.25. *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 $G(u)=\frac{2u}{\pi}+2(1-u)\cot(\pi u)$ 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 5.26. *If X,Y are complex random variables such that there exists a positive continuous function $g:\mathbb{R}^2\to\mathbb{R}$ 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

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

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

Lemma 5.27. *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

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

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

Proof. By independence of the X_i, we have $\phi_H(u,v) = \phi\left(\frac{u}{\sqrt{H}}, \frac{v}{\sqrt{H}}\right)^H$ 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. □

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

Proposition 5.28. *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 $S(H) = \frac{X_1+\cdots+X_H}{\sqrt{H}}$. 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 $\mathcal{N}$,

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

□

5.3.9. Proof of Theorem 5.6. Combining the above results, we can finally prove Theorem 5.6, conditionally on Proposition 5.9. Let us consider the characteristic functions

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

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

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

of the random model

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

where $H = |I|$. Recall that by (5.10), 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

$$N = 2M \leqslant \varepsilon \frac{\log q}{\log(c^6 H)} \tag{5.13}$$

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 5.19, 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 5.26 after making a change of variable with (5.11) 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

$$\begin{aligned} P(\tilde{S}_q(x, I) \in A) &= P(S(H) \in A) \\ &\quad + O\left(\frac{1}{t} \int_0^t (|\phi_H(\pi u, \pi u)| + |\phi_H(i\pi u, -i\pi u)|) du\right) \\ &\quad + O\left(\int_0^t \int_0^t g(u, v) du dv\right) \\ &\quad + O\left(\frac{1}{t} \int_0^t (g(u, 0) + g(0, u)) du\right) \end{aligned} \tag{5.14}$$

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 (5.14) 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 5.27 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

$$2\pi t \leqslant H^{\frac{R-1}{2R}}, \text{ i.e. } M \leqslant H^{\frac{R-1}{2R\alpha}}. \tag{5.15}$$

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

$$\frac{\tilde{M}_{\text{prob}}(M,M;H)}{(2M)!}\frac{(2\pi t)^{2M+2}}{M} + q^{-1/2+\varepsilon}\left((2\pi t)^2 + \frac{(2\pi t)^{2M+1}}{M}\right). \tag{5.16}$$

By Propositions 5.20 (non-self-dual case), 5.22 (Kummer case) and 5.24 (self-dual case),

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

By Stirling's approximation, the first summand of (5.16) 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:
$$M^{2\alpha-\frac{3}{2}}\left(\frac{e^4}{4}\left(M^{2\alpha-1}+HM^{2\alpha-2}-M^{2\alpha-2}\right)\right)^M \ll M^{2\alpha-\frac{3}{2}} \tag{5.17}$$
if $\alpha < 1/2$ and under the additional condition $M \gg H^{\frac{1}{2-2\alpha}}$. With (5.13), this imposes the more restrictive range
$$H = o\left((\log q)^{\frac{2-2\alpha}{1+\varepsilon(2-2\alpha)}}\right) \tag{5.18}$$
and the condition
$$\frac{1}{2-2\alpha} \leqslant \frac{R-1}{2R\alpha}, \text{ i.e. } \alpha \leqslant \frac{R-1}{2R-1} \tag{5.19}$$
because of (5.15).

By (5.15), the second summand of (5.16) is
$$O\left(q^{-\frac{1}{2}+2\varepsilon}\right)$$
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 (5.14) is bounded by the first one.

Hence, the error term in (5.14) 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 $\alpha=\frac{M\left(1-\frac{\log(e/2)}{\log M}\right)+1}{2M+3}$, which leads to an error term of

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

– In the non-self-dual case,

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

(since $2\alpha-3/2\leqslant-\alpha$ when $\alpha\leqslant 1/2$). By (5.19), we optimize by taking $\alpha=\frac{R-1}{2R-1}$ and we obtain the error term

$$O\left(M^{-\frac{R-1}{2R-1}}+q^{-\frac{1}{2}+2\varepsilon}\right)$$

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 5.28 to $S(H)$, and combining with (5.14) gives Theorem 5.6.

5.4. Traces of random matrices in classical groups

In this section, we prove Proposition 5.9, which will conclude the proof of Theorem 5.6. 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.

5.4.1. Special linear case.

Proposition 5.29. *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 — resp. $\lambda+(a^N)=\lambda+(a,\dots,a)$.

(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 $\lambda = (\lambda_1, \ldots, \lambda_l)$, recall the *power symmetric polynomials*

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

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,

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

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

$$\int_{\mathrm{SU}_N(\mathbb{C})} \mathrm{tr}(g)^k \overline{\mathrm{tr}(g)^r} dg = \sum_{\substack{\mu_1 \vdash k \\ l(\mu_1) \leqslant N}} \sum_{\substack{\mu_2 \vdash r \\ l(\mu_2) \leqslant N}} \dim S_{\mu_1} \dim S_{\mu_2} \delta_{S_{\mu_1}(\mathrm{Std}) \cong S_{\mu_2}(\mathrm{Std})}. \tag{5.20}$$

The Cauchy-Schwarz inequality yields

$$M(k,r)^2 \leqslant \sum_{\substack{\mu_1 \vdash k \\ l(\mu_1) \leqslant N}} (\dim S_{\mu_1})^2 \sum_{\substack{\mu_2 \vdash r \\ l(\mu_2) \leqslant N}} (\dim S_{\mu_2})^2 \leqslant k!r! \tag{5.21}$$

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 (5.20) 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 5.30. (see also Remarks 5.8 and 5.10). The second bound we have given in (5.21) 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 5.6). 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

$$C(N) = N^{N^2/2} \left(\prod_{n=1}^{N-1} n! \right) \left(\frac{1}{\sqrt{2\pi}} \right)^{N-1} \left(\frac{1}{2} \right)^{\frac{N^2-1}{2}}.$$

For all $\varepsilon > 0$, we get by (5.21) the bound

$$M(k,r) \leqslant (1+\varepsilon) C(N) \frac{N^{k+r}}{(kr)^{N^2-1}}$$

and the bound of Proposition 5.20 becomes

$$M_{\mathrm{prob}}(M, M; H) \leqslant H^{2M} (1+\varepsilon)^H C(N)^H N^{2M},$$

which still has an additional factor of H^M. Hence, the bound (5.17) becomes

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

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

5.4.2. Symplectic case.

Proposition 5.31. *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 $(\varnothing = \mu_0, \ldots, \mu_k = \mu)$ 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 $(\varnothing = \mu_0, \ldots, \mu_k = \mu)$ 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 5.32. 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.

5.4.3. Special orthogonal case.

Proposition 5.33. *Let $N \geqslant 2$ and $X = \mathrm{tr}\,\theta$, 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 $(\varnothing = \mu_0, \ldots, \mu_k = \mu)$ 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 5.31. 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 5.34. As for the symplectic case (see Remark 5.32), 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 used 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.

5.5. Examples: coherent families

In this final section, we finish the proof that the families of sheaves of Section 4.4.3 are coherent (eventually up to twisting by Weil numbers of weight 0), and hence satisfy Theorems 5.2 and 5.6 (eventually up to multiplying the covariance matrix by an orthonormal matrix).

For each of them, except Kummer sheaves, it remains to show:

(1) The independence of shifts (see Section 4.5).

(2) The equality of arithmetic and geometric monodromy groups, eventually up to twisting (see Section 3.5.7).

5.5.1. Kummer sheaves.

Proposition 5.35. *A family $(\mathcal{F})_q$ of Kummer sheaves $\mathcal{L}_{\chi(f)}$, where $\deg(f)$ bounded independently from q and f has no zero or pole of order divisible by $\mathrm{ord}(\chi)$, is coherent.*

Proof. This is Propositions 2.45 and 3.56. □

5.5.2. Kloosterman sheaves.

Proposition 5.36. *Let $n \geqslant 2$ be an integer. The family $(Kl_{n,q})_q$ of ℓ-adic Kloosterman sheaves over $\mathbb{F}_q$ (see Proposition 2.46) is coherent.*

Proof. The geometric irreducibility, conductor bound, and condition on the monodromy groups follow from Proposition 2.46 and Theorem 3.23. The independence of shifts follows from Lemma 4.39, which can be applied thanks to Proposition 3.19 (1). □

5.5.3. Hypergeometric sheaves.

Proposition 5.37. *Let $n \geqslant m \geqslant 0$ be integers with $m + n \geqslant 1$ and let $\boldsymbol{\chi}_q = (\chi_{i,q})_{1\leqslant i\leqslant n}$, $\boldsymbol{\rho}_q = (\rho_{j,q})_{1\leqslant j\leqslant m}$ be tuples of pairwise distinct characters of $\mathbb{F}_q^\times$. We assume that $\Lambda = \prod_i \chi_{i,q} = 1$ and either:*

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

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

Then the family $(\mathcal{H}(\boldsymbol{\chi}_q, \boldsymbol{\rho}_q))_q$ of hypergeometric sheaves (see Proposition 2.50) is coherent.

Proof. The geometric irreducibility and conductor bound follow from Proposition 2.50.

By Proposition 3.57, we have $G^0_{\mathrm{geom}} = G^{0,\mathrm{der}}_{\mathrm{geom}} = \mathrm{SL}_n(\mathbb{C})$ under the assumptions. To make the arithmetic and geometric monodromy group coincide, we use the strategy of Section 3.5.7. 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 4.39. □

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.

5.5.4. Supermorse functions and sums of the form (2.5).

Proposition 5.38. *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, let $(\mathcal{G}_{f,q})_q$ be the family of ℓ-adic sheaves of Proposition 2.53, with trace functions

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

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. Moreover, we can take $\alpha_q = 1$ in the (H') case.

Proof. The geometric irreducibility and conductor bound follow from Proposition 2.53. The computation of G^0_{geom} was recalled in Proposition 3.58. By Section 3.5.7, 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 $\mathcal{G}_f$ from [Kat90, 7.10.4]: there is a geometric isomorphism

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

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 Proposition 2.16.

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

$$[+a]^* \mathcal{G}_f \cong \mathcal{G}_f \otimes \mathcal{L} \tag{5.22}$$

for $\mathcal{L}$ a rank 1 sheaf and $a \in \mathbb{F}_q$, the argument with $D(\mathcal{G}_f)$ being similar. We adapt the multiplicative case treated in the proof of [Mic98, Théorème 2.3]. By Lemma 4.36 (1) and Proposition 2.53, 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], $\mathcal{G}_f$ as I_∞-representation is

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

where χ_z is a multiplicative character, and we view $Z_{f'}$ in $\overline{\mathbb{F}}_q$. Hence, by Proposition 2.23 (2) all the breaks are at 1 and as representations of the wild inertia group P_∞, we have

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

We distinguish two cases:

– If $\infty \notin \mathrm{Sing}(\mathcal{L})$, then Lemma 4.37 (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 Proposition 2.23, $\mathrm{Swan}_\infty(\mathcal{L}) \in \{0, 1\}$ because all the breaks of $\mathcal{G}_f$ 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 (5.22) 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 $b = 0$).

□

Example 5.39. In particular, the families of Example 3.60 are coherent, under the condition $r \geqslant 2$ even for (1).

Remark 5.40. Lemma 4.40 does not apply here because $\mathcal{F}_1$ is trivial.

Remark 5.41. Note that there is a misprint in [FM02, Section II.1]: $\alpha_{f,q}$ therein actually depends on a, unless further assumptions are made. This is not important in [FM02], but in our situation we need to select examples so that α precisely does *not* depend on a.

5.5.5. Sums of the form (2.3) with $f = X$, $\chi = 1$, h polynomial..

Proposition 5.42. *Let $h = \sum_{i=1}^n a_i X^i \in \mathbb{Z}[X]$ be a polynomial of degree $n \geqslant 3$, $n \notin \{6, 8\}$, with $a_{n-1} = 0$. For q large enough, let $(\mathcal{G}_{h,q})_q$ be the family of ℓ-adic sheaves of Proposition 2.54, corresponding to the trace functions*
$$x \mapsto \frac{-1}{\sqrt{q}} \sum_{y\in\mathbb{F}_q} e\left(\frac{\mathrm{tr}(xy + h(y))}{p}\right) \quad (x \in \mathbb{F}_q).$$

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. Moreover, $\alpha_q = 1$ if n is odd and h has no monomial of even positive degree.

Proof. The geometric irreducibility and conductor bound are given in Proposition 2.54.

The geometric monodromy group was given in Proposition 3.61. In the symplectic case, Section 3.5.7 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 3.5.7.

The independence of shifts follows directly from Lemmas 4.40 and 4.41, similarly to Kloosterman sheaves. □

5.5.6. Sums of the form (2.3) with f polynomial, $\chi \neq 1$.

Proposition 5.43. *Let $f, g, h \in \mathbb{Q}(X)$ and $(\chi_q)_q$ be as in Proposition 3.63, and consider for q large enough the associated family $(\mathcal{G}_q)_q$ of ℓ-adic sheaves with trace functions*

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

Assume that $n > 2d$, either g is nonconstant or $h \notin \mathbb{Z}[X]$, and either $N \neq 7, 8$ 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. Moreover, $\alpha_q = 1$ if L is odd.

Proof. Proposition 2.55 gives the geometric irreducibility and the conductor bound.

The geometric monodromy groups are given by Proposition 3.63 under the above assumptions, and the statement follows by Section 3.5.7.

We finally show the independence of shifts. Let us assume that there is a geometric isomorphism of the form (4.8) for $\mathcal{G}$ with $a \neq 0$. By Lemmas 4.40 and 4.41, 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 $\mathrm{Sing}(\mathcal{F}_2) = \{\infty\}$. By Proposition 2.52 and the fact that 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. □

5.5.7. Families of hyperelliptic curves.

Proposition 5.44. *Let $f \in \mathbb{Z}[X]$ be a squarefree polynomial of degree $2g \geqslant 2$. For q large enough, the family $(\mathcal{F}_{f,q})_q$ of ℓ-adic sheaves over $\mathbb{F}_q$ from Proposition 2.57 is coherent.*

Proof. The geometric irreducibility and bound on the conductor can be found in Proposition 2.57, and the computation of the monodromy group in Proposition 3.64. It remains to show the independence of shifts. Let us assume that there exists an isomorphism of the form (4.8) for $\mathcal{F}_q$. By Lemma 4.36 (2), if q is large enough, there exists $x \in \mathrm{Sing}(\mathcal{F}) \cap \mathbb{A}^1(\mathbb{F}_q)$ such that $\mathcal{F}_q^{I_x} = 0$, which is a contradiction with Proposition 2.57. □

Remark 5.45. More generally, this argument for the independence of shifts applies to all sheaves with pseudoreflection monodromy.

Chapter 6

Trace functions with image in the cyclotomic integers

As we explained in the introduction (see Section 1.4), the goal of this chapter is to study the reduction of trace functions modulo prime ideals in the cyclotomic rings of integers in which they lie, or more generally distribution questions for sheaves of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$.

Under some technical assumptions (i.e. the corresponding reduced family is coherent), we will get:

– An equidistribution result for values and/or shifted sums of such trace functions (Section 6.4).

– Generalizations of [LZ12] to the distribution of families of sums of reduced trace functions (Section 6.5). In particular, this gives an analogue of the results Chapter 5 and a generalization of [LZ12] to all multiplicative characters and to Kloosterman sums.

– Zero-density estimates for arguments where the trace functions take values in some algebraic subsets of the cyclotomic integers (Section 6.6). For example, for $m \geqslant 2$, we show that if p is large enough, then $\mathrm{Kl}_{n,p}(x) \notin \mathbb{Q}(\zeta_{4p})^m$ for all $x \in \mathbb{F}_p^\times$.

This applies in particular to multiplicative characters of any order, Kloosterman sums and trace functions counting points on families hyperelliptic curves (see Section 2.4).

This chapter is structured as follows:

– In Section 6.1, we recall the technical setup to handle reductions of trace functions in the ℓ-adic formalism, the examples we will consider, and finish to prove that the latter are coherent.

– In Section 6.2, we prove that the probabilistic model we developed in Chapter 4 is accurate for coherent families.

– In Section 6.3, we make preliminary computations and observations in the model, in particular regarding "Gaussian sums" in monodromy groups.

– In Sections 6.4, 6.5 and 6.6, we transfer the results from the model to the actual probability space to get the results mentioned above.

6.1. Setup and examples

We start by reviewing the general setup and the examples we will examine.

6.1.1. Reduction of sheaves of $\mathbb{Z}[\zeta_d]_\lambda$-modules. Let $\mathbb{F}_q$ be a finite field of odd characteristic p. For an integer $d \geqslant 2$, let $E = \mathbb{Q}(\zeta_d)$ be the dth cyclotomic field with ring of integers $\mathcal{O}$. We fix an auxiliary prime $\ell \neq p$ and a prime ideal $\mathfrak{q} \trianglelefteq \mathcal{O}$ above ℓ, corresponding to a valuation λ of E extending the ℓ-adic valuation on $\mathbb{Z}$. Let E_λ and $\mathcal{O}_\lambda$ be the completions, and let

$$\pi : \mathcal{O}_\lambda \to \mathcal{O}_\lambda/\mathfrak{q}\mathcal{O}_\lambda \cong \mathbb{F}_\lambda$$

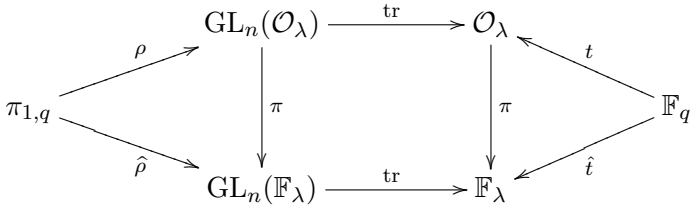
be the reduction map.

We consider a sheaf $\mathcal{F}$ of $\mathcal{O}_\lambda$-modules over $\mathbb{F}_q$, corresponding to an ℓ-adic representation

$$\rho = \rho_{q,\lambda} : \pi_{1,q} \to \mathrm{GL}_n(\mathcal{O}_\lambda),$$

and with trace function $t : \mathbb{F}_q \to \mathcal{O}_\lambda$.

We are interested in the reduction modulo $\mathfrak{q}$ of the latter, namely $\hat{t} = \pi \circ t : \mathbb{F}_q \to \mathbb{F}_\lambda$.



By reduction of $\mathcal{F}$ modulo $\mathfrak{q}$, we get a sheaf of $\mathbb{F}_\lambda$-modules corresponding to the representation

$$\widehat{\rho} : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\lambda),$$

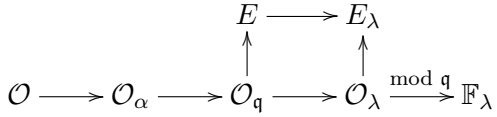
and with trace function equal to $\widehat{t}$.

Remark 6.1. By the theory of ramification in cyclotomic fields, we have $|\mathbb{F}_\lambda| = \ell^m$ with m the multiplicative order of ℓ modulo d (see [Was97, Theorem 2.13]). In particular,

$$|\mathbb{F}_\lambda| \equiv 1 \pmod{d}, \quad d < |\mathbb{F}_\lambda|,$$

and $\mathbb{F}_\lambda = \mathbb{F}_\ell$ (i.e. ℓ splits completely) if and only if $\ell \equiv 1 \pmod{d}$.

Remark 6.2. In practice, $t : \mathbb{F}_q \to \mathcal{O}_\lambda$ will actually have image in $\mathcal{O}$ (or $\mathcal{O}_\alpha$ for some $\alpha \in \mathcal{O}\backslash\mathfrak{q}$ when we normalize), but this cannot be assumed in general and will play no role in the arguments except for the large sieve in the last section. Nonetheless, if $t(\mathbb{F}_q) \subset \mathcal{O}_\alpha$, we can study the reduction of t modulo any prime ideal $\mathfrak{q} \trianglelefteq \mathcal{O}$ such that $\alpha \notin \mathfrak{q}$. This is the reason why we allow λ to vary in the definition of a coherent family in the finite case (see Section 4.4).



6.1.2. Examples. Our arguments will apply to families of sheaves of $\mathbb{Z}[\zeta_d]_\lambda$-modules whose reductions form a coherent family:

Proposition 6.3 (Multiplicative characters)**.** *A family $(\mathcal{L}_{\chi(f)})$ of Kummer sheaves of $\mathbb{F}_\lambda$-modules, with $\deg(f)$ bounded uniformly, is coherent.*

Proof. This is Propositions 2.45 and 3.56. □

Proposition 6.4 (Kloosterman sums)**.** *Let $n \geqslant 2$ be fixed and let $(\mathcal{K}l_n)$ be a family of Kloosterman sheaves of $\mathbb{F}_\lambda$-modules of rank n over $\mathbb{F}_q$, where λ lies above a prime $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$ and $(n, [\mathbb{F}_\lambda : \mathbb{F}_\ell]) = 1$ (as in Theorem 3.27). Then the family is coherent. The same result holds true without restriction on $\ell \pmod 4$ if $p \equiv 1 \pmod 3$ or if n is odd, with $\mathcal{O} = \mathbb{Z}[\zeta_p]$.*

Proof. This is Proposition 2.46 (construction) and Theorem 3.27 (monodromy groups), the independence of shifts being proven as in Proposition 5.36. □

Proposition 6.5 (Point counting on families of hyperelliptic curves)**.** *Let $f \in \mathbb{Z}[X]$ be a squarefree polynomial of degree $2g \geqslant 2$. A family $(\mathcal{F})$ of sheaves of $\mathbb{Z}_\ell$-modules with respect to the reductions of f as in Proposition 2.57 is coherent.*

Proof. This is Propositions 2.57 and 3.64, the argument for the independence of shifts being as in Proposition 5.44. □

Note that this setup also applies to hypergeometric sums (Proposition 2.50) and general exponential sums (Section 2.4.3), as sheaves of $\mathbb{F}_\lambda$-modules, but we did not compute their finite monodromy groups (see Remark 3.55). If we showed that they are still classical groups (or more particularly special linear and symplectic groups), the results would hold as well.

6.2. Accuracy of the model

Let $\mathcal{F}$ be a sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$, with monodromy groups $G_\lambda = G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F})$, corresponding to a representation $\rho : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\lambda)$, and with trace function $t : \mathbb{F}_q \to \mathbb{F}_\lambda$. Recall from Chapter 4 that for any $I \subset \mathbb{F}_q$ of cardinality $L \geqslant 1$, we model the random vector

$$\Big(\rho(\mathrm{Frob}_{x+a})_{a\in I}\Big)_{x\in\mathbb{F}_q}$$

(see also Convention 4.1) by the random vector $(Y_1, \dots, Y_L)$, where the Y_i are independent uniformly distributed in the set $G_\lambda^\sharp$ of conjugacy classes of G_λ. The random vector

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

is then modeled by $(Z_1, \dots, Z_L)$, where $Z_i = \operatorname{tr} Y_i$.

We now prove that this model is accurate in the sense of convergence in law (with respect to some ranges of the parameters).

6.2.1. Statements.

Definition 6.6. For G a finite group and $m \geqslant 1$ an integer, we let $d_m(G) = \sum_{\chi\in\widehat{G}} (\dim\chi)^m$, where $\widehat{G}$ is the set of characters of irreducible complex representations.

Theorem 6.7. *We assume that $\mathcal{F}$ as above is part of a coherent family. Let $I \subset \mathbb{F}_q$ of cardinality L and $h : (G_\lambda^\sharp)^L \to \mathbb{R}$ any function. If $\mathcal{F}$ is I-compatible,*

then

$$\mathbb{E}\Big(h\big(\rho(\mathrm{Frob}_{x+a})\big)_{a\in I}\Big) = \mathbb{E}\left(h(Y_1,\dots,Y_L)\right) + O\Big(L||h||_\infty q^{-1/2}E(G_\lambda,L)\Big),$$

where

$$E(G_\lambda,L) = \begin{cases} |\mathbb{F}_\lambda|^{L\beta_+(G_\lambda)+2\beta_-(G_\lambda)} & : \text{ classical case} \\ d^L & : \text{ cyclic simple case} \\ d^{L+1} & : \text{ Kummer case,} \end{cases}$$

with $\beta_\pm(G_\lambda) = (\dim G_\lambda \pm \operatorname{rank} G_\lambda)/2$ *given in Table 6.1. Moreover, if* h *takes values in* $\mathbb{R}_{\geqslant 0}$*, then*

$$\mathbb{E}\Big(h\big(\rho(\mathrm{Frob}_{x+a})\big)_{a\in I}\Big) = \mathbb{E}\left(h(Y_1,\dots,Y_L)\right)\Big(1+O(Lq^{-1/2}E(G_\lambda,L))\Big),$$

Remark 6.8. Again, we recall that the I-compatibility of $\mathcal{F}$ is a restriction only for Kummer sheaves $\mathcal{L}_{\chi(f)}$ with $f \neq X$, and holds if $I \subset [1\dots p/\deg(f))^e \subset \mathbb{F}_q \cong \mathbb{F}_p^e$ by Example 4.12.

Remark 6.9. When $I = \{0\}$, this is Chebotarev's theorem as it appears for example in [Kow06b].

G	$\dim G$	$\operatorname{rank} G$	$\alpha(G)$	$\beta_+(G)$	$\beta_-(G)$
SL_n	n^2-1	$n-1$	$\frac{n^2-1}{2}$	$\frac{n^2+n-2}{2}$	$\frac{n(n-1)}{2}$
Sp_n (n even)	$\frac{n(n+1)}{2}$	$\frac{n}{2}$	$\frac{n(n+2)}{8}$	$\frac{n(n+2)}{4}$	$\frac{n^2}{4}$
SO_n (n odd)	$\frac{n(n-1)}{2}$	$\frac{n-1}{2}$	$\frac{n^2-1}{8}$	$\frac{(n+1)(n-1)}{4}$	$\frac{(n-1)^2}{4}$
$\mathrm{SO}_n^\pm$ (n even)	$\frac{n(n+1)}{2}$	$\frac{n}{2}$	$\frac{n(n\mp 2)}{8}$	$\frac{n^2}{4}$	$\frac{n(n-2)}{4}$

Table 6.1: Constants for the groups considered.

Corollary 6.10. *Under the hypotheses of Theorem 6.7, for any function* $h : \mathbb{F}_\lambda^L \to \mathbb{R}$*, we have*

$$\mathbb{E}\Big(h\big(t(x+a)\big)_{a\in I}\Big) = \mathbb{E}\left(h(Z_1,\dots,Z_L)\right) + O\Big(L||h||_\infty q^{-1/2}E(G_\lambda,L))\Big).$$

and if h *takes values in* $\mathbb{R}_{\geqslant 0}$*,*

$$\mathbb{E}\Big(h\big(t(x+a)\big)_{a\in I}\Big) = \mathbb{E}\left(h(Z_1,\dots,Z_L)\right)\Big(1+O(Lq^{-1/2}E(G_\lambda,L))\Big).$$

Proof. Apply the previous result with $h \circ \mathrm{tr}$. □

Remark 6.11. Note that we must in particular take $L < q^{1/2}$ to have $E(G_\lambda,L)L = o(q^{1/2})$ as $q \to +\infty$.

6.2.2. Proof of Theorem 6.7. For $I = \{a_1,\dots,a_L\} \subset \mathbb{F}_q$, we write

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q} h(\rho(\mathrm{Frob}_{x+a_1}),\dots,\rho(\mathrm{Frob}_{x+a_L})) = \sum_{\boldsymbol{v}\in(G_\lambda^\sharp)^L} h(\boldsymbol{v})\frac{|D(\boldsymbol{v})|}{q}$$

where

$$D(\boldsymbol{v}) = \{x\in\mathbb{F}_q : \rho(\mathrm{Frob}_{x+a_i}) = v_i \ (1\leqslant i\leqslant L)\}.$$

Lemma 6.12. *Under the notations above, we have*

$$\frac{|D(\boldsymbol{v})|}{q} = \frac{\prod_{i=1}^{L}|v_i|}{|G_\lambda|^L}\left[1 + \sum_{\substack{\chi_1,\dots,\chi_L\in\widehat{G}_\lambda \\ \text{not all trivial}}}\left(\prod_{i=1}^{L}\overline{\chi}_i(v_i)\right)\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^{L}\chi_i(\rho(\mathrm{Frob}_{x+a_i}))\right],$$

where $|v|$ denotes the size of a conjugacy class $v \in G_\lambda^\sharp$.

Proof. By the second orthogonality relations in the finite group G_λ,

$$\begin{aligned}\frac{|D(\boldsymbol{v})|}{q} &= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^{L}\delta_{\rho(\mathrm{Frob}_{x+a_i})=v_i} \\ &= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^{L}\left(\frac{|v_i|}{|G_\lambda|}\sum_{\chi\in\widehat{G}_\lambda}\chi(\rho(\mathrm{Frob}_{x+a_i}))\right)\overline{\chi}(v_i) \\ &= \frac{\prod_{i=1}^{L}|v_i|}{|G_\lambda|^L}\sum_{\chi_1,\dots,\chi_L\in\widehat{G}_\lambda}\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^{L}\chi_i(\rho(\mathrm{Frob}_{x+a_i}))\overline{\chi}_i(v_i).\end{aligned}$$

□

Since

$$\mathbb{E}(h(Y_1,\dots,Y_L)) = \frac{1}{|G_\lambda|^L}\sum_{\substack{\boldsymbol{v}\in(G_\lambda^\sharp)^L \\ \boldsymbol{v}=(v_1,\dots,v_L)}}\left(\prod_{i=1}^{L}|v_i|\right)h(\boldsymbol{v}),$$

it suffices to show that the error term in Lemma 6.12 is small. Under the hypothesis of coherence (and compatibility for Kummer sheaves), Proposition 4.34 gives that

$$\sum_{\substack{\chi_1,\dots,\chi_L\in\widehat{G}_\lambda \\ \text{not all trivial}}}\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^{L}\chi_i(\rho(\mathrm{Frob}_{x+a_i}\, v_i^{-1}) \ll Lq^{-1/2}d_1(G_\lambda)^{L-1}d_3(G_\lambda)^{1+\delta},$$

with $\delta = 1$ in the Kummer case, $\delta = 0$ otherwise. Theorem 6.7 then follows from Lemma 6.13 below.

6.2.3. Upper bounds for group constants.

Lemma 6.13. *For any finite group G, $d_1(G) \leqslant |G|^{1/2}|G^\sharp|^{1/2}$, $d_2(G) = |G|$ and for every $m \geqslant 3$, $d_m(G) \leqslant |G|^{m/2}|G^\sharp|$. Moreover:*

(1) If G is abelian, $d_m(G) = |G|$ for every $m \geqslant 1$.

(2) If $G \leqslant \mathrm{GL}_n(k)$ is a finite classical group of Lie type over the finite field k, we have $d_1(G) \ll_n |k|^{\frac{\dim G+\mathrm{rank}\, G}{2}}$, $d_2(G) = \Theta_n(|k|^{\dim G})$, $|G^\sharp| = \Theta_n(|k|^{\mathrm{rank}\, G})$, and $d_m(G) \ll_n |k|^{\frac{m\dim(G)+2\,\mathrm{rank}(G)}{2}}$ for every $m \geqslant 3$.

(3) If $G = \mathrm{SL}_n(k)$ or $\mathrm{Sp}_n(k)$ (n even), the upper bounds can be improved to $d_m(G) \ll_n |k|^{\frac{m\dim(G)+(2-m)\,\mathrm{rank}(G)}{2}}$ for every $m \geqslant 1$.

Proof. The relations for finite and finite abelian groups are well-known (see e.g. [Kow08, Proposition 5.2]), the ones for classical groups follow from the former, and [MT11, Corollary 24.6, Corollary 26.10], while the ones for SL_n and Sp_n are [Kow08, Proposition 5.4] (using Deligne-Lusztig theory). □

Remark 6.14. According to Remark 4.29, we do not keep track of implicit constants depending on the rank of the monodromy group in the classical case.

6.2.4. Comments on the ranges. Let us consider the above in the context of Section 6.1 and Remark 6.2, i.e. when the sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$ from Theorem 6.7 arises from the reduction of a sheaf of $\mathbb{Z}[\zeta_d]_\lambda$-modules, allowing to study the reduction of a trace function $t : \mathbb{F}_q \to \mathbb{Z}[\zeta_d]$ modulo various ideals.

By Remark 6.1, recall that if $\mathbb{F}_\lambda$ is the residue field of $\mathbb{Z}[\zeta_d]_\lambda$ at some prime ideal above ℓ, then

$$d < |\mathbb{F}_\lambda| = \ell^{\mathrm{ord}(\ell \in (\mathbb{Z}/d)^\times)}.$$

Choice of the parameters. Thus, we may want to choose our parameters (q, ℓ, λ, d) so that

$$d < |\mathbb{F}_\lambda| < |\mathbb{F}_q| = p^e.$$

Given p, ℓ and d, this is holds true for any λ above ℓ if $e \geqslant \frac{\varphi(d)\log \ell}{\log p}$.

Limitation. Together with the condition

$$L \ll \begin{cases} \frac{\log q}{\log |\mathbb{F}_\lambda|} & : G_\lambda \text{ classical} \\ \frac{\log q}{\log d} & : G_\lambda = \mu_d(\mathbb{F}_\lambda) \end{cases}$$

from Theorem 6.7, the relation $d < |\mathbb{F}_\lambda|$ implies that $L \ll e$ if G_λ is classical and $d = p$ (e.g. for Kloosterman sums). Hence, we must in this case take e large enough with respect to L, which is a limitation of the method to keep in mind. Note however that it is not unusual to encounter results stated in fixed characteristic with the degree e going to infinity (see e.g. [KS99, Chapter 9] and [Kat88, Chapter 3]).

6.3. Computations in the model

In this section, we carry out preliminary computations and observations in the probabilistic model.

Throughout, we let $G_\lambda \leqslant \mathrm{GL}_n(\mathbb{F}_\lambda)$, $X_1, \dots, X_L$ independent random variables uniformly distributed in G, $Y_i = \pi(X_i)$ for $\pi : G_\lambda \to G_\lambda^\sharp$ the projection, and $Z_i = \operatorname{tr} Y_i$.

6.3.1. Random walks in monodromy groups.

Proposition 6.15. *For all $A \subset \mathbb{F}_\lambda$ and $L \geqslant 1$, the probability $P(Z_1 + \cdots + Z_L \in A)$ is given by*

$$\frac{|A|}{|\mathbb{F}_\lambda|} + O\left(\max_{0 \neq \psi \in \widehat{\mathbb{F}}_\lambda} \left| \sum_{a \in A} \psi(-a) \right| \left| \frac{1}{|G_\lambda|} \sum_{x \in G_\lambda} \psi(\operatorname{tr} x) \right|^L \right).$$

In particular, for $a \in \mathbb{F}_\lambda$,

$$P(Z_1 + \cdots + Z_L = a) = \frac{1}{|\mathbb{F}_\lambda|} + O\left(\max_{0 \neq \psi \in \widehat{\mathbb{F}}_\lambda} \left|\frac{1}{|G_\lambda|} \sum_{x \in G_\lambda} \psi(\operatorname{tr} x)\right|^L\right).$$

Proof. By the second orthogonality relations in $\mathbb{F}_\lambda$,

$$\begin{aligned} P(Z_1 + \cdots + Z_L = a) &= \frac{|\boldsymbol{v} = (v_1, \dots, v_L) \in G_\lambda^L : \operatorname{tr} \sum v_i = a|}{|G_\lambda|^L} \\ &= \frac{1}{|G_\lambda|^L} \sum_{\boldsymbol{v} \in G_\lambda^L} \delta_{\operatorname{tr} \sum v_i = a} \\ &= \frac{1}{|\mathbb{F}_\lambda|} \sum_{\psi \in \widehat{\mathbb{F}}_\lambda} \psi(-a) \left(\frac{1}{|G_\lambda|} \sum_{v \in G_\lambda} \psi(\operatorname{tr} v)\right)^L \\ &= \frac{1}{|\mathbb{F}_\lambda|} \left[1 + \sum_{0 \neq \psi \in \widehat{\mathbb{F}}_\lambda} \psi(-a) \left(\frac{1}{|G_\lambda|} \sum_{v \in G_\lambda} \psi(\operatorname{tr} v)\right)^L\right]. \end{aligned}$$

The first statement follows from summing the previous equation over $a \in A$. □

Gaussian sums. For ψ a nontrivial character of $\mathbb{F}_\lambda$, the sum $\frac{1}{|G_\lambda|} \sum_{v \in G_\lambda} \psi(\operatorname{tr} v)$ is a "Gaussian sum over G_λ", which we expect to be small uniformly with respect to ψ, say

$$\frac{1}{|G_\lambda|} \sum_{v \in G_\lambda} \psi(\operatorname{tr} v) \ll |\mathbb{F}_\lambda|^{-\alpha(G_\lambda)} \tag{6.1}$$

with $\alpha(G_\lambda) > 0$ and square-root cancellation corresponds to $\alpha(G_\lambda) \geqslant \frac{\log |G_\lambda|}{2 \log |\mathbb{F}_\lambda|}$. Alternatively, we can also write

$$\sum_{v \in G_\lambda} \psi(\operatorname{tr} v) \ll |G_\lambda|^{\alpha'(G_\lambda)} \text{ with } \alpha'(G_\lambda) < 1. \tag{6.2}$$

Similarly, if A is "well-distributed" in $\mathbb{F}_\lambda$, we expect

$$\frac{1}{|A|} \sum_{x \in A} \psi(-x) \ll |\mathbb{F}_\lambda|^{-\alpha(A)} \tag{6.3}$$

for some $\alpha(A) > 0$, uniformly with respect to $\psi \in \widehat{\mathbb{F}}_\lambda$. The trivial bound corresponds to $\alpha(A) = 0$.

Thus, we can rewrite Proposition 6.15 as:

Corollary 6.16. *Let $A \subset \mathbb{F}_\lambda$. If the bounds (6.1) and (6.3) hold, then*

$$P(Z_1 + \cdots + Z_L \in A) = \frac{|A|}{|\mathbb{F}_\lambda|} \left(1 + O\left(\frac{1}{|\mathbb{F}_\lambda|^{L\alpha(G_\lambda) + \alpha(A) - 1}}\right)\right)$$

for all $L \geqslant 1$. In particular,

$$P(Z_1 + \cdots + Z_L = a) = \frac{1}{|\mathbb{F}_\lambda|} \left(1 + O\left(\frac{1}{|\mathbb{F}_\lambda|^{L\alpha(G_\lambda) - 1}}\right)\right)$$

uniformly for all $a \in \mathbb{F}_\lambda$.

Author(s)	Nontrivial if
Korobov (1989)	$d \geqslant \ell^{1/2+\varepsilon}$
Shparlinski (1991)	$d \geqslant \ell^{3/7+\varepsilon}$
Heath-Brown and Konyagin (2000)	$d \geqslant \ell^{1/3+\varepsilon}$
Konyagin (2002)	$d \geqslant \ell^{1/4+\varepsilon}$
Bourgain-Glibichuk-Konyagin (2006)	$d \geqslant \ell^{\varepsilon}$

Table 6.2: Bound on exponential sums over subgroups of $\mathbb{F}_\ell^\times$ of size d.

It is insightful to distinguish the following cases to analyze the ranges of the parameters in Corollary 6.16:

(1) If either

- $\alpha(G_\lambda) > 1$, or
- $\alpha(G_\lambda) \leqslant 1$ and $L > 1/\alpha(G_\lambda)$,

we have asymptotic equidistribution of $Z_1 + \cdots + Z_L$ in $\mathbb{F}_\lambda$.

(2) If $\alpha(G_\lambda) \leqslant 1$ and $L \leqslant 1/\alpha(G_\lambda)$, then we have

$$P(Z_1 + \cdots + Z_L = a) \ll |\mathbb{F}_\lambda|^{-L\alpha(G_\lambda)},$$

which shows that $Z_1 + \cdots + Z_L$ is "not too concentrated" at any point $a \in \mathbb{F}_\lambda$.

Example 6.17. We will see that for $G_\lambda = \mathrm{SL}_n(\mathbb{F}_\lambda)$ or $\mathrm{Sp}_n(\mathbb{F}_\lambda)$, we always have $\alpha(G_\lambda) > 1$. On the other hand, $\alpha(\mu_d(\mathbb{F}_\lambda)) < 1$.

6.3.2. Gaussian sums in G_λ. Let us investigate bounds of the form (6.1) (or (6.2)) for the monodromy groups G_λ we are interested in: roots of unity and classical groups over finite fields.

Roots of unity: exponential sums over subgroups of $\mathbb{F}_\lambda^\times$. We assume that $\mathbb{F}_\lambda$ contains a primitive dth root of unity. For $G_\lambda = \mu_d(\mathbb{F}_\lambda) \leqslant \mathbb{F}_\lambda^\times$, the sum (6.1) is a "character sum with exponentials"

$$\sum_{v \in \mu_d(\mathbb{F}_\lambda)} \psi(v) = \sum_{i=1}^{d} \psi(\zeta_d^i),$$

or equivalently a sum over a subgroup of $\mathbb{F}_\lambda^\times$.

For $\mathbb{F}_\lambda = \mathbb{F}_\ell$, the latter appear in works of Korobov, Shparlinski, Heath-Brown-Konyagin, Konyagin, Bourgain-Glibichuk-Konyagin and others, which give nontrivial bounds for d not too small compared to ℓ (see Table 6.2). Square-root cancellation corresponds to $\alpha(G_\lambda) \geqslant \frac{\log d}{2\log \ell}$, and $\frac{\log d}{\log \ell} < 1$ since $\ell \equiv 1 \pmod d$.

We first review the results of Shparlinski and Heath-Brown-Konyagin which give explicit bounds for d at least of the order of $\ell^{1/3}$.

Theorem 6.18 ([Shp91, Theorem 2]). *Let $H \leqslant \mathbb{F}_\ell^\times$ be a subgroup and ψ be a nontrivial additive character of $\mathbb{F}_\ell$. We have*

$$\frac{1}{|H|} \sum_{x \in H} \psi(x) \ll |H|^{-7/12} \ell^{1/4}$$

uniformly with respect to ψ. Thus (6.1) for $G_\lambda = \mu_d(\mathbb{F}_\ell)$ holds with $\alpha(G_\lambda) \in (0, 1/12)$ if we restrict $d \gg \ell^{3/4+12\alpha(G_\lambda)/4}$.

Theorem 6.19 ([HBK00, Theorem 1])**.** *Let $H \leqslant \mathbb{F}_\ell^\times$ be a subgroup and ψ be a nontrivial additive character of $\mathbb{F}_\ell$. We have the nontrivial bounds*

$$\frac{1}{|H|}\sum_{x\in H}\psi(x) \ll \begin{cases} \ell^{1/8}|H|^{-3/8} & \text{if } \ell^{1/3} < |H| \ll \ell^{1/2} \\ \ell^{1/4}|H|^{-5/8} & \text{if } \ell^{1/2} < |H| \ll \ell^{2/3} \\ \ell^{1/2}|H|^{-1} & \text{if } \ell^{2/3} < |H| \ll \ell \end{cases}$$

uniformly with respect to ψ. Thus (6.1) for $G_\lambda = \mu_d(\mathbb{F}_\ell)$ holds with $\alpha(G_\lambda) = \alpha > 0$ in the following cases:

$$\begin{cases} d \gg \ell^{1/3+8\alpha/3} & : \alpha \leqslant 1/16 \\ d \gg \ell^{2/5+8\alpha/5} & : \alpha \leqslant 1/6 \\ d \gg \ell^{1/2+\alpha} & : \alpha \leqslant 1/2. \end{cases}$$

On the other hand, the results of Bourgain and others give (non-explicit) bounds for d as small as desired:

Theorem 6.20 ([BK03, Theorem 2.1])**.** *Let $x, y \in \mathbb{F}_\ell^\times$ and $d = \mathrm{ord}(y \in \mathbb{F}_\ell^\times)$. For every $\delta > 0$, there exists $\alpha = \alpha(\delta) > 0$ such that if $d \geqslant \ell^\delta$, then*

$$\sum_{i=1}^{d}\psi(y^i x) \ll d\ell^{-\alpha}$$

uniformly for all nontrivial $\psi \in \widehat{\mathbb{F}}_\ell$, with an absolute implicit constant. Thus, (6.1) for $G_\lambda = \mu_d(\mathbb{F}_\ell)$ holds with $\alpha(G_\lambda) = \alpha$ if $d \geqslant \ell^\delta$.

Remark 6.21. The $\alpha(\delta)$ arising from Theorem 6.20 are not estimated explicitly in [BK03][1], but one typically expects them to be very small.

The situation is more complicated when $\mathbb{F}_\lambda$ has nonprime order.

By using the formalism of trace functions (or the properties of general Artin-Schreier sheaves in the case of additive characters), we can get a result valid in the range of Korobov's:

Proposition 6.22. *Let H be a subgroup of $\mathbb{F}_q^\times$ of index k and $t : \mathbb{F}_q \to \mathbb{C}$ be a trace function corresponding to a geometrically irreducible ℓ-adic sheaf $\mathcal{F}$ over $\mathbb{F}_q$. If either $\mathrm{rank}(\mathcal{F}) > 1$ or if the function $x \mapsto t(x^k)$ is not constant on $\mathbb{F}_q$, then*

$$\sum_{x\in H} t(x) \ll \mathrm{cond}(\mathcal{F})^2\sqrt{q}.$$

Proof. Since $\mathbb{F}_q^\times$ is cyclic, we have $H = \{x^k : x \in \mathbb{F}_q^\times\}$ and

$$\sum_{x\in H} t(x) = \frac{1}{k}\sum_{x\in\mathbb{F}_q^\times} t(x^k).$$

[1] This could be done with some effort using e.g. [Gar07] (see also [Kow11]).

The sheaf $\mathcal{F}' = [x \mapsto x^k]^*\mathcal{F}$ (see Proposition 2.24) is geometrically irreducible and by Corollary 2.31,

$$\sum_{x\in H} t(x) \ll \frac{\operatorname{cond}(\mathcal{F}')}{k}\sqrt{q},$$

unless $\mathcal{F}'$ is geometrically trivial, which is excluded by hypothesis (see Proposition 2.16). It remains to observe that $\operatorname{cond}(\mathcal{F}') \ll k\operatorname{cond}(\mathcal{F})^2$ by Proposition 2.24. □

Corollary 6.23. *The bound (6.1) for $G_\lambda = \mu_d(\mathbb{F}_\lambda)$ holds uniformly with respect to all nontrivial $\psi \in \widehat{\mathbb{F}}_\lambda$ with $\alpha(G_\lambda) = \alpha \in (0, 1/2)$ whenever $d \geqslant |\mathbb{F}_\lambda|^{1/2+\alpha}$.*

Remark 6.24. Alternatively, one could also proceed by completion as in [Kor89].

By [BC06], the strong results of Bourgain and others (Theorem 6.20) generalize to all finite fields, up to adding an assumption involving subfields:

Theorem 6.25 ([BC06, Theorem 2])**.** *For every $\delta > 0$, there exists $\alpha = \alpha(\delta) > 0$ such that (6.1) for $G_\lambda = \mu_d(\mathbb{F}_\lambda)$ holds with $\alpha(G_\lambda) = \alpha$ if*

$$\frac{d}{(d, |F^\times|)} \geqslant |\mathbb{F}_\lambda|^\delta \tag{6.4}$$

for every subfield $F \not\leqslant \mathbb{F}_\lambda$ with $\log_\ell |F|$ dividing $\log_\ell |\mathbb{F}_\lambda|$.

Remark 6.26. Note that Condition (6.4) amounts to $d \geqslant |\mathbb{F}_\lambda|^\delta$ in the following situations:

- d is prime and $\mathbb{F}_\lambda = \mathbb{F}_\ell(\mu_d)$, or
- $\log_\ell |\mathbb{F}_\lambda|$ is equal to 1 or is prime (e.g. $\mathbb{F}_\lambda = \mathbb{F}_\ell$, recovering Theorem 6.20), or
- $\delta > 1/2$ (recovering Corollary 6.23).

Classical groups. Let us now assume that G_λ is a finite classical group of Lie type in $\mathrm{GL}_n(\mathbb{F}_\lambda)$. By Lemma 6.13,

$$\frac{\log|G_\lambda|}{\log|\mathbb{F}_\lambda|} = \dim G_\lambda + O_n\left(\frac{1}{\log|\mathbb{F}_\lambda|}\right),$$

so square-root cancellation corresponds to $\alpha(G_\lambda) > \dim(G_\lambda)/2$.

Proposition 6.27. *Let $\mathbb{F}_\lambda$ be a finite field and $n \geqslant 2$ be an integer. The bound (6.1) holds for*

G_λ	$\alpha(G_\lambda) > 0$
$\mathrm{GL}_n(\mathbb{F}_\lambda)$	$\frac{n(n-1)}{2}$
$\mathrm{SL}_n(\mathbb{F}_\lambda)$	$\frac{n^2-1}{2}$
$\mathrm{Sp}_n(\mathbb{F}_\lambda)$, $\mathrm{SO}_n^-(\mathbb{F}_\lambda)$ (n even)	$\frac{n(n+2)}{8}$
$\mathrm{SO}_n(\mathbb{F}_\lambda)$ (n odd)	$\frac{n^2-1}{8}$
$\mathrm{SO}_n^+(\mathbb{F}_\lambda)$ (n even)	$\frac{n(n-2)}{8}$

Remark 6.28. Hence, by the dimensions given in Table 6.1, there is square-root cancellation in the special linear case, but not for the others.

Remark 6.29. By using Deligne's analogue of the Riemann hypothesis over finite fields for the restriction of a Lang torsor on $\mathbb{A}^{n^2}/\mathbb{F}_\lambda$ (see [KR15, Example 7.17]) to G_λ, we could get

$$\sum_{g\in G_\lambda} \psi(\mathrm{tr}(g)) \ll |\mathbb{F}_\lambda|^{\dim G_\lambda - 1/2}$$

up to obtaining bounds on sums of Betti numbers (see Remark 2.36, and [Kat01, Section II] for such bounds). Hence, Bound (6.1) would hold with $\alpha(G_\lambda) = 1/2$ by Lemma 6.13. Proposition 6.27 improves that estimate (in particular as n grows).

Proof. We use the explicit evaluation of Gaussian sums over finite classical groups carried out in [Kim97a], [Kim98a] and [Kim98b] using the Bruhat decomposition. Let $a \in \mathbb{F}_\lambda^\times$ corresponding to ψ through the isomorphism $\widehat{\mathbb{F}}_\lambda \cong \mathbb{F}_\lambda$.

(1) By [Kim97a, Theorem 4.2], the Gaussian sum (6.1) for $\mathrm{GL}_n(\mathbb{F}_\lambda)$ is equal to $(-1)^n|\mathbb{F}_\lambda|^{\frac{n(n-1)}{2}}$.

(2) By [Kim97a, Corollary 5.2], Deligne's bound for hyper-Kloosterman sums (Corollary 2.49) and Lemma 6.13, the Gaussian sum (6.1) for $\mathrm{SL}_n(\mathbb{F}_\lambda)$ is equal to

$$\frac{|\mathbb{F}_\lambda|^{\binom{n}{2}}\,\mathrm{Kl}_n(a^n)}{|G_\lambda|} \ll_n |\mathbb{F}_\lambda|^{\frac{n^2-n}{2}+\frac{n-1}{2}-n^2+1} = |\mathbb{F}_\lambda|^{\frac{-n^2+1}{2}}.$$

(3) By [Kim98b, Theorem A], the Gaussian sum $\sum_{v\in \mathrm{Sp}_{2m}(\mathbb{F}_\lambda)} \psi(\mathrm{tr}\, v)$ is equal to

$$\begin{aligned} L^{m^2-1} \sum_{r=0}^{\lfloor m/2\rfloor} L^{r(r+1)} \binom{m}{2r}_L \prod_{i=1}^{r} (L^{2i-1}-1) \\ \times \sum_{l=1}^{\lfloor m/2\rfloor - r+1} L^l\,\mathrm{Kl}_2(a^2)^{m-2r+2-2l} \\ \times \sum_{j_1,\dots,j_{l-1}} (L^{j_1}-1)\dots(L^{j_{l-1}}-1) \end{aligned}$$

for $L = |\mathbb{F}_\lambda|$, where the last sum is over integers $2l-3 \leqslant j_1 \leqslant m-2r-1$, $2l-5 \leqslant j_2 \leqslant j_1-2$, $\dots$, $1 \leqslant j_{l-1} \leqslant j_{l-2}-2$ and

$$\binom{m}{r}_L = \prod_{j=0}^{r-1} \frac{L^{m-j}-1}{L^{r-j}-1} \ll_m L^{r(m-r)}.$$

Using that

$$\begin{aligned} &\prod_{i=1}^{r}(L^{2i-1}-1) < L^{r^2} \text{ and} \\ &\mathrm{Kl}_2(a^2)^{t+2-2l} \sum_{j_1,\dots,j_{l-1}} (L^{j_1}-1)\dots(L^{j_{l-1}}-1) \ll_n L^{(l-1)(t-(l-1))} \end{aligned}$$

for $t = m-2r$ (see [Kim98b, Remark (1) p. 65] for the second one), we find that the Gaussian sum is

$$\ll_m \begin{cases} |\mathbb{F}_\lambda|^{\frac{3m^2+m}{2}} & : m \text{ even} \\ |\mathbb{F}_\lambda|^{\frac{2m^2+m-1}{2}} & : m \text{ odd} \end{cases} \leqslant |\mathbb{F}_\lambda|^{\frac{3m^2+m}{2}}$$

and the result follows by Lemma 6.13.

(4) By [Kim98a, Theorem A],

$$\sum_{v\in \mathrm{SO}_{2m+1}(\mathbb{F}_\lambda)} \psi(\operatorname{tr} v) = \psi(1) \sum_{v\in \mathrm{Sp}_{2m}(\mathbb{F}_\lambda)} \psi(\operatorname{tr} v),$$

the result follows by the previous bound and Lemma 6.13.

(5) Similarly, by [KL96, Theorem 4.3],

$$\sum_{v\in \mathrm{SO}^+_{2m}(\mathbb{F}_\lambda)} \psi(\operatorname{tr} v) = |\mathbb{F}_\lambda|^{-m} \sum_{v\in \mathrm{Sp}_{2m}(\mathbb{F}_\lambda)} \psi(\operatorname{tr} v).$$

(6) The is analogous to (3), using [Kim97b, Theorem A].

□

6.3.3. Gaussian sums in $\mathbb{F}_\lambda$. We now look at Gaussian sums (6.3) in $\mathbb{F}_\lambda$, namely sums of the form

$$\frac{1}{|A|}\sum_{x\in A}\psi(-x)$$

for some $A \subset \mathbb{F}_\lambda$ and $\psi \in \widehat{\mathbb{F}}_\lambda$ nontrivial.

Squares. Let $A = \mathbb{F}_\lambda^{\times 2}$ be the subgroup of squares in $\mathbb{F}_\lambda^\times$. If $\mathbb{F}_\lambda = \mathbb{F}_\ell$, we can use the Legendre symbol to write, for $y \in \mathbb{F}_\ell^\times$,

$$\begin{aligned}\sum_{x\in A}\psi(-xy) &= 1 + \frac{1}{2}\sum_{x\in\mathbb{F}_\ell^\times}\left(1+\left(\frac{x}{\ell}\right)\right)\psi(-xy)\\ &= \frac{1}{2}\left(1+\left(\frac{-y}{\ell}\right)\sum_{x\in\mathbb{F}_\ell^\times}\left(\frac{x}{\ell}\right)\psi(x)\right)\end{aligned}$$

where $\psi(x) = e(x/\ell)$ $(x \in \mathbb{F}_\ell)$. By the evaluation of the classical quadratic Gauss sum,

$$\sum_{x\in A}\psi(-xy) = \frac{1}{2}\left(1+\varepsilon_\ell\left(\frac{-y}{\ell}\right)\sqrt{\ell}\right) \ll \sqrt{\ell} \quad (\varepsilon_\ell \in \{1, i\}),$$

uniformly with respect to y. Hence (6.3) with $\alpha(A) = 1/2$, corresponding to square-root cancellation since $|A| = (\ell-1)/2$.

Multiplicative subgroups. More generally, if $H \leqslant \mathbb{F}_\ell^\times$ is a multiplicative subgroup, the results presented in Section 6.3.2 give a nontrivial bound (6.3) being given that $|H|$ is large enough (but can still be chosen arbitrarily small by the results of Bourgain).

When $H \leqslant \mathbb{F}_\lambda^\times$ with $\mathbb{F}_\lambda$ non-necessarily of prime order, Corollary 6.23 gives a nontrivial bound (6.3) with $\alpha \in (0, 1/2)$ if $|H| > |\mathbb{F}_\lambda|^{1/2+\alpha}$.

Definable subsets. For R a ring and $\varphi(x)$ a first-order formula in one variable in the language of rings, we define

$$\varphi(R) = \{a \in R : \varphi(a) \text{ holds}\}.$$

In particular, we can consider the subsets $\varphi(\mathbb{F}_\lambda)$ of $\mathbb{F}_\lambda$.

Example 6.30. For $\varphi(x) = (\exists y : x = y^2)$, the set $\varphi(R)$ is the subset of squares, which is the example of the previous section. More generally, we can take $\varphi(x) = (\exists y : x = g(y))$ for any polynomial $g \in \mathbb{Z}[Y]$.

Theorem 6.31 (Chatzidakis-van den Dries-Macintyre [CvdDM92])**.** *For every formula $\varphi(x)$ in one variable in the language of rings, there exists a finite set $C(\varphi) \subset (0,1] \cap \mathbb{Q}$ such that for every finite field $\mathbb{F}_\lambda$*

$$\begin{aligned} |\varphi(\mathbb{F}_\lambda)| &= C(\lambda,\varphi)|\mathbb{F}_\lambda| + O_\varphi(|\mathbb{F}_\lambda|^{1/2}) \\ &\quad \textit{with } C(\lambda,\varphi) \in C(\varphi), \textit{ or} \\ |\varphi(\mathbb{F}_\lambda)| &\ll_\varphi |\mathbb{F}_\lambda|^{-1/2}. \end{aligned} \tag{6.5}$$

where the implicit constants depend only on φ.

When $\varphi(x) = (\exists y : f(y) = x)$ for some polynomial $f \in \mathbb{Z}[X]$, Theorem 6.31 also appears in [BSD59] (using the Weil conjectures for curves) as:

Proposition 6.32. *If $f \in \mathbb{F}_\lambda[X]$ of degree d is such that $f(X) - y \in \mathbb{F}_\lambda(y)[X]$ is separable with full Galois group $\mathfrak{S}_d$ over $\mathbb{F}_\lambda(y)$, then*

$$|f(\mathbb{F}_\lambda)| = \left(\sum_{n=1}^{d} \frac{(-1)^{n+1}}{n!}\right)|\mathbb{F}_\lambda| + O\left(|\mathbb{F}_\lambda|^{1/2}\right).$$

Hence, (6.5) holds with $C(\varphi) \in (0,1)$.

This is extended to $f \in \mathbb{Q}(X)$ in [Coh70].

Remark 6.33. By [BSD59, Lemma 1], if $f \in \mathbb{Z}[X]$ is such that the Galois group of $f(X) - y \in \mathbb{C}(y)$ over $\mathbb{C}(y)$ is equal to $\mathfrak{S}_d$, then for all but finitely many primes ℓ, the reduction $f \pmod{\ell}$ satisfies the hypotheses of Proposition 6.32. By [BSD59, p. 422], the condition on $f \in \mathbb{Z}[X]$ holds if $\operatorname{disc}(\operatorname{disc}(f)) \neq 0$, so it does for almost all polynomials of fixed degree.

The following combined with Theorem 6.31 shows that Gaussian sums over definable subsets exhibit square-root cancellation:

Theorem 6.34 ([Kow07, Theorem 1, Corollary 12, Remark 19])**.** *Let $\varphi(x)$ be a formula in one variable in the language of rings such that $|\varphi(\mathbb{F}_\lambda)|$ is not bounded as $|\mathbb{F}_\lambda| \to +\infty$. Then, if $\psi \in \widehat{\mathbb{F}}_\lambda$ is nontrivial, the bound (6.3) for $A = \varphi(\mathbb{F}_\lambda)$ holds with $\alpha(A) = 1/2$:*

$$\frac{1}{|\varphi(\mathbb{F}_\lambda)|}\sum_{x \in \varphi(\mathbb{F}_\lambda)} \psi(x) \ll_\varphi |\mathbb{F}_\lambda|^{-1/2}.$$

6.4. Equidistribution of values and shifted short sums

As a first application of our probabilistic model in the finite case, we investigate the distribution of shifted sums over a subset $I \subset \mathbb{F}_q$ of a reduced trace function $t : \mathbb{F}_q \to \mathbb{F}_\lambda$, this is to say, we study the random variable

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

This includes in particular the most natural case of the distribution of the values $(t(x))_{x\in\mathbb{F}_q}$ by taking $I = \{0\}$. This particular case will also appear in the next section.

6.4.1. Statement of the result.

Theorem 6.35. *Let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be a trace function associated to a sheaf $\mathcal{F}$ in a coherent family with monodromy group G_λ. For $a \in \mathbb{F}_\lambda$ and $I \subset \mathbb{F}_q$ of size L such that $\mathcal{F}$ is I-compatible, let us consider the probability*

$$P\big(S(t, I + x) \equiv a\big) \tag{6.6}$$

with respect to the uniform measure on $\mathbb{F}_q$.

(1) If G_λ is classical, then the probability (6.6) is equal to

$$\frac{1}{|\mathbb{F}_\lambda|} + O\left(\frac{1}{|\mathbb{F}_\lambda|^{L\alpha(G_\lambda)}} + \frac{L|\mathbb{F}_\lambda|^{L\beta_+(G_\lambda)+2\beta_-(G_\lambda)-1}}{q^{1/2}}\right), \tag{6.7}$$

uniformly with respect to a, where $\alpha(G_\lambda), \beta_\pm(G_\lambda) > 0$ are given explicitly in Table 6.1.

(2) If $G_\lambda = \mu_d(\mathbb{F}_\lambda)$, for every $\delta \in (0, 1)$ there exists $\alpha = \alpha(\delta) > 0$ such that the probability (6.6) is

$$\frac{1}{|\mathbb{F}_\lambda|} + O\left(\frac{1}{|\mathbb{F}_\lambda|^{L\alpha}} + \frac{Ld^{L+1}}{q^{1/2}|\mathbb{F}_\lambda|^{\min(L\alpha,1)}}\right) \tag{6.8}$$

uniformly with respect to a, when Condition (6.4) holds[2] for every subfield $F \nleqslant \mathbb{F}_\lambda$ with $\log_\ell |F| \mid \log_\ell |\mathbb{F}_\lambda|$. Moreover:

- *If $\delta > 1/2$, we can choose $\alpha(\delta) = \delta - 1/2$. If d is prime, the factor d^{L+1} can be replaced by d^L.*
- *If $\mathbb{F}_\lambda = \mathbb{F}_\ell$, then Condition (6.4) is $d \geqslant \ell^\delta$ and explicitly, we can choose*

$$\alpha(\delta) = \begin{cases} \frac{3\delta-1}{8} & \text{if } \delta \in (1/3, 1/2] \\ \frac{5\delta-2}{8} & \text{if } \delta \in (1/2, 2/3] \\ \delta - \frac{2}{3} & \text{if } \delta \in (2/3, 1]. \end{cases} \tag{6.9}$$

Proof. By Corollary 6.10 and Proposition 6.15, we have for all $a \in \mathbb{F}_\lambda$ that the probability $P\left(S(t, I + x) \equiv a\right)$ is equal to

$$\frac{1}{|\mathbb{F}_\lambda|} + O\left(\frac{1}{|\mathbb{F}_\lambda|^{L\alpha(G_\lambda)}} + \frac{LE(G_\lambda, L)}{q^{1/2}|\mathbb{F}_\lambda|^{\min(L\alpha(G_\lambda),1)}}\right) \tag{6.10}$$

In the classical case, note that $\alpha(G_\lambda) > 1$ by Table 6.1. □

[2] See also Remark 6.26.

6.4.2. Analysis of the ranges.

Case G_λ classical. Since $\alpha(G_\lambda) > 1$, the error term of (6.7) is negligible with respect to the main term (i.e. with a ratio that is $o(1)$) when

$$L|\mathbb{F}_\lambda|^{L\beta_+(G_\lambda)+2\beta_-(G_\lambda)} = o(q^{1/2}).$$

Note that:

- When $L = 1$, this is $|\mathbb{F}_\lambda| = o\left(q^{1/\dim(G_\lambda)}\right)$.
- When $d = p$ (e.g. for Kloosterman sums), this implies that $e > 2(L\beta_+(G_\lambda) + 2\beta_-(G_\lambda))$ (see Section 6.2.4).

Case G_λ cyclic. The error term of (6.7) is negligible with respect to the main term when

$$L > 1/\alpha > 1 \text{ and } Ld^{L+1} = o(q^{1/2}).$$

In particular, $1 < 1/\alpha < L < \log q/2$.

6.4.3. Examples.

Kloosterman sums.

Corollary 6.36 (Kloosterman sums)**.** *For $n \geqslant 2$, and $\mathfrak{q} \trianglelefteq \mathbb{Z}[\zeta_{4p}]$ a prime ideal above a prime $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$ and $(n, [\mathbb{F}_\mathfrak{q} : \mathbb{F}_\ell]) = 1$, let*

$$\mathrm{Kl}_{n,q} : \mathbb{F}_q \to \mathbb{Z}[\zeta_{4p}]_{q^{(n-1)/2}} \to \mathbb{Z}[\zeta_{4p}]_\mathfrak{q}/\mathfrak{q} \cong \mathbb{F}_\lambda$$

be the reduction modulo $\mathfrak{q}$ of the Kloosterman sum over $\mathbb{F}_q$. For any $I \subset \mathbb{F}_q$ of size L, the probability

$$P\big(S(\mathrm{Kl}_{n,q}, I + x) \equiv a\big)$$

is given by

$$\frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O_n\left(|\mathbb{F}_\lambda|^{-L\frac{n^2-1}{2}} + |\mathbb{F}_\lambda|^{L\frac{n^2+n-2}{2}+n(n-1)-1}q^{-\frac{1}{2}}\right) & \text{if } n \text{ odd} \\ O_n\left(|\mathbb{F}_\lambda|^{-L\frac{n(n+2)}{8}} + |\mathbb{F}_\lambda|^{L\frac{n(n+2)}{4}+\frac{n^2-2}{2}}q^{-\frac{1}{2}}\right) & \text{if } n \text{ even} \end{cases}$$

uniformly for all $a \in \mathbb{F}_\lambda$. In particular, the probability $P\left(\mathrm{Kl}_{n,q}(x) \equiv a\right)$ is given by

$$\frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O_n\left(|\mathbb{F}_\lambda|^{-\frac{n^2-1}{2}} + |\mathbb{F}_\lambda|^{\frac{3n^2-n-4}{2}}q^{-\frac{1}{2}}\right) & : n \text{ odd} \\ O_n\left(|\mathbb{F}_\lambda|^{-\frac{n(n+2)}{8}} + |\mathbb{F}_\lambda|^{\frac{3n^2+2n-2}{4}}q^{-\frac{1}{2}}\right) & : n \text{ even.} \end{cases}$$

Remark 6.37. Replacing a by $aq^{(n-1)/2}$ and using the uniformity with respect to a, these results hold as well for unnormalized Kloosterman sums.

Point-counting on families of curves. With $\mathbb{F}_\lambda = \mathbb{F}_\ell$, the case n even of Corollary 6.36 also applies to the point-counting on families of hyperelliptic curves from Proposition 6.5 (normalized or not, see Remark 6.37).

Multiplicative characters.

Corollary 6.38 (Multiplicative characters)**.** *Let $d \geqslant 2$ be an integer, $\mathfrak{q} \trianglelefteq \mathbb{Z}[\zeta_d]$ be a prime ideal,*

$$\chi : \mathbb{F}_q^\times \to \mathbb{Z}[\zeta_d] \to \mathbb{Z}[\zeta_d]/\mathfrak{q} \cong \mathbb{F}_\lambda$$

be the reduction modulo $\mathfrak{q}$ of a multiplicative character of order d, and $f \in \mathbb{Q}(X)$ with a well-defined reduction modulo q, whose zeros and poles have order not divisible by d. Let $\delta \in (0,1)$ be such that[3]

$$\frac{d}{(d, |F^\times|)} \geqslant |\mathbb{F}_\lambda|^\delta$$

for every subfield $F \not\leqslant \mathbb{F}_\lambda$ with $\log_\ell |F| \mid \log_\ell |\mathbb{F}_\lambda|$.

Let $I \subset \mathbb{F}_q$ be of size L. If $\deg(f) > 1$, we assume that $L = 1$ or $I \subset [1 \dots p/\deg(f))^e \subset \mathbb{F}_p^e \cong \mathbb{F}_q$. Then $\alpha = \alpha(\delta) > 0$ such that

$$P\big(S(\chi \circ f, I + x) \equiv a\big) = \frac{1}{|\mathbb{F}_\lambda|} + O_f\left(\frac{1}{|\mathbb{F}_\lambda|^{L\alpha}} + \frac{Ld^{L+1}}{q^{1/2}|\mathbb{F}_\lambda|^{\min(L\alpha,1)}}\right) \tag{6.11}$$

uniformly for all $a \in \mathbb{F}_\lambda$. In particular,

$$P\big(\chi(f(x)) \equiv a\big) \ll_f \frac{1}{|\mathbb{F}_\lambda|^\alpha}\left(1 + \frac{d^2}{q^{1/2}}\right). \tag{6.12}$$

If d is prime, the factor d^{L+1} in (6.11) (respectively d^2 in (6.12)) can be replaced by d^L (resp. d). When $\delta > 1/2$, we can choose $\alpha(\delta) = 1/2 - \delta$, and more explicit pairs (δ, α) are given by (6.9) when $\mathbb{F}_\lambda = \mathbb{F}_\ell$.

Example 6.39. By Example 4.12, the condition on I if $f \neq X$ holds if $I \subset \{1, \dots, L\}$ with $L < p/\deg(f)$.

6.5. Distribution of families of short sums

As a second application of the probabilistic model developed above, we generalize the results of [LZ12] on the distribution of residues of sums over partial intervals of the Legendre symbol to the distribution of coherent families of sums of reduced trace functions in coherent families. As we have seen in Section 6.1.2, this includes multiplicative characters of any order, Kloosterman sums and functions counting points on families of hyperelliptic curves.

6.5.1. Families of short sums.

Definition and examples.

Definition 6.40. Let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be any function. A *family of sums with respect to t* is a family

$$\Big(S(t, \mathcal{I}(k))\Big)_{k \in \mathcal{I}} \tag{6.13}$$

for a finite parameter space $\mathcal{I}$ with an injective map $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, $k \mapsto \mathcal{I}(k)$.

[3] If $\mathbb{F}_\lambda = \mathbb{F}_\ell$ or if d is prime, this condition is simply $d \geqslant |\mathbb{F}_\lambda|^\delta$.

Examples 6.41.

(1) (Intervals) When $q = p$, we can study sums over the intervals

$$\{\mathcal{I}(k) = [1 \dots k] : k \in \mathcal{I}\}$$

for a parameter set $\mathcal{I} \subset [1 \dots p]$, identifying $\mathbb{F}_p$ with the latter interval.

(2) (Boxes) More generally, when $q = p^e$, $\mathbb{F}_q = \mathbb{F}_p(\alpha) \cong \mathbb{F}_p^e$, we can study sums over the "boxes"[4]

$$\mathcal{I}(k) = [1 \dots k_1] + [1 \dots k_2]\alpha + \cdots + [1 \dots k_e]\alpha^{e-1},$$

with $k = (k_1, \dots, k_e) \in \mathcal{I} \subset [1 \dots p]^e$.

(3) (Shifted subsets) For $\mathcal{I}, E \subset \mathbb{F}_q$, we can consider the translates

$$\mathcal{I}(x) = E + x = \{y + x : y \in E\}$$

of E by elements $x \in \mathcal{I}$.

(4) (Combining families) Given $\mathcal{I}_i \to \mathcal{P}(\mathbb{F}_p)$ $(i = 1, \dots, e)$, we can form the family $\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_e$ over $\mathbb{F}_q \cong \mathbb{F}_p^e$ defined by

$$\mathcal{I}(k_1, \dots, k_e) = \prod_{i=1}^{e} \mathcal{I}_i(k_i) \subset \mathbb{F}_q.$$

Distribution questions. We are interested in the distribution of the random variable (6.13) (with the uniform measure on $\mathcal{I}$), asymptotically with respect to the parameters q and $|\mathbb{F}_\lambda|$. Thus, we are led to study the density

$$\Phi(t, \mathcal{I}, a) := \frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}(k)) \equiv a\}|}{|\mathcal{I}|} \quad (a \in \mathbb{F}_\lambda).$$

Example 6.42. Let $\ell \geqslant 2$ be an integer and consider the family $\mathcal{I}$ of Example 6.41 (1) with $t = \left(\frac{\cdot}{p}\right) : \mathbb{F}_p \to \mathbb{F}_\ell$ the Legendre symbol, a multiplicative character of order 2. As we mentioned in Section 1.4.5, one of the main results of [LZ12] is that

$$\Phi(t, \mathcal{I}, a) = \frac{1}{\ell} + O\left(\left(\frac{\ell}{\log p}\right)^{\frac{1}{2}}\right)$$

uniformly with respect to $a \in \mathbb{F}_\ell$. Therefore, the random variable (6.13) converges in law to the uniform distribution on $\mathbb{F}_\ell$ if ℓ is fixed, $p \to +\infty$, and more generally we have $\Phi(t, \mathcal{I}, a) \sim \frac{1}{\ell}$ if $\ell = o((\log p)^{1/3})$.

Our goal is to generalize this result in different directions: for other reductions of trace functions (such as multiplicative characters of any order, Kloosterman sums and point-counting functions on families of curves), for other families of short sums, and in the case $q > p$.

Example 6.43. The study of $\Phi(t, \mathcal{I}, a)$ for the family of Example 6.41 (3) is the finite analogue of the distribution questions considered in Chapter 5.

[4] Of course, one should not replace the sums over $\{[1 \dots k] : 1 \leqslant k \leqslant p\}$ by the sums over $\{[1 \dots k] : 1 \leqslant k \leqslant q\}$.

6.5.2. Equidistribution on average/for shifted families. Given a rather generic family $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, we could expect the random variable (6.13) to converge to the uniform distribution on $\mathbb{F}_\lambda$. Albeit we cannot show that in this most general setting, we have nonetheless a result on average over shifts.

Definition 6.44. For a family $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, we denote by $\mathcal{I}' = \mathcal{I} \times \mathbb{F}_q \to \mathcal{P}(\mathbb{F}_q)$ the shifted family defined by $\mathcal{I}'(k,x) = \mathcal{I}(k) + x$ and we let the families

$$\begin{aligned} \mathcal{I} + x = \mathcal{I}'(\,\cdot\,, x) : &\qquad \mathcal{I} \to \mathcal{P}(\mathbb{F}_q) &&\qquad \text{for } x \in \mathbb{F}_q, \\ \mathcal{I}_k = \mathcal{I}'(k, \,\cdot\,) : &\qquad \mathbb{F}_q \to \mathcal{P}(\mathbb{F}_q) &&\qquad \text{for } k \in \mathcal{I}. \end{aligned}$$

Hence, for a family $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, we have $\mathcal{I} = \mathcal{I} + 0 = \mathcal{I}'(\,\cdot\,, 0)$ and

$$\begin{aligned} \Phi(t, \mathcal{I}', a) &= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \Phi(t, \mathcal{I} + x, a) = \frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} \Phi(t, \mathcal{I}_k, a), \qquad (6.14) \\ \Phi(t, \mathcal{I} + x, a) &= \frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}(k) + x) \equiv a\}|}{|\mathcal{I}|} \quad (x \in \mathbb{F}_q), \\ \Phi(t, \mathcal{I}_k, a) &= \frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}(k) + x) \equiv a\}|}{q} \quad (k \in \mathcal{I}) \end{aligned}$$

for any function $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ and $a \in \mathbb{F}_\lambda$.

Definition 6.45. For a family $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, a real number $\alpha > 0$ and integers $n > 0$, $d \geqslant 0$, we define the quantities

$$\begin{aligned} M_{\mathcal{I}} &= \Big| \bigcup_{k \in \mathcal{I}} \mathcal{I}(k) \Big|, \ m_{\mathcal{I}} = \max_{k \in \mathcal{I}} |\mathcal{I}(k)|, \qquad G_{\mathcal{I}}(\alpha, n) = \frac{1}{|\mathcal{I}|} \sum_{d \geqslant 1} \frac{g_{\mathcal{I}}(d)}{n^{\alpha d}}, \\ g_{\mathcal{I}}(d) &= |\{k \in \mathcal{I} : |\mathcal{I}(k)| = d\}|, \qquad H_{\mathcal{I}}(\alpha, n) = \frac{1}{|\mathcal{I}|} \sum_{d \geqslant 1} \frac{h_{\mathcal{I}}(d)}{n^{\alpha d}}, \\ h_{\mathcal{I}}(d) &= \Big| \{k_1, k_2 \in \mathcal{I} : k_2 \neq k_2, \ |\mathcal{I}(k_1) \Delta \mathcal{I}(k_2)| = d\} \Big|. \end{aligned}$$

Theorem 6.46. *Let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be a trace function associated to a sheaf $\mathcal{F}$ in a coherent family with monodromy group G_λ and $\mathcal{I}$ be a family of sums with respect to t. We assume that $\mathcal{F}$ is $\bigcup_{k \in \mathcal{I}} \mathcal{I}(k)$-compatible. The averaged variance*

$$V(q, G_\lambda, \mathcal{I}) = \sum_{a \in \mathbb{F}_\lambda} \frac{1}{q} \sum_{x \in \mathbb{F}_q} \left(\Phi(t, \mathcal{I} + x, a) - \frac{1}{|\mathbb{F}_\lambda|} \right)^2 \qquad (6.15)$$

is equal to

$$\frac{1}{|\mathcal{I}|} \left(1 + O\left(\tilde{V}(q, G_\lambda, \mathcal{I}) \right) \right)$$

with $\tilde{V}(q, G_\lambda, \mathcal{I})$ given by

$$H_{\mathcal{I}}(\alpha(G_\lambda), |\mathbb{F}_\lambda|) \left(1 + \frac{M_{\mathcal{I}}}{q^{1/2}} \times \begin{cases} |\mathbb{F}_\lambda|^{\beta_+(G_\lambda) M_{\mathcal{I}} + 2\beta_-(G_\lambda)} & : G_\lambda \text{ classical} \\ d^{M_{\mathcal{I}}+1} & : G_\lambda \text{ cyclic} \end{cases} \right),$$

for $\alpha(G_\lambda), \beta_\pm(G_\lambda) > 0$ given in Table 6.1.

Thus, $V(q, G_\lambda, \mathcal{I})$ should be small as $|\mathcal{I}| \to +\infty$, and we have by the Cauchy-Schwarz inequality

$$\Phi(t, \mathcal{I}', a) = \frac{1}{|\mathbb{F}_\lambda|} + O\left(V(q, G_\lambda, \mathcal{I})^{1/2}\right) \tag{6.16}$$

uniformly with respect to $a \in \mathbb{F}_\lambda$. Note that the bound on V depends on the size of $\mathcal{I}$ and on the size/structure of the subsets $\mathcal{I}(k)$.

6.5.3. Consequences. Using Theorem 6.46 in Equation (6.16), we can obtain results for unshifted "complete" (i.e. parametrized by $\mathbb{F}_q$) families by averaging over an auxiliary family of appropriate size. This is the idea exploited in [LZ12] for the family of Example 6.42.

Shifts of small subsets. First, we consider shifts of subsets of moderate size following Example 6.41 (3). The Gaussian distribution for complex-valued trace functions from Chapter 5 becomes a uniform distribution when the latter are reduced in $\mathbb{F}_\lambda$:

Proposition 6.47 (Shifts of small subsets)**.** *Let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be a trace function associated to a sheaf $\mathcal{F}$ in a coherent family with monodromy group G_λ. Let $\varepsilon, \varepsilon' \in (0, 1/2)$, $\delta \in (0, 1)$, and let $E \subset \mathbb{F}_q$. We assume that:*

- *$|B_E| < q^{1/2-\varepsilon'}$ and $B_E \subset \prod_{i=1}^{e}[0, \delta p) \subset \mathbb{F}_p^e \cong \mathbb{F}_q$, where B_E is the bounding box[5] of E.*
- *If $\mathcal{F} = \mathcal{L}_{\chi(f)}$ is a Kummer sheaf, $\delta < 1/\deg(f)$.*
- *If $G_\lambda = \mu_d(\mathbb{F}_\lambda)$ with $\mathbb{F}_\lambda \neq \mathbb{F}_\ell$ and d is nonprime, then Condition (6.4) holds (e.g. if $d \geqslant |\mathbb{F}_\lambda|^{1/2+\alpha}$ for some $\alpha > 0$).*

Then

$$P\big(S(t, E + x) \equiv a\big) = \frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{|E| \log |\mathbb{F}_\lambda|}{\log q}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ classical} \\ O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{|E| \log d}{\log q}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ cyclic} \end{cases}$$

uniformly for all $a \in \mathbb{F}_\lambda$, where the implicit constants depend on ε, ε', δ, and on the type of G_λ in the classical case.

Remark 6.48. This is nontrivial if

$$|E| \log |\mathbb{F}_\lambda| = o(\log q) \quad (\text{resp. } |E| \log d = o(\log q)).$$

Note that when the sheaf $\mathcal{F}$ of $\mathbb{F}_\lambda$-modules from which t arises comes from the reduction of a sheaf of $\mathbb{Z}[\zeta_{4p}]_\lambda$-modules (e.g. for Kloosterman sums), we must thus take $|E| = o(e)$ (see Section 6.2.4).

Remark 6.49. The first condition about B_E in the statement can be included in the second one by taking $\delta < p^{-1/2-\varepsilon'}$.

[5] See Lemma 6.63 for a precise definition.

By taking $E = \{0\}$, we get the following corollary, which should be compared with the case $I = \{0\}$ of Theorem 6.35:

Corollary 6.50. *Let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be a trace function associated to a sheaf $\mathcal{F}$ in a coherent family with monodromy group G_λ and let $\varepsilon \in (0, 1/4)$. We assume that if $G_\lambda = \mu_d(\mathbb{F}_\lambda)$ with $\mathbb{F}_\lambda \neq \mathbb{F}_\ell$ and d nonprime, then Condition (6.4) holds (e.g. $d \geqslant |\mathbb{F}_\lambda|^{1/2+\alpha}$ for some $\alpha > 0$). The density*

$$P\big(t(x) \equiv a\big) = \frac{|\{x \in \mathbb{F}_q : t(x) \equiv a\}|}{q}$$

is given by

$$\frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{\log|\mathbb{F}_\lambda|}{\log q}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ classical} \\ O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{\log d}{\log q}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ cyclic} \end{cases}$$

uniformly for all $a \in \mathbb{F}_\lambda$, where the implicit constants depend on ε, and on the type of G_λ in the classical case.

Example 6.51. Proposition 6.47 and Corollary 6.50 apply to Kloosterman sums of fixed rank (normalized or not, see Remark 6.37), multiplicative characters composed with rational functions, and point-counting functions for families of hyperelliptic curves (normalized or not).

Partial intervals. The second example notably generalizes the result of [LZ12] (see Example 6.42) to all multiplicative characters:

Proposition 6.52 (Partial intervals)**.** *Let $t : \mathbb{F}_p \to \mathbb{F}_\lambda$ be a trace function associated to a sheaf over $\mathbb{F}_p$ in a coherent family with monodromy group G_λ, and let $\varepsilon, \varepsilon' > 0$. We assume that if $G_\lambda = \mu_d(\mathbb{F}_\lambda)$ with $\mathbb{F}_\lambda \neq \mathbb{F}_\ell$ and d nonprime, then Condition (6.4) holds (e.g. $d \geqslant |\mathbb{F}_\lambda|^{1/2+\alpha}$ for some $\alpha > 0$). The density*

$$P\big(S(t, [1 \dots x]) \equiv a\big) = \frac{|\{1 \leqslant k \leqslant p : S(t, [1 \dots k]) \equiv a\}|}{p}$$

is given by

$$\frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O\left(\frac{1}{p^{1/4-\varepsilon/2}} + \left(\frac{\log|\mathbb{F}_\lambda|}{\log p}\right)^{\frac{1}{2}} + \delta_{S(t,\mathbb{F}_p)\neq 0}\left(\frac{|\mathbb{F}_\lambda|\log p}{p\log|\mathbb{F}_\lambda|}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ classical} \\ O\left(\frac{1}{p^{1/4-\varepsilon/2}} + \left(\frac{\log d}{\log p}\right)^{\frac{1}{2}} + \delta_{S(t,\mathbb{F}_p)\neq 0}\left(\frac{|\mathbb{F}_\lambda|\log p}{p\log d}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ cyclic} \end{cases}$$

uniformly for all $a \in \mathbb{F}_\lambda$, where the implicit constants depend on $\varepsilon, \varepsilon'$.

Examples 6.53. (1) This applies to multiplicative characters of $\mathbb{F}_p^\times$ of order d composed with $f \in \mathbb{Q}(X)$ whose zeros and poles have orders not divisible by d, as in Corollary 6.38. When χ is the Legendre symbol, this is the result of [LZ12]. By the orthogonality relations, the third summand of the error term vanishes if $f = X$.

(2) With $d = 2$ and $\mathbb{F}_\lambda = \mathbb{F}_\ell$, this also applies to the point-counting functions on families of hyperelliptic curves from Proposition 6.5. See also [MZ14] for an analogue of [LZ12] to the counting of points of a plane curve in rectangles.

Remark 6.54. We will see that it is unclear whether this can be generalized to the case $e \geqslant 2$ (see Example 6.41 (2)) because of "diagonal" terms in the errors. Since the case $d = p$, G_λ classical forces to take $e \to +\infty$ (see Section 6.2.4 and Remark 6.48), Proposition 6.52 does not make sense for Kloosterman sums.

Even though Proposition 6.52 does not extend to "boxes" in $\mathbb{F}_q \cong \mathbb{F}_p^e$ with $e \geqslant 2$, we nonetheless have the following for a family of type (4) from Example 6.41.

Proposition 6.55 (Partial intervals with shifts of small subsets)**.** *Let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be a trace function associated to a sheaf $\mathcal{F}$ in a coherent family with monodromy group G_λ. Let $\varepsilon, \varepsilon' \in (0, 1/2)$, $\delta \in (0, 1)$, and let $E_2, \dots, E_e \subset \mathbb{F}_p$. We assume that:*

- *$|B_E| \leqslant q^{1/2-\varepsilon'}$ and $E_i \subset [0, \delta p)$ for all $2 \leqslant i \leqslant e$, where B_E is the bounding box of $E = E_2 \times \cdots \times E_e$ in $\mathbb{F}_p^{e-1}$.*
- *If $\mathcal{F}$ is a Kummer sheaf $\mathcal{L}_{\chi(f)}$, $\delta < 1/\deg(f)$.*
- *If $G_\lambda = \mu_d(\mathbb{F}_\lambda)$ with $\mathbb{F}_\lambda \neq \mathbb{F}_\ell$ and d is nonprime, then Condition (6.4) holds (e.g. if $d \geqslant |\mathbb{F}_\lambda|^{1/2+\alpha}$ for some $\alpha > 0$).*

Then the density

$$\frac{|\{(x_1, \dots, x_e) \in \mathbb{F}_p^e \cong [1 \dots p]^e : S(t, [1 \dots x_1] \times \prod_{i=2}^e (E_i + x_i)) \equiv a\}|}{q}$$

(with respect to any $\mathbb{F}_p$-basis of $\mathbb{F}_q$) is equal to

$$\frac{1}{|\mathbb{F}_\lambda|} + \begin{cases} O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{|E| \log |\mathbb{F}_\lambda|}{\log q}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ classical} \\ O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{|E| \log d}{\log q}\right)^{\frac{1}{2}}\right) & : G_\lambda \text{ cyclic} \end{cases}$$

uniformly for all $a \in \mathbb{F}_\lambda$, where the implicit constants depend on ε, ε' and δ.

Example 6.56. As for Proposition 6.47, this applies to Kloosterman sums of fixed rank, multiplicative characters composed with rational functions, and point-counting functions on families of hyperelliptic curves.

We will prove Theorem 6.46 and its applications in the next sections.

6.5.4. Probabilistic model. Let $\mathcal{F}$ be a sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$, part of a coherent family, with monodromy group $G_\lambda \leqslant \mathrm{GL}_n(\mathbb{F}_\lambda)$. We first apply the probabilistic model from Section 6.2 to study of the distribution of families of short sums.

Again, we let X be a random variable uniformly distributed in G_λ, and Z be its image through the map $G_\lambda \to G_\lambda^\sharp \xrightarrow{\mathrm{tr}} \mathbb{F}_\lambda$. Moreover, let $(Z_i)_{i \in \mathbb{N}}$ be a sequence of independent random variables distributed like Z.

For a finite subset $I \subset \mathbb{N}$, we define the random variable

$$S(I) = \sum_{i \in I} Z_i$$

on the probability space $G_\lambda^{\mathbb{N}}$. For a finite parameter space $\mathcal{I}$ with a map $\mathcal{I} \to \mathcal{P}_f(\mathbb{N})$, we consider for all $a \in \mathbb{F}_\lambda$ the random variable

$$\Phi(\mathcal{I}, a) = \frac{|\{k \in \mathcal{I} : S(\mathcal{I}(k)) \equiv a\}|}{|\mathcal{I}|}.$$

In this setting, Corollary 6.10 gives information about the distribution of $\Phi(t, \mathcal{I}, a)$ averaged over shifts of the family $\mathcal{I}$ by elements of $\mathbb{F}_q$:

Proposition 6.57. *In the above setting, if $\mathcal{F}$ is $\bigcup_{k\in\mathcal{I}} \mathcal{I}(k)$-compatible, for any function $h : \mathbb{F}_\lambda \to \mathbb{R}_{\geqslant 0}$ and any $a \in \mathbb{F}_\lambda$, we have*

$$\mathbb{E}\Big(h(\Phi(t, \mathcal{I} + x, a))\Big) = \mathbb{E}\Big(h(\Phi(\mathcal{I}, a))\Big)\left(1 + O\left(\frac{M_{\mathcal{I}} E(G_\lambda, M_{\mathcal{I}})}{q^{1/2}}\right)\right).$$

In other words, for all $a \in \mathbb{F}_\lambda$ the random variable $(\Phi(t, \mathcal{I}+x, a))_{x\in\mathbb{F}_q}$ converges in law (with respect to the parameters, q, $|\mathbb{F}_\lambda|$, $\mathcal{I}$) to the random variable $\Phi(\mathcal{I}, a)$ if the error term is $o(1)$ as the parameters vary.

6.5.5. Expected value. We first consider the expected value of $\Phi(\mathcal{I}, a)$, which gives a preliminary version of Theorem 6.46 and a motivation for the next section, where the former will be improved by analyzing the variance. The improvement will concern the quality of the error term, the uniformity with respect to a, and the ability to obtain Proposition 6.52 by removing the shifts for some specific families.

Computation in the model.

Proposition 6.58. *For $a \in \mathbb{F}_\lambda$, in the notations of Section 6.5.4, we have*

$$\mathbb{E}\left(\Phi(\mathcal{I}, a)\right) = \frac{1}{|\mathbb{F}_\lambda|} + O\left(G_{\mathcal{I}}(\alpha(G_\lambda), |\mathbb{F}_\lambda|)\right).$$

Proof. By Corollary 6.16,

$$\mathbb{E}\left(\Phi(\mathcal{I}, a)\right) = \frac{1}{|\mathbb{F}_\lambda|} + O\left(\frac{1}{|\mathcal{I}|}\sum_{k\in\mathcal{I}} |\mathbb{F}_\lambda|^{-|\mathcal{I}(k)|\alpha(G_\lambda)}\right).$$

□

Conclusion. By Propositions 6.57 and 6.58, we get the following preliminary version of Theorem 6.46:

Proposition 6.59. *Let $t : \mathbb{F}_q \to \mathbb{F}_\lambda$ be a trace function associated to a sheaf in a coherent family with monodromy group G_λ and $\mathcal{I}$ be a family of sums such that $\mathcal{F}$ is $\bigcup_{k\in\mathcal{I}} \mathcal{I}(k)$-compatible. For all $a \in \mathbb{F}_\lambda$,*

$$\mathbb{E}(\Phi(t, \mathcal{I} + x, a)) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} \Phi(t, \mathcal{I} + x, a) = \frac{1}{|\mathbb{F}_\lambda|} + O(\varepsilon(q, G_\lambda, \mathcal{I})),$$

where

$$\varepsilon(q, G_\lambda, \mathcal{I}) = G_{\mathcal{I}}(\alpha(G_\lambda), |\mathbb{F}_\lambda|) + \frac{M_{\mathcal{I}} E(G_\lambda, M_{\mathcal{I}})}{q^{1/2}}.$$

As a corollary, we obtain as well a preliminary version of Proposition 6.68 about unshifted "complete" families:

Corollary 6.60. *In the setting of Proposition 6.59, assume that for all $a \in \mathbb{F}_\lambda$, $\Phi(t, \mathcal{I}_k, a)$ does not depend on k. Then*

$$\Phi(t, \mathcal{I}_k, a) = \frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}_k'(x)) \equiv a\}|}{q} = \frac{1}{|\mathbb{F}_\lambda|} + O(\varepsilon(q, G_\lambda, \mathcal{I})).$$

Proof. This follows by exchanging summations (see (6.14)). □

Example 6.61. In particular, for the family $\mathcal{I}$ of Example 6.41 (3), we have for all $k \in \mathcal{I}$ that

$$\{\mathcal{I}(k) + x : x \in \mathbb{F}_q\} = \{E + y + x : x \in \mathbb{F}_q\} = \{E + x : x \in \mathbb{F}_q\},$$

so for all $a \in \mathbb{F}_\lambda$ the density $\Phi(t, \mathcal{I}_k, a)$ does not depend on k. By choosing $\mathcal{I}$ as an "averaging set" of appropriate size, we would obtain a preliminary version of Proposition 6.47.

6.5.6. Approximate variance. As in [LZ12], we now consider the "approximate variance"

$$\left(\Phi(\mathcal{I}, a) - \frac{1}{|\mathbb{F}_\lambda|}\right)^2,$$

in the sense that we replace the true expected value of the random variable $\Phi(\mathcal{I}, a)$ by the approximation given by Proposition 6.58. This corresponds to the quantity

$$\left(\Phi(t, \mathcal{I}, a) - \frac{1}{|\mathbb{F}_\lambda|}\right)^2,$$

and it is clear that bounding the latter gives a result about the distribution of $\Phi(t, \mathcal{I}, a)$, uniformly with respect to $a \in \mathbb{F}_\lambda$.

Computation in the model.

Proposition 6.62. *In the notations of Section 6.5.4, we have*

$$\sum_{a \in \mathbb{F}_\lambda} \mathbb{E}\left(\left(\Phi(\mathcal{I}, a) - \frac{1}{|\mathbb{F}_\lambda|}\right)^2\right) = \frac{1}{|\mathcal{I}|}\left(1 + O\Big(H_{\mathcal{I}}(\alpha(G_\lambda), |\mathbb{F}_\lambda|)\Big)\right).$$

Proof. As in Proposition 6.15, we have by orthogonality that

$$\begin{aligned}
\left(\Phi(\mathcal{I}, a) - \frac{1}{|\mathbb{F}_\lambda|}\right)^2 &= \left|\frac{1}{|\mathcal{I}|}\sum_{k \in \mathcal{I}} \frac{1}{|\mathbb{F}_\lambda|} \sum_{0 \neq \psi \in \widehat{\mathbb{F}}_\lambda} \psi\left(S(\mathcal{I}(k)) - a\right)\right|^2 \\
&= \frac{1}{|\mathcal{I}|^2|\mathbb{F}_\lambda|^2}\left|\sum_{0 \neq \psi \in \widehat{\mathbb{F}}_\lambda} \psi(-a) \sum_{k \in \mathcal{I}} \psi\left(S(\mathcal{I}(k))\right)\right|^2 \\
&= \frac{1}{|\mathcal{I}|^2|\mathbb{F}_\lambda|^2} \sum_{0 \neq \psi_1, \psi_2 \in \widehat{\mathbb{F}}_\lambda} \psi_1(-a)\overline{\psi_2(-a)} \\
&\quad \times \sum_{k_1, k_2 \in \mathcal{I}} \psi_1\left(S(\mathcal{I}(k_1))\right) \overline{\psi_2\left(S(\mathcal{I}(k_2))\right)}.
\end{aligned}$$

Again by orthogonality, $\sum_{a\in\mathbb{F}_\lambda}\left(\Phi(\mathcal{I},a)-|\mathbb{F}_\lambda|^{-1}\right)^2$ is equal to

$$\frac{1}{|\mathcal{I}|}\left(\frac{|\mathbb{F}_\lambda|-1}{|\mathbb{F}_\lambda|}+\frac{1}{|\mathcal{I}||\mathbb{F}_\lambda|}\sum_{0\neq\psi\in\widehat{\mathbb{F}}_\lambda}\sum_{\substack{k_1,k_2\in\mathcal{I}\\ k_1\neq k_2}}\frac{\psi(S(\mathcal{I}(k_1)))}{\psi(S(\mathcal{I}(k_2)))}\right).$$

Since

$$S(\mathcal{I}(k_1))-S(\mathcal{I}(k_2))=S(\mathcal{I}(k_1)\backslash\mathcal{I}(k_2))-S(\mathcal{I}(k_2)\backslash\mathcal{I}(k_1))$$

with $\mathcal{I}(k_1)\backslash\mathcal{I}(k_2)$, $\mathcal{I}(k_2)\backslash\mathcal{I}(k_1)$ disjoint, we have by independence

$$\sum_{\substack{k_1,k_2\in\mathcal{I}\\ k_1\neq k_2}}\mathbb{E}\left[\psi\Big(S(\mathcal{I}(k_1))-S(\mathcal{I}(k_2))\Big)\right]=\sum_{\substack{k_1,k_2\in\mathcal{I}\\ k_1\neq k_2}}\frac{\mathbb{E}(\psi(Z))^{|\mathcal{I}(k_1)\backslash\mathcal{I}(k_2)|}}{\mathbb{E}(\psi(Z))^{|\mathcal{I}(k_2)\backslash\mathcal{I}(k_1)|}}.$$

By the bound on Gaussian sums (6.1),

$$\mathbb{E}\left(\psi(Z)\right),\mathbb{E}\left(\psi(-Z)\right)\ll|\mathbb{F}_\lambda|^{-\alpha(G_\lambda)}$$

uniformly with respect to ψ, whence the result. □

Conclusion. Theorem 6.46 then follows immediately from Proposition 6.57 and Proposition 6.62.

6.5.7. Estimate and analysis of the error term. We now estimate and analyze the error term

$$V(q,G_\lambda,\mathcal{I})\ll\frac{1}{|\mathcal{I}|}+\frac{H_{\mathcal{I}}(\alpha,|\mathbb{F}_\lambda|)}{|\mathcal{I}|}+\frac{H_{\mathcal{I}}(\alpha,|\mathbb{F}_\lambda|)M_{\mathcal{I}}}{|\mathcal{I}|}\frac{E(G_\lambda,M_{\mathcal{I}})}{q^{1/2}}\tag{6.17}$$

in Equation (6.16), where $\alpha=\alpha(G_\lambda)$.

Estimates for $V(q,G_\lambda,\mathcal{I})$.

Lemma 6.63. *In the notations of Definition 6.45, we have the bounds*

$$\begin{aligned}M_{\mathcal{I}}&\leqslant|\mathcal{I}|m_{\mathcal{I}},\\ H_{\mathcal{I}}(\alpha,n)&\ll\frac{\max(h_{\mathcal{I}}(d):1\leqslant d\leqslant 2\max_{k\in\mathcal{I}}|\mathcal{I}(k)|)}{|\mathcal{I}|n^{\alpha A_{\mathcal{I}}}}\leqslant\frac{|\mathcal{I}|}{n^{\alpha A_{\mathcal{I}}}},\end{aligned}$$

where

$$1\leqslant A_{\mathcal{I}}=\min_{\substack{k_1,k_2\in\mathcal{I}\\ k_1\neq k_2}}|\mathcal{I}(k_1)\Delta\mathcal{I}(k_2)|\leqslant 2M_{\mathcal{I}}.$$

The bound for $H_{\mathcal{I}}(\alpha,n)$ can be improved for the following families:

(1) If $\mathcal{I}$ is totally ordered by some order $<$ with $\mathcal{I}(k_1)\subset\mathcal{I}(k_2)$ for $k_1<k_2$, and if $\mathcal{I}$ is determined by its cardinality, then

$$H_{\mathcal{I}}(\alpha,n)\ll\frac{1}{n^{\alpha A_{\mathcal{I}}}}.$$

In particular, this holds for the family $\mathcal{I}\subset[1\dots p]$, $\mathcal{I}(k)=[1\dots k]^e\subset\mathbb{F}_p^e\cong\mathbb{F}_q$ of Example 6.41 (1).

(2) For the family $\mathcal{I}$ of Example 6.41 (3), we have

$$H_{\mathcal{I}}(\alpha, n) \ll \frac{\max_{0\leqslant d<|E|}\big|\{y\in B_{\mathcal{I}} : |E\cap(E+y)|=d\}\big|}{n^{\alpha A_{\mathcal{I}}}}$$

where $B_{\mathcal{I}} = \{y_2 - y_2 : y_1, y_2 \in \mathcal{I} \text{ distinct}\}$. In particular, if

$$\mathcal{I} \subset \prod_{i=1}^{e}[0, p - \max_{x\in E} x_i], \tag{6.18}$$

then

$$H_{\mathcal{I}}(\alpha, n) \ll \frac{|B_E|}{n^{\alpha A_{\mathcal{I}}}},$$

where B_E is the bounding box $\mathbb{F}_q^\times \supset B_E = \prod_{i=1}^{e}[\min_{x\in E} x_i, \max_{x\in E} x_i] \supset E$. This is an improvement over the previous bound if $|\mathcal{I}| > |E|$.

Proof. The trivial bound $1 \leqslant h_{\mathcal{I}}(d) \leqslant |\mathcal{I}|^2$ gives the first bound for $H_{\mathcal{I}}(\alpha)$.

(1) Under the first hypothesis,

$$h_{\mathcal{I}}(d) = 2|\{k_1 < k_2 : |\mathcal{I}(k_2)| = |\mathcal{I}(k_1)| + d\}|.$$

for all $d \geqslant 1$. If $\mathcal{I}(k)$ is moreover is determined by its cardinality, then $h_{\mathcal{I}}(d) \leqslant 2|\mathcal{I}|$.

(2) We have

$$\begin{aligned} h_{\mathcal{I}}(d) &= \big|\{y_1, y_2 \in \mathcal{I} \text{ distinct } : |E\cap(E+(y_2-y_1))| = |E| - d/2\}\big| \\ &\ll |\mathcal{I}|\cdot\big|\{y\in B_{\mathcal{I}} : |E\cap(E+y)| = |E| - d/2\}\big|, \end{aligned}$$

whence the first statement. If $y \in \prod_{i=1}^{e}[0, p - \max_{x\in E} x_i]^e \subset \mathbb{F}_p^e \cong \mathbb{F}_q$ (to avoid reductions modulo p), then $B_E \cap (B_E + y) = \varnothing$ if $y \notin B_E$, which gives the second assertion.

□

Remark 6.64. For Lemma 6.63 (2), we may want to estimate

$$\max_{0\leqslant d<|E|}\big|\{y\in B_{\mathcal{I}} : |B_E\cap(B_E+y)| = d\}\big|$$

more precisely than by $|B_E|$. If Condition (6.18) holds, then we can bound the former by

$$\max_{0\leqslant d<|E|}\tau_e(d) \ll_{e,\varepsilon} \max_{0\leqslant d<|E|} d^\varepsilon < |E|^\varepsilon$$

for any $\varepsilon > 0$ (see [IK04, Section 1.6]). However, if we keep track of the dependency with e, this gives

$$\max_{0\leqslant d<|E|}\tau_e(d) \ll_m |E|^{\frac{1}{m}}(C\log|E|)^{\frac{e^m-1}{m}}$$

for some absolute constant $C > 0$ and any $m \geqslant 1$. If $e \to +\infty$, it is however less convenient to deal with this better bound because of the exponential in e.

Analysis of the parameters. The next lemma provides a general analysis of the error term (6.17) that we will use to handle the various examples of Theorem 6.46.

Lemma 6.65. *We have $V(q, G_\lambda, \mathcal{I}) = o(1)$ if the following three conditions hold:*

(1) $|\mathcal{I}| \to +\infty$.

(2) $H_\mathcal{I} := H_\mathcal{I}(\alpha(G_\lambda), |\mathbb{F}_\lambda|) = o(|\mathcal{I}|)$.

(3) The sum

$$M_\mathcal{I} + \frac{2\left(\log(M_\mathcal{I}/|\mathcal{I}|) + \log H_\mathcal{I}\right)}{\log(|G_\lambda||G_\lambda^\sharp|)} \tag{6.19}$$

is strictly smaller than

$$\begin{cases} \frac{1}{\beta_+(G_\lambda)}\frac{\log q}{\log|\mathbb{F}_\lambda|} - \frac{2\beta_-(G_\lambda)}{\beta_+(G_\lambda)} & : G_\lambda \text{ classical} \\ \frac{\log q}{\log d} - 1 & : G_\lambda \text{ cyclic.} \end{cases}$$

If we have

$$M_\mathcal{I} = |\mathcal{I}| \text{ and } \log H_\mathcal{I} \ll \log(|G_\lambda||G_\lambda^\sharp|), \tag{6.20}$$

this implies that

$$\begin{cases} \log|\mathbb{F}_\lambda| = o(\log q) & : G_\lambda \text{ classical} \\ \log d = o(\log q) & : G_\lambda \text{ cyclic.} \end{cases}$$

Remarks 6.66.

(1) By Lemma 6.63, $H_\mathcal{I}/|\mathcal{I}| \leqslant |\mathbb{F}_\lambda|^{-\alpha A_\mathcal{I}}$, so the second condition holds if $|\mathbb{F}_\lambda| \to +\infty$ or if $H_\mathcal{I} = O(1)$ (e.g. for the family of Lemma 6.63 (1)).

(2) If $\log|\mathbb{F}_\lambda| = o(\log q)$ and $p < |\mathbb{F}_\lambda|$, note that we must take $e \to +\infty$ (see Section 6.2.4).

Remark 6.67. The optimal size for $M_\mathcal{I}$ is therefore

$$M_\mathcal{I} \approx \frac{2\varepsilon\log q - \log(|G_\lambda|/|G_\lambda^\sharp|)}{\log(|G_\lambda||G_\lambda^\sharp|)}$$

for some $\varepsilon \in (0, 1/2)$, giving

$$V(q, G_\lambda, \mathcal{I}) \ll_\varepsilon \Big(m_\mathcal{I} + H_\mathcal{I}(\alpha(G_\lambda), |\mathbb{F}_\lambda|)\Big)\frac{\log(|G_\lambda||G_\lambda^\sharp|)}{\log q} + \frac{1}{q^{1/2-\varepsilon}}.$$

6.5.8. Removing the shifts. The general setting to obtain asymptotic equidistribution for unshifted "complete" families from Theorem 6.46 is the following:

Proposition 6.68. *Under the hypotheses of Theorem 6.46, assume furthermore that:*

(1) For some family $\mathcal{I}_2$ and functions $f_1 : \mathbb{F}_q \times \mathcal{I} \to \mathcal{I}_2$, $f_2 : \mathbb{F}_q \to \mathbb{F}_\lambda$ we have

$$S(t, \mathcal{I}'(k, x)) = S\big(t, \mathcal{I}_2(f_1(x, k))\big) + f_2(x) \quad (k \in \mathcal{I}, x \in \mathbb{F}_q).$$

(2) *There exists a function* $f_3 : \mathcal{I} \to \mathbb{R}_+$ *and a family* $\mathcal{I}_3 : \mathbb{F}_q \to \mathcal{P}(\mathbb{F}_q)$ *such that for all* $a \in \mathbb{F}_\lambda$ *and* $k \in \mathcal{I}$

$$|\{x \in \mathbb{F}_q : S(t, \mathcal{I}_2(f_1(x,k))) \equiv a\}| = |\{x \in \mathbb{F}_q : S(t, \mathcal{I}_3(x)) \equiv a\}| + O(f_3(k)).$$

In particular, if the set $\{\mathcal{I}_2(f_1(x,k)) : x \in \mathbb{F}_q\}$ *does not depend on* $k \in \mathcal{I}$*, then this holds true with* $f_3 = 0$ *and* $\mathcal{I}_3(x) = \mathcal{I}_2(f_1(x,k_0))$ *for any* $k_0 \in \mathcal{I}$.

Then, if $||f_3||_\infty/q \leqslant 1$,

$$\Phi(t, \mathcal{I}_3, a) = \frac{1}{|\mathbb{F}_\lambda|} + O\left(V(q, G_\lambda, \mathcal{I})^{1/2} + \left(\frac{|\mathbb{F}_\lambda| ||f_3||_\infty}{q}\right)^{1/2}\right)$$

uniformly with respect to $a \in \mathbb{F}_\lambda$.

In other words, we use $\mathcal{I}$ as an "averaging family" to get asymptotic equidistribution for the complete family $\mathcal{I}_3$, and the error term depends on $\mathcal{I}$. Note that the averaging over $a \in \mathbb{F}_\lambda$ gives some additional freedom in comparison with the preliminary version from Corollary 6.60.

Proof. Under Condition (1), Theorem 6.46 gives

$$\sum_{a \in \mathbb{F}_\lambda} \frac{1}{q} \sum_{x \in \mathbb{F}_q} \left(\frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}_2(f_1(x,k))) \equiv a\}|}{|\mathcal{I}|} - \frac{1}{|\mathbb{F}_\lambda|}\right)^2 \ll V(q, G_\lambda, \mathcal{I})$$

by exchanging the summation over a and x and exploiting the averaging over a. By the Cauchy-Schwarz inequality,

$$\sum_{a \in \mathbb{F}_\lambda} \left(\frac{1}{q} \sum_{x \in \mathbb{F}_q} \frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}_2(f_1(x,k))) \equiv a\}|}{|\mathcal{I}|} - \frac{1}{|\mathbb{F}_\lambda|}\right)^2 \ll V(q, G_\lambda, \mathcal{I})$$

By exchanging the summations over k and x, this is equal to

$$\sum_{a \in \mathbb{F}_\lambda} \left(\frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} \frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}_2(f_1(x,k))) \equiv a\}|}{q} - \frac{1}{|\mathbb{F}_\lambda|}\right)^2.$$

Finally, by Condition (2),

$$\sum_{a \in \mathbb{F}_\lambda} \left(\frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}_3(x)) \equiv a\}|}{q} - \frac{1}{|\mathbb{F}_\lambda|} + O\left(\frac{||f_3||_\infty}{q}\right)\right)^2 \ll V(q, G_\lambda, \mathcal{I}).$$

□

Example 6.69. For the family $\mathcal{I}$ of Example 6.41 (3), we have by Example 6.61 that:

- Condition (1) of Proposition 6.68 holds with $\mathcal{I}_2 = \mathcal{I}$, $f_1(x,k) = k + x$ and $f_2 = 0$.
- Condition (2) holds with $f_3 = 0$ and $\mathcal{I}_3 = \mathcal{I}_0 = \mathcal{I}'(0, \cdot)$, since $\{x + k : x \in \mathbb{F}_q\} = \mathbb{F}_q$ for all $k \in \mathbb{F}_q$.

6.5.9. Applications of Proposition 6.68. In the following paragraphs, we use Proposition 6.68 to prove Propositions 6.47, 6.52 and 6.55.

The general idea is to find an averaging family $\mathcal{I}$ of size large enough to get asymptotic equidistribution in (6.16), and the assumptions we make are precisely to allow that, according to Lemma 6.65.

Choice of the averaging family. When $e > 1$, we will have $\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_e$ with $\mathcal{I}_i$ of determined structure and whose size can be chosen freely in some range. Since the final bound depends only on the size of $\mathcal{I}$, we need to choose the sizes of the $\mathcal{I}_i$ to attain the optimal/desired size for $\mathcal{I}$. Note however that in the case $|\mathcal{I}| \leqslant \frac{\log q}{\log|\mathbb{F}_\lambda|}$ and $p < |\mathbb{F}_\lambda|$ (see Section 6.2.4), we have

$$|\mathcal{I}|^{1/e} \leqslant \left(\frac{\log q}{\log|\mathbb{F}_\lambda|}\right)^{1/e} = e^{1/e}\left(\frac{\log p}{\log|\mathbb{F}_\lambda|}\right)^{1/e} \leqslant 1,$$

which shows that the choice $|\mathcal{I}_1| = \cdots = |\mathcal{I}_e| \approx |\mathcal{I}|^{1/e}$ is impossible. More carefully, we take $|\mathcal{I}_1| = \cdots = |\mathcal{I}_a| \approx |\mathcal{I}|^{1/a}$ with $1 \leqslant a < e$ of optimal size given by:

Lemma 6.70. *Let $I \geqslant 1$, $p \geqslant 2$, $e \geqslant 2$ be integers, and let $0 < \delta \leqslant 1$. If $\log I \leqslant (e-1)\log(\delta p)$, there exist integers $I_1 \in [1 \dots \delta p]$ and $1 \leqslant a \leqslant e$ such that $I_1^a = I\,(1 + o(1))$ for I large enough.*

Proof. It suffices to take $I_1 = \left\lfloor I^{1/a} \right\rfloor$ with $a = \lceil \log I / \log(\delta p) \rceil \geqslant 1$ so that $I_1 \in [1 \dots \delta p]$, $a = o(I^{1/a})$,

$$I_1^a = I + O\left(aI^{1-1/a}\right) = I\left(1 + O(aI^{-1/a})\right) = I\,(1 + o(1))\,,$$

and the condition $a \leqslant e$ holds if $\log I \leqslant (e-1)\log(\delta p)$ □

Example 6.71. The condition $\log I \leqslant (e-1)\log(\delta p)$ is satisfied if $I \leqslant \log q = e \log p$ as in Lemma 6.65, up to taking p large enough if $\delta < 1$.

Shifts of subsets (Proposition 6.47). We first consider the family of Example 6.41 (3): for $\mathcal{I}, E \subset \mathbb{F}_q$, we let $\mathcal{I}(k) = E + k$ $(k \in \mathcal{I})$. Proposition 6.68 can be applied by Example 6.69.

By Lemma 6.63, since $m_{\mathcal{I}} = |E|$, the sum (6.19) is

$$\leqslant |\mathcal{I}||E| + \frac{2(\log|E| + \log|B_E| - \alpha(G_\lambda)A_{\mathcal{I}}|\mathbb{F}_\lambda|)}{\log(|G_\lambda||G_\lambda^\sharp|)}$$

if $\mathcal{I} \subset \prod_{i=1}^e [1 \dots p - \max_{x\in E} x_i]$. By Lemma 6.65, we want that for some $\varepsilon \in (0, 1/2)$,

$$|\mathcal{I}| < \frac{1}{|E|}\left(\frac{2\varepsilon \log q - 2\log|E| - 2\log|B_E|}{\beta_+(G_\lambda)\log|\mathbb{F}_\lambda|} - \frac{2\beta_-(G_\lambda)}{\beta_+(G_\lambda)} + 2\alpha(G_\lambda)A_{\mathcal{I}}\right)$$

if G_λ is classical, and

$$|\mathcal{I}| < \frac{1}{|E|}\left(\frac{2\varepsilon \log q - 2\log|E| - 2\log|B_E|}{\log d} + 2\alpha(G_\lambda)A_{\mathcal{I}} - 1\right)$$

if $G_\lambda = \mu_d(\mathbb{F}_\lambda)$.

When the sheaf is of the form $\mathcal{L}_{\chi(f)}$ with $f \neq X$, we impose that $\mathcal{I} \subset \prod_{i=1}[1 \dots p/\deg(f) - \max_{x\in E} x_i)$, so that it is $\bigcup_{k\in\mathcal{I}} \mathcal{I}(k)$-compatible by Example 4.12.

Under the assumptions of Proposition 6.47, we can choose $\mathcal{I}$ as large as possible satisfying the above conditions by Lemma 6.70.

Intervals (Proposition 6.52). Let us now analyze the family $\mathcal{I} \subset [1 \dots p]$, $k \mapsto [1 \dots k]$ of Example 6.41 (1). For the Legendre symbol, this is the case of [LZ12].

Condition (1) of Proposition 6.68 holds with $\mathcal{I}_2 = \mathcal{I}$, $f_1(x,k) = k + x$ and $f_2(x) = S(t, \mathcal{I}(x))$ since

$$S(t, [1 + x \dots k + x]) = S(t, [1 \dots k + x]) - S(t, [1 \dots x])$$

for $k \in \mathcal{I}$, $x \in \mathbb{F}_p$.

Concerning Condition (2), we use the following:

Lemma 6.72. *For any $f : \mathbb{N} \to \mathbb{C}$ and $k \in \mathbb{N}$,*

$$\sum_{x=1}^{p} f(x+k) = \sum_{x=1}^{p} f(x) + O(k||f||_\infty),$$

and the error term can be removed if f is p-periodic.

Proof. It suffices to write

$$\begin{aligned} \sum_{x=1}^{p} f(x+k) &= \sum_{x=1+k}^{p+k} f(x) = \left(\sum_{x=1}^{p} - \sum_{x=1}^{k} + \sum_{x=p+1}^{p+k} \right) f(x) \\ &= \sum_{x=1}^{p} f(x) + O(k||f||_\infty). \end{aligned}$$

□

Example 6.73. For $f(x) = \delta_{S(t,[1\dots x])\equiv a}$, we have

$$f(x+p) = \delta_{S(t,\mathbb{F}_p)+S(t,[p+1\dots x+p])\equiv a} = \delta_{S(t,[1\dots p])+S(t,[1\dots x])\equiv a},$$

and f is p-periodic if

$$S(t, [1 \dots p]) = 0 \tag{6.21}$$

(i.e. orthogonality with constant functions).

Hence, Condition (2) of Proposition 6.68 holds with $||f_3||_\infty \leqslant \max_{k\in\mathcal{I}} k$, and no error term if the trace function considered satisfies (6.21).

If the sheaf is a Kummer sheaf $\mathcal{L}_{\chi(f)}$ we impose $\max_{k\in\mathcal{I}} k < p/\deg(f)$, so that it is $\bigcup_{k\in\mathcal{I}} \mathcal{I}(k)$-compatible by Example 4.12.

We may then choose $\mathcal{I}$ as large as permitted by Lemma 6.65, i.e. $|\mathcal{I}| \approx \frac{\log p}{\log d}$, noting that for Kummer sheaves as above, we have $\frac{p}{\deg(f)} > \frac{\log p}{\log d}$ for p large enough ($\deg(f)$ being bounded independently from q).

If (6.21) is not satisfied, we need to add the error term

$$\left(\frac{|\mathbb{F}_\lambda||\mathcal{I}|}{p}\right)^{1/2} \ll \left(\frac{|\mathbb{F}_\lambda| \log p}{p \log d}\right)^{1/2}.$$

This concludes the proof of Proposition 6.52.

Remark 6.74. For Kloosterman sums, we have seen in Section 6.2.4 that it is necessary to take $e \to +\infty$ so that $V(q, G_\lambda, \mathcal{I}) = o(1)$. Hence, Proposition 6.52 does not apply to them. Unfortunately, issues arise when we try to generalize the proposition to $e > 1$. Indeed, for the family

$$\mathcal{I} \subset [1 \dots p]^e,\ \mathcal{I}(k) = \prod_{i=1}^{e} [1 \dots k_i],\ k = (k_1, \dots, k_e) \in \mathcal{I},$$

of Example 6.41 (2), we have $\mathcal{I}'(k, x) = \prod_{i=1}^{e} [1 + x_i \dots x_i + k_i]$ for all $x = (x_1, \dots, x_e) \in \mathbb{F}_q$ and as above, we can decompose $[1 + x_i \dots x_i + k_i] = [1 \dots x_i + k_i] \backslash [1 \dots x_i]$ and write

$$S(t, \mathcal{I}'(k, x)) = \sum_{a_1, \dots, a_e \in \{0,1\}} (-1)^{\sum_{i=1}^{e} (a_i+1)} S\big(t, \mathcal{I}((x_i + a_i k_i)_i)\big).$$

However, there are now "diagonal terms" including x_i and $x_j + k_j$ $(i \neq j)$, preventing us from applying Proposition 6.68 with $f_1(x, k) = x + k$ and $f_3 = 0$ as before. On the other hand, using Lemma 6.72 would give a large error $||f_3||_\infty \approx e p^{e-1}$ because small intervals of size k_i combine with large intervals of size $p - k_j$ into large "diagonal" terms. This would give an error term

$$\frac{|\mathbb{F}_\lambda| e p^{e-1}}{q} = \frac{|\mathbb{F}_\lambda| e}{p} > e$$

in the final expression for the density, which is not acceptable when $e \to +\infty$. These diagonal terms compensate each other if complete sums in one parameter of the form $S(t, E_1 \times \dots \times E_i \times \mathbb{F}_p \times E_{i+2} \times \dots \times E_e)$ vanish, for $E_i \subset \mathbb{F}_p$. Being defined as Fourier transforms of functions vanishing at 0, Kloosterman sums verify $S(\mathrm{Kl}_{n,q}, [1 \dots p]^e) = 0$, but the former sums do not vanish in general.

Small intervals with shifts of subsets (Proposition 6.55). To conclude this section, we prove Proposition 6.55 about a family of type of Example 6.41 (4), which allows to get a variant of Proposition 6.52 for $e > 1$ (in particular for Kloosterman sums).

Let us write $\mathcal{I} = \mathcal{I}_1 \times \mathcal{I}_2 \subset \mathbb{F}_p \times \mathbb{F}_p^{e-1}$ and let $E = E_2 \times \dots \times E_e$. Then

$$\begin{aligned} M_{\mathcal{I}} &= \Big| \bigcup_{(k_1, k_2) \in \mathcal{I}} [1 \dots k_1] \times (E + k_2) \Big| \\ &\leqslant \Big| \bigcup_{k_1 \in \mathcal{I}_1} [1 \dots k_1] \Big| \times |\mathcal{I}_2||E| \leqslant |\mathcal{I}||E| \end{aligned}$$

and for any $\varepsilon > 0$ we have for $d \geqslant 1$

$$\begin{aligned} h_{\mathcal{I}}(d) &\leqslant \sum_{k_1, k_1' \in \mathcal{I}_1} \Big| \{k_2, k_2' \in \mathcal{I}_2 : |k_1 - k_1'||E \Delta (E + (k_2 - k_2'))| = d\} \Big| \\ &= |\mathcal{I}_1| \sum_{1 \leqslant d' | d} \Big| \{k_2, k_2' \in \mathcal{I}_2 : |E \Delta (E + (k_2 - k_2'))| = d/d'\} \Big| \\ &\leqslant |\mathcal{I}_1||B_E||\mathcal{I}_2| \tau(d) \ll_\varepsilon (|\mathcal{I}||B_E|)^{1+\varepsilon} \end{aligned}$$

if $\mathcal{I}_2 \subset \prod_{i=2}^{e} [1, p - \max_{x \in E} x_i]$, by Lemma 6.63. As for Propositions 6.47 and 6.52, if the sheaf is a Kummer sheaf $\mathcal{L}_{\chi(f)}$, we impose $\max_{k \in \mathcal{I}_1} k < p/\deg(f)$ and $\mathcal{I}_2 \subset \prod_{i=2}^{e} [1, p/\deg(f))$, to ensure $\bigcup_{k \in \mathcal{I}} \mathcal{I}(k)$-compatibility.

The conclusion then follows by using Lemmas 6.65 and 6.70 as in Proposition 6.47.

6.6. Application of the large sieve

Finally, we use the large sieve developed in [Kow06a] and [Kow08] to obtain information about trace functions with images in the cyclotomic integers from their reductions modulo various ideals. Here, we use the fact that in the examples we consider, the trace function $t : \mathbb{F}_q \to \mathcal{O}_\lambda$ corresponding to a sheaf of $\mathcal{O}_\lambda$-modules over $\mathbb{F}_q$ actually has image in $\mathcal{O}_\alpha$ for some $\alpha \in \mathcal{O}\backslash\mathfrak{q}$ (in $\mathcal{O}$ if we do not normalize) and does not depend on λ. This holds in particular when the family forms a compatible system.

This will for example lead to zero-density estimates of the form

$$\frac{|x \in \mathbb{F}_q : \mathrm{Kl}_{n,q}(x) \in A|}{q} = o(1) \quad (q \to +\infty) \tag{6.22}$$

for "algebraic" subsets $A \subset \mathbb{Q}(\zeta_{4p})$.

The application of the large sieve to the families of hyperelliptic curves of Proposition 2.57 (and other curves over function fields) was the subject of [Kow06a] and [Kow08].

6.6.1. The large sieve for Frobenius in compatible systems. First, we state a version of the large sieve for Frobenius adapted to our needs.

Theorem 6.75. *Let $\mathbb{F}_q$ be a finite field of characteristic p, $\mathcal{O}$ be the ring of integers of a number field E and Λ be a set of prime ideals $\mathfrak{q}$ of $\mathcal{O}$ (or equivalently, valuations λ) which do not lie above p. For $L \geqslant 1$, we write $\Lambda_L = \{\mathfrak{q} \in \Lambda : N(\mathfrak{q}) \leqslant L\}$.*

Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family, where $\mathcal{F}_\lambda$ is a sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$, corresponding to a representation $\rho_\lambda : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\lambda)$ with classical monodromy group $G_\lambda \in \{\mathrm{SL}_m, \mathrm{Sp}_{2m}\}$.

For every $\lambda \in \Lambda$, let $\Omega_\lambda \subset G_\lambda$ be a conjugacy-invariant subset. Then for all $L \geqslant 1$,

$$\frac{|\{x \in U_{\mathcal{F}_\lambda}(\mathbb{F}_q) : \rho_\lambda(\mathrm{Frob}_x) \notin \Omega_\lambda \text{ for all } \lambda \in \Lambda_L\}|}{q} \ll \left(1 + \frac{L^B}{q^{1/2}}\right)\frac{1}{P(L)},$$

where

$$P(L) = \sum_{\lambda\in\Lambda_L} \frac{|\Omega_\lambda|}{|G_\lambda|} \text{ and } B = \begin{cases} \frac{2n^2+n-1}{2} & : G_\lambda = \mathrm{SL}_n(\mathbb{F}_\lambda) \\ \frac{2n^2+3n+4}{4} & : G_\lambda = \mathrm{Sp}_n(\mathbb{F}_\lambda) \ (n \text{ even}) \end{cases}$$

Proof. This is a variant of [Kow06a, Proposition 3.3] (see also [Kow08, Chapter 8]). For $\lambda, \lambda' \in \Lambda$ distinct, the product map

$$\pi_{1,q} \to G_\lambda(\mathbb{F}_\lambda) \times G_{\lambda'}(\mathbb{F}_{\lambda'})$$

is surjective by [Kow06a, Corollary 2.6] (a variant of Goursat's Lemma), which extends with no modification to the case where $\mathbb{F}_\lambda$ and $\mathbb{F}_{\lambda'}$ do not necessarily have prime order (see [MT11, Part III]). By Lemma 6.13, $B = 1 + \dim(G_\lambda) + \mathrm{rank}(G_\lambda)/2$. □

Remark 6.76. This cannot be applied to the case $G_\lambda = \mu_d(\mathbb{F}_\lambda)$ because the monodromy groups are isomorphic for all $\lambda \in \Lambda$, and we cannot exclude that the image

of the product map is the diagonal subgroup. This is related with the fact that the Kummer representation associated with a character of order d has image in $\mathbb{Z}[\zeta_d] \leqslant \mathbb{Z}[\zeta_d]_\lambda$.

Remark 6.77. A point to keep in mind is that while Kowalski only needs to consider sheaves which arise as reductions of sheaves of $\mathbb{Z}_\ell$–modules (associated to families of L-functions), our sheaves are reductions of sheaves of $\mathbb{Z}[\zeta_d]_\lambda$-modules. In particular, the size of the residue field $\mathbb{F}_\lambda$ corresponding to a prime ideal $\mathfrak{q} \trianglelefteq \mathbb{Z}[\zeta_d]$ depends on the multiplicative order of d modulo the prime ℓ above which $\mathfrak{q}$ lies (see Remark 6.1).

6.6.2. Zero-density estimates for values of trace functions in subsets.

Proposition 6.78. *Let $\mathbb{F}_q$, E, $\mathcal{O}$ and Λ be as in Theorem 6.75, and let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a family where $\mathcal{F}_\lambda$ is a sheaf of $\mathcal{O}_\lambda$-modules over $\mathbb{F}_q$. We assume that the trace function*

$$t = t_\lambda : \mathbb{F}_q \to \mathcal{O}_\lambda$$

has image in $\mathcal{O}_\mathfrak{q}$ and does not depend on λ. By reduction modulo the maximal ideal of $\mathcal{O}_\lambda$, we obtain a family $(\widehat{\mathcal{F}}_\lambda)_{\lambda\in\Lambda}$ where $\widehat{\mathcal{F}}_\lambda$ is a sheaf of $\mathbb{F}_\lambda$-modules over $\mathbb{F}_q$, for $\mathbb{F}_\lambda$ the corresponding residue field. We assume that this family is coherent, with classical monodromy groups.

For $A \subset E$ and $\lambda \in \Lambda$ corresponding to an ideal $\mathfrak{q}$, we denote by $A_\lambda \subset \mathbb{F}_\lambda$ the reduction of $A \cap \mathcal{O}_\mathfrak{q}$ modulo $\mathfrak{q}$. Then for any $L \geqslant 1$,

$$P\big(t(x) \in A\big) = \frac{|\{x \in \mathbb{F}_q : t(x) \in A\}|}{q} \ll \left(1 + \frac{L^B}{q^{1/2}}\right) \frac{1}{|\Lambda_L|\left(1 - \max_{\lambda\in\Lambda_L} \frac{|A_\lambda|}{|\mathbb{F}_\lambda|}\right)},$$

where $B > 0$ is as in Theorem 6.75. In particular, if

$$\sup_{\lambda\in\Lambda} \frac{|A_\lambda|}{|\mathbb{F}_\lambda|} < 1, \tag{6.23}$$

then

$$P\big(t(x) \in A\big) \ll \frac{1}{|\Lambda_L|} \text{ with } L = \left\lfloor q^{\frac{1}{2B}} \right\rfloor. \tag{6.24}$$

Proof. For all $\lambda \in \Lambda$, we let $\Omega_\lambda = \{g \in G_\lambda : \operatorname{tr} g \notin A_\lambda\}$, which is clearly conjugacy-invariant. By Theorem 6.75,

$$P(t(x) \in A) \leqslant \frac{|\{x \in \mathbb{F}_q : t(x) \in A_\lambda \text{ for all } \lambda \in \Lambda_L\}|}{q} \ll \left(1 + \frac{L^B}{q^{1/2}}\right) \frac{1}{P(L)},$$

where

$$P(L) = \sum_{\lambda\in\Lambda_L} \frac{|\Omega_\lambda|}{|G_\lambda|} = \sum_{\lambda\in\Lambda_L} \left(1 - \frac{|\{g \in G_\lambda : \operatorname{tr} g \in A_\lambda\}|}{|G_\lambda|}\right).$$

By Corollary 6.16,

$$P(\operatorname{tr} g \in A_\lambda) = \frac{|A_\lambda|}{|\mathbb{F}_\lambda|}\left(1 + O\left(\frac{1}{|\mathbb{F}_\lambda|^{\alpha(G_\lambda)+\alpha(A_\lambda)-1}}\right)\right) \ll \frac{|A_\lambda|}{|\mathbb{F}_\lambda|},$$

even using the trivial bound $\alpha(A_\lambda) = 0$, since $\alpha(G_\lambda) > 1$ for classical groups (see Table 6.1). □

Remark 6.79. In Theorem 6.75, we replaced the original hypothesis that the family forms a compatible system by the assumption that it is coherent. The "independence of shifts" part is not needed, but it is quite generic anyway. On the other hand, our definition of coherent families does not include an hypothesis of "independence with respect to λ" of the characteristic polynomial of the Frobenius, but this is also true for all examples that arise in applications (see also Remark 6.2).

To apply Proposition 6.78, we need lower bounds on $|\Lambda_L|$ and the local densities assumption (6.23). We treat these aspects in the next two sections.

6.6.3. Lower bound on $|\Lambda_L|$. For our applications, we will mainly consider Λ to be either:

Examples 6.80. (1) The full set of prime ideals of $\mathcal{O}$ which do not lie above p.

(2) For $m \geqslant 2$ and $C \subset (\mathbb{Z}/m)^\times$, the set of prime ideals $\mathfrak{q}$ of $\mathcal{O}$ not lying above p such that $|\mathbb{F}_\mathfrak{q}| \in C$.

(3) The restriction of these to ideals having degree 1 over $\mathbb{Q}$.

In a more general setting, we recall:

Theorem 6.81 (Chebotarev density theorem)**.** *Let F/E be a fixed finite Galois extension of number fields with Galois group G, and let $C \subset G$ be a conjugacy-stable subset. For*

$$\begin{aligned} \Lambda(C) &= \{\mathfrak{q} \trianglelefteq E \text{ prime, not ramified in } F : \mathrm{Frob}_\mathfrak{q} \in C\}, \\ \Lambda_1(C) &= \{\mathfrak{q} \in \Lambda(C) \text{ degree 1 over } \mathbb{Q}\}, \end{aligned} \tag{6.25}$$

we have $|\Lambda(C)_L| \sim |\Lambda_1(C)| \sim \frac{|C|}{|G|}\frac{L}{\log L}$ as $L \to +\infty$.

Example 6.80 (1) then corresponds to $E = F$ (and the theorem is Landau's prime ideal theorem), while (2) corresponds to $F = E(\zeta_m)$, $G \cong (\mathbb{Z}/m)^\times$.

Hence, if F and E do not depend on p, then

$$|\Lambda(C)_L| \geqslant |\Lambda_1(C)_L| \gg \frac{|C|}{|G|}\frac{L}{\log L} \quad (L \to +\infty) \tag{6.26}$$

with an absolute implicit constant, and (6.24) is thus

$$P\big(t(x) \in A\big) \ll_{C,G} \frac{\log q}{Bq^{\frac{1}{2B}}} \to 0 \quad (q \to +\infty). \tag{6.27}$$

If E and/or F depend on p (e.g. for Kloosterman sums, where $E = \mathbb{Q}(\zeta_{4p})$), we must either fix p or deal with uniformity with respect to E and F in Theorem 6.81. We discuss this situation in the following paragraphs.

Uniformity in the prime ideal theorem. The most direct result is the lower bound of Friedlander [Fri80] for the number of prime ideals, obtained by extending Chebyshev's method: for $E/\mathbb{Q}$ in a tower of normal extensions, there exists an effective constant $c > 0$ such that

$$\pi_E(L) = |\{\mathfrak{q} \trianglelefteq E : N(\mathfrak{q}) \leqslant L\}| \geqslant \frac{L}{\log(2L)^2 \Delta_E^c} - 1,$$

for $\Delta_E = |\operatorname{disc}_{\mathbb{Q}}(E)|$. If $E/\mathbb{Q}$ is normal, this can be improved to

$$\pi_E(L) \gg_\varepsilon \frac{L}{\log(2L)^{1+\varepsilon}\Delta_E^{1/2+\varepsilon}}$$

for any $\varepsilon > 0$ if $n_E = [E : \mathbb{Q}] \gg_\varepsilon 1$, by using more a precise version of Stark's estimates on the residue at 1 of the Dedekind zeta function of E. The latter is nontrivial only when $L \gg \Delta_E^{1/2+\varepsilon'}$ for some $\varepsilon' > 0$.

Uniformity in Chebotarev's density theorem. The best unconditional result is due to Lagarias-Odlyzko and Serre (see [Ser81, Section 2.2]), showing that (6.26) holds with an absolute implicit constant under the restriction $\log L \gg n_E(\log \Delta_E)^2$.

Assuming the generalized Riemann hypothesis (GRH) for the Dedekind zeta function of E, this range can be improved to $L \gg (\log \Delta_E)^{2+\varepsilon}$ for an arbitrary $\varepsilon > 0$ (see [Ser81, Section 2.4]).

Cyclotomic fields. If $E = \mathbb{Q}(\zeta_d)$, $F = E(\zeta_m)$ are cyclotomic fields, it is possible to improve the unconditional uniform range in Chebotarev's density theorem by relying on estimates for primes in arithmetic progressions.

Lemma 6.82. *For $d, m \geqslant 1$ coprime integers, let $E = \mathbb{Q}(\zeta_d)$ and $F = E(\zeta_m)$. In the notations of Theorem 6.81, for $C \subset \operatorname{Gal}(F/E) \cong (\mathbb{Z}/m)^\times$,*

$$|\Lambda(C)_L| \geqslant |\Lambda_1(C)_L| \geqslant \varphi(d)\left[\sum_{c\in C}\pi(c, dm, L) - \omega(d)\right].$$

Proof. Since every unramified rational prime of ramification index $f_\ell = \operatorname{ord}(\ell \in (\mathbb{Z}/d)^\times)$ gives rise to $\varphi(d)/f_\ell$ primes ideals with norm ℓ^{f_ℓ},

$$\begin{aligned} |\Lambda(C)_L| &\geqslant \varphi(d)\sum_{f|\varphi(d)}\frac{|\{\ell \leqslant L^{1/f} \text{ prime } : \ell \nmid \Delta_E,\ f_\ell = f,\ \ell^f \in C\}|}{f} \\ &\geqslant \varphi(d)|\{\ell \leqslant L \text{ prime } : \ell \nmid \Delta_E,\ \ell \equiv 1 \pmod d,\ \ell \in C\}|. \end{aligned}$$

If $(d, m) = 1$, then by the Chinese remainder theorem

$$|\Lambda(C)_L| \geqslant \varphi(d)\left[\sum_{c\in C}\pi(c, dm, L) - \omega(\Delta_E)\right],$$

where $\pi(a, d, L) = |\{\ell \leqslant L \text{ prime } : \ell \equiv a \pmod d\}|$ for $a \in (\mathbb{Z}/d)^\times$. □

By Dirichlet's theorem on primes in arithmetic progressions (a particular case of Theorem 6.81), we have $\pi(a, d, L) \sim \frac{L}{\varphi(d)\log L}$ as $L \to +\infty$, when d is fixed. Uniformly, one may expect

$$\pi(a, d, L) \gg \frac{L}{\varphi(d)d^\delta \log L} \tag{6.28}$$

for some $\delta \geqslant 0$, under a restriction on the range, e.g. $L \gg d^E$ for some $E \geqslant 1$. Indeed:

(1) The Siegel-Walfisz Theorem gives (6.28) with $\delta = 0$ if $\varphi(d) \ll (\log L)^A$ for some $A > 0$ (with ineffective implicit constants depending on A).

(2) The generalized Riemann hypothesis would give (6.28) with $\delta = 0$, and any $E > 2$. This holds for all a for almost all d by the Bombieri-Vinogradov theorem (and when a is fixed, for almost all $d \leqslant L^{1/2+o(1)}$ by Bombieri-Friedlander-Iwaniec and Fouvry).

(3) A conjecture of Montgomery would give (6.28) with $\delta = 0$ and any $E > 1$. By Barban-Davenport-Halberstam, Montgomery and Hooley, this holds true for almost all d and almost all a.

(4) The best unconditional result for our needs can be found in Maynard's recent article [May13, Theorem 3.3]. Using Linnik-type argument in the explicit formula for $\pi(a, d, L)$, it is shown that (6.28) holds with any $\delta > 0$ and $E = 8$.

Therefore, by Lemma 6.82,

$$|\Lambda(C)_L| \geqslant |\Lambda_1(C)_L| \gg \frac{|C|L}{(dm)^\delta \varphi(m) \log L}$$

for L large enough depending on m, d, as indicated in Table 6.4. Thus, in return of a loss in the lower bound (when $\delta > 0$), we get an improvement on the previous ranges, summarized in Table 6.3.

Consequence for Proposition 6.78.

Proposition 6.83. *Under the hypotheses of Proposition 6.78 and (6.23), with $E/\mathbb{Q}$ normal, F/E a finite Galois extension with Galois group G, $C \subset G$ a conjugacy-invariant subset and $\Lambda = \Lambda(C)$ or $\Lambda_1(C)$ as in (6.25), we have for any $\varepsilon > 0$:*

(1) If $F = E$ is normal,

$$P\big(t(x) \in A\big) \ll_\varepsilon \frac{\Delta_E^{1/2+\varepsilon} (\log q)^{1+\varepsilon}}{B^{1+\varepsilon} q^{1/(2B)}},$$

which is nontrivial when $\Delta_E^{B+\varepsilon'} = o(q)$ for some $\varepsilon' > 0$.

(2) Under GRH, if $q \gg (\log \Delta_E)^{2B+\varepsilon}$,

$$P\big(t(x) \in A\big) \ll_\varepsilon \frac{m}{|C| B q^{1/(2B)}} \ll_{m,C} \frac{\log q}{B q^{\frac{1}{2B}}}.$$

(3) Assume that $E = \mathbb{Q}(\zeta_d)$ and $F = \mathbb{Q}(\zeta_m)$ with $(d, m) = 1$. If $e \gg (dm)^{16B}$, then

$$P\big(t(x) \in A\big) \ll_\varepsilon \frac{m (dm)^\varepsilon \log q}{|C| B q^{1/(2B)}} \ll_{m,C} \frac{d^\varepsilon \log q}{B q^{\frac{1}{2B}}}.$$

The case $E = \mathbb{Q}(\zeta_{4p})$. For exponential sums, we are interested in the case $E = \mathbb{Q}(\zeta_{4p})$, with $n_E = 2(p-1)$ and $\Delta_E = 4^{2p-3} p^{2(p-2)}$. The restrictions $q \gg g(E)$ (for some $g(E) = g(n_E, \Delta_E) \geqslant 1$) of Proposition 6.83 impose limitations on the range of e, p when $q = p^e \to +\infty$, given in the last column of Tables 6.3 and 6.4.

The best results are:

Reference	Range	Limitation in (6.24)
Friedlander	$L \gg \Delta_E^c$ $(c > 0)$	$e \gg p$
Friedlander ($E/\mathbb{Q}$ normal)	$L \gg \Delta_E^{1/2}$	$e \gg p$
Lagarias-Odlyzko	$\log L \gg n_E (\log \Delta_E)^2$	$e \gg p^2 \log p$
Lagarias-Odlyzko (GRH)	$L \gg (\log \Delta_E)^{2+\varepsilon}$	$e \geqslant 2B(2+\varepsilon)$

Table 6.3: Uniformity in the prime ideal theorem and/or Chebotarev's density theorem, and the corresponding limitations in (6.24) for $E = \mathbb{Q}(\zeta_{4p})$.

Reference	δ	Range	Limitation in (6.24)
Siegel-Walfisz	0	$(\log L)^A \gg \varphi(d)\varphi(m)$	$e \gg_A (p-1)^A / \log p$
Maynard	Any $\delta > 0$	$L \gg (dm)^8$	$e \geqslant 16B$
GRH	0	$L \gg (dm)^{2+\varepsilon}$	$e \geqslant 4B(2+\varepsilon)$
Montgomery's conj.	0	$L \gg (dm)^{1+\varepsilon}$	$e \geqslant 2B(1+\varepsilon)$

Table 6.4: Uniformity in Chebotarev's density theorem for $E = \mathbb{Q}(\zeta_{4p})$ and $F = E(\zeta_m)$ for $(d, m) = 1$, with the corresponding limitations in (6.24).

Corollary 6.84. *Under the hypotheses of Proposition 6.83 with $E = \mathbb{Q}(\zeta_{4p})$ and $F = \mathbb{Q}(\zeta_m)$ with $(m, 4p) = 1$, we have*

$$P\big(t(x) \in A\big) \ll_\varepsilon \frac{m(pm)^\varepsilon \log q}{|C| B q^{1/(2B)}} \ll_{m,C} \frac{p^\varepsilon \log q}{B q^{\frac{1}{2B}}} \to 0 \quad (q = p^e \to +\infty)$$

when either

$$\text{(1) } \varepsilon > 0 \text{ and } e \geqslant 16B, \text{ or (2) under GRH, } \varepsilon = 0 \text{ and } e > 4B.$$

Remark 6.85. Had we not taken advantage of the fact that E is a cyclotomic field, the best unconditional results would have forced to take $q = p^e \to +\infty$ with $e \gg p$ (see Table 6.3), which is not a very natural condition.

6.6.4. Local densities. In this section, we finally give examples of sets $A \subset E$ for which the local densities assumption (6.23) holds.

Powers/finite index subgroups.

Proposition 6.86. *Let E, $\mathcal{O}$ be as in Proposition 6.78 and for $m \geqslant 2$, let*

$$\Lambda = \{\mathfrak{q} \trianglelefteq \mathcal{O} : |\mathbb{F}_\mathfrak{q}| \equiv 1 \pmod m\}$$

be the set of Example 6.80 (2). Then (6.23) holds for $A = E^m \subset E$.

Proof. We have $A_\lambda = \mathbb{F}_\lambda^m$, and for $|\mathbb{F}_\lambda| \geqslant 3$,

$$\frac{|A_\lambda|}{|\mathbb{F}_\lambda|} = \left(1 - \frac{1}{|\mathbb{F}_\lambda|}\right) \frac{1}{(|\mathbb{F}_\lambda^\times|, m)} + \frac{1}{|\mathbb{F}_\lambda|} < \frac{1}{m} + \frac{1}{|\mathbb{F}_\lambda|} < 1.$$

□

Definable subsets.

Proposition 6.87. *Let E, $\mathcal{O}$ and Λ be as in Proposition 6.78 and let $\varphi(x)$ be a first order formula in one variable in the language of rings (see Section 6.3.3) such that:*

(1) Neither $|\varphi(\mathbb{F}_\lambda)|$ nor $|\neg\varphi(\mathbb{F}_\lambda)|$ is bounded as $|\mathbb{F}_\lambda| \to +\infty$.

(2) For all $\lambda \in \Lambda$ corresponding to an ideal $\mathfrak{q}$, $\varphi(E) \cap \mathcal{O}_\mathfrak{q} \pmod{\mathfrak{q}} \subset \varphi(\mathbb{F}_\lambda)$.

Then (6.23) holds for $A = \varphi(E) \subset E$

Proof. Condition (2) implies that $A_\lambda \subset \varphi(\mathbb{F}_\lambda)$ for all $\lambda \in \Lambda$, so that by Theorem 6.31,

$$\limsup_{|\mathbb{F}_\lambda|\to+\infty} \frac{|A_\lambda|}{|\mathbb{F}_\lambda|} \leqslant \max C(\varphi) < 1.$$

□

Remark 6.88. Condition (2) of Proposition 6.87 holds if both

(a) $\varphi(E) \cap \mathcal{O}_\mathfrak{q} \subset \varphi(\mathcal{O}_\mathfrak{q})$, and (b) $\varphi(\mathcal{O}_\mathfrak{q}) \pmod{\mathfrak{q}} \subset \varphi(\mathbb{F}_\lambda)$

hold. Note that:

– Condition (a) holds when $\mathrm{char}(\mathbb{F}_\lambda) \gg_f 1$ if $\varphi(x) = (\exists y : f(x) = y)$ for some $f \in \mathbb{Z}[X]$. Indeed, for $x \in E$, we have $\lambda(\varphi(x)) = \deg(\varphi)\lambda(x)$ if no coefficient of φ is divisible by $\mathrm{char}(\mathbb{F}_\lambda)$.

– Condition (b) hold if φ contains no negations or implications. On the other hand, for $\varphi(x) = \neg(y : x = y^2)$, the reduction of a nonsquare in $\mathcal{O}$ may be a square in $\mathbb{F}_\lambda$.

Example 6.89. Consider the case $\varphi(x) = (\exists y : f(x) = y)$ for $f \in \mathbb{Z}[X]$. Then:

– By Proposition 6.32, Condition (1) of Proposition 6.87 holds for almost all f of fixed degree.

– Condition (2) holds if $\mathrm{char}(\mathbb{F}_\lambda) \gg_f 1$ by Remark 6.88.

Hence Proposition 6.87 applies for almost all f of fixed degree.

6.6.5. Application to Kloosterman sums. Let $n \geqslant 2$ and q be fixed. The family $(\mathcal{K}l_n)_{\lambda\in\Lambda}$ of Kloosterman sheaves of $\mathbb{Z}[\zeta_{4p}]_\lambda$-modules over $\mathbb{F}_q$ satisfies the hypotheses[6] of Proposition 6.78, for

$$\begin{aligned}\Lambda &= \{\mathfrak{q} \trianglelefteq \mathbb{Z}[\zeta_{4p}] \text{ degree } 1, \text{ above } \ell \gg_n 1, \ \ell \neq p\} \\ &\subset \{\mathfrak{q} \trianglelefteq \mathbb{Z}[\zeta_{4p}] \text{ above } \ell \gg_n 1, \ \ell \equiv 1 \pmod 4, \ (n, [\mathbb{F}_\mathfrak{q} : \mathbb{F}_\ell]) = 1 \ \ell \neq p\}\end{aligned}$$

Hence, we can apply Corollary 6.84 with the sets of Section 6.6.4.

[6] Actually, they more precisely form a compatible system, see [Kat88, Section 8.9].

Powers/finite index subgroups. By Proposition 6.86, we get:

Corollary 6.90. *For $n \geqslant 2$, $m \geqslant 2$ coprime to p and $\varepsilon > 0$, we have*

$$P\Big(\mathrm{Kl}_{n,q}(x) \in \mathbb{Q}(\zeta_{4p})^m\Big) \ll_{m,\varepsilon} \frac{p^\varepsilon \log q}{B_n q^{1/(2B_n)}} \to 0,$$

when $q = p^e \to +\infty$ with $e \geqslant 16B_n$, where $B_n = \frac{2n^2+n-1}{2}$ if n is odd and $B_n = \frac{2n^2+3n+4}{4}$ if n is even.

Remark 6.91. Note that if $\mathrm{Kl}_{2n,q}(x) \in \mathbb{R} \cap \mathbb{Q}(\zeta_{4p})$ is a square, then it is positive. However, we would need a lower bound on the above density to conclude something about signs of Kloosterman sums.

Definable subsets. Similarly, Proposition 6.86 yields:

Corollary 6.92. *Let $\varphi(x)$ be as in the first part of Proposition 6.87 (e.g. φ contains no negations or implications). Then, for $n \geqslant 2$ and $\varepsilon > 0$,*

$$P\Big(\mathrm{Kl}_{n,q}(x) \in \varphi(\mathbb{Q}(\zeta_{4p}))\Big) \ll_{\varphi,\varepsilon} \frac{p^\varepsilon \log q}{B_n q^{1/(2B_n)}} \to 0$$

when $q = p^e \to +\infty$ with $e \geqslant 16B_n$, for B_n as in Corollary 6.90.

Finally, by Example 6.89:

Corollary 6.93. *Let $n \geqslant 2$ be an integer and let $\varepsilon > 0$. For almost all $f \in \mathbb{Z}[X]$ of fixed degree, then*

$$P\Big(\mathrm{Kl}_{n,q}(x) \in f(\mathbb{Q}(\zeta_{4p}))\Big) \ll_{\varphi,\varepsilon} \frac{p^\varepsilon \log q}{B_n q^{1/(2B_n)}} \to 0$$

when $q = p^e \to +\infty$ with $e \geqslant 16B_n$, for B_n as in Corollary 6.90.

Remark 6.94. Replacing A by $q^{(n-1)/2}A$ in Proposition 6.78, these results also hold for unnormalized Kloosterman sums.

Remark 6.95. The determination of the integral monodromy groups when ℓ is large enough depending only on the rank (Theorem3.27) is vital to obtain results uniform in p. The results of Gabber and Nori would have forced to take p fixed.

Galois actions. When considering densities of the form (6.22), it is interesting to take into account the following Galois actions:

(1) For all $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/e$ and $x \in \mathbb{F}_q$,

$$\mathrm{Kl}_{n,q}(x) = \mathrm{Kl}_{n,q}(\sigma(x)).$$

The orbit of x has size $\deg(x) \in [1 \dots e]$. Fisher [Fis92, Corollary 4.25] has actually shown that if $p > (2n^{2e} + 1)^2$, the Kloosterman sums are distinct up to this action.

(2) For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^\times$ corresponding to $c \in \mathbb{F}_p^\times$ and $x \in \mathbb{F}_q^\times$, we have

$$\sigma(\mathrm{Kl}_{n,q}(x)) = \mathrm{Kl}_{n,q}(c^n x).$$

Moreover, orbits have size $|\{c^n : c \in \mathbb{F}_p^\times\}| = \frac{p-1}{(p-1,n)} \in [(p-1)/n \dots p-1]$.

In the setting of Proposition 6.87, let $A_p = \varphi(\mathbb{Q}(\zeta_{4p}))$. Since $\sigma(A_p) = A_p$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we can define an equivalence relation $\sim$ on

$$\{x \in \mathbb{F}_q^\times : \mathrm{Kl}_{n,q}(x) \in A_p\}$$

generated by $x \sim c^n x$ for all $c \in \mathbb{F}_p^\times$, $x \in \mathbb{F}_q^\times$, and we have

$$\begin{aligned} |\{x \in \mathbb{F}_q^\times : \mathrm{Kl}_{n,q}(x) \in A_p\}/\sim| &= \frac{|\{x \in \mathbb{F}_q^\times : \mathrm{Kl}_{n,q}(x) \in A_p\}|(p-1,n)}{p-1} \\ &\ll_n \frac{|\{x \in \mathbb{F}_q^\times : \mathrm{Kl}_{n,q}(x) \in A_p\}|}{p-1}. \end{aligned}$$

By Corollary 6.92,

$$|\{x \in \mathbb{F}_q^\times : \mathrm{Kl}_{n,q}(x) \in A_p\}/\sim| \ll_{n,\varepsilon} \frac{q^{1-1/(2B)}\log q}{Bp^{1-\varepsilon}}.$$

Remark 6.96. For any $\varepsilon' > 0$, the right-hand side is

$$\ll_{\varepsilon'} p^{e(1-1/(2B)+\varepsilon')-1+\varepsilon},$$

which goes to 0 when $p \to +\infty$ and $e < (1-\varepsilon)\left(1 - \frac{1}{2B} + \varepsilon'\right)^{-1}$. Since $\frac{2B}{2B-1} \in (1,2)$, the latter can hold only when $e = 1$. Unfortunately, our estimate on the number of primes ideals in $\mathbb{Q}(\zeta_{4p})$ from Section 6.6.3 requires to take $e > 1$. If the result could be extended to $e = 1$, the above would show that for p large enough, there is no $x \in \mathbb{F}_p^\times$ such that $\mathrm{Kl}_{n,p}(x) \in \varphi(\mathbb{Q}(\zeta_{4p}))$.

Remark 6.97. To take into account the first action, we should evaluate the weighted sum

$$\frac{1}{q}\sum_{x \in \mathbb{F}_q} \frac{\delta_{\mathrm{Kl}_{n,q}(x) \in A}}{\deg(x)},$$

but it is not clear how to handle that with our formalism.

Appendix A

Sums of products and polynomial bounds

In Proposition 4.4, we proved that if $\mathcal{F}$ is a geometrically irreducible ℓ-adic sheaf over $\mathbb{F}_q$ of rank r and conductor c associated to a trace function $t : \mathbb{F}_q \to \mathbb{C}$, then for all $L \geqslant 1$ and $a_1, \dots, a_L \in \mathbb{F}_q$ we have

$$\sum_{x \in \mathbb{F}_q} t(x + a_1) \dots t(x + a_L) = \mathrm{tr}(\mathrm{Frob}_q \mid H_c^2(\mathbb{A}^1 \times \overline{\mathbb{F}}_q, \mathcal{F}_L)) + O(r^L L c^2 \sqrt{q})$$

for $\mathcal{F}_L = \bigotimes_{1 \leqslant i \leqslant L} [+a_i]^* \mathcal{F}$. Note that the error term is exponential in L, unless $r = 1$.

In Remark 4.5, we were wondering whether it is possible to obtain an error term polynomial in L when $r > 1$, using the same technique as for Proposition 4.4 (applying the Grothendieck-Lefschetz trace formula and Deligne's estimate (Theorem 2.28). We show in this appendix that the answer is negative.

First reduction. First we need to avoid the exponentials in L arising from the passages:

- from the products of trace functions to the trace function of the product of the sheaves (see (4.6)).
- from the sum over $U_{\mathcal{F}_L}(\mathbb{F}_q)$ to the sum over $\mathbb{F}_q$.

To do so, we need to assume that $\mathcal{F}$ is lisse on $\mathbb{A}^1 \times \mathbb{F}_q$, and we have

$$\sum_{x \in \mathbb{F}_q} t(x + a_1) \dots t(x + a_L) = \mathrm{tr}(\mathrm{Frob}_q \mid H_c^2(\mathbb{A}^1 \times \overline{\mathbb{F}}_q, \mathcal{F}_L)) + O(h_1(L) \sqrt{q})$$

for $h_i(L) = \dim H_c^i(\mathbb{A}^1 \times \overline{\mathbb{F}}_q, \mathcal{F}_L)$. Hence the question becomes: when do we have a bound

$$h_1(L) \leqslant f_{r,c}(L)$$

with $f_{r,c}$ polynomial in L, assuming that $\mathcal{F}$ is lisse on $\mathbb{A}^1 \times \mathbb{F}_q$?

Remark A.1. A variant of the question would be to ask for an error term of the form $g_{r,c}(L) + f_{r,c}(L)\sqrt{q}$ with $f_{r,c}$ polynomial in L (but not necessarily $g_{r,c}$). However, this is more difficult to treat, since we cannot anymore assume that $\mathcal{F}$ is lisse on $\mathbb{A}_1$, and thus has a rather rigid structure (see below).

Lisse ℓ-adic sheaves on the affine line. First, we gather some properties of a geometrically irreducible ℓ-adic sheaf $\mathcal{F}$ over $\mathbb{F}_q$ that is lisse on $\mathbb{A}^1 \times \mathbb{F}_q$.

Lemma A.2. *(1) If* $\mathrm{Swan}_\infty(\mathcal{F}) = 0$, *then* $\mathcal{F}$ *is geometrically trivial.*

(2) If $\mathrm{Swan}_\infty(\mathcal{F}) = 1$, *then* $\mathcal{F}$ *is geometrically isomorphic to a nontrivial Artin-Schreier sheaf* $\mathcal{L}_\psi$.

(3) *If $\mathcal{F}$ is nontrivial, then* $\mathrm{Swan}_\infty(\mathcal{F}) \geqslant \mathrm{rank}(\mathcal{F})$ *with equality if and only if $\mathcal{F}$ is geometrically isomorphic to a nontrivial Artin-Schreier sheaf $\mathcal{L}_\psi$.*

Proof. The first two results follow from Lemma 4.37 (2),(4), and the third one from [FKM13, Lemma 5.4(1)], also using the Euler-Poincaré formula (Theorem 2.37). □

Lemma A.3. *$\mathcal{F}$ has a unique break at ∞.*

Proof. This argument appears in [FKM13, Lemma 5.4]: the geometric étale fundamental group $\pi_{1,q}^{\mathrm{geom}}$ is topologically generated by the inertia subgroups I_x for $x \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$. Since $\mathcal{F}$ is lisse on $\mathbb{A}^1 \times \overline{\mathbb{F}}_q$, the restrictions of the corresponding representation to the inertia subgroups I_x for $x \in \mathbb{A}^1(\overline{\mathbb{F}}_q)$ are trivial. Since $\mathcal{F}$ is irreducible, it follows that it is irreducible as a representation of the inertia subgroup I_∞. Hence, it has a unique break at ∞. □

Hence, we let $t \in \mathbb{R}_{\geqslant 0}$ be the unique break of $\mathcal{F}$ at ∞.

Lemma A.4. *(1) If $t < 1$, then $\mathcal{F}$ is geometrically trivial.*

(2) We have $\mathrm{Swan}_\infty(\mathcal{F}) = 1$ *if and only if $t = 1$, if and only if $\mathcal{F}$ is geometrically isomorphic to a nontrivial Artin-Schreier sheaf $\mathcal{L}_\psi$.*

Proof. (1) If $t = 0$, this is Lemma A.2 (1). More generally, for $t < 1$, this is Lemma A.2 (3).

(2) By Lemma A.2 (2), $\mathrm{Swan}_\infty(\mathcal{F}) = 1$ if and only if $\mathcal{F}$ is geometrically isomorphic to a nontrivial Artin-Schreier sheaf, which holds true if and only if $t = 1$ by Lemma A.2 (3).

□

Conclusion. By Lemma A.2, we can assume that $\mathrm{Swan}_\infty(\mathcal{F}) \geqslant 2$ and $t > 1$. Note that the break decompositions at ∞ of $[+a]^*\mathcal{F}$ have the same breaks and multiplicities for all $a \in \mathbb{F}_q$.

For every $L \geqslant 1$, we decompose $\mathcal{F}_L = \mathcal{F}^{\otimes L}$ as a sum of geometrically irreducible components $\mathcal{G}_i$ lisse on $\mathbb{A}^1$. We distinguish several cases, using Lemma A.4:

(1) $\mathrm{Swan}_\infty(\mathcal{G}_i) = 0$ with unique break 0. Then $\mathcal{G}_i$ is geometrically trivial.

(2) $\mathrm{Swan}_\infty(\mathcal{G}_i) = 1$ with unique break 1. Then $\mathcal{G}_i$ is geometrically isomorphic to a nontrivial Artin-Schreier sheaf.

(3) $\mathrm{Swan}_\infty(\mathcal{G}_i) \geqslant 2$ with unique break $s > 1$. By Lemma A.2, we have $\mathrm{Swan}_\infty(\mathcal{G}_i) \geqslant \mathrm{rank}(\mathcal{G}_i) + 1$, i.e. $s \geqslant 1 + \frac{1}{\mathrm{rank}(\mathcal{G}_i)}$. We furthermore distinguish the cases:

   a) $1 < s < t$,

   b) $s = t$.

We have the geometric

$$\mathcal{F}_L \cong h_2(L)1 \bigoplus \left(\bigoplus_{i=1}^{n_1(L)} \mathcal{L}_i^{(L)} \right) \bigoplus \left(\bigoplus_{j=1}^{2} \bigoplus_{i=1}^{m_j(L)} \mathcal{G}_i^{(j,L)} \right),$$

where 1 is the trivial representation, $\mathcal{L}_i^{(L)}$ is a nontrivial Artin-Schreier sheaf, $\mathcal{G}_i^{(1,L)}$ is of type (3a) and $\mathcal{G}_i^{(2,L)}$ is of type (3b). For $j = 1, 2$ and $1 \leqslant i \leqslant m_j(L)$, let $d_j(L) = \sum_{i=1}^{m_j(L)} \dim \mathcal{G}_i^{(j,L)}$ and $s_i^{(L)} > 1$ be the unique break of $\mathcal{G}_i^{(j,L)}$. We have

$$\begin{aligned} \mathrm{Swan}_\infty(\mathcal{F}_L) &= n_1(L) + \sum_{i=1}^{m_1(L)} s_i^{(L)} \dim \mathcal{G}_i^{(1,L)} + td_2(L) \\ &\geqslant n_1(L) + d_1(L) + td_2(L). \end{aligned}$$

Since $r^L = \mathrm{rank}(\mathcal{F}_L) = h_2(L) + n_1(L) + \sum_{j=1}^2 d_j(L)$, it follows by the Euler-Poincaré formula (Theorem 2.37) that

$$\begin{aligned} h_1(L) &= h_2(L) - r^L + \mathrm{Swan}_\infty(\mathcal{F}_L) \\ &= \mathrm{Swan}_\infty(\mathcal{F}_L) - n_1(L) - \sum_{j=1}^{2} d_j(L) \\ &\geqslant (t-1)d_2(L) \end{aligned}$$

If $f_{r,c}(L) \geqslant h_1(L)$ for $f_{r,c}$ polynomial in L, this implies that $d_2(L) = o(r^L)$, or equivalently $n_1(L) + d_1(L) + h_2(L) \sim r^L$. But at rank $L+1$ we have

$$\mathcal{F}_{L+1} = (h_2(L)\mathcal{F}) \bigoplus \left(\bigoplus_{i=1}^{n_1^{(L)}} \left(\mathcal{L}_i^{(L)} \otimes \mathcal{F} \right) \right) \bigoplus \left(\bigoplus_{j=1}^{2} \bigoplus_{i=1}^{m_j(L)} \left(\mathcal{G}_i^{(j,L)} \otimes \mathcal{F} \right) \right)$$

and note that by Proposition 2.23:

- $\mathcal{F}$ has unique break at t, so it is of type (3b).
- $\mathcal{L}_i^{(L)} \otimes \mathcal{F}$ has unique break at t, so it is of type (3b).
- $\mathcal{G}_i^{(1,L)} \otimes \mathcal{F}$ has unique break at t, so it is of type (3b).
- $\mathcal{G}_i^{(2,L)} \otimes \mathcal{F}$ has all breaks $\leqslant t$.

Therefore

$$h_2(L+1) + n_1(L+1) + d_1(L+1) \leqslant rd_2(L),$$

so

$$\begin{aligned} 1 = \lim_{L\to\infty} \frac{n_1(L+1) + d_1(L+1) + h_2(L+1)}{r^{L+1}} &\leqslant \lim_{L\to\infty} \frac{rd_2(L)}{r^{L+1}} \\ &= \lim_{L\to\infty} \frac{d_2(L)}{r^L} = 0, \end{aligned}$$

a contradiction. This shows as desired that we cannot have a bound $h_1(L) \leqslant f_{r,c}(L)$ with f polynomial in L and $\mathcal{F}$ lisse on $\mathbb{A}^1$, unless $\mathrm{rank}(\mathcal{F}) = 1$ or $\mathcal{F}$ is geometrically trivial.

Remark A.5. The hypothesis that $\mathcal{F}$ is irreducible is important. For example, take $\mathcal{F} = \mathcal{L}_{\psi_1} \oplus \mathcal{L}_{\psi_2}$ for $\psi_1 \neq \psi_2$ two additive characters of $\mathbb{F}_p$, say $\psi_i(x) = e(b_i x/p)$ for $b_i \in \mathbb{F}_p$. Then, from the decomposition

$$\mathcal{F}_L = \bigoplus_{a=0}^{L} \binom{L}{a} \mathcal{L}_{\psi_1}^{\otimes a} \otimes \mathcal{L}_{\psi_2}^{\otimes (L-a)} = \bigoplus_{a=0}^{L} \binom{L}{a} \mathcal{L}_{e((ab_1+(L-a)b_2)x/p)},$$

we find that $\mathrm{rank}(\mathcal{F}_L) = 2^L$ and

$$\begin{aligned}
\mathrm{Swan}_\infty(\mathcal{F}_L) &= \sum_{a=0}^{L} \binom{L}{a} \delta_{a \not\equiv \frac{-Lb_2}{b_1-b_2} \pmod p}, \\
h_2(L) &= \sum_{a=0}^{L} \binom{L}{a} \delta_{a \equiv \frac{-Lb_2}{b_1-b_2} \pmod p}, \text{ but} \\
h_1(L) &= h_2(L) - \mathrm{rank}(\mathcal{F}_L) + \mathrm{Swan}_\infty(\mathcal{F}_L) = 0.
\end{aligned}$$

Bibliography

[Asc84] Michael Aschbacher. On the maximal subgroups of the finite classical groups. *Inventiones mathematicae*, 76(3):469–514, 1984.

[BC06] Jean Bourgain and Mei-Chu Chang. A Gauss sum estimate in arbitrary finite fields. *Comptes Rendus Mathematique*, 342(9):643–646, 2006.

[BK03] Jean Bourgain and Sergei Konyagin. Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order. *Comptes Rendus Mathématiques*, 337(2):75–80, 2003.

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

[BSD59] Bryan Birch and Peter Swinnerton-Dyer. Note on a problem of Chowla. *Acta Arithmetica*, 5(4):417–423, 1959.

[Car72] Roger W. Carter. *Simple groups of Lie type*. John Wiley & Sons, 1972.

[CI00] John B. Conrey and Henryk Iwaniec. The cubic moment of central values of automorphic L-functions. *Annals of Mathematics. Second Series*, 151(3):1175–1216, 2000.

[Coh70] Stephen Cohen. The distribution of polynomials over finite fields. *Acta Arithmetica*, 17(3):255–271, 1970.

[CvdDM92] Zoé Chatzidakis, Lou van den Dries, and Angus Macintyre. Definable sets over finite fields. *Journal für die reine und angewandte Mathematik*, 427:107–136, 1992.

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

[Del69] Pierre Deligne. Formes modulaires et représentations ℓ-adiques. *Séminaire Bourbaki*, 11:139–172, 1968-1969.

[Del74] Pierre Deligne. La conjecture de Weil. I. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 43(1):273–307, 1974.

[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. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 52(1):137–252, 1980.

[DS94] Persi Diaconis and Mehrdad Shahshahani. On the eigenvalues of random matrices. *Journal of Applied Probability*, 31:49–62, 1994.

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

[FI85] John B. Friedlander and Henryk Iwaniec. Incomplete Kloosterman sums and a divisor problem. *Annals of Mathematics*, 121(2):319–344, 1985.

[Fis92] Benji Fisher. Distinctness of Kloosterman sums. In *p-adic methods in number*

theory and algebraic geometry, volume 133 of *Contemporary Mathematics*, pages 81–102. American Mathematical Society, 1992.

[Fis95] Benji Fisher. Kloosterman sums as algebraic integers. *Mathematische Annalen*, 301(1):485–505, 1995.

[FK01] Étienne Fouvry and Nicholas M. Katz. A general stratification theorem for exponential sums, and applications. *Journal für die reine und angewandte Mathematik*, 2001(504):115–166, 2001.

[FKM13] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. An inverse theorem for Gowers norms of trace functions over $\mathbb{F}_p$. *Mathematical Proceedings of the Cambridge Philosophical Society*, 155:277–295, 2013.

[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. *Geometric and Functional Analysis*, 25(2):580–657, 2015.

[FKM15b] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. A study in sums of products. *Philosophical Transactions of the Royal Society of London A*, 373(2040), 2015.

[FKM+16] Étienne Fouvry, Emmanuel Kowalski, Philippe Michel, Chander Sekhar Raju, Joël Rivat, and Kannan Soundararajan. On short sums of trace functions. May 2016. http://arxiv.org/abs/1508.00512.

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

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

[Fri80] John B. Friedlander. Estimates for prime ideals. *Journal of Number Theory*, 12(1):101–105, 1980.

[Fu10] Lei Fu. Calculation of ℓ-adic local Fourier transformations. *Manuscripta mathematica*, 133(3-4):409–464, 2010.

[Gar07] Moubariz Z. Garaev. An explicit sum-product estimate in $\mathbb{F}_p$. *International Mathematics Research Notices*, 2007.

[GLS94] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, 1994.

[Gor82] Daniel Gorenstein. *Finite simple groups: an introduction to their classification*. University Series in Mathematics. Springer, 1982.

[GT92] R. Gow and Maria Chiara Tamburini. Generation of $\mathrm{SL}(n, p)$ by two Jordan block matrices. *Bollettino dell'Unione Matematica Italiana*, 7(6A):346–357, 1992.

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

Springer, 2005.

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

[HBK00] David R. Heath-Brown and Sergei Konyagin. New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum. *The Quarterly Journal of Mathematics*, 51(2):221–235, 2000.

[Hum80] James E. Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer, 1980.

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

[Kat80] Nicholas M. Katz. *Sommes exponentielles*, volume 79 of *Astérisque*. Société mathémathique de France, 1980.

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

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

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

[Kat01] Nicholas M. Katz. Sums of Betti numbers in arbitrary characteristic. *Finite fields and their Applications*, 7(1):29–44, 2001.

[Kat09] Nicholas M. Katz. *Twisted L-functions and monodromy*, volume 150 of *Annals of Mathematics Studies*. Princeton University Press, 2009.

[Kat12] Nicholas M. Katz. Report on the irreducibility of L-functions. In Dorian Goldfeld, Jay Jorgenson, Peter Jones, Dinakar Ramakrishnan, Kenneth Ribet, and John Tate, editors, *Number Theory, Analysis and Geometry*, pages 321–353. Springer, 2012.

[Kim97a] Dae San Kim. Gauss sums for general and special linear groups over a finite field. *Archiv der Mathematik*, 69(4):297–304, 1997.

[Kim97b] Dae San Kim. Gauss sums for $O^-(2n, q)$. *Acta Arithmetica*, 78(1):75–89, 1997.

[Kim98a] Dae San Kim. Gauss sums for $O(2n + 1, q)$. *Finite Fields and Their Applications*, 4(1):62–86, 1998.

[Kim98b] Dae San Kim. Gauss sums for symplectic groups over a finite field. *Monatshefte für Mathematik*, 126(1):55–71, 1998.

[KL90a] William M. Kantor and Alexander Lubotzky. The probability of generating a finite classical group. *Geometriae Dedicata*, 36(1):67–87, 1990.

[KL90b] Peter B. Kleidman and Martin W. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Notes*. Cambridge University Press, 1990.

[KL96] Dae San Kim and In-Sok Lee. Gauss sums for $O^+(2n, q)$. *Acta Arithmetica*, 78(1):75–89, 1996.

[KMS16] Emmanuel Kowalski, Philippe Michel, and William F. Sawin. Bilin-

ear forms with Kloosterman sums and applications. January 2016. http://arxiv.org/abs/1511.01636.

[Kor89] Nikolai M. Korobov. *Exponential sums and their applications*, volume 80 of *Mathematics and its Applications*. Springer, 1989.

[Kow06a] Emmanuel Kowalski. The large sieve, monodromy and zeta functions of curves. *Journal für die reine und angewandte Mathematik*, 601:29–69, 2006.

[Kow06b] Emmanuel Kowalski. On the rank of quadratic twists of elliptic curves over function fields. *International Journal of Number Theory*, 62(2), 2006.

[Kow06c] Emmanuel Kowalski. Weil numbers generated by other Weil numbers and torsion field of abelian varieties. *Journal of the London Mathematical Society*, 74(2):273–288, 2006.

[Kow07] Emmanuel Kowalski. Exponential sums over definable subsets of finite fields. *Israel Journal of Mathematics*, 160(1):219–251, 2007.

[Kow08] Emmanuel Kowalski. *The large sieve and its applications: Arithmetic geometry, random walks and discrete groups*, volume 175 of *Cambridge Tracts in Mathematics*. Cambridge University Press, 2008.

[Kow11] Emmanuel Kowalski. Explicit multiplicative combinatorics. Unpublished note, https://people.math.ethz.ch/~kowalski/combinatorics.pdf, October 2011.

[KR15] Lars Kindler and Kay Rülling. *Introductory course on ℓ-adic sheaves and their ramification theory on curves*. September 2015. http://arxiv.org/abs/1409.6899.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues and monodromy*, volume 45 of *Colloquium Publications*. American Mathematical Society, 1999.

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

[Lam13] Youness Lamzouri. The distribution of short character sums. *Mathematical Proceedings of the Cambridge Philosophical Society*, 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.

[Lar95] Michael Larsen. Maximality of Galois actions for compatible systems. *Duke Mathematical Journal*, 80(3):601–630, 1995.

[Lie85] Martin W. Liebeck. On the orders of maximal subgroups of the finite classical groups. *Proceedings of the London Mathematical Society*, 3(3):426–446, 1985.

[LP11] Michael Larsen and Richard Pink. Finite subgroups of algebraic groups. *Journal of the American Mathematical Society*, 24(4):1105–1158, 2011.

[LS74] Vicente Landazuri and Gary M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *Journal of Algebra*, 32(2):418–443, 1974.

[LS98] Martin W. Liebeck and Gary M. Seitz. On the subgroup structure of classical groups. *Inventiones mathematicae*, 134(2):427–453, 1998.

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

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

[May13] James Maynard. On the Brun-Titchmarsh theorem. *Acta Arith.*, 157(3):249–296, 2013.

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

[Mil12] James S. Milne. Reductive groups, 2012. Available at http://www.jmilne.org/math/.

[Mil13] James S. Milne. Lie algebras, algebraic groups, and Lie groups, 2013. Available at http://www.jmilne.org/math/.

[MT11] Gunther Malle and Donna Testerman. *Linear algebraic groups and finite groups of Lie type*, volume 133 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2011.

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

[MZ14] Kit-Ho Mak and Alexandru Zaharescu. On the distribution of the number of points on a family of curves over finite fields. *Journal of Number Theory*, 140:277–298, July 2014.

[Nor87] Madhav V. Nori. On subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$. *Inventiones mathematicae*, 88(2):257–275, 1987.

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

[Pro90] Robert A. Proctor. A Schensted algorithm which models tensor representations of the orthogonal group. *Canadian Journal of Mathematics. Journal Canadien de Mathématiques*, 42(1):28–49, 1990.

[PV04] Luc Pastur and Vladimir Vasilchuk. On the moments of traces of matrices of classical groups. *Communications in Mathematical Physics*, 252, 2004.

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

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

[Rib76] Kenneth A. Ribet. Galois action on division points of abelian varieties with real multiplications. *American Journal of Mathematics*, 98(3):751–804, 1976.

[Rob96] Derek Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer, 1996.

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

[Sei88] Gary M. Seitz. Representations and maximal subgroups of finite groups of Lie type. *Geometriae Dedicata*, 25(1-3):391–406, 1988.

[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.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de chebotarev. *Publications Mathématiques de l'IHÉS*, 54:123–201, 1981.

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

[Shp91] Igor Shparlinski. Estimates of Gaussian sums. *Matematicheskie Zametki*, 50(1):122–130, 1991.

[SS97] Jan Saxl and Gary M. Seitz. Subgroups of algebraic groups containing regular unipotent elements. *Journal of the London Mathematical Society*, 55(02):370–386, 1997.

[ST90] Gary M. Seitz and Donna M. Testerman. Extending morphisms from finite to algebraic groups. *Journal of Algebra*, 131(2):559–574, 1990.

[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 $\mathrm{SO}(2n + 1)$. *Journal of Combinatorial Theory, Series A*, 53(2):239–256, 1990.

[Sup95] Irina D. Suprunenko. Irreducible representations of simple algebraic groups containing matrices with big Jordan blocks. *Proceedings of the London Mathematical Society*, 3(2):281–332, 1995.

[Sza09] Tamás Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2009.

[TZ13] Donna Testerman and Alexandre Zalesski. Irreducibility in algebraic groups and regular unipotent elements. *Proceedings of the American Mathematical Society*, 141(1):13–28, 2013.

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

[Wag77] Ascher Wagner. The faithful linear representations of least degree of S_n and A_n over a field of odd characteristics. *Mathematische Zeitschrift*, 154:103–114, 1977.

[Wan95] Daqing Wan. Minimal polynomials and distinctness of Kloosterman sums. *Finite Fields and Their Applications*, 1(2):189–203, 1995.

[Was97] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1997.

[Wil09] Robert A. Wilson. *The finite simple groups*, volume 251 of *Graduate Texts in Mathematics*. Springer, 2009.