# Distribution questions for trace functions with values in cyclotomic integers and their reductions

Corentin Perret-Gentil

Abstract. We consider $\ell$-adic trace functions over finite fields taking values in cyclotomic integers, such as characters and exponential sums. Through ideas of Deligne and Katz, we explore probabilistic properties of the reductions modulo a prime ideal, exploiting especially the determination of their integral monodromy groups. In particular, this gives a generalization of a result of Lamzouri-Zaharescu on the distribution of short sums of the Legendre symbol reduced modulo an integer to all multiplicative characters and to hyper-Kloosterman sums.

## Contents



## 1. Introduction

The distribution of normalized exponential sums over finite fields in compact subsets of the complex numbers is an interesting question that has been studied by numerous authors such as Kummer, Hasse, Heath-Brown and Patterson (cubic Gauss sums), Deligne (Gauss sums), Katz (hyper-Kloosterman sums), or Duke, Friedlander and Iwaniec (Salié sums).

For example, Katz [Kat88] showed that for $n \geqslant 2$ and $q$ an odd prime power, the normalized hyper-Kloosterman sums

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

for $e(z) = e^{2i\pi z}$ $(z \in \mathbb{C})$, are equidistributed as $q \to +\infty$ in $\mathrm{tr}\,\mathrm{SU}_n(\mathbb{C})$ if $n$ is odd (resp. $\mathrm{tr}\,\mathrm{USp}_n(\mathbb{C})$ if $n$ is even), with respect to the pushforward of the Haar measure. This result builds on Deligne's construction of the Kloosterman sums as $\ell$-adic trace functions on $\mathbb{P}^1_{\mathbb{F}_q}$ [Del80], through Deligne's

Date: October 2016. Revised June 2017.
2010 *Mathematics Subject Classification.* 11L05, 11T24, 11N64, 14F20, 60G50.

general equidistribution theorem and Katz's determination of monodromy groups.

1.1. **Exponential sums in cyclotomic fields.** Exponential sums are usually considered as complex numbers, but in general they 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 $d$th 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 $\mathbb{F}_p$ by taking sums, products or convolutions (e.g. discrete Fourier transform), will take values in $\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_{p-1}) = \mathbb{Q}(\zeta_{p(p-1)})$.

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

1.2. **Exponential sums in cyclotomic integers.** A step further is to consider exponential sums, and functions $f : \mathbb{F}_q \to \mathbb{C}$ formed from them, as having values in cyclotomic integers, say $\mathcal{O} = \mathbb{Z}[\zeta_d]$ for some $d \geqslant 1$. This holds true for characters and this property is again stable by the operations we mentioned above.

Wan [Wan95] adopted such a point of view and studied the minimal polynomial of Kloosterman sums, improving some of Fisher's results.

Up to localizing[1], we can also consider normalizations: indeed, by the evaluation of quadratic Gauss sums, $\sqrt{p} \in \mathbb{Z}[\zeta_{4p}]$, so for example $\mathrm{Kl}_{n,q}(\mathbb{F}_q^\times) \subset \mathbb{Z}[\zeta_{4p}]_{q^{(n-1)/2}}$.

1.3. **Reductions of exponential sums in residue fields.** For any nonzero prime ideal $\mathfrak{l} \trianglelefteq \mathcal{O}$ (possibly restricted to be above a large enough prime to handle normalizations), we can then study the reductions modulo $\mathfrak{l}$ of exponential sums and related functions $f : \mathbb{F}_q \to \mathcal{O}$ in the corresponding residue field $\mathbb{F}_\mathfrak{l} = \mathcal{O}/\mathfrak{l} \cong \mathcal{O}_\mathfrak{l}/\mathfrak{l}\mathcal{O}_\mathfrak{l}$.

In the case of Kloosterman sums, if $\mathfrak{l}$ is a prime ideal of $\mathcal{O} = \mathbb{Z}[\zeta_{4p}]$ above an odd prime $\ell \neq p$, then we have the reduction

$$\mathrm{Kl}_{n,q} : \mathbb{F}_q^\times \to \mathcal{O}_\mathfrak{l} \to \mathbb{F}_\mathfrak{l}.$$

Distribution questions concerning the values in $\mathbb{F}_\mathfrak{l}$ as $q \to +\infty$ can then be examined. For example, Lamzouri and Zaharescu [LZ12] studied the distribution of short sums of the Legendre symbol $\chi_p : \mathbb{F}_p \to \{\pm 1\}$ reduced modulo an integer $\ell \geqslant 2$. Specifically, they show that

$$\frac{|\{1 \leqslant k \leqslant p : \sum_{x=1}^k \chi_p(x) \equiv a \pmod{\ell}\}|}{p} = \frac{1}{\ell} + O\left(\left(\frac{\ell}{\log p}\right)^{\frac{1}{2}}\right)$$

[1] For $\alpha \in \mathcal{O}$ (resp. a prime ideal $\mathfrak{l} \trianglelefteq \mathcal{O}$), we denote by $\mathcal{O}_\alpha$ (resp. $\mathcal{O}_\mathfrak{l}$) the localization at $\alpha$ (resp. at $\mathfrak{l}$).

uniformly with respect to $a \in \mathbb{Z}/\ell$. A probabilistic model with sums of independent random variables uniformly distributed in $\{\pm 1\}$ is used; its accuracy is proved through a bound derived from the Riemann hypothesis for curves over finite fields.

1.4. **Trace functions over finite fields.** Additive and multiplicative characters of finite fields, hyper-Kloosterman sums and more general exponential sums are particular examples of trace functions of constructible middle-extension sheaves of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, as they appear in particular in the works of Katz (see for example [Kat88] and [Kat90]), and more recently in the series of papers by Fouvry, Kowalski, Michel and others (see [FKM14], [Pol14, Section 6] or [PG16] for surveys).

Herein, we will mainly consider:

- Multiplicative characters $\chi : \mathbb{F}_q \to \mathbb{Z}[\zeta_d]$ of order $d$, eventually composed with a rational polynomial, realized as trace functions of *Kummer sheaves*, with $\chi(0) = \chi(\infty) = 0$.
- Hyper-Kloosterman sums (1) $\mathrm{Kl}_{n,q} : \mathbb{F}_q \to \mathbb{Z}[\zeta_{4p}]_{q^{(n-1)/2}}$, realized as trace functions of *Kloosterman sheaves*, with $\mathrm{Kl}_{n,q}(0) = (-\sqrt{q})^{1-n}$.
- Functions $f : \mathbb{F}_q \to \mathbb{N}$ counting points on families of curves on $\mathbb{P}^1_{\mathbb{F}_q}$ parametrized by an open of $\mathbb{P}^1$. For example, for $f \in \mathbb{F}_q[X]$ a fixed squarefree polynomial of degree $2g \geqslant 2$, we have the family of hyperelliptic curves given by the affine models
$$X_z : y^2 = f(x)(x - z) \ (z \in \mathbb{F}_q),$$
as constructed by Katz-Sarnak [KS91, Chapter 10].

The observations on the images of these functions from Sections 1.1–1.3 happen to translate on the level of sheaves: they are actually sheaves of $\mathcal{O}_\lambda \leqslant \overline{\mathbb{Q}}_\ell$-modules, where $\mathcal{O}$ is the ring of integers of a cyclotomic field and $\lambda$ is an $\ell$-adic valuation corresponding to a prime ideal $\mathfrak{l} \trianglelefteq \mathcal{O}$ above an auxiliary prime $\ell \neq p$.

For the second example, this follows from the fact that the $\ell$-adic Fourier transform is defined on the level of $\mathcal{O}_\lambda$-modules (see [Kat88, Chapter 5]).

1.4.1. *Reductions.* The reduction of the trace function modulo $\mathfrak{l}$ then corresponds to the trace function of the reduced sheaf of $\mathbb{F}_\mathfrak{l}$-modules, for $\mathbb{F}_\mathfrak{l} \cong \mathcal{O}_\lambda/\mathfrak{l}\mathcal{O}_\lambda$ the residue field. This implies that we can use the $\ell$-adic formalism and the ideas of Deligne and Katz to study distribution questions of these reduced trace functions.

As in [Lam13] (that we generalized in [PG17]) and [LZ12], a key idea is to use a probabilistic model, based on Deligne's equidistribution theorem.

1.4.2. *Monodromy groups.* For Kloosterman sums, an important input is the determination of the $\mathcal{O}_\lambda$-integral monodromy groups of Kloosterman sheaves [PG18], analogous to the determination of the monodromy groups over $\overline{\mathbb{Q}}_\ell$ by Katz [Kat88], when $\ell$ is large enough depending only on the rank.

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

1.4.3. *Other examples.* The above setup also applies to other $\ell$-adic trace functions such as hypergeometric sums (as defined by Katz in [Kat90, Chapter 8]) and 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 $\chi$ a multiplicative character on $\mathbb{F}_q^\times$.

However, the determination of their $\mathcal{O}_\lambda$-integral monodromy groups is the object of future work. If we showed that these are as large as possible (hence classical groups), as is the case for the monodromy groups over $\overline{\mathbb{Q}}_\ell$ by Katz's work [Kat90], the results below would hold as well.

1.5. **Overview of the results.** Given an abelian group $A$, a function $f:\mathbb{F}_q\to A$ and a subset $E\subset\mathbb{F}_q$, we denote by

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

the partial sum over $E$. For $x\in\mathbb{F}_q$, we let $E+x=\{e+x : e\in E\}$ be the translate of $E$ by $x$. With the uniform measure on $\mathbb{F}_q$, we can consider the $A$-valued random variable $(S(f,E+x))_{x\in\mathbb{F}_q}$.

1.5.1. *Equidistribution for shifted sums.* The first results concern the distribution of short shifted sums, and are analogues of the questions answered in [Lam13] and [PG17] (where the random variables were shown to be gaussian under some ranges, generalizing a result of Erdős-Davenport).

**Proposition 1.1** (Kloosterman sums)**.** *For $n\geqslant 2$, $q$ an odd prime power, and $\mathfrak{l}\trianglelefteq\mathbb{Z}[\zeta_{4p}]$ a prime ideal above a prime $\ell\gg_n 1$ distinct from $p$ with $\ell\equiv 1 \pmod 4$, let $\mathrm{Kl}_{n,q}:\mathbb{F}_q\to\mathbb{F}_\mathfrak{l}$ be the reduction modulo $\mathfrak{l}$ of the (normalized) Kloosterman sum on $\mathbb{P}^1_{\mathbb{F}_q}$. 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*

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|}+\begin{cases} O_n\left(|\mathbb{F}_\mathfrak{l}|^{-L\frac{n^2-1}{2}}+|\mathbb{F}_\mathfrak{l}|^{L\frac{n^2+n-2}{2}+n(n-1)-1}q^{-\frac12}\right) & \text{if } n \text{ odd}\\ O_n\left(|\mathbb{F}_\mathfrak{l}|^{-L\frac{n(n+2)}{8}}+|\mathbb{F}_\mathfrak{l}|^{L\frac{n(n+2)}{4}+\frac{n^2-2}{2}}q^{-\frac12}\right) & \text{if } n \text{ even}\end{cases}$$

*uniformly for all $a\in\mathbb{F}_\mathfrak{l}$. This also holds for unnormalized Kloosterman sums.*

*Remark* 1.2. When $p\equiv 1 \pmod 4$ or $n$ is odd, one may replace $\zeta_{4p}$ by $\zeta_p$ and the result holds without restriction on $\ell \pmod 4$. The same remark will apply to the subsequent statements involving Kloosterman sums.

A similar result is valid for point-counting functions on families of hyperelliptic curves.

**Proposition 1.3** (Multiplicative characters)**.** *We let:*

*(1)* $d \geqslant 2$ *be an integer,* $\mathfrak{l} \trianglelefteq \mathcal{O} = \mathbb{Z}[\zeta_d]$ *be a nonzero prime ideal,*

$$\chi : \mathbb{F}_q \to \mathbb{F}_{\mathfrak{l}}$$

*be the reduction modulo* $\mathfrak{l}$ *in* $\mathbb{F}_{\mathfrak{l}} = \mathcal{O}/\mathfrak{l}$ *of a multiplicative character of order* $d$*;*

*(2)* $f = f_1/f_2 \in \mathbb{Q}(X)$ *whose poles and zeros have order not divisible by* $d$*;*

*(3)* $\delta \in (0,1)$ *be such that*[2] $d > |\mathbb{F}_{\mathfrak{l}}|^{\delta}$ *and* $d/(d, |F^{\times}|) \geqslant |\mathbb{F}_{\mathfrak{l}}|^{\delta}$ *for every proper subfield* $F \leqslant \mathbb{F}_{\mathfrak{l}}$*;*

*(4)* $I \subset \mathbb{F}_q$ *of size* $L$*; if* $f \neq X$*, we assume moreover that* $|I| = 1$ *or* $I \subset [1, p/\deg(f_1))^e$ *with respect to an arbitrary* $\mathbb{F}_p$*-basis of* $\mathbb{F}_q$*, identifying the latter with* $\{1, \dots, p\}^e$*.*

*Then there exists* $\alpha = \alpha(\delta) > 0$ *such that*

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

*uniformly for all* $a \in \mathbb{F}_{\mathfrak{l}}$*. Moreover, if* $\delta > 1/2$*, we can choose* $\alpha(\delta) = \delta - 1/2$*; if* $\mathbb{F}_{\mathfrak{l}} = \mathbb{F}_{\ell}$ *with* $\delta > 1/3$*, we can choose*

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

The ranges of the various parameters will be studied in due time. Propositions 1.1 and 1.3 will be particular cases of Theorem 6.1 below.

1.5.2. *Generalizations of [LZ12] to trace functions: distribution of families of short sums.* Next, we generalize a result of Lamzouri-Zaharescu [LZ12] to the distribution of various families of sums of reduced trace functions, in particular multiplicative characters of any order and Kloosterman sums.

**Proposition 1.4** (Shifts of small subsets)**.** *Let* $\varepsilon \in (0, 1/4)$ *and let* $t : \mathbb{F}_q \to \mathbb{F}_{\mathfrak{l}}$ *be either* $t = \mathrm{Kl}_{n,q}$ *as in Proposition 1.1 or* $t = \chi \circ f$ *as in Proposition 1.3. Let* $E \subset \mathbb{F}_q$ *be a "small" subset. Then*

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

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

(This will be a particular case of Proposition 7.10, where the conditions on $E$ will be made precise).

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

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

**Proposition 1.5** (Partial intervals). *Let $\varepsilon \in (0, 1/4)$ and let $t = \chi \circ f : \mathbb{F}_p \to \mathbb{F}_\mathfrak{l}$ be as in Proposition 1.4. Then*

$$\frac{|\{1 \leqslant k \leqslant p : S(\chi \circ f, \{1, \dots, k\}) \equiv a\}|}{p}$$

*is equal to*

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|} + O_{\varepsilon,f}\left(\frac{1}{p^{1/4-\varepsilon}} + \left(\frac{\log d}{\log p}\right)^{\frac{1}{2}} + \delta_{f\neq X}\left(\frac{|\mathbb{F}_\mathfrak{l}|\log p}{p\log d}\right)^{\frac{1}{2}}\right)$$

*uniformly for all $a \in \mathbb{F}_\mathfrak{l}$.*

(This will be a particular case of Proposition 7.15).

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

**Proposition 1.6** (Partial intervals with shifts of small subsets). *We consider the situation of Proposition 1.4 with a fixed choice of a $\mathbb{F}_p$-basis of $\mathbb{F}_q$ giving an identification $\mathbb{F}_q \cong \mathbb{F}_p^e = \{1, \dots, p\}^e$. We let $E_2, \dots, E_e \subset \mathbb{F}_p$ be "small" subsets. Then the density*

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

*is equal to*

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|} + \begin{cases} O_{\varepsilon,n}\left(\frac{1}{q^{1/4-\varepsilon}} + \left(\frac{\log|\mathbb{F}_\mathfrak{l}|\prod_{i=2}^e|E_i|}{\log q}\right)^{\frac{1}{2}}\right) \\ O_{\varepsilon,f}\left(\frac{1}{q^{1/4-\varepsilon}} + \left(\frac{\log d\prod_{i=2}^e|E_i|}{\log q}\right)^{\frac{1}{2}}\right) \end{cases}$$

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

(This will be a particular case of Proposition 7.18, where the condition on $E_i$ will be made precise).

Again, these examples also apply to unnormalized Kloosterman sums and functions counting points on families of hyperelliptic curves (normalized or not).

1.6. **Structure of the paper.** This article is structured as follows:

- In Section 2, we set up the technical framework we will work in to handle reductions of $\ell$-adic trace functions over finite fields, and we define precisely the examples we will consider.
- In Section 3, we define a probabilistic model for short sums of $\ell$-adic trace functions, inspired by Deligne's equidistribution theorem.
- In Section 4, we prove that this model is accurate (akin to what is done in [PG17] for sheaves of $\overline{\mathbb{Q}}_\ell$-modules).
- In Section 5, we make preliminary computations and observations in the model, in particular regarding "Gaussian sums" in monodromy groups.

– In Sections 6 and 7, we finally prove the results introduced in Sections 1.5.1 and 1.5.2, respectively.

*Acknowledgements.* The author would like to thank his supervisor Emmanuel Kowalski for guidance and advice during this project, as well as the anonymous referees for careful readings and valuable comments. It is a pleasure to acknowledge in particular the influence of the works of Étienne Fouvry, Nicholas Katz, Emmanuel Kowalski, Youness Lamzouri, Philippe Michel and Alexandru Zaharescu. This work was partially supported by DFG-SNF lead agency program grant 200021L_153647. The final corrections were made while the author was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Spring 2017 semester, supported by the National Science Foundation under Grant No. DMS-1440140. The results also appear in the author's PhD thesis [PG16].

## 2. Technical setup and examples

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 $d$th cyclotomic field with ring of integers $\mathcal{O}$. We fix an auxiliary prime $\ell \neq p$ and a prime ideal $\mathfrak{l} \trianglelefteq \mathcal{O}$ above $\ell$, corresponding to a valuation $\lambda$ of $E$ extending the $\ell$-adic valuation on $\mathbb{Q}$. Let $E_\lambda$ and $\mathcal{O}_\lambda$ be the completions, and let

$$\pi : \mathcal{O}_\lambda \to \mathbb{F}_\mathfrak{l}$$

be the reduction map in the residue field $\mathbb{F}_\mathfrak{l} = \mathcal{O}/\mathfrak{l} \cong \mathcal{O}_\lambda/\mathfrak{l}\mathcal{O}_\lambda$.

### 2.1. Review of $\ell$-adic sheaves on $\mathbb{P}^1_{\mathbb{F}_q}$.

In the following, let $A$ be either $\overline{\mathbb{Q}}_\ell$, $E_\lambda$, $\mathcal{O}_\lambda$ or $\mathbb{F}_\mathfrak{l}$.

2.1.1. *Definitions and basic properties.* As in [Kat88], we consider a constructible sheaf $\mathcal{F}$ of $A$-modules on $\mathbb{P}^1/\mathbb{F}_q$ which is middle-extension, i.e. for every nonempty open $j : U \to \mathbb{P}^1$ on which $j^*\mathcal{F}$ is lisse, we have $\mathcal{F} \cong j_*j^*\mathcal{F}$. For simplicity, we shall from now on simply call $\mathcal{F}$ an "*$\ell$-adic sheaf of $A$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$*".

We write $\mathrm{Sing}(\mathcal{F}) = X(\overline{\mathbb{F}}_q)\backslash U_\mathcal{F}(\overline{\mathbb{F}}_q)$ for the set of *singularities* of $\mathcal{F}$, where $U_\mathcal{F}$ is the maximal open set of lissity of $\mathcal{F}$.

We recall that the category of $\ell$-adic sheaves of $A$-modules of generic rank $n$ on $\mathbb{P}^1_{\mathbb{F}_q}$ is equivalent to the category of continuous $\ell$-adic Galois representations

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

for $\pi_{1,q} = \mathrm{Gal}\left(\mathbb{F}_q(T)^{\mathrm{sep}}/\mathbb{F}_q(T)\right)$ the étale fundamental group (see [KR15, Theorem 7.13]) and $A = \mathcal{F}_{\overline{\eta}}$ for $\overline{\eta}$ the geometric generic point of $\mathbb{P}^1_{\mathbb{F}_q}$ corresponding to the chosen separable closure.

We say that $\mathcal{F}$ is *irreducible* (resp. *geometrically irreducible*) if $\rho_\mathcal{F}$ (resp. the restriction of $\rho_\mathcal{F}$ to $\pi_{1,q}^{\mathrm{geom}} := \mathrm{Gal}(\mathbb{F}_q(T)^{\mathrm{sep}}/\overline{\mathbb{F}}_q(T)) \trianglelefteq \pi_{1,q}$) is an irreducible representation.

For $x \in \mathbb{P}^1(\mathbb{F}_q)$, we denote by

– $I_x \trianglelefteq D_x \leqslant \pi_{1,q}$ *inertia (resp. decomposition) groups* at (the valuation corresponding to) $x$.

- $\mathrm{Frob}_{x,q} \in D_x/I_x \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ an element mapping to the geometric Frobenius $\mathrm{Frob}_q$.
- $\mathcal{F}_{\overline{\eta}}^{I_x}$ the space of invariants of $\mathcal{F}_{\overline{\eta}}$ with respect to the action of $I_x$. Note that $\rho_{\mathcal{F}}(\mathrm{Frob}_{x,q}) \in \mathrm{GL}(\mathcal{F}_{\overline{\eta}}^{I_x})$ is well-defined.
- $\mathrm{Swan}_x(\mathcal{F}) \in \mathbb{Z}_{\geqslant 0}$ the *Swan conductor* of $\mathcal{F}$ at $x$.

These are defined up to conjugation. As in the works of Fouvry-Kowalski-Michel (see e.g. [FKM15a]), we consider the *conductor*

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

of $\mathcal{F}$, which combines three invariants of the sheaf to measure its "complexity" (with respect to dimension and ramification).

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

$$\begin{aligned} t_{\mathcal{F}} : \quad & \mathbb{P}^1(\mathbb{F}_q) \to A \\ & x \mapsto \mathrm{tr}\left(\rho_{\mathcal{F}}(\mathrm{Frob}_{x,q}) \mid \mathcal{F}_{\overline{\eta}}^{I_x}\right). \end{aligned}$$

If $A$ has characteristic zero, we say that $\mathcal{F}$ is *pointwise pure of weight* 0 if for every finite extension $\mathbb{F}_{q'}/\mathbb{F}_q$ and every $x \in U_{\mathcal{F}}(\mathbb{F}_{q'})$, the eigenvalues of $\rho_{\mathcal{F}}(\mathrm{Frob}_{x,q'})$ are Weil numbers $\alpha$ of weight 0, i.e. $\alpha \in \overline{\mathbb{Q}}$ and for any embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$, we have $|\iota(\alpha)| = 1$. In this case,

$$||t_{\mathcal{F}}||_{\iota,\infty} := \max_{x \in \mathbb{P}^1(\mathbb{F}_q)} |\iota(t_{\mathcal{F}}(x))| \leqslant \mathrm{rank}(\mathcal{F}) \leqslant \mathrm{cond}(\mathcal{F}),$$

for any such $\iota$, which is clear at lisse points and a result of Deligne [Del80, (1.8.9)] at singularities.

For $\mathcal{F}, \mathcal{G}$ two sheaves of $A$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, we denote by:

- $\mathcal{F} \otimes \mathcal{G}$ the "middle tensor product", i.e. the sheaf of $A$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ corresponding to the representation $\rho_{\mathcal{F}} \otimes \rho_{\mathcal{G}}$
- $D(\mathcal{F})$ the "dual sheaf", i.e. the sheaf of $A$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ corresponding to the dual/contragredient representation of $\rho_{\mathcal{F}}$.

2.1.2. *Sums of trace functions.* Deligne's analogue of the Riemann hypothesis over finite field for weights of étale cohomology groups [Del80] along with the Grothendieck-Lefschetz trace formula and the Euler-Poincaré formula of Grothendieck-Ogg-Safarevich gives the following asymptotic estimate for sums of trace functions:

**Theorem 2.1.** *If $A$ as above has characteristic zero and if $\mathcal{F}$ is a sheaf of $A$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ which is pointwise pure of weight 0, we have*

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

*with respect to an arbitrary embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$, where $\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}}$ is the space of coinvariants of the representation $\rho_{\mathcal{F}}$ restricted to $\pi_{1,q}^{\mathrm{geom}}$, with the action*

*of* $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \pi_{1,q}/\pi_{1,q}^{\mathrm{geom}}$*, and*

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

*Moreover, the same relation holds for* $\sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x)$.

*Proof.* See for example [Del77, Exposé 6], [Kat88, Chapter 2], [FKM15a, Section 9] or [PG16, Section 2.2]. □

It follows that geometrically irreducible $\ell$-adic trace functions on $\mathbb{P}^1_{\mathbb{F}_q}$ are "almost orthogonal":

**Corollary 2.2.** *If $A$ as above has characteristic zero and if $\mathcal{F}$, $\mathcal{G}$ are geometrically irreducible sheaves of $A$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ which are pointwise pure of weight 0, 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, the conjugate being interpreted with respect to any embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$.*

*Proof.* The sheaf $\mathcal{H} = \mathcal{F} \otimes D(\mathcal{G})$ satisfies $t_{\mathcal{F}}(x)\overline{t_{\mathcal{G}}(x)} = t_{\mathcal{H}}(x)$ when $x \notin \operatorname{Sing}(\mathcal{F}) \cup \operatorname{Sing}(\mathcal{G})$, and $\mathrm{cond}(\mathcal{H}) \ll \mathrm{cond}(\mathcal{F})^2\,\mathrm{cond}(\mathcal{G})^2$ (see the references above). Hence

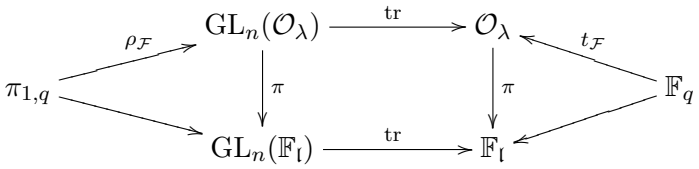
$$\begin{aligned}
\sum_{x\in\mathbb{F}_q} t_{\mathcal{F}}(x)\overline{t_{\mathcal{G}}(x)} &= \sum_{x\in U_{\mathcal{H}}(\mathbb{F}_q)} t_{\mathcal{G}}(x) + O\left(||t_{\mathcal{F}}t_{\mathcal{G}}||_{\iota,\infty}(|\operatorname{Sing}(\mathcal{F})| + |\operatorname{Sing}(\mathcal{G})|)\right) \\
&= \sum_{x\in\mathbb{F}_q} t_{\mathcal{G}}(x) + O\left(\mathrm{cond}(\mathcal{F})^2\,\mathrm{cond}(\mathcal{G})^2\right) \\
&= q \cdot \mathrm{tr}\left(\mathrm{Frob}_q \mid \mathcal{H}_{\pi_{1,q}^{\mathrm{geom}}}\right) + O\left(\mathrm{cond}(\mathcal{F})^2\,\mathrm{cond}(\mathcal{G})^2\sqrt{q}\right),
\end{aligned}$$

where the last equality is Theorem 2.1. By Schur's Lemma, $\dim \mathcal{H}_{\pi_{1,q}^{\mathrm{geom}}} = 1$ if $\mathcal{F}$ and $\mathcal{G}$ are geometrically isomorphic, and is zero otherwise. If $\mathcal{F} = \mathcal{G}$, the action of the Frobenius on the 1-dimensional vector space $\mathcal{H}_{\pi_{1,q}^{\mathrm{geom}}}$ is moreover trivial. □

2.2. **Reductions.** Let $\mathcal{F}$ be an $\ell$-adic sheaf of $\mathcal{O}_\lambda$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, corresponding to a representation

$$\rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}_n(\mathcal{O}_\lambda).$$

By reduction modulo $\mathfrak{l}$, we obtain an $\ell$-adic sheaf of $\mathbb{F}_\mathfrak{l}$-modules, corresponding to the representation $\pi \circ \rho_{\mathcal{F}}$, with trace function $\pi \circ t_{\mathcal{F}}$.



*Remark* 2.3. By the theory of ramification in cyclotomic fields, we have $|\mathbb{F}_\mathfrak{l}| = \ell^m$ with $m$ the multiplicative order of $\ell$ modulo $d$ (see [Was97, Theorem 2.13]). In particular,

$$|\mathbb{F}_\mathfrak{l}| \equiv 1 \pmod{d} \text{ and } d < |\mathbb{F}_\mathfrak{l}|.$$

Moreover, $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$ (i.e. $\ell$ splits completely) if and only if $\ell \equiv 1 \pmod{d}$.

*Remark* 2.4. In practice, $t_\mathcal{F} : \mathbb{F}_q \to \mathcal{O}_\lambda$ will actually have image in $\mathcal{O}$ or $\mathcal{O}_\alpha$ for some $\alpha \in \mathcal{O}\backslash\mathfrak{l}$ when we normalize (see the examples given in the introduction). We recall that our motivation is to study the reduction of a function $\mathbb{F}_q \to \mathcal{O}$ modulo almost any prime ideal of $\mathcal{O}$. The following diagram summarizes the different rings considered and natural maps between them:

$$\begin{array}{ccccccccc} & & & & E & \longrightarrow & E_\lambda & & \\ & & & & \uparrow & & \uparrow & & \\ \mathcal{O} & \longrightarrow & \mathcal{O}_\alpha & \longrightarrow & \mathcal{O}_\mathfrak{l} & \longrightarrow & \mathcal{O}_\lambda & \xrightarrow{\bmod \mathfrak{l}} & \mathbb{F}_\mathfrak{l}. \end{array}$$

## 2.3. **Examples.**

### 2.3.1. *Kummer sheaves.*

**Proposition 2.5.** *Let $\mathcal{O} = \mathbb{Z}[\zeta_d]$ and let $\chi : \mathbb{F}_q^\times \to \mathcal{O}^\times$ be a multiplicative character of order $d \geqslant 2$, $\lambda$ be an $\ell$-adic valuation on $\mathcal{O}$ corresponding to a prime ideal $\mathfrak{l}$ above $\ell$, and $f = f_1/f_2 \in \mathbb{F}_q(X)$ which is not a $d$-power. We assume that $f$ has no zero or pole of order divisible by $d$. There exists a sheaf $\mathcal{L}_{\chi(f)} = \mathcal{L}_{\chi(f),\lambda}$ of $\mathcal{O}_\lambda$-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) $\operatorname{cond}(\mathcal{L}_{\chi(f)}) \leqslant 1 + \deg(f_1) + \deg(f_2)$.*

*By reduction modulo $\mathfrak{l}$, this gives a sheaf of $\mathbb{F}_\mathfrak{l}$-modules with the same properties and trace function $\chi \circ f \pmod{\mathfrak{l}}$, for $\mathbb{F}_\mathfrak{l} = \mathcal{O}_\lambda/\mathfrak{l}\mathcal{O}_\lambda$.*

*Proof.* See e.g. [Kat88, Section 4.3]. □

NOTATION 2.6. For $f = f_1/f_2 \in \mathbb{F}_q(X)$ with $f_1, f_2 \in \mathbb{F}_q[X]$ coprime, we write $\deg(f) = \max(\deg(f_1), \deg(f_2))$, so that $\operatorname{cond}(\mathcal{L}_{\chi(f)}) \ll \deg(f)$.

### 2.3.2. *Kloosterman sheaves.*

**Proposition 2.7.** *Let $n \geqslant 2$ be an integer and $\lambda$ be an $\ell$-adic valuation on $\mathcal{O} = \mathbb{Z}[\zeta_{4p}]$ corresponding to a prime ideal $\mathfrak{l}$ above $\ell$. There exists a Kloosterman sheaf $\mathcal{K}l_n = \mathcal{K}l_{n,\lambda}$ of $\mathcal{O}_\lambda$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, of rank $n$ and with trace function corresponding to the Kloosterman sum*

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

*and $\operatorname{Kl}_{n,q}(0) = (-\sqrt{q})^{n-1}$. Moreover, $\mathcal{K}l_n$ is geometrically irreducible, lisse on $\mathbb{G}_m$, $\operatorname{Swan}_\infty(\mathcal{K}l_n) = 1$, $\operatorname{Swan}_0(\mathcal{K}l_n) = 0$, $\operatorname{cond}(\mathcal{K}l_n) = n + 3$, and we note*

*that*

$$\mathrm{Kl}_{n,q}(x) \in \mathcal{O}_{q^{(n-1)/2}} \leqslant \mathcal{O}_{\mathfrak{l}}$$

*for all* $x \in \mathbb{F}_q^\times$.

*By reduction modulo* $\mathfrak{l}$*, this gives a sheaf of* $\mathbb{F}_{\mathfrak{l}}$*-modules on* $\mathbb{P}^1_{\mathbb{F}_q}$ *with the same properties and trace function equal to* $\mathrm{Kl}_{n,q} \pmod{\mathfrak{l}}$*, for* $\mathbb{F}_{\mathfrak{l}} = \mathcal{O}_\lambda/\mathfrak{l}\mathcal{O}_\lambda$.

*If* $p \equiv 1 \pmod 4$ *or* $n$ *is odd, we may replace* $\mathcal{O}$ *by* $\mathbb{Z}[\zeta_p]$.

*Proof.* Recall that

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

by the evaluation of quadratic Gauss sums, so $\sqrt{p} \in \mathbb{Z}[\zeta_p, \zeta_4] \leqslant \mathbb{Z}[\zeta_{4p}]$ and $\sqrt{p} \in \mathbb{Z}[\zeta_{4p}]_{\mathfrak{l}}^\times$ since $\ell \neq p$. The proposition is then a consequence of the construction and investigation of the $\ell$-adic Fourier transform by Deligne, Laumon and Brylinski: see [Kat88, Chapters 4, 5, 8]. □

2.3.3. *Point counting on families of curves.*

**Proposition 2.8.** *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 in* $\mathbb{F}_q$*, we consider the family of smooth projective hyperelliptic curves of genus* $g$ *parametrized by* $z \in \mathbb{F}_q \backslash Z_f$ *with affine models*

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

*Let* $\lambda$ *be an* $\ell$*-adic valuation on* $\mathcal{O} = \mathbb{Z}[\zeta_{4p}]$ *corresponding to a prime ideal* $\mathfrak{l}$*. There exists a geometrically irreducible sheaf of* $\mathcal{O}_\lambda$*-modules* $\mathcal{F} = \mathcal{F}_\lambda$ *on* $\mathbb{P}^1_{\mathbb{F}_q}$ *of generic rank* $2g$*, corresponding to a representation* $\rho : \pi_{1,q} \to \mathrm{GL}(V) = \mathrm{GL}_{2g}(\mathcal{O}_\lambda)$ *such that for all* $z \notin Z_f$*,*

$$\frac{\det(1 - q^{1/2}T\rho(\mathrm{Frob}_z))}{(1-T)(1-qT)} = Z(X_z, T) := \exp\left(\sum_{n \geqslant 1} |X_z(\mathbb{F}_{q^n})| \frac{T^n}{n}\right),$$

$$t_{\mathcal{F}}(z) = \frac{q + 1 - |X_z(\mathbb{F}_q)|}{q^{1/2}} \in \mathcal{O}_{q^{1/2}} \leqslant \mathcal{O}_{\mathfrak{l}}.$$

*Moreover:*

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

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

*By reduction modulo* $\mathfrak{l}$*, this gives a sheaf of* $\mathbb{F}_{\mathfrak{l}}$*-modules on* $\mathbb{P}^1_{\mathbb{F}_q}$ *with the same properties and trace function* $t_{\mathcal{F}} \pmod{\mathfrak{l}}$*, where* $\mathbb{F}_{\mathfrak{l}} = \mathcal{O}_\lambda/\mathfrak{l}\mathcal{O}_\lambda$.

*Proof.* By [KS91, Section 10.1] or [Hal08, Section 4] (using middle-convolutions), there exists a sheaf of $\mathbb{Z}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ of generic rank $2g$, pointwise pure of weight 1, such that for all $z \notin Z_f$,

$$Z(X_z, T) = \frac{\det(1 - T\rho(\mathrm{Frob}_z))}{(1-T)(1-qT)} \text{ and } t_{\mathcal{F}}(z) = q + 1 - |X_z(\mathbb{F}_q)| \ (z \notin Z_f),$$

along with properties (1) and (2) above. Normalizing by a Tate twist gives the sheaf with the desired properties.

□

Other examples of families of curves are given in [KS91, Chapter 10].

## 3. Probabilistic model

Let $\mathcal{F}$ be a sheaf of $\mathbb{F}_\mathfrak{l}$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, lisse on an open $U$, and corresponding to a representation $\rho_\mathcal{F} : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\mathfrak{l}) = \mathrm{GL}(V)$.

In this section, we set up a probabilistic model for short sums of the trace function $t_\mathcal{F}$ and show that it is accurate (with respect to density functions).

### 3.1. Monodromy groups.

Definition 3.1. The *arithmetic and geometric monodromy groups* of $\mathcal{F}$ are the groups $G_{\mathrm{geom}}(\mathcal{F}) = \rho_\mathcal{F}\big(\pi_{1,q}^{\mathrm{geom}}\big) \leqslant G_{\mathrm{arith}}(\mathcal{F}) = \rho_\mathcal{F}(\pi_{1,q}) \leqslant \mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$.

Definition 3.2. For $G = G_{\mathrm{arith}}(\mathcal{F})$ or $G = G_{\mathrm{geom}}(\mathcal{F})$, the inclusion $G \hookrightarrow \mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$ is called the *standard representation* of $G$.

The determination of integral or finite monodromy groups is usually more difficult than that of monodromy groups over $\overline{\mathbb{Q}}_\ell$ (as Zariski closures of the images of the representations), because we consider simply subgroups of $\mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$ instead of (reductive[3]) algebraic subgroups of $\mathrm{GL}_n(\mathbb{C})$.

3.1.1. *Examples.* Nonetheless, for the examples we consider:

**Proposition 3.3** (Kummer sheaves)**.** *The arithmetic and geometric monodromy groups of a Kummer sheaf of $\mathbb{F}_\mathfrak{l}$-modules as in Proposition 2.5 are equal to $\mu_d(\mathbb{F}_\mathfrak{l})$, the group of $d$th roots of unity in $\mathbb{F}_\mathfrak{l}$.*

*Proof.* This is clear by the explicit construction of the Kummer sheaf (see e.g. [Del77, Section 4.7]). □

The following two propositions extend the results over $\overline{\mathbb{Q}}_\ell$ from [Kat88], respectively [KS91], and show that the finite monodromy groups are still as large as possible.

**Proposition 3.4** (Kloosterman sheaves)**.** *Let $n \geqslant 2$ be an integer coprime with $p$ and let $\mathcal{K}l_n$ be the sheaf of $\mathbb{F}_\mathfrak{l}$-modules from Proposition 2.7. If $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$ and $([\mathbb{F}_\mathfrak{l} : \mathbb{F}_\ell], n) = 1$, then*

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

*If $p \equiv 1 \pmod 4$ and $\mathcal{O}$ is replaced by $\mathbb{Z}[\zeta_p]$, then this holds without restriction on $\ell \pmod 4$.*

*Proof.* See [PG18, Theorem 1.6]. □

[3] By a result of Deligne, the connected component at the identity of the geometric monodromy group of a pointwise pure of weight 0 sheaf of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ is semisimple, see e.g. [KS91, 9.0.12].

**Proposition 3.5** (Families of hyperelliptic curves)**.** *In the setting of Proposition 2.8, assume that $\mathfrak{l}$ is completely split, i.e. $\mathbb{F}_{\mathfrak{l}} = \mathbb{F}_\ell$. For $\mathcal{F}$ the normalized sheaf of $\mathbb{F}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ from Proposition 2.8, we have $G_{\mathrm{geom}}(\mathcal{F}) = G_{\mathrm{arith}}(\mathcal{F}) = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.*

*Proof.* It follows from a theorem of Hall [Hal08, Section 5] and Proposition 2.8 (2) (i.e. the geometric monodromy group contains a transvection) that $G_{\mathrm{geom}}(\mathcal{F}) = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.

Since we normalized, [KS91, Lemma 10.1.9] shows that the arithmetic monodromy group preserves the same pairing (without normalization, it is a group of symplectic similitudes with multiplicator $q$), so that $\mathrm{Sp}_{2g}(\mathbb{F}_\ell) = G_{\mathrm{geom}}(\mathcal{F}) \leqslant G_{\mathrm{arith}}(\mathcal{F}) \leqslant \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. □

3.2. **Model.** We are interested in the $\mathbb{F}_{\mathfrak{l}}$-valued random variable

$$\Big(t_{\mathcal{F}}(x)\Big)_{x\in\mathbb{F}_q} \tag{3}$$

with respect to the uniform measure on $\mathbb{F}_q$.

Motivated by Chebotarev's density theorem/Deligne's equidistribution theorem (see e.g. [KS91, Chapter 9]), the idea is to model the $G_{\mathrm{arith}}(\mathcal{F})^\sharp$-valued random variable

$$\Big(\rho^\sharp_{\mathcal{F}}(\mathrm{Frob}_x)\Big)_{x\in U(\mathbb{F}_q)}$$

by the random variable $Y = \pi(X)$, where $X$ is uniformly distributed in $G_{\mathrm{arith}}(\mathcal{F})$, $\pi : G_{\mathrm{arith}}(\mathcal{F}) \to G_{\mathrm{arith}}(\mathcal{F})^\sharp$ is the projection to the conjugacy classes, and $\rho^\sharp_{\mathcal{F}} : \pi^\sharp_{1,q} \to G_{\mathrm{arith}}(\mathcal{F})^\sharp$ is the natural map induced by $\rho_{\mathcal{F}}$.

We shall then naturally model (3) by the random variable $Z = \mathrm{tr}(Y)$.

3.2.1. *Shifts.*

Definition 3.6. For $I \subset \mathbb{F}_q$, we define

$$U_{\mathcal{F},I}(\mathbb{F}_q) = \bigcap_{a\in I}(U_{\mathcal{F}}(\mathbb{F}_q) - a) = \mathbb{F}_q \backslash \bigcup_{a\in I}((\mathrm{Sing}(\mathcal{F}) \cap \mathbb{F}_q) - a),$$

where $E - a = \{x - a : x \in E\}$ for any $E \subset \mathbb{F}_q$ and $a \in \mathbb{F}_q$.

For $I \subset \mathbb{F}_q$ of size $L \geqslant 1$, we will then model the random vector

$$\Big(\Big(\rho^\sharp_{\mathcal{F}}(\mathrm{Frob}_{x+a})\Big)_{a\in I}\Big)_{x\in U_{\mathcal{F},I}(\mathbb{F}_q)} \tag{4}$$

(with respect to the uniform measure on $U_{\mathcal{F},I}(\mathbb{F}_q)$) by the random vector $(Y_1, \dots, Y_L)$, for $Y_i$ independent distributed like $Y$.

Correspondingly, we will model the random vector $((t_{\mathcal{F}}(x + a))_{a\in I})_{x\in\mathbb{F}_q}$ 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] for multiplicative characters.

This is also to be compared with the model used in [PG16] and [PG17] for sheaves of $\overline{\mathbb{Q}}_\ell$-modules.

*Remark* 3.7. When $x \in \mathrm{Sing}(\mathcal{F})$, $\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x,q})$ is not a well-defined conjugacy class in $G_{\mathrm{arith}}(\mathcal{F})$ (rather one in $\mathrm{GL}(V^{I_x})$). On the other hand, $t_{\mathcal{F}}(x)$ is a well-defined element of $\mathbb{F}_\mathfrak{l}$ for all $x \in \mathbb{P}^1(\mathbb{F}_q)$.

3.3. **Coherent families.** We define a family of sheaves for which this model is accurate.

3.3.1. *Definition.*

Definition 3.8. Let $\mathcal{F}$ be a sheaf of $\mathbb{F}_\mathfrak{l}$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ corresponding to a representation $\rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$. If $\sigma \in \mathrm{Aut}(\mathbb{F}_\mathfrak{l})$, we let $\sigma(\mathcal{F})$ be the sheaf corresponding to the representation $\sigma \circ \rho_{\mathcal{F}} : \pi_{1,q} \to \mathrm{GL}_n(\mathbb{F}_\mathfrak{l}) \to \mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$.

Definition 3.9 (Coherent family). Let $E$ be a number field and $\Lambda$ be a set of valuations on $E$. A family $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$, where $\mathcal{F}_\lambda$ is an irreducible sheaf of $\mathbb{F}_\mathfrak{l}$-modules over a finite field $\mathbb{F}_q = \mathbb{F}_{q(\lambda)}$, for $\mathfrak{l}$ the prime ideal corresponding to $\lambda$, is *coherent* if:

(1) (Conductor) $\mathrm{cond}(\mathcal{F}_\lambda)$ is uniformly bounded for $\lambda \in \Lambda$.

and either:

(2) *Kummer case*: There exists an integer $d \geqslant 2$ such that every $\mathcal{F}_\lambda$ is a Kummer sheaf with monodromy group $\mu_d(\mathbb{F}_\mathfrak{l})$.

(2′) *Cyclic simple case*: There exists a prime $d \geqslant 2$ such that for every $\lambda \in \Lambda$:
   (a) (Monodromy groups) The arithmetic and geometric monodromy groups of $\mathcal{F}_\lambda$ coincide and are equal to $\mu_d(\mathbb{F}_\mathfrak{l})$.
   (b) (Independence of shifts) There is no geometric isomorphism of the form $[+a]^*\mathcal{F}_\lambda \cong \mathcal{F}_\lambda^{\otimes i}$ for $1 \leqslant i < d$, $a \in \mathbb{F}_{q(\lambda)}^\times$.

(2″) *Classical case*: There exists $G \in \{\mathrm{SL}_n : n \geqslant 2\} \bigcup \{\mathrm{Sp}_n : n \geqslant 2 \text{ even}\}$ such that for every $\lambda \in \Lambda$:
   (a) (Monodromy groups) The geometric and arithmetic monodromy groups of $\mathcal{F}_\lambda$ coincide and are conjugate to $G(\mathbb{F}_\mathfrak{l})$ in $\mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$ (with respect to the standard representation).
   (b) (Independence of shifts) There is no geometric isomorphism of the form
   $$[+a]^*\mathcal{F}_\lambda \cong \mathcal{L} \otimes \sigma(\mathcal{F}_\lambda) \text{ or } [+a]^*\mathcal{F}_\lambda \cong \mathcal{L} \otimes D(\sigma(\mathcal{F}_\lambda)) \tag{5}$$
   for $a \in \mathbb{F}_{q(\lambda)}^\times$, $\sigma \in \mathrm{Aut}(\mathbb{F}_\mathfrak{l})$ and $\mathcal{L}$ a sheaf of $\mathbb{F}_\mathfrak{l}$-modules of generic rank 1 on $\mathbb{P}^1_{\mathbb{F}_{q(\lambda)}}$.

We call $\mu_d$, resp. $\mathrm{SL}_n$ or $\mathrm{Sp}_n$ the *monodromy group structure* of the family, and a *bound on the conductor of the family* is any uniform bound for $\mathrm{cond}(\mathcal{F}_\lambda)$ $(\lambda \in \Lambda)$.

*Remark* 3.10. We fix the structure of the monodromy group, while we let $\mathbb{F}_q$ and $\mathbb{F}_\mathfrak{l}$ vary to study for example the reductions of a trace function whose

values do not depend on $\lambda$, modulo various ideals (see Remark 2.4) as $q \to +\infty$. We could also let $d$, resp. $n$ vary (in the Kummer, resp. classical case), but this is not a natural aspect in applications. Nonetheless, we note that the implied constants will *not* depend on $d$ in our results.

*Remark* 3.11. This is to be compared with the coherent families of sheaves of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ defined in [PG17].

3.3.2. *Examples.*

**Proposition 3.12** (Kummer sheaves)**.** *Let $d \geqslant 2$ be an integer and let $\Lambda$ be a set of valuations of $\mathbb{Q}(\zeta_d)$. A family $(\mathcal{L}_{\chi(f_\lambda),\lambda})_{\lambda\in\Lambda}$ of Kummer sheaves, with monodromy group structure $\mu_d$ and $\deg(f_\lambda)$ bounded uniformly, is coherent.*

*Proof.* By Propositions 2.5 and 3.3, Conditions (1) and (2) of Definition 3.9 are satisfied. □

**Proposition 3.13** (Kloosterman sheaves)**.** *Let $n \geqslant 2$ be an integer and let $\Lambda$ be a set of valuations of $\mathbb{Q}(\zeta_{4p})$. We assume that every $\lambda \in \Lambda$ lies above a prime $\ell \gg_n 1$ with $\ell \equiv 1 \pmod 4$ and $(n, [\mathbb{F}_\mathfrak{l} : \mathbb{F}_\ell]) = 1$ as in Proposition 3.4. A family $(\mathcal{K}l_{n,\lambda})_{\lambda\in\Lambda}$ of Kloosterman sheaves of rank $n$, as in Proposition 2.7, is coherent.*

*Proof.* By Propositions 2.7 and 3.4, Conditions (1) and (2″a) of Definition 3.9 are satisfied. It remains to show the independence of shifts (Condition (2″b)), which can be done exactly as in the $\overline{\mathbb{Q}}_\ell$ case in [PG17, Section 7] by analyzing the local ramification on both sides of an isomorphism of the form (5). □

**Proposition 3.14** (Families of hyperelliptic curves)**.** *Let $f \in \mathbb{Z}[X]$ be a squarefree polynomial of degree $2g \geqslant 2$ and let $\Lambda$ be a set of valuations of $\mathbb{Q}(\zeta_{4p})$ of degree 1 (i.e. corresponding to completely split ideals). A family $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ of sheaves of $\mathbb{F}_\ell$-modules with respect to the reductions of $f$ as in Proposition 2.8 is coherent.*

*Proof.* By Propositions 2.8 and 3.5, Conditions (1) and (2″a) of Definition 3.9 are satisfied, and it suffices to verify the independence of shifts (Condition (2″b)). Again, the argument is the same as the one over $\overline{\mathbb{Q}}_\ell$ in [PG17, Section 7]. □

| $G$ | $\dim G$ | $\operatorname{rank} G$ | $\alpha(G)$ | $\beta_+(G)$ | $\beta_-(G)$ |
|---|---|---|---|---|---|
| $\mathrm{SL}_n$ | $n^2-1$ | $n-1$ | $\frac{n^2-1}{2}$ | $\frac{n^2+n-2}{2}$ | $\frac{n(n-1)}{2}$ |
| $\mathrm{Sp}_n$ ($n$ even) | $\frac{n(n+1)}{2}$ | $\frac{n}{2}$ | $\frac{n(n+2)}{8}$ | $\frac{n(n+2)}{4}$ | $\frac{n^2}{4}$ |

TABLE 1. Constants for the groups considered.

## 3.4. **Accuracy of the model.**

DEFINITION 3.15. Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family with monodromy group structure $G$ and let $I \subset \mathbb{F}_q$. We say that a sheaf of $\mathbb{F}_\mathfrak{l}$-modules $\mathcal{F}_\lambda$ on $\mathbb{P}^1_{\mathbb{F}_q}$ in the family is *$I$-compatible* if either:

- The family is in the cyclic simple case or the classical case (cases $(2')$ and $(2'')$ of Definition 3.9).
- The family is in the Kummer case (case (2) of Definition 3.9), so that $\mathcal{F}_\lambda = \mathcal{L}_{\chi(f)}$ for $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ a character of order $d$, $f = f_1/f_2 \in \mathbb{F}_q(X)$ with $(f_1, f_2) = 1$, and we have that

$$\sum_{i=1}^{m} x_i \neq 0 \text{ for all } x_1, \dots, x_m \in I, 1 \leqslant m \leqslant \deg(f_1). \tag{6}$$

*Example* 3.16. Condition (6) holds if $\deg(f) = 1$ or if for an arbitrary $\mathbb{F}_p$-basis of $\mathbb{F}_q$ with coordinates $\pi_i : \mathbb{F}_q \to \{1, \dots, p\}$ we have $\max_{a\in I} \pi_i(a) < p/\deg(f_1)$ for some $1 \leqslant i \leqslant e$.

DEFINITION 3.17. Let $L \geqslant 1$ be an integer and $G$ be the monodromy group structure of a coherent family. We define

$$E(G, L, \mathbb{F}_\mathfrak{l}) = \begin{cases} |\mathbb{F}_\mathfrak{l}|^{L\beta_+(G)+2\beta_-(G)} & G \text{ classical} \\ d^L & G = \mu_d,\ d \text{ prime} \\ d^{L+1} & \text{otherwise} \end{cases}$$

with $\beta_\pm(G) = (\dim G \pm \operatorname{rank} G)/2$, given in Table 1.

**Theorem 3.18.** *Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda \in \Lambda$, let $I \subset \mathbb{F}_q = \mathbb{F}_{q(\lambda)}$ be of cardinality $L$ and $h : (G(\mathbb{F}_\mathfrak{l})^\sharp)^I \to \mathbb{R}$ be any function. If $\mathcal{F} = \mathcal{F}_\lambda$ is an $I$-compatible sheaf on $\mathbb{P}^1_{\mathbb{F}_q}$, then*

$$\mathbb{E}\left[h\Big((\rho^\sharp_{\mathcal{F}}(\mathrm{Frob}_{x+a}))_{a\in I}\Big)\right] = \mathbb{E}\left(h(Y_1, \dots, Y_L)\right) + O\Big(L||h||_\infty q^{-1/2} E(G, L, \mathbb{F}_\mathfrak{l})\Big),$$

*where the random variables $Y_i$ and probability spaces are as in Section 3.2, $||h||_\infty = \max_{x\in(G(\mathbb{F}_\mathfrak{l})^\sharp)^I} |h(x)|$. Moreover, if $h$ takes values in $\mathbb{R}_{\geqslant 0}$, then the above is*

$$\mathbb{E}\left(h(Y_1, \dots, Y_L)\right)\Big(1 + O(Lq^{-1/2}E(G, L, \mathbb{F}_\mathfrak{l}))\Big).$$

*The implied constants depend only on the monodromy group structure and a bound on the conductor of the family.*

*Remark* 3.19. When $I = \{0\}$, this is Chebotarev's theorem as it appears for example in [Kow06].

**Corollary 3.20.** *Under the hypotheses of Theorem 3.18, for any function $h : \mathbb{F}_\mathfrak{l}^I \to \mathbb{R}$, we have*

$$\mathbb{E}\left[h\Big((t_{\mathcal{F}}(x + a))_{a\in I}\Big)\right] = \mathbb{E}\left(h(Z_1, \dots, Z_L)\right) + O\Big(L||h||_\infty q^{-1/2} E(G, L, \mathbb{F}_\mathfrak{l}))\Big),$$

*where the random variables $Z_i$ and probability spaces are as in Section 3.2. If $h$ takes values in $\mathbb{R}_{\geqslant 0}$, then the above is*

$$\mathbb{E}\left(h(Z_1, \dots, Z_L)\right)\Big(1 + O(Lq^{-1/2}E(G, L, \mathbb{F}_\mathfrak{l}))\Big).$$

*The implied constants depend only on the monodromy group structure and a bound on the conductor of the family.*

*Remark* 3.21. Note that we must take $L < q^{1/2}$ to have $E(G, L, \mathbb{F}_\mathfrak{l})L = o(q^{1/2})$ as $q \to +\infty$.

3.5. **Comments on the ranges.** Let us consider the above in the context of Section 2.2 and Remark 2.4, i.e. when the sheaf of $\mathbb{F}_\mathfrak{l}$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ from Theorem 3.18 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 2.3, recall that if $\mathbb{F}_\mathfrak{l}$ is the residue field of $\mathbb{Z}[\zeta_d]_\lambda$ at some prime ideal above $\ell$, then $d < |\mathbb{F}_\mathfrak{l}| = \ell^m$, for $m$ the order of $\ell$ in $(\mathbb{Z}/d)^\times$.

3.5.1. *Choice of the parameters.* Thus, we may want to choose our parameters $(q, \ell, \mathfrak{l}, d)$ so that $d < |\mathbb{F}_\mathfrak{l}| < |\mathbb{F}_q| = p^e$. Given $p$, $\ell$ and $d$, this is holds true for any $\mathfrak{l}$ above $\ell$ if $e \geqslant \frac{\varphi(d)\log \ell}{\log p}$.

3.5.2. *Limitation.* Together with the condition

$$L \ll \begin{cases} \frac{\log q}{\log |\mathbb{F}_\mathfrak{l}|} & \text{if } G \text{ classical} \\ \frac{\log q}{\log d} & \text{if } G = \mu_d \end{cases}$$

from Theorem 3.18, the relation $d < |\mathbb{F}_\mathfrak{l}|$ implies that $L \ll e$ if $G$ 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. [KS91, Chapter 9] and [Kat88, Chapter 3]).

## 4. Proof of Theorem 3.18 and Corollary 3.20

In the following, we use the notations of Theorem 3.18 and we let $I = \{a_1, \dots, a_L\} \subset \mathbb{F}_q$, $V(\mathbb{F}_q) = U_{\mathcal{F},I}(\mathbb{F}_q)$.

Definition 4.1. For $\boldsymbol{v} = (v_1, \dots, v_L) \in (G^\sharp)^I$ and $\widehat{G}$ the set of characters of irreducible complex representations of $G$, we define

$$E(\boldsymbol{v}) = \sum_{\substack{\chi_1,\dots,\chi_L \in \widehat{G} \\ \text{not all trivial}}} \left(\prod_{i=1}^L \overline{\chi}_i(v_i)\right) \frac{1}{|V(\mathbb{F}_q)|} \sum_{x \in V(\mathbb{F}_q)} \prod_{i=1}^L \chi_i(\rho^\sharp_\mathcal{F}(\mathrm{Frob}_{x+a_i})).$$

We start with the following relation between the expected values we are interested in:

**Proposition 4.2.** *For $I = \{a_1, \dots, a_L\} \subset \mathbb{F}_q$, the expected value*

$$\mathbb{E}\left[h\Big((\rho^\sharp_\mathcal{F}(\mathrm{Frob}_{x+a}))_{a\in I}\Big)\right] \tag{7}$$

*is given by*

$$\mathbb{E}(h(Y_1, \dots, Y_L)) + O\left(||h||_\infty \max_{\boldsymbol{v}\in(G^\sharp)^I} |E(\boldsymbol{v})|\right).$$

*When $h$ is nonnegative, (7) is also*

$$\mathbb{E}(h(Y_1,\dots,Y_L))\left[1+O\left(\max_{\boldsymbol{v}\in(G^\sharp)^I}|E(\boldsymbol{v})|\right)\right].$$

*Proof.* By definition, the left-hand side of (7) is

$$\frac{1}{|V(\mathbb{F}_q)|}\sum_{x\in V(\mathbb{F}_q)}h(\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_1}),\dots,\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_L}))=\sum_{\boldsymbol{v}\in(G^\sharp)^I}h(\boldsymbol{v})\frac{|D(\boldsymbol{v})|}{|V(\mathbb{F}_q)|},$$

where

$$D(\boldsymbol{v})=\{x\in V(\mathbb{F}_q):\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_i})=v_i\ (1\leqslant i\leqslant L)\}$$

for $\boldsymbol{v}=(v_1,\dots,v_L)$. By Schur's orthogonality relations for the finite group $G$,

$$\begin{aligned}
\frac{|D(\boldsymbol{v})|}{|V(\mathbb{F}_q)|} &= \frac{1}{|V(\mathbb{F}_q)|}\sum_{x\in V(\mathbb{F}_q)}\prod_{i=1}^{L}\delta_{\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_i})=v_i}\\
&= \frac{1}{|V(\mathbb{F}_q)|}\sum_{x\in V(\mathbb{F}_q)}\prod_{i=1}^{L}\left(\frac{|v_i|}{|G|}\sum_{\chi\in\hat{G}}\chi(\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_i}))\overline{\chi}(v_i)\right)\\
&= \frac{\prod_{i=1}^{L}|v_i|}{|G|^L}\sum_{\chi_1,\dots,\chi_L\in\hat{G}}\frac{1}{|V(\mathbb{F}_q)|}\sum_{x\in V(\mathbb{F}_q)}\prod_{i=1}^{L}\chi_i(\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_i}))\overline{\chi}_i(v_i)\\
&= \frac{\prod_{i=1}^{L}|v_i|}{|G|^L}\left(1+E(\boldsymbol{v})\right),
\end{aligned}$$

where $|v|$ denotes the size of a conjugacy class $v\in G^\sharp$. On the other hand,

$$\mathbb{E}(h(Y_1,\dots,Y_L))=\frac{1}{|G|^L}\sum_{\boldsymbol{v}\in(G^\sharp)^I}h(\boldsymbol{v})\prod_{i=1}^{L}|v_i|.$$

□

To prove Theorem 3.18, we thus want to show that the expression

$$\sum_{x\in V(\mathbb{F}_q)}\prod_{i=1}^{L}\chi_i(\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_i})) \tag{8}$$

in $E(\boldsymbol{v})$ is small for $\chi_1,\dots,\chi_L\in\hat{G}$ not all trivial and $\boldsymbol{v}\in(G^\sharp)^I$.

### 4.1. **Reinterpretation of (8).**

Definition 4.3. We fix an isomorphism of fields $\iota:\overline{\mathbb{Q}}_\ell\to\mathbb{C}$. For $\eta:G\to\mathrm{GL}(V)$ a complex representation, we let $\mathcal{F}_\eta$ be the sheaf of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$ corresponding to the representation

$$\iota^{-1}\circ\eta\circ\rho_{\mathcal{F}}:\pi_{1,q}\to G\to\mathrm{GL}(V)\to\mathrm{GL}(\iota^{-1}(V)).$$

*Remark* 4.4. Since $G$ is discrete, there are no issues with the continuity of the composition $\iota^{-1}\circ\eta\circ\rho_{\mathcal{F}}$, even if $\iota$ is not continuous.

Note that the trace function of $\mathcal{F}_\eta$ at unramified points is

$$\chi \circ \rho_{\mathcal{F}}^\sharp \circ \mathrm{Frob} : U_{\mathcal{F}_\eta}(\mathbb{F}_q) \to \pi_{1,q}^\sharp \to G(\mathbb{F}_\mathfrak{l})^\sharp \to \mathbb{C},$$

where $\chi$ is the character of $\eta$. Thus, we can rewrite (8) as

$$\sum_{x \in V(\mathbb{F}_q)} \prod_{i=1}^{L} t_{\mathcal{F}_i}(x), \text{ where } \mathcal{F}_i = [+a_i]^* \mathcal{F}_{\eta_i} \tag{9}$$

is a sheaf of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, for $\eta_i$ the representation corresponding to $\chi_i$.

4.2. **Sums of products of trace functions.** The estimation of sums of products of the form $\sum_{x \in \mathbb{F}_q} \prod_{i=1}^{H} t_i(x)$, for $t_i$ the trace function of a sheaf of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, is precisely the question surveyed in [FKM15b].

We need the following estimate, where the dependency with respect to the conductors is precisely tracked:

**Proposition 4.5.** *Let $(\mathcal{F}_i)_{1 \leqslant i \leqslant L}$ be a tuple of pointwise pure of weight 0 sheaves of $\overline{\mathbb{Q}}_\ell$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, with corresponding trace functions $(t_i : \mathbb{F}_q \to \mathbb{C})_{1 \leqslant i \leqslant L}$. We assume that the arithmetic and geometric monodromy groups of $\mathcal{G} = \bigoplus_{i=1}^L \mathcal{F}_i$ coincide and are as large as possible, i.e. isomorphic to $\prod_{i=1}^L G_{\mathrm{geom}}(\mathcal{F}_i)$. Then, for $S = \bigcup_{i=1}^L \mathrm{Sing}(\mathcal{F}_i)$,*

$$\sum_{x \in \mathbb{F}_q \setminus S} t_1(x) \dots t_L(x) = q \prod_{i=1}^{L} \dim(\mathcal{F}_i)_{\pi_{1,q}^{\mathrm{geom}}} + O(E\sqrt{q})$$

*with an absolute implied constant, where*

$$E \ll \sqrt{q} \left( \prod_{i=1}^{L} \mathrm{rank}(\mathcal{F}_i) \right) \left( |S| + \sum_{x \in S} \sum_{i=1}^{L} \mathrm{Swan}_x(\mathcal{F}_i) \right).$$

*Proof.* Let $\mathcal{F} = \bigotimes_{i=1}^L \mathcal{F}_i$, which satisfies $\mathrm{Sing}(\mathcal{F}) \subset S$. For any embedding $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$,

$$\begin{aligned} \sum_{x \in \mathbb{F}_q \setminus S} t_1(x) \dots t_L(x) &= \sum_{x \in U_{\mathcal{F}}(\mathbb{F}_q)} t_{\mathcal{F}}(x) + O\left( ||t_1||_{\iota,\infty} \dots ||t_L||_{\iota,\infty} |S| \right) \\ &= \sum_{x \in U_{\mathcal{F}}(\mathbb{F}_q)} t_{\mathcal{F}}(x) + O\left( \mathrm{rank}(\mathcal{F}) |S| \right). \end{aligned}$$

By [Kat88, Lemma 1.3], we also have $\mathrm{Swan}_x(\mathcal{F}) \leqslant \mathrm{rank}(\mathcal{F}) \sum_{i=1}^L \mathrm{Swan}_x(\mathcal{F}_i)$ for any $x \in \mathrm{Sing}(\mathcal{F})$. Thus, Theorem 2.1 yields

$$\begin{aligned} \sum_{x \in \mathbb{F}_q \setminus S} t_1(x) \dots t_L(x) &= q \cdot \mathrm{tr}\left( \mathrm{Frob}_q \mid \mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}} \right) \\ &\quad + O\left( \sqrt{q}\, \mathrm{rank}(\mathcal{F}) \left( |S| + \sum_{x \in S} \sum_{i=1}^{L} \mathrm{Swan}_x(\mathcal{F}_i) \right) \right). \end{aligned}$$

If $\mathcal{F}_i$ corresponds to the representation $\rho_i : \pi_{1,q} \to \mathrm{GL}_{n_i}(\overline{\mathbb{Q}}_\ell)$ with arithmetic monodromy group $G_i$, we let $\mathrm{Std}_i : G_i \to \mathrm{GL}_{n_i}(\overline{\mathbb{Q}}_\ell)$ be the standard representation of $G_i$. If $\rho_{\mathcal{G}}$ is the representation of $\pi_{1,q}$ corresponding to $\mathcal{G}$, then

the sheaf $\mathcal{F}$ corresponds to the representation $\Lambda \circ \rho_{\mathcal{G}}$ for $\Lambda = \boxtimes_{i=1}^{L} \mathrm{Std}_i$ and

$$\mathcal{F}_{\pi_{1,q}} \cong \Lambda_{G_{\mathrm{arith}}(\mathcal{G})},\ \mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}} \cong \Lambda_{G_{\mathrm{geom}}(\mathcal{G})},$$

where $\Lambda_H$ is the space of coinvariants of $\Lambda$ with respect to the action of a subgroup $H \leqslant G_{\mathrm{arith}}(\mathcal{G})$. If the geometric monodromy group of $\mathcal{G}$ is as large as possible, then

$$\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}} \cong \Lambda_{G_{\mathrm{geom}}(\mathcal{G})} \cong \bigotimes_{i=1}^{L} (\mathrm{Std}_i)_{G_{\mathrm{geom}}(\mathcal{F}_i)}.$$

If moreover $G_{\mathrm{arith}}(\mathcal{G}) = G_{\mathrm{geom}}(\mathcal{G})$, the Frobenius acts trivially on $\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}} \cong \Lambda_{G_{\mathrm{geom}}(\mathcal{G})} = \Lambda_{G_{\mathrm{arith}}(\mathcal{G})}$ and

$$\mathrm{tr}\left(\mathrm{Frob}_q \mid \mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}}\right) \quad = \quad \dim(\mathcal{F}_{\pi_{1,q}^{\mathrm{geom}}}) = \prod_{i=1}^{L} \dim(\mathrm{Std}_i)_{G_{\mathrm{geom}}(\mathcal{F}_i)}.$$

□

This leads to the following estimates for (8):

**Proposition 4.6.** *For $L \geqslant 1$, let $a_1, \dots, a_L \in \mathbb{F}_q$ be distinct, and let $\eta_i$ be complex irreducible representations of $G$, not all trivial, with characters $\chi_i$ $(1 \leqslant i \leqslant L)$. We assume that one of the following holds:*

*(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, if $L \ll q$,*

$$\max_{\boldsymbol{v}\in(G^\sharp)^I} |E(\boldsymbol{v})| \ll \frac{\mathrm{cond}(\mathcal{F})^2|G|^\delta}{\sqrt{q}} \sum_{\chi_1,\dots,\chi_L\in G^\sharp} \left(\prod_{i=1}^{L} \dim\eta_i\right)^2 \sum_{i=1}^{L} \dim\eta_i,$$

*with $\delta = 0$ in case (1) and $\delta = 1$ otherwise.*

*Proof.* It suffices to show that the sum of products (8) is

$$\ll \sqrt{q}\,\mathrm{cond}(\mathcal{F})^2|G|^\delta \left(\prod_{i=1}^{L} \dim\eta_i\right) \sum_{i=1}^{L} \dim\eta_i$$

whenever $\chi_1, \dots, \chi_L$ are not all trivial, since we then have

$$|E(\boldsymbol{v})| \leqslant \mathrm{cond}(\mathcal{F})^2|G|^\delta \frac{\sqrt{q}}{|V(\mathbb{F}_q)|} \sum_{\substack{\chi_1,\dots,\chi_L\in\widehat{G}\\ \text{not all trivial}}} \left(\prod_{i=1}^{L} \dim\eta_i\right)^2 \sum_{i=1}^{L} \dim\eta_i$$

and $\sqrt{q}/|V(\mathbb{F}_q)| \leqslant q^{-1/2}|1 - q^{-1}L\,\mathrm{cond}(\mathcal{F})|$.

(1) We note that $\mathcal{F}_\eta$ is geometrically irreducible, $\mathrm{rank}(\mathcal{F}_\eta) = \dim\eta$, $\mathrm{Sing}(\mathcal{F}_\eta)$ is contained in $\mathrm{Sing}(\mathcal{F})$ and $\mathrm{Swan}_x(\mathcal{F}_\eta) \leqslant \dim\eta\,\mathrm{Swan}_x(\mathcal{F})$ for all $x \in$

$\mathbb{P}^1(\overline{\mathbb{F}}_q)$ (by [Kat88, 3.6.2]). By Proposition 4.5 applied with $\mathcal{F}_i = [+a_i]^*\mathcal{F}_{\eta_i}$, the sum (8) 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, $\dim(\mathcal{F}_{\eta_i}^G)$ is equal to 1 if $\eta_i$ is trivial, zero otherwise.

(2) For every $i = 1, \dots, L$, there exists an integer $0 \leqslant b_i < d$ such that $\eta_i$ is the one-dimensional representation $x \mapsto x^{b_i}$. By multiplicativity,

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q}\prod_{i=1}^L \chi_i(\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a_i})) = \frac{1}{q}\sum_{x\in\mathbb{F}_q} t_{\mathcal{G}}(x)$$

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 2.2 gives

$$\frac{1}{q}\sum_{x\in\mathbb{F}_q} t_{\mathcal{G}}(x) = \delta_{g \text{ is a } d-\text{power}} + O(Ld\deg(f)q^{-1/2}).$$

As in [PG17, Section 4], we see that, under the compatibility assumption, $g$ cannot be a $d$-power unless all $b_i$ are zero.

□

4.3. **Finite Goursat-Kolchin-Ribet criteria.** It remains to determine when Hypothesis (1) of Proposition 4.6 holds. For sheaves of $A = \overline{\mathbb{Q}}_\ell$-modules, this is handled by the Goursat-Kolchin-Ribet criterion of Katz (see [FKM15b]). We give here an analogue for sheaves of $\mathbb{F}_\mathfrak{l}$-modules.

4.3.1. *Preliminaries.* First, recall the classical Goursat Lemma:

**Lemma 4.7** (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.*

$$\begin{array}{ccccc} & & G_1 & \longrightarrow & G_1/\ker p_2 \\ & \overset{p_1}{\nearrow} & \uparrow & & \uparrow \\ H & \longrightarrow & G_1 \times G_2 & \longrightarrow & (G_1/\ker p_2)\times(G_2/\ker p_1) \\ & \underset{p_2}{\searrow} & \downarrow & & \downarrow \\ & & G_2 & \longrightarrow & G_2/\ker p_1 \end{array}$$

*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 4.8** ([Rib76, Lemma 5.2.2 and p. 791])**.** *Let $G_1, \dots, G_n$ be non-trivial finite groups with no proper nontrivial abelian quotients 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 $G = G_1 \times \cdots \times G_n$.*

*Proof.* In [Rib76], this is stated when $G_i$ has no nontrivial abelian quotient, and the condition is used at the end of the proof of the sublemma, [Rib76, p. 764]. In the notations of the latter, $B'/K'$ is abelian, and if $B' = S_n$ has no *proper nontrivial* abelian quotient, then either $K' = B'$ and one can conclude, or $K'$ is trivial, which implies that $S_n$ is trivial. □

DEFINITION 4.9. 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 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.

*Example* 4.10. Let $G \in \{\mathrm{PSL}_n(k) : n \geqslant 2\} \bigcup \{\mathrm{PSp}_{n/2}(k) : n \geqslant 2 \text{ even}\}$ for $k$ a finite field. If $G_1, G_2$ are conjugate to $G$, then $(G_i, \mathrm{Std})_{i=1,2}$ is Goursat-adapted, where Std is the natural embedding in $\mathrm{PGL}_n(k)$. Indeed, by [Gor82, 4.237] and [Car72, Theorem 12.5.1], if $G$ is a finite simple group of Lie type defined over $k$, every automorphism can be written as the product of an inner, graph, diagonal, and field automorphism; more precisely,

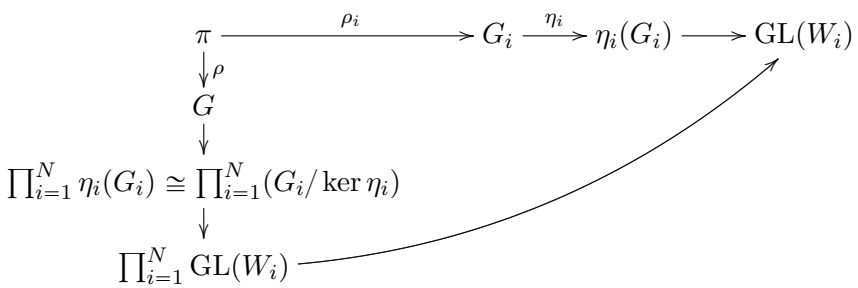
$$\mathrm{Out}(G) \cong (\mathrm{Diag}(G)\,\mathrm{Aut}(k))\,.\,\mathrm{Graph}(G),$$

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). But for $n \geqslant 2$, $\mathrm{Graph}(A_{n-1}) \cong \mathbb{Z}/2$ (corresponding to the transpose-inverse map) while $\mathrm{Graph}(C_n)$ is trivial, with the standard nomenclature for Dynkin diagrams.

4.3.2. *Finite groups of Lie type.*

**Proposition 4.11** (Goursat-Kolchin-Ribet for quasisimple groups)**.** *Let $\pi$ be a topological group, $k$ be a finite field, $F$ be a field, and for $i = 1, \dots, N$, let $\rho_i : \pi \to \mathrm{GL}(V_i)$ be a finite-dimensional representation over $k$ with finite monodromy group $G_i = \rho_i(\pi) \leqslant \mathrm{GL}(V_i)$, and $\eta_i : G_i \to \mathrm{GL}(W_i)$ be a nontrivial representation over $F$.*

*We consider the representation $\rho = \oplus_{i=1}^N(\eta_i \circ \rho_i) : \pi \to \mathrm{GL}(\oplus_{i=1}^N W_i) \cong \prod_{i=1}^N \mathrm{GL}(W_i)$ with monodromy group $G = \rho(\pi)$.*




*We 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 $i \neq j$, $\big(G_l' \to \mathrm{PGL}(V_l)\big)_{l=i,j}$ 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 $\chi$ a 1-dimensional representation of $\pi$ over $k$ and $\sigma \in \mathrm{Aut}(k)$.*

*Then $G$ is as large as possible, i.e. $G = \prod_i (G_i/\ker\eta_i)$.*

*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 $\eta_i$ 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 $G' = \prod_i (G_i/\ker\eta_i)' \cong \prod_i G_i'$.

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 4.8.

By Goursat's Lemma 4.7 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). □

*Remarks* 4.12. Proposition 4.11 should be compared with Katz's version over an algebraically closed field [Kat90, 1.8.2]. Here, we more generally compute the monodromy group of $\oplus_{i=1}^N(\eta_i \circ \rho_i)$ instead of $\oplus_{i=1}^N \rho_i$, while still assuming Condition (3) only on $\rho_i$ (and not on $\eta_i \circ \rho_i$). Over an algebraically closed field, the 1-dimensional representations appear when passing from $G$ to $G^{0,\mathrm{der}}$, while in Proposition 4.11 they appear when passing from $G$ to $G'$. Moreover, the assumption of quasisimplicity here plays the role of the semisimplicity hypothesis in [Kat90].

*Example* 4.13. Let $k$ be a finite field and $n \geqslant 1$ be an integer. By [MT11, Theorem 24.17], $\mathrm{SL}_n(k)$ and $\mathrm{Sp}_{2n}(k)$ with their standard representations are quasisimple as soon as $|k| > 3$. Hence, by Example 4.10, conditions (1) and (2) of Proposition 4.11 hold if there exists $G \in \{\mathrm{PSL}_n(k) : n \geqslant 2\} \cup \{\mathrm{PSp}_{2n}(k) : n \geqslant 1\}$ such that every $G_i$ is conjugate to $G$.

4.3.3. *Roots of unity.* Lastly, we give a version of the Goursat-Kolchin-Ribet criterion for cyclic groups of prime order.

**Proposition 4.14.** *For $i = 1, \dots, L$, let $\rho_i : \pi \to k^\times$ be a one-dimensional representations over a field $k$ of a topological group $\pi$, with monodromy group $G_i = \rho_i(\pi) \cong \mathbb{Z}/d$ ($d$ prime), and let $\eta_i : G_i \to F^\times$ be a nontrivial representation over a field $F$. Consider the representation $\rho = \oplus_i(\eta_i \circ \rho_i) : \pi \to \prod_i F^\times$ with monodromy group $G = \rho(\pi)$. If there is no isomorphism of the form $\rho_i \cong \rho_j^{\otimes a}$ for $i \neq j$, $1 \leqslant a < d$, then $G$ is as large as possible, i.e. $G \cong \prod_i \mathbb{Z}/d$.*

*Proof.* Since $\mathbb{Z}/d$ is simple, we can apply Lemma 4.8 to reduce to the case of two representations as before. By Goursat's Lemma 4.7, 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. **Sums of dimensions of irreducible representations.**

Definition 4.15. For a finite group $G$ and $m \geqslant 1$ an integer, we define $d_m(G) = \sum_{\chi \in \widehat{G}} (\dim \chi)^m$.

**Lemma 4.16.** *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[4] $d_1(G) \ll_n |k|^{\frac{\dim G + \mathrm{rank}\, G}{2}}$, $d_2(G) = \Theta_n(|k|^{\dim G})$, $|G^\sharp| = \Theta_n(|k|^{\mathrm{rank}\, G})$, 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 $\mathrm{SL}_n$ and $\mathrm{Sp}_n$ are [Kow08, Proposition 5.4]. □

*Remark* 4.17. According to Remark 3.10, we do not keep track of implied constants depending on the rank of the monodromy group.

### 4.5. **Conclusion.**

*Proof of Theorem 3.18.* By Proposition 4.2,

$$\begin{aligned}\mathbb{E}\left[h\left((\rho_{\mathcal{F}}^\sharp(\mathrm{Frob}_{x+a}))_{a\in I}\right)\right] &= \mathbb{E}(h(Y_1,\dots,Y_L)) \\ &\quad + O\left(||h||_\infty \max_{\boldsymbol{v}\in(G^\sharp)^L} |E(\boldsymbol{v})|\right)\end{aligned}$$

By Proposition 4.6 (which applies by Propositions 4.11 and 4.14) and Lemma 4.16,

$$\begin{aligned}\frac{\max_{\boldsymbol{v}\in(G^\sharp)^L} |E(\boldsymbol{v})|\sqrt{q}}{\mathrm{cond}(\mathcal{F})^2|G|^\delta} &\ll \sum_{\chi_1,\dots,\chi_L\in\widehat{G}} \left(\prod_{i=1}^L \dim \eta_i\right)^2 \sum_{i=1}^L \dim \eta_i \\ &= L d_1(G)^{L-1} d_3(G).\end{aligned}$$

The case $h$ nonnegative is treated similarly by the second part of Proposition 4.2. □

[4] Here, the notation $f_1(G) = \Theta_n(f_2(G))$ means that there exists constants $C_1(n), C_2(n) > 0$ depending only on $n$ such that $C_1(n)f_2(G) \leqslant f_1(G) \leqslant C_2(n)f_2(G)$ for all $G$.

*Proof of Corollary 3.20.* By writing

$$\begin{aligned}\mathbb{E}\left[h\Big((t_{\mathcal{F}}(x+a))_{a\in I}\Big)\right] &= \frac{q}{|U_{\mathcal{F},I}(\mathbb{F}_q)|}\mathbb{E}\left[(h\circ\mathrm{tr})\Big((\rho_{\mathcal{F}}^{\sharp}(\mathrm{Frob}_{x+a}))_{a\in I}\Big)\right]\\ &= \mathbb{E}\left[(h\circ\mathrm{tr})\Big((\rho_{\mathcal{F}}^{\sharp}(\mathrm{Frob}_{x+a}))_{a\in I}\Big)\right]\\ &\quad +O\left(q^{-1}||h||_{\infty}L\,\mathrm{cond}(\mathcal{F})\right),\end{aligned}$$

the first relation follows by Theorem 3.18, and one argues similarly for the second one. □

## 5. Computations in the model

In this section, we carry out preliminary computations and observations in the probabilistic model.

Throughout, we let $G\leqslant \mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$, $X_1,\dots,X_L$ independent random variables uniformly distributed in $G$, $Y_i=\pi(X_i)$ for $\pi: G\to G^\sharp$ the projection, and $Z_i=\mathrm{tr}\,Y_i$.

### 5.1. Random walks in monodromy groups.

**Proposition 5.1.** *For all $A\subset\mathbb{F}_\mathfrak{l}$ and $L\geqslant 1$, the probability $P(Z_1+\cdots+Z_L\in A)$ is given by*

$$\frac{|A|}{|\mathbb{F}_\mathfrak{l}|}+O\left(\max_{0\neq\psi\in\widehat{\mathbb{F}}_\mathfrak{l}}\left|\sum_{a\in A}\psi(-a)\right|\left|\frac{1}{|G|}\sum_{x\in G}\psi(\mathrm{tr}\,x)\right|^L\right).$$

*In particular, for $a\in\mathbb{F}_\mathfrak{l}$,*

$$P(Z_1+\cdots+Z_L=a)=\frac{1}{|\mathbb{F}_\mathfrak{l}|}+O\left(\max_{0\neq\psi\in\widehat{\mathbb{F}}_\mathfrak{l}}\left|\frac{1}{|G|}\sum_{x\in G}\psi(\mathrm{tr}\,x)\right|^L\right).$$

*Proof.* By Schur's orthogonality relations for the finite group $\mathbb{F}_\mathfrak{l}$,

$$\begin{aligned}P(Z_1+\cdots+Z_L=a) &= \frac{|\boldsymbol{v}=(v_1,\dots,v_L)\in G^L:\mathrm{tr}\sum v_i=a|}{|G|^L}\\ &= \frac{1}{|G|^L}\sum_{\boldsymbol{v}\in G^L}\delta_{\mathrm{tr}\sum v_i=a}\\ &= \frac{1}{|\mathbb{F}_\mathfrak{l}|}\sum_{\psi\in\widehat{\mathbb{F}}_\mathfrak{l}}\psi(-a)\left(\frac{1}{|G|}\sum_{v\in G}\psi(\mathrm{tr}\,v)\right)^L\\ &= \frac{1}{|\mathbb{F}_\mathfrak{l}|}\left[1+\sum_{0\neq\psi\in\widehat{\mathbb{F}}_\mathfrak{l}}\psi(-a)\left(\frac{1}{|G|}\sum_{v\in G}\psi(\mathrm{tr}\,v)\right)^L\right].\end{aligned}$$

The first statement follows from summing the previous equation over $a\in A$. □

5.1.1. *Gaussian sums.* For $\psi$ a nontrivial character of $\mathbb{F}_\mathfrak{l}$, we will call the sum $\sum_{v\in G}\psi(\operatorname{tr} v)$ a "Gaussian sum over $G$", by analogy with the case $G=\mu_d(\mathbb{F}_\mathfrak{l})$ (see Section 5.2 below). We can expect it to be small uniformly with respect to $\psi$, say

$$\frac{1}{|G|}\sum_{v\in G}\psi(\operatorname{tr} v)\ll |\mathbb{F}_\mathfrak{l}|^{-\alpha(G)} \tag{10}$$

with $\alpha(G)>0$, and square-root cancellation corresponds to $\alpha(G)\geqslant \frac{\log|G|}{2\log|\mathbb{F}_\mathfrak{l}|}$. Alternatively, we can also write

$$\sum_{v\in G}\psi(\operatorname{tr} v)\ll |G|^{\alpha'(G)} \text{ with } \alpha'(G)<1. \tag{11}$$

Similarly, if $A$ is "well-distributed" in $\mathbb{F}_\mathfrak{l}$, we expect

$$\frac{1}{|A|}\sum_{x\in A}\psi(-x)\ll |\mathbb{F}_\mathfrak{l}|^{-\alpha(A)} \tag{12}$$

for some $\alpha(A)>0$, uniformly with respect to $\psi\in\widehat{\mathbb{F}}_\mathfrak{l}$. The trivial bound corresponds to $\alpha(A)=0$.

Thus, we can rewrite Proposition 5.1 as:

**Corollary 5.2.** *Let $A\subset\mathbb{F}_\mathfrak{l}$. If the bounds (10) and (12) hold, then*

$$P(Z_1+\cdots+Z_L\in A)=\frac{|A|}{|\mathbb{F}_\mathfrak{l}|}\left(1+O\left(\frac{1}{|\mathbb{F}_\mathfrak{l}|^{L\alpha(G)+\alpha(A)-1}}\right)\right)$$

*for all $L\geqslant 1$. In particular,*

$$P(Z_1+\cdots+Z_L=a)=\frac{1}{|\mathbb{F}_\mathfrak{l}|}\left(1+O\left(\frac{1}{|\mathbb{F}_\mathfrak{l}|^{L\alpha(G)-1}}\right)\right)$$

*uniformly for all $a\in\mathbb{F}_\mathfrak{l}$.*

It is insightful to distinguish the following cases to analyze the ranges of the parameters in Corollary 5.2:

(1) If either
   - $\alpha(G)>1$, or
   - $\alpha(G)\leqslant 1$ and $L>1/\alpha(G)$,

   we have equidistribution of $Z_1+\cdots+Z_L$ in $\mathbb{F}_\mathfrak{l}$ as $|\mathbb{F}_\mathfrak{l}|\to+\infty$.
(2) If $\alpha(G)\leqslant 1$ and $L\leqslant 1/\alpha(G)$, then we have $P(Z_1+\cdots+Z_L=a)\ll |\mathbb{F}_\mathfrak{l}|^{-L\alpha(G)}$, which shows that $Z_1+\cdots+Z_L$ is "not too concentrated" at any point $a\in\mathbb{F}_\mathfrak{l}$.

*Example* 5.3. We will see that for $G=\mathrm{SL}_n(\mathbb{F}_\mathfrak{l})$ or $\mathrm{Sp}_n(\mathbb{F}_\mathfrak{l})$, we always have $\alpha(G)>1$. On the other hand, $\alpha(\mu_d(\mathbb{F}_\mathfrak{l}))<1$.

In the next two sections, we investigate bounds of the form (10) (or (11)) for the monodromy groups $G$ we are interested in: roots of unity and classical groups over finite fields.

5.2. **Gaussian sums in $\mu_d(\mathbb{F}_\mathfrak{l})$: exponential sums over subgroups of $\mathbb{F}_\mathfrak{l}^\times$.** We assume that $\mathbb{F}_\mathfrak{l}$ contains a primitive $d$th root of unity. For $G = \mu_d(\mathbb{F}_\mathfrak{l}) \leqslant \mathbb{F}_\mathfrak{l}^\times$, the sum (10) is a "character sum with exponentials"

$$\sum_{v\in\mu_d(\mathbb{F}_\mathfrak{l})} \psi(v) = \sum_{i=1}^{d} \psi(\zeta_d^i),$$

or equivalently a sum over a subgroup of $\mathbb{F}_\mathfrak{l}^\times$.

For $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$, 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 $\ell$. Square-root cancellation corresponds to $\alpha(G) \geqslant \frac{\log d}{2\log \ell}$, and $\frac{\log d}{\log \ell} < 1$ since $\ell \equiv 1 \pmod d$.

We first review the results of Heath-Brown-Konyagin which give explicit bounds for $d$ at least of the order of $\ell^{1/3}$.

**Theorem 5.4** ([HBK00, Theorem 1])**.** *For $\psi$ a nontrivial additive character of $\mathbb{F}_\ell$, (10) holds with $G = \mu_d(\mathbb{F}_\ell)$ and $\alpha(G) = \alpha$ in any of the following three cases:*

$$0 < \alpha \leqslant 1/16 \quad \text{and} \quad d \gg \ell^{1/3+8\alpha/3} \tag{13}$$

$$0 < \alpha \leqslant 1/6 \quad \text{and} \quad d \gg \ell^{2/5+8\alpha/5} \tag{14}$$

$$0 < \alpha \leqslant 1/2 \quad \text{and} \quad d \gg \ell^{1/2+\alpha}. \tag{15}$$

On the other hand, the results of Bourgain and others give (non-explicit) bounds for $d$ as small as desired:

**Theorem 5.5** ([BK03, Theorem 2.1])**.** *Let $x, y \in \mathbb{F}_\ell^\times$ and let $d$ be the order of $y$. 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 implied constant. Thus, (10) for $G = \mu_d(\mathbb{F}_\ell)$ holds with $\alpha(G) = \alpha(\delta)$ if $d \geqslant \ell^\delta$.*

*Remark* 5.6. The $\alpha(\delta)$ arising in Theorem 5.5 are not estimated explicitly in [BK03][5], but one typically expects them to be very small.

The situation is more complicated when $\mathbb{F}_\mathfrak{l}$ 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 5.7.** *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 $\ell$-adic sheaf $\mathcal{F}$ on $\mathbb{P}^1_{\mathbb{F}_q}$. If either $\operatorname{rank}(\mathcal{F}) > 1$ or if the function $x \mapsto t(x^k)$ is nonconstant*

[5]This could be done with some effort using e.g. [Gar07] (see also [Kow11]).

*for $x^k \in U_{\mathcal{F}}(\mathbb{F}_q)$, 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 $\sum_{x\in H} t(x) = \frac{1}{k}\sum_{x\in\mathbb{F}_q^\times} t(x^k)$. The sheaf $\mathcal{F}' = [x \mapsto x^k]^*\mathcal{F}$ is geometrically irreducible and $t_{\mathcal{F}'}(x) = t(x)$ when $x^k \in U_{\mathcal{F}}(\mathbb{F}_q)$. By Theorem 2.1, the sum is

$$\ll \frac{\mathrm{rank}(\mathcal{F}')\,\mathrm{cond}(\mathcal{F}')}{k}\sqrt{q} \ll \frac{\mathrm{rank}(\mathcal{F})k\,\mathrm{cond}(\mathcal{F})}{k}\sqrt{q} \leqslant \mathrm{cond}(\mathcal{F})^2\sqrt{q},$$

unless $\mathcal{F}'$ is geometrically trivial. In the latter case $\mathcal{F}' \cong \alpha\otimes\overline{\mathbb{Q}}_\ell$ for some $\alpha \in \overline{\mathbb{Q}}_\ell$ by Clifford theory (since $\pi_{1,q}/\pi_{1,q}^{\mathrm{geom}} \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$), so that $t_{\mathcal{F}}(x^k) = \alpha$ whenever $x^k \in U_{\mathcal{F}}(\mathbb{F}_q)$. □

**Corollary 5.8.** *The bound (10) for $G = \mu_d(\mathbb{F}_\mathfrak{l})$ holds uniformly with respect to all nontrivial $\psi \in \widehat{\mathbb{F}}_\mathfrak{l}$ with $\alpha(G) = \alpha \in (0, 1/2)$ whenever $d \geqslant |\mathbb{F}_\mathfrak{l}|^{1/2+\alpha}$.*

*Remark* 5.9. Alternatively, one could also proceed by completion as in [Kor89].

By [BC06], the results of Bourgain and others (Theorem 5.5) generalize to all finite fields, up to adding an assumption involving subfields:

**Theorem 5.10** ([BC06, Theorem 2])**.** *For every $\delta > 0$, there exists $\alpha = \alpha(\delta) > 0$ such that with $\alpha(G) = \alpha$, (10) for $G = \mu_d(\mathbb{F}_\mathfrak{l})$ holds if*

$$d > |\mathbb{F}_\mathfrak{l}|^\delta \text{ and } \frac{d}{(d, |F^\times|)} \geqslant |\mathbb{F}_\mathfrak{l}|^\delta \tag{16}$$

*for all proper subfields $F \leqslant \mathbb{F}_\mathfrak{l}$.*

*Remark* 5.11. Note that Condition (16) amounts to $d > |\mathbb{F}_\mathfrak{l}|^\delta$ in the following situations:

- $d$ is prime and $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell(\mu_d)$, or
- $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$ (recovering Theorem 5.5) or $[\mathbb{F}_\mathfrak{l} : \mathbb{F}_\ell]$ is prime, or
- $\delta > 1/2$ (recovering Corollary 5.8).

5.3. **Gaussian sums in classical groups over finite fields.** Let us now assume that $G$ is a finite classical group of Lie type in $\mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$.

**Proposition 5.12.** *Let $\mathbb{F}_\mathfrak{l}$ be a finite field and $n \geqslant 2$ be an integer. The bound (10) holds for*

| $G$ | $\alpha(G)$ |
|---|---|
| $\mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$ | $\frac{n(n-1)}{2}$ |
| $\mathrm{SL}_n(\mathbb{F}_\mathfrak{l})$ | $\frac{n^2-1}{2}$ |
| $\mathrm{Sp}_n(\mathbb{F}_\mathfrak{l})$, $\mathrm{SO}_n^-(\mathbb{F}_\mathfrak{l})$ ($n$ even) | $\frac{n(n+2)}{8}$ |
| $\mathrm{SO}_n(\mathbb{F}_\mathfrak{l})$ ($n$ odd) | $\frac{n^2-1}{8}$ |
| $\mathrm{SO}_n^+(\mathbb{F}_\mathfrak{l})$ ($n$ even) | $\frac{n(n-2)}{8}$ |

*Remark* 5.13. By Lemma 4.16,

$$\frac{\log|G|}{\log|\mathbb{F}_\mathfrak{l}|} = \dim G + O_n\left(\frac{1}{\log|\mathbb{F}_\mathfrak{l}|}\right),$$

so square-root cancellation corresponds to $\alpha(G) > \dim(G)/2$. Hence, by the dimensions given in Table 1, there is square-root cancellation in the special linear case, but not for the others. Note that the quality of the bounds improves 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 $a \in \mathbb{F}_\mathfrak{l}^\times$ corresponding to $\psi$ through the isomorphism $\widehat{\mathbb{F}}_\mathfrak{l} \cong \mathbb{F}_\mathfrak{l}$.

(1) By [Kim97a, Theorem 4.2], the Gaussian sum (10) for $\mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$ is equal to $(-1)^n|\mathbb{F}_\mathfrak{l}|^{\frac{n(n-1)}{2}}$.

(2) By [Kim97a, Corollary 5.2], Deligne's bound for hyper-Kloosterman sums and Lemma 4.16, the Gaussian sum (10) for $\mathrm{SL}_n(\mathbb{F}_\mathfrak{l})$ is

$$\frac{|\mathbb{F}_\mathfrak{l}|^{\binom{n}{2}}\,\mathrm{Kl}_n(a^n)}{|G|} \ll_n |\mathbb{F}_\mathfrak{l}|^{\frac{n^2-n}{2}+\frac{n-1}{2}-n^2+1} = |\mathbb{F}_\mathfrak{l}|^{\frac{-n^2+1}{2}}.$$

(3) By [Kim98b, Theorem A], the Gaussian sum $\sum_{v\in \mathrm{Sp}_{2m}(\mathbb{F}_\mathfrak{l})}\psi(\mathrm{tr}\, v)$ is equal to

$$L^{m^2-1}\sum_{r=0}^{\lfloor m/2\rfloor} L^{r(r+1)}\binom{m}{2r}_L \prod_{i=1}^{r}(L^{2i-1}-1) \times \sum_{l=1}^{\lfloor m/2\rfloor - r+1} L^l\,\mathrm{Kl}_2(a^2)^{m-2r+2-2l} \times \sum_{j_1,\dots,j_{l-1}} (L^{j_1}-1)\dots(L^{j_{l-1}}-1)$$

for $L = |\mathbb{F}_\mathfrak{l}|$, 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 $\prod_{i=1}^{r}(L^{2i-1}-1) < L^{r^2}$ and

$$\mathrm{Kl}_2(a^2)^{t+2-2l}\sum_{j_1,\dots,j_{l-1}}(L^{j_1}-1)\dots(L^{j_{l-1}}-1) \ll_n L^{(l-1)(t-(l-1))}$$

for $t = m-2r$ (see [Kim98b, Remark (1) p. 65] for the second one), we find that the Gaussian sum is

$$\ll_m \begin{cases} |\mathbb{F}_\mathfrak{l}|^{\frac{3m^2+m}{2}} & \text{if } m \text{ even} \\ |\mathbb{F}_\mathfrak{l}|^{\frac{2m^2+m-1}{2}} & \text{if } m \text{ odd,} \end{cases}$$

and the result follows by Lemma 4.16.

(4) By [Kim98a, Theorem A],

$$\sum_{v\in \mathrm{SO}_{2m+1}(\mathbb{F}_\mathfrak{l})} \psi(\operatorname{tr} v) = \psi(1) \sum_{v\in \mathrm{Sp}_{2m}(\mathbb{F}_\mathfrak{l})} \psi(\operatorname{tr} v),$$

the result follows by the previous bound and Lemma 4.16.

(5) Similarly, by [KL96, Theorem 4.3],

$$\sum_{v\in \mathrm{SO}^+_{2m}(\mathbb{F}_\mathfrak{l})} \psi(\operatorname{tr} v) = |\mathbb{F}_\mathfrak{l}|^{-m} \sum_{v\in \mathrm{Sp}_{2m}(\mathbb{F}_\mathfrak{l})} \psi(\operatorname{tr} v).$$

(6) This is analogous to (3), using [Kim97b, Theorem A].

□

## 6. Equidistribution of shifted short sums

As a first application of Theorem 3.18, we prove in particular Propositions 1.1 and 1.3 introduced in Section 1.5.1.

### 6.1. Statement of the result.

**Theorem 6.1.** *Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda\in\Lambda$, let $t : \mathbb{F}_q \to \mathbb{F}_\mathfrak{l}$ be the trace function associated to the sheaf $\mathcal{F} = \mathcal{F}_\lambda$, $I \subset \mathbb{F}_q$ of size $L$ such that $\mathcal{F}$ is $I$-compatible, and $a \in \mathbb{F}_\mathfrak{l}$.*

*(1) If $G$ is classical, then the probability $P\big(S(t, I + x) \equiv a\big)$ (with respect to the uniform measure on $\mathbb{F}_q$) is equal to*

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|} + O\left(\frac{1}{|\mathbb{F}_\mathfrak{l}|^{L\alpha(G)}} + \frac{L|\mathbb{F}_\mathfrak{l}|^{L\beta_+(G)+2\beta_-(G)-1}}{q^{1/2}}\right), \tag{17}$$

*uniformly with respect to $a$, where $\alpha(G), \beta_\pm(G) > 0$ are given explicitly in Table 1.*

*(2) If $G = \mu_d$, for every $\delta \in (0, 1)$ there exists $\alpha = \alpha(\delta) > 0$ such that the probability the probability $P\big(S(t, I + x) \equiv a\big)$ is*

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|} + O\left(\frac{1}{|\mathbb{F}_\mathfrak{l}|^{L\alpha}} + \frac{Ld^{L+1}}{q^{1/2}|\mathbb{F}_\mathfrak{l}|^{\min(L\alpha,1)}}\right) \tag{18}$$

*uniformly with respect to $a$, when Condition (16) holds[6] for all proper subfields $F \leqslant \mathbb{F}_\mathfrak{l}$. 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 $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$, then Condition (16) is $d \geqslant \ell^\delta$ and explicitly, we can choose $\alpha(\delta)$ as in (2).*

*The implied constants depend only on the monodromy group structure and on a bound on the conductor of the family.*

*Proof.* By Corollary 3.20 and Proposition 5.1, we have for all $a \in \mathbb{F}_\mathfrak{l}$ that the probability $P\left(S(t, I + x) \equiv a\right)$ is equal to

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|} + O\left(\frac{1}{|\mathbb{F}_\mathfrak{l}|^{L\alpha(G)}} + \frac{LE(G, L, \mathbb{F}_\mathfrak{l})}{q^{1/2}|\mathbb{F}_\mathfrak{l}|^{\min(L\alpha(G),1)}}\right) \tag{19}$$

[6] See also Remark 5.11.

In the classical case, note that $\alpha(G) > 1$ by Table 1. □

### 6.2. **Analysis of the ranges.**

6.2.1. *Case $G$ classical.* Since $\alpha(G) > 1$, the error term of (17) is negligible with respect to the main term (i.e. with a ratio which is $o(1)$) when $L|\mathbb{F}_{\mathfrak{l}}|^{L\beta_+(G)+2\beta_-(G)} = o(q^{1/2})$. Note that:

- When $L = 1$, this is $|\mathbb{F}_{\mathfrak{l}}| = o\left(q^{1/\dim(G)}\right)$.
- Let $q = p^e$. When $d = p$ (e.g. for Kloosterman sums), this implies that $e > 2(L\beta_+(G) + 2\beta_-(G))$ (see Section 3.5).

6.2.2. *Case $G$ cyclic.* The error term of (17) is negligible with respect to the main term when $L > 1/\alpha > 1$ and $Ld^{L+1} = o(q^{1/2})$. In particular, $1 < 1/\alpha < L < \log q/2$.

### 6.3. **Examples.**

6.3.1. *Kloosterman sums.* By Proposition 3.13, Theorem 6.1 gives Proposition 1.1. Replacing $a$ by $aq^{(n-1)/2}$ and using the uniformity statement shows that the results hold as well for unnormalized Kloosterman sums.

6.3.2. *Point-counting on families of curves.* The case $n$ even of Proposition 1.1 also applies to the point-counting on families of hyperelliptic curves from Proposition 3.14 when $\mathbb{F}_{\mathfrak{l}} = \mathbb{F}_\ell$, normalized or not.

6.3.3. *Multiplicative characters.* By Proposition 3.12 and Example 3.16, Theorem 6.1 yields Proposition 1.3.

## 7. 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 sums of reduced trace functions in coherent families, giving in particular the results from Section 1.5.2.

### 7.1. **Families of short sums.**

7.1.1. *Definition and examples.*

Definition 7.1. Let $t : \mathbb{F}_q \to \mathbb{F}_{\mathfrak{l}}$ be any function. A *family of sums with respect to $t$* is a family

$$\Big(S(t, \mathcal{I}(k))\Big)_{k\in\mathcal{I}} \tag{20}$$

for a finite parameter space $\mathcal{I}$ with an injective map $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, $k \mapsto \mathcal{I}(k)$, where $\mathcal{P}(\mathbb{F}_q)$ is the set of subsets of $\mathbb{F}_q$.

*Examples* 7.2.

(1) (Intervals) When $q = p$, we can study sums over the integer intervals $\{\mathcal{I}(k) = \{1, \dots, k\} : k \in \mathcal{I}\}$ for a parameter set $\mathcal{I} \subset \{1, \dots, p\} \cong \mathbb{F}_p$.

(2) (Boxes) More generally, when $q = p^e$, we can fix a $\mathbb{F}_p$-basis of $\mathbb{F}_q$, identify $\mathbb{F}_q$ with $\{1, \dots, p\}^e$, and study sums over the "boxes"[7]

$$\mathcal{I}(k) = \{1, \dots, k_1\} \times \{1, \dots, k_2\} \times \cdots \times \{1, \dots, k_e\},$$

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 families $\mathcal{I}_i \to \mathcal{P}(\mathbb{F}_p)$ $(i = 1, \dots, e)$, 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

$$\mathcal{I}(k_1, \dots, k_e) = \prod_{i=1}^{e} \mathcal{I}_i(k_i) \subset \mathbb{F}_q.$$

7.1.2. *Distribution questions.* We are interested in the distribution of the random variable (20) with the uniform measure on $\mathcal{I}$, asymptotically with respect to the parameters $q$ and $|\mathbb{F}_\mathfrak{l}|$. Thus, we are led to study the density

$$\Phi(t, \mathcal{I}, a) := \frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}(k)) \equiv a\}|}{|\mathcal{I}|} \quad (a \in \mathbb{F}_\mathfrak{l}).$$

*Example* 7.3. Let $\ell \geqslant 2$ be an integer and consider the family $\mathcal{I}$ of Example 7.2 (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 the introduction, 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 $a \in \mathbb{F}_\ell$, as $p \to +\infty$. Therefore, the random variable (20) converges in law to the uniform distribution on $\mathbb{F}_\ell$ if $\ell$ 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* 7.4. The study of $\Phi(t, \mathcal{I}, a)$ for the family of Example 7.2 (3) is the finite analogue of the distribution questions considered in [PG17], generalizing [Lam13] to trace functions.

7.2. **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 (20) to converge to the uniform distribution on $\mathbb{F}_\mathfrak{l}$. Albeit we cannot show that in this most general setting, we have nonetheless a result on average over shifts.

[7] Of course, one should not replace the sums over $\{\{1, \dots, k\} : 1 \leqslant k \leqslant p\}$ by the sums over $\{\{1, \dots, k\} : 1 \leqslant k \leqslant q\}$.

DEFINITION 7.5. 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

$$\begin{aligned} \mathcal{I} + x = \mathcal{I}'(\cdot\,, x) : &\qquad \mathcal{I} \to \mathcal{P}(\mathbb{F}_q) &&\text{for } x \in \mathbb{F}_q, \\ \mathcal{I}_k = \mathcal{I}'(k, \cdot\,) : &\qquad \mathbb{F}_q \to \mathcal{P}(\mathbb{F}_q) &&\text{for } k \in \mathcal{I}. \end{aligned}$$

Hence, for a family $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, we have $\mathcal{I} = \mathcal{I} + 0 = \mathcal{I}'(\cdot\,, 0)$ and

$$\begin{aligned} \Phi(t, \mathcal{I}', a) &= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \Phi(t, \mathcal{I} + x, a) = \frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} \Phi(t, \mathcal{I}_k, a), \qquad (21) \\ \Phi(t, \mathcal{I} + x, a) &= \frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}(k) + x) \equiv a\}|}{|\mathcal{I}|} \quad (x \in \mathbb{F}_q), \\ \Phi(t, \mathcal{I}_k, a) &= \frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}(k) + x) \equiv a\}|}{q} \quad (k \in \mathcal{I}), \end{aligned}$$

for any function $t : \mathbb{F}_q \to \mathbb{F}_\mathfrak{l}$ and $a \in \mathbb{F}_\mathfrak{l}$.

DEFINITION 7.6. For a family $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, we define the quantities

$$\begin{aligned} M_\mathcal{I} &= \Big| \bigcup_{k \in \mathcal{I}} \mathcal{I}(k) \Big|, \\ h_\mathcal{I}(d) &= \Big| \{(k_1, k_2) \in \mathcal{I}^2 : |\mathcal{I}(k_1) \Delta \mathcal{I}(k_2)| = d\} \Big| \ (d \geqslant 1), \\ H_\mathcal{I}(\alpha, n) &= \frac{1}{|\mathcal{I}|} \sum_{d \geqslant 1} \frac{h_\mathcal{I}(d)}{n^{\alpha d}} \ (n > 0,\ \alpha > 0), \end{aligned}$$

where $\Delta$ denotes the symmetric difference operator.

The following will be proven in Sections 7.4–7.6:

**Theorem 7.7.** *Let $(\mathcal{F}_\lambda)_{\lambda \in \Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda \in \Lambda$, let $t : \mathbb{F}_q \to \mathbb{F}_\mathfrak{l}$ be the trace function associated to the sheaf $\mathcal{F} = \mathcal{F}_\lambda$, and let $\mathcal{I}$ be a family of sums with respect to $t$ so that $\mathcal{F}$ is $\bigcup_{k \in \mathcal{I}} \mathcal{I}(k)$-compatible. The averaged variance*

$$V(t, \mathcal{I}) = \sum_{a \in \mathbb{F}_\mathfrak{l}} \frac{1}{q} \sum_{x \in \mathbb{F}_q} \left( \Phi(t, \mathcal{I} + x, a) - \frac{1}{|\mathbb{F}_\mathfrak{l}|} \right)^2 \qquad (22)$$

*is equal to*

$$\frac{1}{|\mathcal{I}|} \left( 1 + O\left( \tilde{V}(t, \mathcal{I}) \right) \right)$$

*with $\tilde{V}(t, \mathcal{I})$ given by*

$$H_\mathcal{I}(\alpha(G), |\mathbb{F}_\mathfrak{l}|) \left( 1 + \frac{M_\mathcal{I}}{q^{1/2}} \times \begin{cases} |\mathbb{F}_\mathfrak{l}|^{\beta_+(G) M_\mathcal{I} + 2\beta_-(G)} & \text{if } G \text{ classical} \\ d^{M_\mathcal{I}+1} & \text{if } G \text{ cyclic} \end{cases} \right),$$

*for $\alpha(G), \beta_\pm(G) > 0$ given in Table 1. The implied constants depend only on the monodromy group structure and on a bound on the conductor of the family.*

Thus, $V(t, \mathcal{I})$ should be small as $|\mathcal{I}| \to +\infty$, and we have:

**Corollary 7.8.** *In the setting of Theorem 7.7,*

$$\Phi(t,\mathcal{I}',a)=\frac{1}{|\mathbb{F}_\mathfrak{l}|}+O\left(V(t,\mathcal{I})^{1/2}\right)$$

*uniformly with respect to* $a\in\mathbb{F}_\mathfrak{l}$.

*Proof.* By the Cauchy-Schwarz inequality applied to the sum over $x$,

$$\begin{aligned}\sum_{a\in\mathbb{F}_\mathfrak{l}}\left(\Phi(t,\mathcal{I}',a)-\frac{1}{|\mathbb{F}_\mathfrak{l}|}\right)^2 &= \sum_{a\in\mathbb{F}_\mathfrak{l}}\left(\frac{1}{q}\sum_{x\in\mathbb{F}_q}\left(\Phi(t,\mathcal{I}+x,a)-\frac{1}{|\mathbb{F}_\mathfrak{l}|}\right)\right)^2\\ &\leqslant V(t,\mathcal{I}).\end{aligned}$$

□

7.3. **Consequences.** Using Corollary 7.8, 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 7.3.

The results presented in this section will be proven in Sections 7.7–7.9.

Definition 7.9. For a subset $E\subset\mathbb{F}_q$ and a fixed choice of a $\mathbb{F}_p$-basis of $\mathbb{F}_q$ which identifies the latter with $\{1,\dots,p\}^e$, the *bounding box* $B_E$ of $E$ is defined as $E\subset B_E=\prod_{i=1}^e[\min_{x\in E}x_i,\max_{x\in E}x_i]\subset\mathbb{F}_q$.

7.3.1. *Shifts of small subsets.* First, we consider shifts of subsets of moderate size following Example 7.2 (3). The Gaussian distribution for complex-valued trace functions from [PG17] becomes a uniform distribution when the latter are reduced in $\mathbb{F}_\mathfrak{l}$:

**Proposition 7.10** (Shifts of small subsets)**.** *Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda\in\Lambda$, let $t:\mathbb{F}_q\to\mathbb{F}_\mathfrak{l}$ be the trace function associated to the sheaf $\mathcal{F}=\mathcal{F}_\lambda$ on $\mathbb{P}^1_{\mathbb{F}_q}$. Let $\varepsilon,\varepsilon'\in(0,1/2)$, $\delta\in(0,1)$, and let $E\subset\mathbb{F}_q$. We assume that:*

- *For a fixed $\mathbb{F}_p$-basis of $\mathbb{F}_q$, identifying the latter with $\{1,\dots,p\}^e$, we have $|B_E|<q^{1/2-\varepsilon'}$ and $B_E\subset[0,\delta p)^e$.*
- *If $\mathcal{F}=\mathcal{L}_{\chi(f)}$ is a Kummer sheaf with $f=f_1/f_2\in\mathbb{F}_q(X)$, $(f_1,f_2)=1$, then $\delta<1/\deg(f_1)$.*
- *If $G=\mu_d$ with $\mathbb{F}_\mathfrak{l}\neq\mathbb{F}_\ell$ and $d$ is nonprime, then Condition (16) holds (e.g. $d\geqslant|\mathbb{F}_\mathfrak{l}|^{1/2+\alpha}$ for some $\alpha>0$).*

*Then the density*

$$P\big(S(t,E+x)\equiv a\big)=\frac{|\{x\in\mathbb{F}_q:S(t,E+x)\equiv a\}|}{q}$$

*is given by*

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|}+\begin{cases}O\left(\frac{1}{q^{1/4-\varepsilon/2}}+\left(\frac{|E|\log|\mathbb{F}_\mathfrak{l}|}{\log q}\right)^{\frac12}\right) & \text{if } G \text{ classical}\\ O\left(\frac{1}{q^{1/4-\varepsilon/2}}+\left(\frac{|E|\log d}{\log q}\right)^{\frac12}\right) & \text{if } G \text{ cyclic}\end{cases}$$

*uniformly for all $a \in \mathbb{F}_\mathfrak{l}$, where the implied constants depend on $\varepsilon$, $\varepsilon'$, $\delta$, on the monodromy structure and on a bound on the conductor of the family.*

*Remark* 7.11. This is nontrivial if

$$|E| \log |\mathbb{F}_\mathfrak{l}| = o(\log q) \quad (\text{resp. } |E| \log d = o(\log q)).$$

Note that when the sheaf $\mathcal{F}$ of $\mathbb{F}_\mathfrak{l}$-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 3.5).

*Remark* 7.12. The first condition about $B_E$ in the statement can be included in the second one by taking $\delta < p^{-1/2-\varepsilon'}$.

By taking $E = \{0\}$, we get the following corollary, which should be compared with the case $I = \{0\}$ of Theorem 6.1:

**Corollary 7.13.** *Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda \in \Lambda$, let $t : \mathbb{F}_q \to \mathbb{F}_\mathfrak{l}$ be the trace function associated to the sheaf $\mathcal{F} = \mathcal{F}_\lambda$ on $\mathbb{P}^1_{\mathbb{F}_q}$, and let $\varepsilon \in (0, 1/2)$. We assume that if $G = \mu_d$ with $\mathbb{F}_\mathfrak{l} \neq \mathbb{F}_\ell$ and $d$ nonprime, then Condition (16) holds (e.g. $d \geqslant |\mathbb{F}_\mathfrak{l}|^{1/2+\alpha}$ for some $\alpha > 0$). Then*

$$P\big(t(x) \equiv a\big) = \frac{1}{|\mathbb{F}_\mathfrak{l}|} + \begin{cases} O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{\log|\mathbb{F}_\mathfrak{l}|}{\log q}\right)^{\frac{1}{2}}\right) & : G \text{ classical} \\ O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{\log d}{\log q}\right)^{\frac{1}{2}}\right) & : G \text{ cyclic} \end{cases}$$

*uniformly for all $a \in \mathbb{F}_\mathfrak{l}$, where the implied constants depend on $\varepsilon$, on a bound on the conductor of the family, and on the type of $G$ in the classical case.*

*Example* 7.14. By Section 3.3.2, Proposition 7.10 and Corollary 7.13 apply to:

- Kloosterman sums of fixed rank (normalized or not) and multiplicative characters composed with rational functions, giving Proposition 1.4.
- Point-counting functions for families of hyperelliptic curves (normalized or not).

7.3.2. *Partial intervals.* The second example notably generalizes the result of [LZ12] (see Example 7.3) to all multiplicative characters:

**Proposition 7.15** (Partial intervals)**.** *Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda \in \Lambda$, let $t : \mathbb{F}_q \to \mathbb{F}_\mathfrak{l}$ be the trace function associated to the sheaf $\mathcal{F} = \mathcal{F}_\lambda$, and let $\varepsilon, \varepsilon' \in (0, 1/2)$. We assume that if $G = \mu_d$ with $\mathbb{F}_\mathfrak{l} \neq \mathbb{F}_\ell$ and $d$ nonprime, then Condition (16) holds (e.g. $d \geqslant |\mathbb{F}_\mathfrak{l}|^{1/2+\alpha}$ for some $\alpha > 0$). Then 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*

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|} + \begin{cases} O\left(\frac{1}{p^{1/4-\varepsilon/2}} + \left(\frac{\log|\mathbb{F}_\mathfrak{l}|}{\log p}\right)^{\frac{1}{2}} + \delta_{S(t,\mathbb{F}_p)\neq 0}\left(\frac{|\mathbb{F}_\mathfrak{l}|\log p}{p\log|\mathbb{F}_\mathfrak{l}|}\right)^{\frac{1}{2}}\right) & \text{if } G \text{ classical} \\ O\left(\frac{1}{p^{1/4-\varepsilon/2}} + \left(\frac{\log d}{\log p}\right)^{\frac{1}{2}} + \delta_{S(t,\mathbb{F}_p)\neq 0}\left(\frac{|\mathbb{F}_\mathfrak{l}|\log p}{p\log d}\right)^{\frac{1}{2}}\right) & \text{if } G \text{ cyclic} \end{cases}$$

*uniformly for all $a \in \mathbb{F}_\mathfrak{l}$, where the implied constants depend on $\varepsilon, \varepsilon'$, on a bound on the conductor of the family, and on the monodromy group structure of the family.*

*Examples* 7.16. By Section 3.3.2:

(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 $d$, giving Proposition 1.3. When $\chi$ 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 $\mathbb{F}_\mathfrak{l} = \mathbb{F}_\ell$, this also applies to the point-counting functions on families of hyperelliptic curves from Proposition 2.8. See also [MZ14] for an analogue of [LZ12] to the counting of points of a plane curve in rectangles.

*Remark* 7.17. We will see that it is unclear whether this can be generalized to the case $e \geqslant 2$ (see Example 7.2 (2)) because of "diagonal" terms in the errors. Since the case $d = p$, $G$ classical forces to take $e \to +\infty$ (see Section 3.5 and Remark 7.11), Proposition 7.15 does not make sense for Kloosterman sums.

Even though Proposition 7.15 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 7.2.

**Proposition 7.18** (Partial intervals with shifts of small subsets)**.** *Let $(\mathcal{F}_\lambda)_{\lambda\in\Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda \in \Lambda$, let $t : \mathbb{F}_q \to \mathbb{F}_\mathfrak{l}$ be the trace function associated to the sheaf $\mathcal{F} = \mathcal{F}_\lambda$ on $\mathbb{P}^1_{\mathbb{F}_q}$, and let $\varepsilon, \varepsilon' \in (0, 1/2)$, $\delta \in (0, 1)$. We fix a $\mathbb{F}_p$-basis of $\mathbb{F}_q$ and identify the latter with $\{1, \dots, p\}^e$. We let $E_2, \dots, E_e \subset \{1, \dots, p\}$ be such that*

$$|B_E| \leqslant q^{1/2-\varepsilon'} \text{ and } E_i \subset [1, \delta p) \ (2 \leqslant i \leqslant e),$$

*where $B_E$ is the bounding box of $E = E_2 \times \cdots \times E_e$ in $\mathbb{F}_p^{e-1}$. Moreover, we assume that:*

- *If $\mathcal{F}$ is a Kummer sheaf $\mathcal{L}_{\chi(f_1/f_2)}$, then $\delta < 1/\deg(f_1)$.*
- *If $G = \mu_d$ and $\mathbb{F}_\mathfrak{l} \neq \mathbb{F}_\ell$ and $d$ is nonprime, then Condition (16) holds (e.g. if $d \geqslant |\mathbb{F}_\mathfrak{l}|^{1/2+\alpha}$ for some $\alpha > 0$).*

*Then the density*

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

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

$$\frac{1}{|\mathbb{F}_\mathfrak{l}|} + \begin{cases} O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{|E|\log|\mathbb{F}_\mathfrak{l}|}{\log q}\right)^{\frac{1}{2}}\right) & \text{if } G \text{ classical} \\ O\left(\frac{1}{q^{1/4-\varepsilon/2}} + \left(\frac{|E|\log d}{\log q}\right)^{\frac{1}{2}}\right) & \text{if } G \text{ cyclic} \end{cases}$$

*uniformly for all $a \in \mathbb{F}_\mathfrak{l}$, where the implied constants depend on $\varepsilon$, $\varepsilon'$ and $\delta$.*

*Example* 7.19. As for Proposition 7.10, this applies by Section 3.3.2 to:

- Kloosterman sums of fixed rank (normalized or not), multiplicative characters composed with rational functions, giving Proposition 1.6.
- Point-counting functions on families of hyperelliptic curves (normalized or not).

7.4. **Probabilistic model.** Let $\mathcal{F}$ be a sheaf of $\mathbb{F}_\mathfrak{l}$-modules on $\mathbb{P}^1_{\mathbb{F}_q}$, part of a coherent family, with monodromy group $G \leqslant \mathrm{GL}_n(\mathbb{F}_\mathfrak{l})$. We apply the probabilistic model from Section 3 to study of the distribution of families of short sums.

Again, we let $X$ be a random variable uniformly distributed in $G$, and $Z$ be its image through the map $G \to G^\sharp \xrightarrow{\mathrm{tr}} \mathbb{F}_\mathfrak{l}$. 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 $G^{\mathbb{N}}$. For a finite parameter space $\mathcal{I}$ with a map $\mathcal{I} \to \mathcal{P}_f(\mathbb{N})$, we consider for all $a \in \mathbb{F}_\mathfrak{l}$ the random variable

$$\Phi(\mathcal{I}, a) = \frac{|\{k \in \mathcal{I} : S(\mathcal{I}(k)) \equiv a\}|}{|\mathcal{I}|}.$$

In this setting, Corollary 3.20 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 7.20.** *In the above setting, if $\mathcal{F}$ is $\bigcup_{k\in\mathcal{I}} \mathcal{I}(k)$-compatible, for any function $h : \mathbb{F}_\mathfrak{l} \to \mathbb{R}_{\geqslant 0}$ and any $a \in \mathbb{F}_\mathfrak{l}$, we have*

$$\mathbb{E}\Big(h(\Phi(t, \mathcal{I}+x, a))\Big) = \mathbb{E}\Big(h(\Phi(\mathcal{I}, a))\Big)\left(1 + O\left(\frac{M_\mathcal{I} E(G, M_\mathcal{I}, \mathbb{F}_\mathfrak{l})}{q^{1/2}}\right)\right).$$

In other words, for all $a \in \mathbb{F}_\mathfrak{l}$ the random variable $(\Phi(t, \mathcal{I}+x, a))_{x\in\mathbb{F}_q}$ converges in law (with respect to the parameters, $q$, $|\mathbb{F}_\mathfrak{l}|$, $\mathcal{I}$) to the random variable $\Phi(\mathcal{I}, a)$ if the error term is $o(1)$ as the parameters vary.

7.5. **Expected value.** We first consider the expected value of $\Phi(\mathcal{I}, a)$, which gives a preliminary version of Theorem 7.7 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 7.15 by removing the shifts for some specific families.

7.5.1. *Computation in the model.*

DEFINITION 7.21. For a family $\mathcal{I} \to \mathcal{P}(\mathbb{F}_q)$, we define

$$\begin{aligned} g_{\mathcal{I}}(d) &= |\{k \in \mathcal{I} : |\mathcal{I}(k)| = d\}| \ (d \geqslant 0), \\ G_{\mathcal{I}}(\alpha, n) &= \frac{1}{|\mathcal{I}|} \sum_{d \geqslant 1} \frac{g_{\mathcal{I}}(d)}{n^{\alpha d}} \ (n > 0, \ \alpha > 0). \end{aligned}$$

**Proposition 7.22.** *In the notations of Section 7.4, we have for $a \in \mathbb{F}_\mathfrak{l}$:*

$$\mathbb{E}\left(\Phi(\mathcal{I}, a)\right) = \frac{1}{|\mathbb{F}_\mathfrak{l}|} + O\left(G_{\mathcal{I}}(\alpha(G), |\mathbb{F}_\mathfrak{l}|)\right).$$

*Proof.* By Corollary 5.2,

$$\begin{aligned} \mathbb{E}\left(\Phi(\mathcal{I}, a)\right) &= \frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} \mathbb{E}(\delta_{S(\mathcal{I}(k)) \equiv a}) = \frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} P(S(\mathcal{I}(k)) \equiv a) \\ &= \frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} \left( \frac{1}{|\mathbb{F}_\mathfrak{l}|} + O\left( |\mathbb{F}_\mathfrak{l}|^{-|\mathcal{I}(k)|\alpha(G)} \right) \right) \\ &= \frac{1}{|\mathbb{F}_\mathfrak{l}|} + O\left( \frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} |\mathbb{F}_\mathfrak{l}|^{-|\mathcal{I}(k)|\alpha(G)} \right). \end{aligned}$$

□

7.5.2. *Conclusion.* By Propositions 7.20 and 7.22, we get the following preliminary version of Theorem 7.7:

**Proposition 7.23.** *Let $(\mathcal{F}_\lambda)_{\lambda \in \Lambda}$ be a coherent family with monodromy group structure $G$. For $\lambda \in \Lambda$, let $t : \mathbb{F}_q \to \mathbb{F}_\mathfrak{l}$ be the trace function associated to the sheaf $\mathcal{F} = \mathcal{F}_\lambda$ on $\mathbb{P}^1_{\mathbb{F}_q}$, and let $\mathcal{I}$ be a family of sums such that $\mathcal{F}$ is $\bigcup_{k \in \mathcal{I}} \mathcal{I}(k)$-compatible. For all $a \in \mathbb{F}_\mathfrak{l}$,*

$$\mathbb{E}(\Phi(t, \mathcal{I} + x, a)) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \Phi(t, \mathcal{I} + x, a) = \frac{1}{|\mathbb{F}_\mathfrak{l}|} + O(\varepsilon(q, G, \mathcal{I})),$$

*where*

$$\varepsilon(q, G, \mathcal{I}) = G_{\mathcal{I}}(\alpha(G), |\mathbb{F}_\mathfrak{l}|) + \frac{M_{\mathcal{I}} E(G, M_{\mathcal{I}}, \mathbb{F}_\mathfrak{l})}{q^{1/2}}.$$

As a corollary, we obtain as well a preliminary version of Proposition 7.32 about unshifted "complete" families, by exchanging summations (see (21)):

**Corollary 7.24.** *In the setting of Proposition 7.23, assume that for all $a \in \mathbb{F}_\mathfrak{l}$, $\Phi(t, \mathcal{I}_k, a)$ does not depend on $k$. Then*

$$\Phi(t, \mathcal{I}_k, a) = \frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}'_k(x)) \equiv a\}|}{q} = \frac{1}{|\mathbb{F}_\mathfrak{l}|} + O(\varepsilon(q, G, \mathcal{I})).$$

*Example* 7.25. In particular, for the family $\mathcal{I}$ of Example 7.2 (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 $a \in \mathbb{F}_\ell$ 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 7.10.

7.6. **Approximate variance.** As in [LZ12], we now consider the "approximate variance"

$$\left(\Phi(\mathcal{I}, a) - \frac{1}{|\mathbb{F}_\ell|}\right)^2,$$

in the sense that we replace the true expected value of the random variable $\Phi(\mathcal{I}, a)$ by the approximation given by Proposition 7.22. This corresponds to the quantity

$$\left(\Phi(t, \mathcal{I}, a) - \frac{1}{|\mathbb{F}_\ell|}\right)^2,$$

and it is clear that bounding the latter gives a result about the distribution of $\Phi(t, \mathcal{I}, a)$, uniformly with respect to $a \in \mathbb{F}_\ell$.

7.6.1. *Computation in the model.*

**Proposition 7.26.** *In the notations of Section 7.4, we have*

$$\sum_{a\in\mathbb{F}_\ell} \mathbb{E}\left(\left(\Phi(\mathcal{I}, a) - \frac{1}{|\mathbb{F}_\ell|}\right)^2\right) = \frac{1}{|\mathcal{I}|}\left(1 + O\Big(H_{\mathcal{I}}(\alpha(G), |\mathbb{F}_\ell|)\Big)\right).$$

*Proof.* As in Proposition 5.1, we have by orthogonality that

$$\begin{aligned}
\left(\Phi(\mathcal{I}, a) - \frac{1}{|\mathbb{F}_\ell|}\right)^2 &= \left|\frac{1}{|\mathcal{I}|}\sum_{k\in\mathcal{I}} \frac{1}{|\mathbb{F}_\ell|} \sum_{0\neq\psi\in\widehat{\mathbb{F}}_\ell} \psi\left(S(\mathcal{I}(k)) - a\right)\right|^2 \\
&= \frac{1}{|\mathcal{I}|^2|\mathbb{F}_\ell|^2}\left|\sum_{0\neq\psi\in\widehat{\mathbb{F}}_\ell} \psi(-a) \sum_{k\in\mathcal{I}} \psi\left(S(\mathcal{I}(k))\right)\right|^2 \\
&= \frac{1}{|\mathcal{I}|^2|\mathbb{F}_\ell|^2} \sum_{0\neq\psi_1,\psi_2\in\widehat{\mathbb{F}}_\ell} \psi_1(-a)\overline{\psi_2(-a)} \\
&\quad \times \sum_{k_1,k_2\in\mathcal{I}} \psi_1\left(S(\mathcal{I}(k_1))\right)\overline{\psi_2\left(S(\mathcal{I}(k_2))\right)}.
\end{aligned}$$

Again by orthogonality, $\sum_{a\in\mathbb{F}_\ell}\left(\Phi(\mathcal{I}, a) - |\mathbb{F}_\ell|^{-1}\right)^2$ is equal to

$$\frac{1}{|\mathcal{I}|}\left(\frac{|\mathbb{F}_\ell| - 1}{|\mathbb{F}_\ell|} + \frac{1}{|\mathcal{I}||\mathbb{F}_\ell|} \sum_{0\neq\psi\in\widehat{\mathbb{F}}_\ell} \sum_{\substack{k_1,k_2\in\mathcal{I}\\ k_1\neq k_2}} \frac{\psi(S(\mathcal{I}(k_1)))}{\psi(S(\mathcal{I}(k_2)))}\right).$$

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 $\mathcal{I}(k_1)\backslash\mathcal{I}(k_2)$ and $\mathcal{I}(k_2)\backslash\mathcal{I}(k_1)$ disjoint, we have by independence

$$\sum_{\substack{k_1,k_2\in\mathcal{I}\\ k_1\neq k_2}}\mathbb{E}\Big[\psi\Big(S(\mathcal{I}(k_1))-S(\mathcal{I}(k_2))\Big)\Big]=\sum_{\substack{k_1,k_2\in\mathcal{I}\\ k_1\neq k_2}}\frac{\mathbb{E}(\psi(Z))^{|\mathcal{I}(k_1)\backslash\mathcal{I}(k_2)|}}{\mathbb{E}(\psi(Z))^{|\mathcal{I}(k_2)\backslash\mathcal{I}(k_1)|}}.$$

By the bound on Gaussian sums (10), $\mathbb{E}\left(\psi(Z)\right),\mathbb{E}\left(\psi(-Z)\right)\ll|\mathbb{F}_{\mathfrak{l}}|^{-\alpha(G)}$ uniformly with respect to $\psi$, whence the result. □

7.6.2. *Conclusion.* Theorem 7.7 then follows immediately from Proposition 7.20 and Proposition 7.26.

7.7. **Estimate and analysis of the error term.** We now estimate and analyze the error term

$$V(t,\mathcal{I})\ll\frac{1}{|\mathcal{I}|}+\frac{H_{\mathcal{I}}(\alpha,|\mathbb{F}_{\mathfrak{l}}|)}{|\mathcal{I}|}+\frac{H_{\mathcal{I}}(\alpha,|\mathbb{F}_{\mathfrak{l}}|)M_{\mathcal{I}}}{|\mathcal{I}|}\frac{E(G,M_{\mathcal{I}},|\mathbb{F}_{\mathfrak{l}}|)}{q^{1/2}}\tag{23}$$

in Corollary 7.8, where $\alpha=\alpha(G)$.

7.7.1. *Estimates for $V(t,\mathcal{I})$.*

Definition 7.27. For a family $\mathcal{I}\to\mathcal{P}(\mathbb{F}_q)$, we define $m_{\mathcal{I}}=\max_{k\in\mathcal{I}}|\mathcal{I}(k)|$ and $A_{\mathcal{I}}=\min_{k_1\neq k_2\in\mathcal{I}}|\mathcal{I}(k_1)\Delta\mathcal{I}(k_2)|$.

**Lemma 7.28.** *In the notations of Definitions 7.6, 7.21 and 7.27, we have the bounds $M_{\mathcal{I}}\leqslant|\mathcal{I}|m_{\mathcal{I}}$, $1\leqslant A_{\mathcal{I}}\leqslant 2M_{\mathcal{I}}$, and*

$$H_{\mathcal{I}}(\alpha,n)\ll\frac{\max(h_{\mathcal{I}}(d):1\leqslant d\leqslant 2m_{\mathcal{I}})}{|\mathcal{I}|n^{\alpha A_{\mathcal{I}}}}\leqslant\frac{|\mathcal{I}|}{n^{\alpha A_{\mathcal{I}}}}.$$

*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 $H_{\mathcal{I}}(\alpha,n)\ll n^{-\alpha A_{\mathcal{I}}}$. 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 7.2 (1).*

*(2) For the family $\mathcal{I}$ of Example 7.2 (3), we have*

$$H_{\mathcal{I}}(\alpha,n)\ll\frac{\max_{0\leqslant d<|E|}\left|\{y\in B_{\mathcal{I}}:|E\cap(E+y)|=d\}\right|}{n^{\alpha A_{\mathcal{I}}}}$$

*where $B_{\mathcal{I}}=\{y_1-y_2:y_1,y_2\in\mathcal{I}\text{ distinct}\}$. In particular, if*

$$\mathcal{I}\subset\prod_{i=1}^{e}[0,p-\max_{x\in E}x_i],\tag{24}$$

*then $H_{\mathcal{I}}(\alpha,n)\ll\frac{|B_E|}{n^{\alpha A_{\mathcal{I}}}}$. 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.

□

7.7.2. *Analysis of the parameters.* The next lemma provides a general analysis of the error term (23) that we will use to handle the various examples of Theorem 7.7.

**Lemma 7.29.** *We have $V(t, \mathcal{I}) = o(1)$ if the following three conditions hold:*

*(1)* $|\mathcal{I}| \to +\infty$.
*(2)* $H_{\mathcal{I}} := H_{\mathcal{I}}(\alpha(G), |\mathbb{F}_\mathfrak{l}|) = o(|\mathcal{I}|)$.
*(3) The sum*

$$M_{\mathcal{I}} + \frac{2\,(\log(M_{\mathcal{I}}/|\mathcal{I}|) + \log H_{\mathcal{I}})}{\log(|G||G^\sharp|)} \tag{25}$$

*is strictly smaller than*

$$\begin{cases} \frac{1}{\beta_+(G)} \frac{\log q}{\log |\mathbb{F}_\mathfrak{l}|} - \frac{2\beta_-(G)}{\beta_+(G)} & \text{if } G \text{ classical} \\ \frac{\log q}{\log d} - 1 & \text{if } G \text{ cyclic.} \end{cases}$$

*If we have*

$$M_{\mathcal{I}} = |\mathcal{I}| \text{ and } \log H_{\mathcal{I}} \ll \log(|G||G^\sharp|), \tag{26}$$

*this implies that*

$$\begin{cases} \log |\mathbb{F}_\mathfrak{l}| = o(\log q) & \text{if } G \text{ classical} \\ \log d = o(\log q) & \text{if } G \text{ cyclic.} \end{cases}$$

*Remarks* 7.30.

(1) By Lemma 7.28, $H_{\mathcal{I}}/|\mathcal{I}| \leqslant |\mathbb{F}_\mathfrak{l}|^{-\alpha A_{\mathcal{I}}}$, so Condition (2) holds if $|\mathbb{F}_\mathfrak{l}| \to +\infty$ or if $H_{\mathcal{I}} = O(1)$ (e.g. for a family satisfying Lemma 7.28 (1)).
(2) If $\log |\mathbb{F}_\mathfrak{l}| = o(\log q)$ and $p < |\mathbb{F}_\mathfrak{l}|$, note that we must take $e \to +\infty$ (see Section 3.5).

*Remark* 7.31. The optimal size for $M_{\mathcal{I}}$ is therefore $M_{\mathcal{I}} \approx \frac{2\varepsilon \log q - \log(|G|/|G^\sharp|)}{\log(|G||G^\sharp|)}$ for some $\varepsilon \in (0, 1/2)$, giving

$$V(t, \mathcal{I}) \ll_\varepsilon \Big(m_{\mathcal{I}} + H_{\mathcal{I}}(\alpha(G), |\mathbb{F}_\mathfrak{l}|)\Big) \frac{\log(|G||G^\sharp|)}{\log q} + \frac{1}{q^{1/2-\varepsilon}}.$$

7.8. **Removing the shifts.** The general setting to obtain asymptotic equidistribution for unshifted "complete" families from Theorem 7.7. is the following:

**Proposition 7.32.** *Under the hypotheses of Theorem 7.7, assume furthermore that:*

*(1) For some family $\mathcal{I}_2$ and functions $f_1 : \mathbb{F}_q \times \mathcal{I} \to \mathcal{I}_2$, $f_2 : \mathbb{F}_q \to \mathbb{F}_\ell$ we have*

$$S(t, \mathcal{I}'(k,x)) = S\big(t, \mathcal{I}_2(f_1(x,k))\big) + f_2(x) \ \ (k \in \mathcal{I}, x \in \mathbb{F}_q).$$

*(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 $a \in \mathbb{F}_\ell$ 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 $k \in \mathcal{I}$, 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 $||f_3||_\infty/q \leqslant 1$,*

$$\Phi(t, \mathcal{I}_3, a) = \frac{1}{|\mathbb{F}_\ell|} + O\left(V(t,\mathcal{I})^{1/2} + \left(\frac{|\mathbb{F}_\ell| ||f_3||_\infty}{q}\right)^{1/2}\right)$$

*uniformly with respect to $a \in \mathbb{F}_\ell$.*

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 $a \in \mathbb{F}_\ell$ gives some additional freedom in comparison with the preliminary version from Corollary 7.24.

*Proof.* Under Condition (1), Theorem 7.7 gives

$$\sum_{a \in \mathbb{F}_\ell} \frac{1}{q} \sum_{x \in \mathbb{F}_q} \left( \frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}_2(f_1(x,k))) \equiv a\}|}{|\mathcal{I}|} - \frac{1}{|\mathbb{F}_\ell|} \right)^2 \ll V(t, \mathcal{I})$$

by exchanging the summations over $a$ and $x$ and exploiting the averaging over $a$. By the Cauchy-Schwarz inequality,

$$\sum_{a \in \mathbb{F}_\ell} \left( \frac{1}{q} \sum_{x \in \mathbb{F}_q} \frac{|\{k \in \mathcal{I} : S(t, \mathcal{I}_2(f_1(x,k))) \equiv a\}|}{|\mathcal{I}|} - \frac{1}{|\mathbb{F}_\ell|} \right)^2 \ll V(t, \mathcal{I})$$

By exchanging the summations over $k$ and $x$, this is equal to

$$\sum_{a \in \mathbb{F}_\ell} \left( \frac{1}{|\mathcal{I}|} \sum_{k \in \mathcal{I}} \frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}_2(f_1(x,k))) \equiv a\}|}{q} - \frac{1}{|\mathbb{F}_\ell|} \right)^2.$$

Finally, by Condition (2),

$$\sum_{a \in \mathbb{F}_\ell} \left( \frac{|\{x \in \mathbb{F}_q : S(t, \mathcal{I}_3(x)) \equiv a\}|}{q} - \frac{1}{|\mathbb{F}_\ell|} + O\left(\frac{||f_3||_\infty}{q}\right) \right)^2 \ll V(t, \mathcal{I}).$$

□

*Example* 7.33. For the family $\mathcal{I}$ of Example 7.2 (3), we have by Example 7.25 that:

- Condition (1) of Proposition 7.32 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 $k \in \mathbb{F}_q$.

7.9. **Applications of Proposition 7.32.** In the following paragraphs, we use Proposition 7.32 to prove Propositions 7.10, 7.15 and 7.18.

The general idea is to find an averaging family $\mathcal{I}$ of size large enough to get asymptotic equidistribution in Corollary 7.8, and the assumptions we make are precisely to allow that, according to Lemma 7.29.

7.9.1. *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 $|\mathcal{I}| \leqslant \frac{\log q}{\log|\mathbb{F}_\mathfrak{l}|}$ and $p < |\mathbb{F}_\mathfrak{l}|$ (see Section 3.5), we have

$$|\mathcal{I}|^{1/e} \leqslant \left(\frac{\log q}{\log|\mathbb{F}_\mathfrak{l}|}\right)^{1/e} = e^{1/e}\left(\frac{\log p}{\log|\mathbb{F}_\mathfrak{l}|}\right)^{1/e} \leqslant 1,$$

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 7.34.** *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* 7.35. The condition $\log I \leqslant (e-1)\log(\delta p)$ is satisfied if $I \leqslant \log q = e \log p$ as in Lemma 7.29, up to taking $p$ large enough if $\delta < 1$.

7.9.2. *Shifts of subsets.* We first consider the family of Example 7.2 (3): for $\mathcal{I}, E \subset \mathbb{F}_q$, we let $\mathcal{I}(k) = E + k$ $(k \in \mathcal{I})$.

*Proof of Proposition 7.10.* By Example 7.33, Proposition 7.32 can be applied.

By Lemma 7.28, since $m_\mathcal{I} = |E|$, the sum (25) is

$$\leqslant |\mathcal{I}||E| + \frac{2(\log|E| + \log|B_E| - \alpha(G)A_\mathcal{I}|\mathbb{F}_\mathfrak{l}|)}{\log(|G||G^\sharp|)}$$

if $\mathcal{I} \subset \prod_{i=1}^e [1, p - \max_{x\in E} x_i]$. By Lemma 7.29, we want that for some $\varepsilon \in (0, 1/2)$,

$$|\mathcal{I}| < \frac{1}{|E|}\left(\frac{2\varepsilon\log q - 2\log|E| - 2\log|B_E|}{\beta_+(G)\log|\mathbb{F}_\mathfrak{l}|} - \frac{\beta_-(G)}{\beta_+(G)} + 2\alpha(G)A_\mathcal{I}\right)$$

if $G$ is classical, and

$$|\mathcal{I}| < \frac{1}{|E|}\left(\frac{2\varepsilon\log q - 2\log|E| - 2\log|B_E|}{\log d} + 2\alpha(G)A_\mathcal{I} - 1\right)$$

if $G = \mu_d$.

When the sheaf is of the form $\mathcal{L}_{\chi(f)}$ with $f \neq X$, we impose that $\mathcal{I} \subset \prod_{i=1}[1, p/\deg(f_1) - \max_{x\in E} x_i)$, so that it is $\bigcup_{k\in\mathcal{I}} \mathcal{I}(k)$-compatible by Example 3.16.

Under the assumptions of Proposition 7.10, we can choose $\mathcal{I}$ as large as possible satisfying the above conditions by Lemma 7.34. □

7.9.3. *Intervals.* Let us now analyze the family $\mathcal{I} \subset \{1, \dots, p\}$, $k \mapsto \{1, \dots, k\}$ of Example 7.2 (1). For the Legendre symbol, this is the case of [LZ12].

**Lemma 7.36.** *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* 7.37. 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

$$S(t, \{1, \dots, p\}) = 0 \tag{27}$$

(i.e. orthogonality with constant functions).

*Proof of Proposition 7.15.* We apply again Proposition 7.32:

Condition (1) 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 $k \in \mathcal{I}$, $x \in \mathbb{F}_p$.

By Lemma 7.36, Condition (2) holds with $||f_3||_\infty \leqslant \max_{k\in\mathcal{I}} k$, and with no error term if the trace function considered satisfies (27). Otherwise, we add the error term

$$\left(\frac{|\mathbb{F}_l||\mathcal{I}|}{p}\right)^{1/2} \ll \left(\frac{|\mathbb{F}_l| \log p}{p \log d}\right)^{1/2}.$$

If the sheaf is a Kummer sheaf $\mathcal{L}_{\chi(f)}$ we impose $\max_{k\in\mathcal{I}} k < p/\deg(f_1)$, so that it is $\bigcup_{k\in\mathcal{I}} \mathcal{I}(k)$-compatible by Example 3.16.

We may then choose $\mathcal{I}$ as large as permitted by Lemma 7.29, i.e. $|\mathcal{I}| \approx \frac{\log p}{\log d}$, noting that for Kummer sheaves as above, we have $\frac{p}{\deg(f_1)} > \frac{\log p}{\log d}$ for $p$ large enough ($\deg(f_1)$ being bounded independently from $q$).

□

*Remark* 7.38. For Kloosterman sums, we have seen in Section 3.5 that it is necessary to take $e \to +\infty$ so that $V(t, \mathcal{I}) = o(1)$. Hence, Proposition 7.15 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 7.2 (2), we have $\mathcal{I}'(k, x) = \prod_{i=1}^{e} \{1 + x_i, \dots, x_i + k_i\}$ for all $x = (x_1, \dots, x_e) \in \mathbb{F}_q$. 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 7.32 with $f_1(x, k) = x + k$ and $f_3 = 0$ as before. On the other hand, using Lemma 7.36 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 $|\mathbb{F}_\mathfrak{l}| e p^{e-1}/q = |\mathbb{F}_\mathfrak{l}| e/p > e$ 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.

7.9.4. *Small intervals with shifts of subsets.* We finally consider Proposition 7.18, which is about a family of type of Example 7.2 (4) and gives a variant of Proposition 7.15 for $e > 1$ (in particular for Kloosterman sums).

*Proof of Proposition 7.18.* 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 $\varepsilon > 0$ and $d \geqslant 1$, we have

$$\begin{aligned} h_\mathcal{I}(d) &\leqslant \sum_{k_1, k_1' \in \mathcal{I}_1} \Big| \{k_2, k_2' \in \mathcal{I}_2 : |k_1 - k_1'||E \Delta (E + (k_2 - k_2'))| = d\} \Big| \\ &= |\mathcal{I}_1| \sum_{1 \leqslant d' | d} \Big| \{k_2, k_2' \in \mathcal{I}_2 : |E \Delta (E + (k_2 - k_2'))| = d/d'\} \Big| \\ &\leqslant |\mathcal{I}_1||B_E||\mathcal{I}_2| \tau(d) \ll_\varepsilon (|\mathcal{I}||B_E|)^{1+\varepsilon} \end{aligned}$$

if $\mathcal{I}_2 \subset \prod_{i=2}^{e} [1, p - \max_{x \in E} x_i]$, by Lemma 7.28. As for Propositions 7.10 and 7.15, if the sheaf is a Kummer sheaf $\mathcal{L}_{\chi(f)}$, we impose $\max_{k \in \mathcal{I}_1} k < p/\deg(f_1)$ and $\mathcal{I}_2 \subset [1, p/\deg(f_1))$, to ensure $\bigcup_{k \in \mathcal{I}} \mathcal{I}(k)$-compatibility.

The conclusion then follows by using Lemmas 7.29 and 7.34 as in Proposition 7.10.

□

## References


[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.

[Car72] Roger W. Carter. *Simple groups of Lie type*. John Wiley & Sons, 1972.

[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.

[Fis95] Benji Fisher. Kloosterman sums as algebraic integers. *Mathematische Annalen*, 301(1):485–505, 1995.

[FKM14] 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.

[Gar07] Moubariz Z. Garaev. An explicit sum-product estimate in $\mathbb{F}_p$. *International Mathematics Research Notices*, 2007.

[Gor82] Daniel Gorenstein. *Finite simple groups: an introduction to their classification*. University Series in Mathematics. Springer, 1982.

[Hal08] Chris Hall. Big symplectic or orthogonal monodromy modulo $\ell$. *Duke Mathematical Journal*, 141(1):179–203, 2008.

[HBK00] David R. Heath-Brown and Sergei Konyagin. New bounds for Gauss sums derived from $k$th powers, and for Heilbronn's exponential sum. *The Quarterly Journal of Mathematics*, 51(2):221–235, 2000.

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

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

[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.

[KL96] Dae San Kim and In-Sok Lee. Gauss sums for $O^+(2n, q)$. *Acta Arithmetica*, 78(1):75–89, 1996.

[Kor89] Nikolai M. Korobov. *Exponential sums and their applications*, volume 80 of *Mathematics and its Applications*. Springer, 1989.

[Kow06] Emmanuel Kowalski. On the rank of quadratic twists of elliptic curves over function fields. *International Journal of Number Theory*, 62(2), 2006.

[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 $\ell$-adic sheaves and their ramification theory on curves*. September 2015. http://arxiv.org/abs/1409.6899.

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

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

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

[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.

[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.

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

[PG17] Corentin Perret-Gentil. Gaussian distribution of short sums of trace functions over finite fields. *Mathematical Proceedings of the Cambridge Philosophical Society*, 163(3):385–422, 2017.

[PG18] Corentin Perret-Gentil. Integral monodromy groups of Kloosterman sheaves. *Mathematika*, 2018. To appear. http://arxiv.org/abs/1609.09628.

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

[Rib76] Kenneth A. Ribet. Galois action on division points of abelian varieties with real multiplications. *American Journal of Mathematics*, 98(3):751–804, 1976.

[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.

ETH Zürich, Department of Mathematics
*Email address*: corentin.perretgentil@{math.ethz.ch,gmail.com}