Math. Res. Lett. **20** (2013), *no.* 02, 305–323

COUNTING SHEAVES USING SPHERICAL CODES

Étienne Fouvry, Emmanuel Kowalski and Philippe Michel

Abstract. Using the Riemann Hypothesis over finite fields and bounds for the size of spherical codes, we give explicit upper bounds, of polynomial size with respect to the size of the field, for the number of geometric isomorphism classes of geometrically irreducible ℓ-adic middle-extension sheaves on a curve over a finite field, which are pointwise pure of weight 0 and have bounded ramification and rank. As an application, we show that "random" functions defined on a finite field cannot usually be approximated by short linear combinations of trace functions of sheaves with small complexity.

1. Introduction

Interesting arithmetic objects often appear in countable sets that can be naturally partitioned into increasing finite subsets. The estimation of the cardinality of these subsets is often both fascinating and important in applications. Well-known examples include the counting function for primes, the counting function of zeros of L-functions over number fields, or the counting function of automorphic forms of certain types.

We consider here a similar counting problem where the objects of interests are certain ℓ-adic sheaves on a smooth curve over a finite field, or (more or less) equivalently, certain ℓ-adic Galois representations over function fields. In that case, it is not obvious how to construct finite subsets, even before asking how large they could be. However, it was shown by Deligne [4], as explained by Esnault and Kerz [10, Th. 2.1, Remark 2.2], that there is, for any smooth separated scheme X of finite type over a finite field k, a natural notion of "bounded ramification" such that the number of irreducible lisse étale $\bar{\mathbf{Q}}_\ell$-sheaves on X is finite, up to twist by geometrically trivial characters. The problem of saying more about the order of these finite sets is then the subject of remarkable conjectures of Deligne in the case of curves predicting, for suitably restricted ramification, a formula similar to that for the number of points of an algebraic variety over a finite field in terms of Weil numbers of suitable weights. This is motivated by the result of Drinfeld [9] computing the number of unramified 2-dimensional representations for a projective curve, and showing it is of this form; see again the survey in [10, Section 8] and the paper of Deligne and Flicker [8, Section 6] (and the lecture [5] of Deligne).

Our goal in this note is relatively modest. We will only consider the case of curves, and our main result is an explicit upper bound for the size of certain sets of (isomorphism classes of) étale sheaves. We do not address the crucial issue of lower bounds,

Received by the editors February 24, 2013.

2010 *Mathematics Subject Classification.* 11G20,11T23,94B60,94B65.

Key words and phrases. Lisse ℓ-adic sheaves, trace functions, spherical codes, Riemann Hypothesis over finite fields.

but the argument is quite short and the fact that it uses ideas from spherical codes is quite appealing. Moreover, the bounds for spherical codes that are used do not seem to be present in the literature. Furthermore, as we will explain below, there are natural applications of the estimates we obtain.

Let p be a prime number and let k be a finite field of characteristic p. Fix an auxiliary prime $\ell \neq p$. Let X/k be a smooth geometrically connected algebraic curve over k, and let Y be its smooth compactification, with genus $g \geqslant 0$.

We will consider *middle-extension sheaves* on X/k, in the sense of [16], i.e., constructible $\bar{\mathbf{Q}}_\ell$-sheaves $\mathcal{F}$ on X/k such that, for any open set U on which $\mathcal{F}$ is lisse, with open immersion $j : U \hookrightarrow X$, we have

$$\mathcal{F} \simeq j_* j^* \mathcal{F}.$$

Slightly more concretely, we see that such a sheaf has a largest open subset U on which it is lisse (defined by the condition that the stalk be of generic rank), and is determined by its restriction to this open set. On U, $\mathcal{F}$ corresponds uniquely to a continuous ℓ-adic representation ϱ of the étale fundamental group $\pi_1(U, \bar{\eta})$, defined with respect to some geometric generic point $\bar{\eta}$ of U. As in [17, Section 7], the middle-extension sheaf $\mathcal{F}$ is called *pointwise pure of weight* 0 if its restriction to U is pointwise pure of weight 0, i.e., the eigenvalues of the local Frobenius automorphisms at points of U are algebraic numbers, all conjugates of which have modulus 1. Furthermore, $\mathcal{F}$ is called *irreducible* (resp. *geometrically irreducible*) if ϱ is an irreducible representation of the fundamental group $\pi_1(U, \bar{\eta})$ (resp. of the geometric fundamental group $\pi_1(U \times \bar{k}, \bar{\eta})$).

The collection of middle-extension sheaves on X/k is infinite. We will measure the complexity of a sheaf over a finite field by its (analytic) conductor, in order to obtain a well-defined counting problem. Note that this is a much rougher invariant than that used in the counting conjectures of Deligne, but it is enough to obtain finiteness, and the argument below does not seem to allow us to get any improvement by fixing, for instance, the local monodromy representations at the missing points for sheaves lisse on a fixed open set of X.

Let $\mathcal{F}$ be a middle-extension sheaf on X/k, of rank $\mathrm{rank}(\mathcal{F})$, with singularities at the finite set $\mathrm{Sing}(\mathcal{F}) \subset Y(\bar{k})$. We define the *analytic conductor* (often just called *conductor*) of $\mathcal{F}$ to be

$$\mathbf{c}(\mathcal{F}) = g(Y) + \mathrm{rank}(\mathcal{F}) + \sum_{x \in \mathrm{Sing}(\mathcal{F})} \max(1, \mathrm{Swan}_x(\mathcal{F})), \tag{1.1}$$

where $g(Y)$ is the genus of $Y \times \bar{k}$.

Now, for a finite field k and a curve X/k as above, we denote by $\mathsf{ME}_X(k)$ the category of geometrically irreducible middle-extension sheaves $\mathcal{F}$ on X/k which are pointwise pure of weight 0, and for $c \geqslant 1$, we denote by $\mathsf{ME}_X(k, c)$ the subcategory of those that satisfy

$$\mathbf{c}(\mathcal{F}) \leqslant c.$$

We denote also by $\mathbf{ME}_X(k)$ (resp. $\mathbf{ME}_X(k, c)$) the set of *geometric isomorphism classes* of sheaves in $\mathsf{ME}_X(k)$ (resp. in $\mathsf{ME}_X(k, c)$). Our results are bounds for the size of these sets:

Theorem 1.1. *There exist absolute constants $B > 0, C \geqslant 1$ such that, with notation and assumptions as above, we have*

$$|\mathbf{ME}_X(k,c)| \leqslant C|k|^{Bc^6},$$

for all finite fields k with $|k| \geqslant 1265c^9$. In particular, for fixed c, we have

$$|\mathbf{ME}_{\mathbf{A}^1}(k,c)| = O(|k|^{Bc^6}).$$

Remark 1.2. (1) For a fixed c, this upper bound is polynomial as a function of k. One can prove lower-bounds which show that this is qualitatively correct. For instance, for $X = \mathbf{A}^1$, one gets using Artin–Schreier sheaves (see Section 4) that

$$|\mathbf{ME}_{\mathbf{A}^1}(k,c)| \geqslant |k|^{c/2-1}$$

for any finite field k and any $c \geqslant 2$. P. Deligne and F. Jouve independently explained to us how to improve the exponent $c/2-1$ to $c-2$ using all rank 1 sheaves, and it seems an interesting problem to improve this using other constructions of sheaves of various type (e.g., those studied by Katz in [17]).

(2) We will in fact give fully explicit inequalities, and not just asymptotic statements, and we can refine the exponent c^6 a little bit (see Proposition 3.1 for these more precise results). It is unclear to us what is the best possible upper-bound achievable by the method of spherical codes that we use: we do not know what is the right order of magnitude for the quantity estimated in Theorem 2.1 below.

As far as we know, Theorem 1.1 is the first explicit bound for this type of questions without much stronger restrictions (e.g., on the rank). One can approach the counting problems by applying the global Langlands correspondence over function fields (as proved by Lafforgue [18]) to reduce to counting automorphic forms or representations, and this is indeed how Deligne and Flicker [8] proceed to obtain a "Lefschetz-type" formula for the counting function for cases where the local monodromy is unipotent. One might hope to derive upper-bounds for a fixed rank by means of some version of the Weyl Law for the distribution of Laplace eigenvalues, but controlling these estimates when the rank varies seems quite a difficult problem.

The basic idea of the proof is quite simple (and has been known, at least with respect to showing finiteness, to Deligne[1] and to Venkatesh): we first show that, for $|k|$ large enough, it is enough to count the *trace functions*

$$t_{\mathcal{F},k} : \begin{cases} X(k) \longrightarrow \bar{\mathbf{Q}}_\ell \\ x \mapsto \mathrm{Tr}(\mathrm{Fr}_k \mid \mathcal{F}_{\bar{x}}) \end{cases}$$

(giving the trace of the geometric Frobenius automorphism of k acting on the stalk of $\mathcal{F}$ at a geometric point $\bar{x}$ over $x \in X(k)$, seen as a finite-dimensional representation of the Galois group of k) of $\mathcal{F} \in \mathsf{ME}_X(k,c)$. We view these trace functions (via some isomorphism $\iota : \bar{\mathbf{Q}}_\ell \longrightarrow \mathbf{C}$) as elements of the finite-dimensional Hilbert space $C_X(k)$ of complex-valued functions on $X(k)$, and then see that Deligne's general form of the Riemann Hypothesis implies that these trace functions form a "quasi-orthonormal" system. In particular, given that the conductor is $\leqslant c$, the angle between any two

[1] We thank H. Esnault for this information.

different trace functions of sheaves in $\mathsf{ME}_X(k,c)$, which are not geometrically isomorphic is at least $\pi/2 - O(1/\sqrt{|k|})$. This means that the trace functions of sheaves in $\mathbf{ME}_X(k,c)$ form what is known as a *spherical code* with this angular separation. This fact immediately implies that the corresponding set is finite, but furthermore, we are in a range of spherical codes where one can use methods of Kabatjanskii and Levenshtein [15] (see also [19] and [3, Ch. 9]) to derive the polynomial-type upper bounds of Theorem 1.1. We did not find the statements for bounds on spherical codes in this range, but these turn out to be relatively easy to derive from the general techniques of Kabatjanskii and Levenshtein, as we present in Section 2 (and they might be of independent interest).

An application of Theorem 1.1, applied to the special case $X = \mathbf{A}^1$, concerns the problem of writing a function defined on a finite field as a short linear combination of trace functions of sheaves. Our earlier results in [12, 11] show that functions with such a decomposition can be used in many arguments of analytic number theory. It is therefore conceptually interesting to show that such functions are still rather rare: "most" functions do not have such a good decomposition. To make this precise, following [12], we define *trace norms*:

Definition 1.3 (Trace norms)**.** Let $s \geqslant 0$ be a real number. Let k be a finite field of characteristic p and let $C(k)$ be the vector space of complex-valued functions on k. Fix $\ell \neq p$ and an isomorphism $\iota : \bar{\mathbf{Q}}_\ell \longrightarrow \mathbf{C}$. For $\varphi \in C(k)$, let

$$\|\varphi\|_{\mathrm{tr},s} = \inf\left\{ \sum_i |\lambda_i| \, \mathbf{c}(\mathcal{F}_i)^s + \sum_j |\mu_j| \right\}$$

where the infimum runs over all decompositions

$$\varphi = \sum_i \lambda_i t_{\mathcal{F}_i,k} + \sqrt{|k|} \sum_j \mu_j \delta_{a_j}$$

where the sums are finite, λ_i, μ_j are complex numbers, $\mathcal{F}_i$ is an object of $\mathsf{ME}(k)$ and, for any $a \in k$, we denote by δ_a the delta function at a, taking value 1 at 0 and taking value 0 elsewhere.

Thus, $\|\cdot\|_{\mathrm{tr},s}$ is a norm on $C(k)$ (although it seems to depend on ℓ and ι, this will not be of any importance for us). Using the tautological expansion

$$\varphi = \frac{1}{\sqrt{|k|}} \sqrt{|k|} \sum_{x \in k} \varphi(x) \delta_x,$$

we get an immediate upper-bound

$$\|\varphi\|_{\mathrm{tr},s} \leqslant |k|^{-1/2} \sum_{x \in k} |\varphi(x)| = |k|^{1/2} \|\varphi\|_1 \tag{1.2}$$

where

$$\|\varphi\|_1 = \frac{1}{|k|} \sum_{x \in k} |\varphi(x)|$$

is the L^1-norm. This inequality means that $\|i_s\| \leqslant |k|^{1/2}$, where i_s is the identity map

$$i_s : (C(k), \|\cdot\|_1) \longrightarrow (C(k), \|\cdot\|_{\mathrm{tr},s}).$$

This is in fact close to the truth, as we show in Section 5:

Theorem 1.4. *Let k be a finite field and let $C(k)$ be the vector space of complex-valued functions on k. Fix ℓ and an isomorphism $\iota : \bar{\mathbf{Q}}_\ell \longrightarrow \mathbf{C}$ to define the trace norms $\|\cdot\|_{\mathrm{tr},s}$. Let i_s be the identity map as above. For $s \geqslant 6$ and $|k|$ large enough, we have $\|i_s\| \gg \frac{|k|^{1/2}}{\log|k|}$, where the implied constant is absolute.*

Although this is not surprising, we view this as a first basic step in understanding the properties of functions in $C(k)$, which have good decompositions in trace functions (an issue that was raised for instance by Sarnak, and which is partly motivated by "higher-order Fourier analysis," in the sense of Gowers and Tao.)

Notation. As usual, $|A|$ denotes the cardinality of a set A, and we write $e(z) = e^{2i\pi z}$ for any $z \in \mathbf{C}$. We write $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

The notation $f \ll g$ for $x \in A$, or $f = O(g)$ for $x \in A$, where A is an arbitrary set on which f is defined, are synonymous.

For any algebraic variety X/k, any finite extension k'/k and $x \in X(k')$, we denote by $t_{\mathcal{F},k'}(x)$ the value at x of the trace function of some ℓ-adic (constructible) sheaf $\mathcal{F}$ on X/k. We will write $t_{\mathcal{F},k'}$ for the function $x \mapsto t_{\mathcal{F},k'}(x)$ defined on $X(k')$.

We will always assume that some isomorphism $\iota : \bar{\mathbf{Q}}_\ell \longrightarrow \mathbf{C}$ has been chosen and we will allow ourselves to use it as an identification. Thus, for instance, by $|t_{\mathcal{F},k}(x)|^2$, we will mean $|\iota(t_{\mathcal{F},k}(x))|^2$.

2. Spherical codes

The range of angles defining spherical codes for which we need bounds is not standard, and we have not found a direct statement of the exact form we need in the literature. We therefore first explain how to use the Kabatjanskii–Levenshtein bounds [15] to obtain what we want, referring to [19] which is a more accessible reference.

Following the notation in [19], we denote by $M(n,\varphi)$ the largest cardinality of a subset $X \subset \mathbf{S}^{n-1}$, the $(n-1)$-dimensional unit sphere of the Euclidean space $\mathbf{R}^n$ (with inner product $\langle\cdot,\cdot\rangle_{\mathbf{R}}$), which satisfies

$$\langle x, y\rangle_{\mathbf{R}} \leqslant \cos\varphi$$

for all $x \neq y$ in X.

Theorem 2.1 (Polynomial Kabatjanskii–Levenshtein). *Let $\gamma > 0$ be a fixed real number. For*

$$\cos\varphi \leqslant \frac{\gamma}{\sqrt{n}}, \tag{2.1}$$

assuming that $n \geqslant 2\gamma\lceil(\gamma+1)^2\rceil$, we have

$$M(n,\varphi) \leqslant \frac{(n-1)^{\gamma^2+2\gamma+3}}{\Gamma(\gamma^2+2\gamma+2)}.$$

Proof. By [19, (6.24)], we have

$$M(n,\varphi) \leqslant 2\binom{n-1+k}{k} \tag{2.2}$$

for any integer $k \geqslant 2$ such that

$$\cos\varphi \leqslant t_k^{1,1},$$

where $t_k^{1,1} = p_k^{(n-1)/2,(n-1)/2}$ denotes the largest root of a certain Gegenbauer polynomial. Furthermore, by [19, (6.25)], we have

$$t_k^{1,1} \geqslant \left(\frac{2(n+k-2)}{(n+2k-2)(n+2k-4)}\right)^{1/2} h_k,$$

where h_k is the largest root of the kth Hermite polynomial H_k (see also [19, Cor. 5.17]; all these polynomials have only real roots).

It is known, using elementary arguments (see [21, (6.2.14)]), that

$$h_k \geqslant \sqrt{\frac{k-1}{2}}.$$

Under our assumption (2.1), we therefore see that (2.2) holds for $k \geqslant 2$ such that

$$\frac{\gamma}{\sqrt{n}} \leqslant \sqrt{\frac{k-1}{2}}\left(\frac{2(n+k-2)}{(n+2k-2)(n+2k-4)}\right)^{1/2}.$$

Writing $\kappa = k-1$, we see that this certainly holds provided

$$\gamma^2 \leqslant \frac{\kappa n^2}{(n+2\kappa)^2} = \frac{\kappa}{(1+2\kappa/n)^2}.$$

If we assume that $2\kappa/n \leqslant \gamma^{-1}$, we can take $\kappa = \lceil(\gamma+1)^2\rceil$, i.e., $k = 1+\lceil(\gamma+1)^2\rceil$. The condition on κ translates then to

$$n \geqslant 2\gamma\lceil(\gamma+1)^2\rceil,$$

as stated in the theorem, and we obtain the conclusion from (2.2) using the trivial estimate

$$2\binom{n-1+k}{k} \leqslant 2\frac{(n-1)^k}{k!} \leqslant \frac{(n-1)^k}{(k-1)!}.$$

□

Remark 2.2. (1) We can improve a bit the result as $k \to +\infty$ by using the asymptotic behavior of the zero h_k of the Hermite polynomial. For instance, it is known (see, e.g., [21, (6.32.8)], where k is replaced by n and h_k is denoted x_1) that

$$h_k = \sqrt{2k} - \frac{i_1}{\sqrt[3]{6}}\frac{1}{(2k)^{1/6}} + o(k^{-1/6})$$

in terms of the first zero $i_1 = 3.3721\ldots > 0$ of the function

$$\mathrm{A}(x) = \frac{\pi}{3}\sqrt{\frac{x}{3}}\left\{J_{1/3}\left(2\left(\frac{x}{3}\right)^{3/2}\right) + J_{-1/3}\left(2\left(\frac{x}{3}\right)^{3/2}\right)\right\}$$

(see [21, Section 1.81]; this function is closely related to the Airy function.)

(2) The point of this result is the polynomial growth of $M(n,\varphi)$ as n tends to infinity for a fixed γ, although it may also be interesting in some ranges when γ grows with n. When $\gamma < 1$, a bound of this type follows from the early result of Delsarte, Goethals and Seidel [20, Example 4.6]. In contrast, it is known that $M(n,\varphi)$ is bounded independently of n if φ is a fixed angle $> \frac{\pi}{2}$, and grows exponentially if φ is fixed and $< \frac{\pi}{2}$. What is usually called the

Kabatjanskii–Levenshtein bound is an estimate for the exponential rate of growth in that case ([19, Th. 6.7]), which corresponds to γ of size $\alpha n^{1/2}$ for some fixed $\alpha > 0$.

(3) In this respect, one can weaken the lower bound $n \geqslant 2\gamma\lceil(\gamma+1)^2\rceil$ at the cost of a worse exponent of n in the estimate. This might also be useful, e.g., in a range where $\gamma \approx n^\delta$ for $1/3 \leqslant \delta < 1/2$, where the Kabatjanskii–Levenshtein bound itself does not apply.

(4) See the paper [13] of Helfgott and Venkatesh for other subtle applications of the bounds of Kabatjanskii and Levenshtein to number-theoretic problems. For an application in analysis that also involves quasi-orthogonality, see the paper [14] of Jaming and Powell.

(5) See T. Tao's blog post `terrytao.wordpress.com/2013/07/18/a-cheap-version-of-the-kabatjanskii-levenstein-bound-for-almost-orthogonal-vectors/` for a shorter proof of a slightly weaker polynomial bound.

3. Proof of the main result

Throughout this section, we consider a finite field k and a smooth geometrically connected curve X/k with compactification Y/k of genus g.

The proof of Theorem 1.1 is based on estimates for certain subsets of $\mathbf{ME}_X(k,c)$, which are of independent interest (in particular, they are more closely related to those considered by Drinfeld and Deligne, and Esnault–Kerz, Deligne–Flicker).

Let U/k be a dense open subset of X/k. We denote by $\mathsf{L}(U/k,c)$ the category of lisse ℓ-adic sheaves $\mathcal{F}$ on U/k which are geometrically irreducible on U, pointwise pure of weight 0, *primitive* in the sense that U is the largest open set of lissité of the middle-extension sheaf $j_*\mathcal{F}$ on X/k, where $j : U \hookrightarrow X$ is the open embedding of U in X, and with

$$\mathbf{c}(j_*\mathcal{F}) \leqslant c.$$

We denote by $\mathbf{L}(U/k,c)$ the set of geometric isomorphism classes of objects in $\mathsf{L}(U/k,c)$, and we further denote by $\mathsf{L}_r(U/k,c)$ (resp. $\mathbf{L}_r(U/k,c)$) the subcategory where the rank is $\leqslant r$ (resp. the set of geometric isomorphism classes of this subcategory).

Our basic estimates are the following:

Proposition 3.1 (**Counting lisse sheaves**). *Let k, X and Y be as above. Let $c \geqslant 1$. For any dense open set $U/k \hookrightarrow X/k$ with $n(U) = |(Y-U)(\bar{k})| \leqslant c$ and for $r \leqslant c$, we have*

$$|\,\mathbf{L}_r(U/k,c)| \leqslant \frac{(2|U(k)|)^{90c^2r^4+6\sqrt{10}cr^2+3}}{\Gamma(90c^2r^4)}$$

provided $|k| \geqslant 1500c^3r^6$.

This implies Theorem 1.1 as follows: a middle-extension sheaf $\mathcal{F}$ is uniquely determined by its restriction to its unique largest open dense subset of lissité, and the complement of such an open set has at most $\mathbf{c}(\mathcal{F})$ points in $Y(\bar{k})$, so that

$$|\,\mathbf{ME}_X(k,c)| \leqslant \sum_{n(U)\leqslant c} |\,\mathbf{L}_c(U/k,c)| \tag{3.1}$$

where the sum runs over all open subsets U/k of X/k which are defined over k and satisfy $n(U) = (|Y - U|)(\bar{k}) \leqslant c$. The number of terms in this sum is at most $c(q^{c/2} + g)^2$ (indeed, each of the $\leqslant c$ missing points is defined over an extension k_d of k of degree $d \leqslant c$, and by the Riemann Hypothesis for Y, there are at most $q^d + 2gq^{d/2} + 1 \leqslant (q^{d/2} + g)^2 \leqslant (q^{c/2} + g)^2$ points on $Y(k_d)$.) Applying Proposition 3.1 to each U, and noting that the condition on $|k|$ implies $g \leqslant c \leqslant |k|^{1/3}$, and hence also $|U(k)| \leqslant |k| + 2g\sqrt{|k|} + 1 \leqslant 4|k|$, the bound of Theorem 1.1 follows.

Remark 3.2. Applying the "automorphic side to Galois side" part of the global Langlands correspondence on Y/k [18, Théorème, (i)], this gives the same upper bound for the number of cuspidal automorphic representations of $\mathrm{GL}_r(\mathbf{A}_F)$ which are unramified on U, where $\mathbf{A}_F$ is the ring of adèles of the function field $F = k(Y)$ of Y/k. Even with automorphic techniques, it is not clear how to prove such a bound.

We now start the proof of Proposition 3.1 with a variant of the well-known upper bounds on the dimension of cohomology groups of lisse sheaves on algebraic curves.

Lemma 3.3. *Let k, X and Y be as above. Let $j : U/k \hookrightarrow X/k$ be the open embedding of a dense open subset with $n(U) = |(Y - U)(\bar{k})|$ missing points, and let $\mathcal{F}_1$, $\mathcal{F}_2$ be lisse ℓ-adic sheaves on U/k of rank r_1 and r_2, respectively, which are geometrically irreducible. Let $c = \max(\mathbf{c}(j_*\mathcal{F}_1), \mathbf{c}(j_*\mathcal{F}_2))$. We have*

$$\dim H_c^1(U \times \bar{k}, \mathcal{F}_1 \otimes \check{\mathcal{F}}_2) \leqslant (2c + n(U))r_1r_2.$$

Proof. Let $\mathcal{F} = \mathcal{F}_1 \otimes \check{\mathcal{F}}_2$, and denote $r_i = \operatorname{rank} \mathcal{F}_i$. Since $H_c^0(U \times \bar{k}, \mathcal{F}) = 0$ (this is true for all lisse sheaves on U), we have

$$\dim H_c^1(U \times \bar{k}, \mathcal{F}) = -\chi_c(U \times \bar{k}, \mathcal{F}) + \dim H_c^2(U \times \bar{k}, \mathcal{F}).$$

The second term is at most 1 by Schur's Lemma, since $H_c^2(U \times \bar{k}, \mathcal{F})$ is the coinvariant of the generic geometric fiber under the action of the geometric fundamental group, and since $\mathcal{F}_1$ and $\mathcal{F}_2$ are geometrically irreducible.

Now the Euler-Poincaré formula of Grothendieck–Ogg–Shafarevich (see, e.g., [16, Ch. 2]) gives

$$\begin{aligned} -\chi_c(U \times \bar{k}, \mathcal{F}) &= -\chi_c(U \times \bar{k}) \operatorname{rank}(\mathcal{F}) + \sum_{x \in \mathrm{Sing}(\mathcal{F})} \mathrm{Swan}_x(\mathcal{F}) \\ &= (n(U) + 2g - 2)r_1r_2 + \sum_{x \in (Y-U)(\bar{k})} \mathrm{Swan}_x(\mathcal{F}). \end{aligned}$$

We have

$$\mathrm{Swan}_x(\mathcal{F}) \leqslant \operatorname{rank}(\mathcal{F})\lambda_x(\mathcal{F}) = r_1r_2\lambda_x(\mathcal{F})$$

at each $x \in (Y - U)(\bar{k})$, where $\lambda_x(\mathcal{F})$ is the largest break of $\mathcal{F}$ at x. Since

$$\lambda_x(\mathcal{F}) \leqslant \max(\lambda_x(\mathcal{F}_1), \lambda_x(\mathcal{F}_2)) \leqslant \lambda_x(\mathcal{F}_1) + \lambda_x(\mathcal{F}_2),$$

we get the upper bound

$$\begin{aligned} \sum_{x \in (Y-U)(\bar{k})} \mathrm{Swan}_x(\mathcal{F}) &\leqslant \operatorname{rank}(\mathcal{F}) \sum_{x \in (Y-U)(\bar{k})} (\lambda_x(\mathcal{F}_1) + \lambda_x(\mathcal{F}_2)) \\ &\leqslant r_1r_2 \sum_{x \in (Y-U)(\bar{k})} (\mathrm{Swan}_x(\mathcal{F}_1) + \mathrm{Swan}_x(\mathcal{F}_2)). \end{aligned}$$

It follows that

$$\dim H^1_c(U \times \bar{k}, \mathcal{F}) \leqslant 1 + r_1 r_2(2c + n(U) - 2) \leqslant (2c + n(U))r_1 r_2.$$

□

Remark 3.4. One might be tempted to estimate $n(U)$ by c, but we allow the possibility that the sheaves be unramified at some of the points in $Y - U$ in this statement (i.e., they are not necessarily primitive), in which case an estimate $n(U) \leqslant c$ is not always valid.

Now we invoke the Riemann Hypothesis to obtain "quasi-orthonormality" relations for trace functions. We only consider primitive sheaves on a common open set for simplicity.

Lemma 3.5 (**Quasi-orthogonality relation**). *Let k, X and $U \hookrightarrow X$ be as above. Let $c \geqslant 1$ be given, and let $\mathcal{F}_1$, $\mathcal{F}_2$ be sheaves in $\mathsf{L}(U/k, c)$ with ranks $r_i = \operatorname{rank}(\mathcal{F}_i)$.*

(1) We have

$$\left| \frac{1}{|k|} \sum_{x \in U(k)} |t_{\mathcal{F}_1,k}(x)|^2 - 1 \right| \leqslant \frac{3cr^2}{\sqrt{|k|}}.$$

(2) If $\mathcal{F}_1$ and $\mathcal{F}_2$ are not geometrically isomorphic, then we have

$$\left| \frac{1}{|k|} \sum_{x \in U(k)} t_{\mathcal{F}_1,k}(x)\overline{t_{\mathcal{F}_2,k}(x)} \right| \leqslant \frac{3cr_1r_2}{\sqrt{|k|}}.$$

Proof. We deal with both cases at the same time by redefining $\mathcal{F}_2 = \mathcal{F}_1$ in (1). By construction, for all $x \in U(k)$, we have therefore

$$t_{\mathcal{F}_1,k}(x)\overline{t_{\mathcal{F}_2,k}(x)} = t_{\mathcal{F},k}(x),$$

where $\mathcal{F} = \mathcal{F}_1 \otimes \check{\mathcal{F}}_2$. The Grothendieck–Lefschetz trace formula gives

$$\sum_{x \in U(k)} t_{\mathcal{F}_1,k}(x)\overline{t_{\mathcal{F}_2,k}(x)} = \operatorname{Tr}(\mathrm{Fr}_k \mid H^2_c(U \times \bar{k}, \mathcal{F})) - \operatorname{Tr}(\mathrm{Fr}_k \mid H^1_c(U \times \bar{k}, \mathcal{F})).$$

Because $\mathcal{F}_1$ and $\mathcal{F}_2$ are geometrically irreducible and pointwise of weight 0, we have

$$\operatorname{Tr}(\mathrm{Fr}_k \mid H^2_c(U \times \bar{k}, \mathcal{F})) = \delta(\mathcal{F}_1, \mathcal{F}_2)|k|,$$

by Schur's Lemma and the coinvariant formula for H^2_c, where this delta symbol is 1 in case (1) and 0 in case (2). Moreover, since $\mathcal{F}$ is also pointwise pure of weight 0, we have

$$|\operatorname{Tr}(\mathrm{Fr}_k \mid H^1_c(U \times \bar{k}, \mathcal{F}))| \leqslant \dim H^1_c(U \times \bar{k}, \mathcal{F})\sqrt{|k|}$$

by Deligne's main result on the Riemann Hypothesis over finite fields [7, Th. 1]. Applying the previous lemma, we obtain the inequalities stated (since here $c \geqslant \mathbf{c}(\mathcal{F}_i) \geqslant n(U)$ because the sheaves are in $\mathsf{L}(U/k, c)$, hence primitive.) □

We can then easily deduce that sheaves are characterized by their trace functions on k when the ramification is sufficiently small (this can be compared with the arguments of Deligne presented in [10, Section 5]).

Corollary 3.6. *Let k, X and Y be as above, and let $U \hookrightarrow X$ be an open dense subset of X/k. Let $c \geqslant 1$ be given.*

(1) If $\mathcal{F} \in \mathsf{L}(U/k, c)$ satisfies

$$3c(\mathrm{rank}(\mathcal{F}))^2 < \sqrt{|k|},$$

then $t_{\mathcal{F},k}$ is non-zero on $U(k)$.

(2) If $\mathcal{F}_1$ and $\mathcal{F}_2$ are sheaves in $\mathsf{L}(U/k, c)$ with

$$3c\,\mathrm{rank}(\mathcal{F}_1)(\mathrm{rank}(\mathcal{F}_1) + \mathrm{rank}(\mathcal{F}_2)) < \sqrt{|k|},$$

then $\mathcal{F}_1$ and $\mathcal{F}_2$ are geometrically isomorphic if and only if their trace functions coincide on $U(k)$, up to a fixed multiplicative constant of modulus 1.

In particular, if $c \geqslant 1$ and $r \geqslant 1$ satisfy $6cr^2 < \sqrt{|k|}$, the map $\mathcal{F} \mapsto t_{\mathcal{F},k}$ is injective on any set of representatives of geometric isomorphism classes of objects in $\mathsf{L}_r(U/k, c)$.

Proof. For (1), it is enough to note that the assumption implies by Lemma 3.5 that

$$\sum_{x \in U(k)} |t_{\mathcal{F},k}(x)|^2 > 0.$$

For (2), only the "only if" part needs proof (by a well-known property of geometric isomorphism: the trace functions coincide on k up to a fixed non-zero scalar). So assume that there exists $\theta \in \mathbf{R}$ such that

$$t_{\mathcal{F}_1,k}(x) = e^{i\theta} t_{\mathcal{F}_2,k}(x)$$

for all $x \in U(k)$. We then obtain

$$\left| \frac{1}{|k|} \sum_{x \in U(k)} t_{\mathcal{F}_1,k}(x)\overline{t_{\mathcal{F}_2,k}(x)} \right| = \frac{1}{|k|} \sum_{x \in U(k)} |t_{\mathcal{F}_1,k}(x)|^2 \geqslant 1 - \frac{3c\,\mathrm{rank}(\mathcal{F}_1)^2}{\sqrt{|k|}}$$

by Lemma 3.5. If, by contraposition, the sheaves were *not* geometrically irreducible, we would get

$$\left| \frac{1}{|k|} \sum_{x \in U(k)} t_{\mathcal{F}_1,k}(x)\overline{t_{\mathcal{F}_2,k}(x)} \right| \leqslant \frac{3c\,\mathrm{rank}(\mathcal{F}_1)\,\mathrm{rank}(\mathcal{F}_2)}{\sqrt{|k|}}$$

by the same lemma, and by comparing we deduce that

$$\sqrt{|k|} \leqslant 3c\,\mathrm{rank}(\mathcal{F}_1)(\mathrm{rank}(\mathcal{F}_1) + \mathrm{rank}(\mathcal{F}_2))$$

in that case. □

We continue with the data k, X/k and Y/k as above. We let V denote the vector space of complex-valued functions $U(k) \longrightarrow \mathbf{C}$. We view V as a complex Hilbert space with the inner product

$$\langle \varphi_1, \varphi_2 \rangle = \frac{1}{|k|} \sum_{x \in U(k)} \varphi_1(x)\overline{\varphi_2(x)},$$

or as a *real* Hilbert space isomorphic to $\mathbf{R}^{2|U(k)|}$ with coordinates given by

$$(\mathrm{Re}\,\varphi(x), \mathrm{Im}\,\varphi(x))_{x \in U(k)},$$

and with inner product

$$\langle v, w\rangle_{\mathbf{R}} = \frac{1}{|k|}\sum_{i=1}^{2|U(k)|} v_i w_i$$

for v, $w \in \mathbf{R}^{2|U(k)|}$.

We have the compatibility

$$\|\varphi\| = \|\varphi\|_{\mathbf{R}}$$

for $\varphi \in V$, with obvious notation. Similarly, the angle $\theta_{\mathbf{R}}(\varphi_1, \varphi_2) \in [0, \pi[$ between φ_1, $\varphi_2 \in V$ (viewed as a real Hilbert space) is defined by

$$\langle \varphi_1, \varphi_2\rangle_{\mathbf{R}} = \|\varphi_1\|\|\varphi_2\| \cos\theta_{\mathbf{R}}(\varphi_1, \varphi_2),$$

and also satisfies

$$\cos\theta_{\mathbf{R}}(\varphi_1, \varphi_2) = \frac{\mathrm{Re}(\langle \varphi_1, \varphi_2\rangle)}{\|\varphi_1\|\|\varphi_2\|}.$$

Fix now $c \geqslant 1$ and $r \leqslant c$. If $|k| > 3cr^2$ and $\mathcal{F} \in \mathsf{L}(U/k, c)$ has rank $\leqslant r$, we can define

$$v_{\mathcal{F}} = \frac{\varphi}{\|\varphi\|}$$

where φ is the restriction to $U(k)$ of $t_{\mathcal{F},k}$, since the trace function is not identically zero by the previous corollary. This is a vector on the unit sphere of V.

Lemma 3.7 (Spherical codes from sheaves)**.** *With notation as above, for fixed $c \geqslant 1$ and $r \leqslant c$ with $12cr^2 < \sqrt{|k|}$, we have*

$$\cos\theta_{\mathbf{R}}(v_{\mathcal{F}_1}, v_{\mathcal{F}_2}) \leqslant \frac{6cr^2}{\sqrt{|k|}} \leqslant \frac{3\sqrt{10}cr^2}{\sqrt{2|U(k)|}}$$

for any sheaves $\mathcal{F}_1$ and $\mathcal{F}_2$ in $\mathsf{L}(U/k, c)$, which are not geometrically isomorphic and have rank $\leqslant r$.

Proof. We have

$$\cos\theta_{\mathbf{R}}(v_{\mathcal{F}_1}, v_{\mathcal{F}_2}) = \frac{\mathrm{Re}(\langle \varphi_1, \varphi_2\rangle)}{\|\varphi_1\|\|\varphi_2\|}$$

where φ_i is the restriction of $t_{\mathcal{F}_i,k}$ to $U(k)$. By Lemma 3.5, we have

$$|\langle \varphi_1, \varphi_2\rangle| \leqslant \frac{3cr^2}{\sqrt{|k|}}, \quad \|\varphi_1\|\|\varphi_2\| \geqslant 1 - \frac{3cr^2}{\sqrt{|k|}}.$$

Since

$$\frac{x}{(1-x)} \leqslant 2x$$

for $0 \leqslant x \leqslant 1/4$, and

$$|U(k)| \leqslant |k| + 2g\sqrt{|k|} + 1 \leqslant |k| + 3g\sqrt{|k|} \leqslant \frac{5}{4}\sqrt{|k|}$$

under our assumption $12cr^2 \leqslant |k|^{1/2}$, we get the result. □

It follows directly from this lemma, Corollary 3.6 and from the definition in Section 2, that for $r \leqslant c$ and $12cr^2 < \sqrt{|k|}$, we have

$$|\,\mathbf{L}_r(U/k,c)| \leqslant M\left(2|U(k)|, \arccos\left(\frac{3\sqrt{10}cr^2}{\sqrt{2|U(k)|}}\right)\right).$$

We can then apply Theorem 2.1 with parameters

$$(n,\gamma) = (2|U(k)|, 3\sqrt{10}cr^2),$$

and the upper-bound in Proposition 3.1 follows as soon as the condition $n \geqslant 2\gamma\lceil(\gamma+1)^2\rceil$ in Theorem 2.1 is satisfied. Since $|U(k)| \geqslant |Y(k)| - c \geqslant |k| - 2g\sqrt{|k|} + 1 - c \geqslant \frac{5}{6}|k| - c$, this condition is satisfied provided

$$\frac{5|k|}{6} \geqslant 3\sqrt{10}cr^2\left\{(3\sqrt{10}cr^2+1)^2+1\right\} + c,$$

which holds for $|k| \geqslant 1265c^3r^6$, a condition that also implies the previous conditions on $|k|$ from Corollary 3.6 and Lemma 3.7.

4. Comments

The bounds we have obtained are certainly far from the truth. In fact, it would be even more interesting to have good lower bounds, but this question is not currently very well understood. This can be illustrated with the following two remarks:

(1) (Pointed out by Venkatesh): We do not know if, given a large enough rank $r \geqslant 1$, there exists a single unramified cusp form on $\mathrm{GL}_r(K)$, where K is the function field of a fixed curve over a finite field of genus > 1; in our notation, the question is, given an open dense set $U \subset \mathbf{A}^1$ defined over k, whether there exists *some* geometrically irreducible lisse sheaf $\mathcal{F}$ on U for *every* large enough rank $r \geqslant 1$.

(2) (Pointed out by Katz): Deligne and Flicker [8, Prop. 7.1] prove, using automorphic methods, that there exist $q = |k|$ lisse sheaves on $(\mathbf{P}^1 - S)/k$, where S is an étale divisor of degree four (e.g., on $\mathbf{P}^1 - \{\text{four points in } k\}$) of rank 2, with "principal unipotent local monodromy" at the singularities (see [8, Section 1] for precise definitions.) However, only a bounded number of such sheaves are explicitly known (bounded as q varies)! Examples include semistable families of elliptic curves with four singular fibers, from Beauville's classification [1].

We now indicate some examples of families of sheaves which give easy lower bounds. We denote by p the characteristic of k, and we consider $X = \mathbf{A}^1$ for simplicity.

(1) If $U \hookrightarrow \mathbf{A}^1$ is a dense open subset (defined over k), and f_1 (resp. f_2) is a regular function $f_1 : U \longrightarrow \mathbf{A}^1$ (resp. a non-zero regular function $f_2 : U \longrightarrow \mathbf{G}_m$) both defined over k, one has the Artin–Schreier–Kummer lisse sheaf

$$\mathcal{F} = \mathcal{L}_{\psi(f_1)} \otimes \mathcal{L}_{\chi(f_2)}$$

defined for any non-trivial additive character $\psi : k \longrightarrow \bar{\mathbf{Q}}_\ell^\times$ and multiplicative character $\chi : k^\times \longrightarrow \bar{\mathbf{Q}}_\ell^\times$, which satisfy

$$t_{\mathcal{F},k}(x) = \psi(f_1(x))\chi(f_2(x))$$

for $x \in U(k)$. These sheaves are all of rank 1 (in particular, they are geometrically irreducible) and pointwise pure of weight 0. Moreover, possible geometric isomorphisms among them are well-understood (see, e.g., [6, Sommes Trig. (3.5.4)]): if (g_1, g_2) are another pair of functions we have a geometric isomorphism

$$\mathcal{L}_{\psi(f_1)} \otimes \mathcal{L}_{\chi(f_2)} \simeq \mathcal{L}_{\psi(g_1)} \otimes \mathcal{L}_{\chi(g_2)}$$

if and only if: (1) $f_1 - g_1$ is of the form

$$f_1 - g_1 = h^p - h + C$$

for some regular function h on U and some constant $C \in \bar{k}$; (2) f_2/g_2 is of the form

$$\frac{f_2}{g_2} = Dh^d$$

where $d \geqslant 2$ is the order of the multiplicative character χ, h is a non-zero regular function on U and $D \in \bar{k}^\times$.

Furthermore, the conductor of these sheaves is fairly easy to compute. The singularities are located (at most) at $x \in \mathbf{P}^1 - U$. For each such x, the Swan conductor at x is determined only by f_1, and is bounded by the order of the pole of f_1 (seen as a function $\mathbf{P}^1 \longrightarrow \mathbf{P}^1$) at x, and there is equality if this order is $< p$.

In particular, if χ is trivial, the conductor of $\mathcal{L}_{\psi(f_1)}$ is $\leqslant 1+\deg(f_1)$. Taking polynomials of degree $\leqslant c-1$, modulo constants and modulo polynomials of the form $h^p - h$ where $\deg(h) \leqslant \lfloor \frac{c-1}{p} \rfloor \leqslant c/2$, we see that we have

$$|\,\mathbf{L}_1(\mathbf{A}^1/k, c)| \geqslant |k|^{c-1-c/2},$$

as indicated in the remark after Theorem 1.1.

(2) The following examples are studied by Katz [17, Ex. 7.10.2]. Let C/k be a smooth projective geometrically connected algebraic curve, and

$$f \,:\, C \longrightarrow \mathbf{P}^1$$

a non-constant map defined over k which is not a p-th power. Let $D \subset C$ be the divisor of poles of f. Let $Z \subset C - D$ be the set of zeros of the differential df, and let $S = f(Z)$ be the set of singular values of f. One says that f is *supermorse* if $\deg(f) < p$, all zeros of df are simple, and f separates these zeros (i.e., $|S| = |Z|$). Then, denoting by

$$f_0 \,:\, C - D \longrightarrow \mathbf{A}^1$$

the restriction of f to $C - D$, the sheaf

$$\mathcal{F}_f = \ker(\mathrm{Tr} \,:\, f_{0,*}\bar{\mathbf{Q}}_\ell \longrightarrow \bar{\mathbf{Q}}_\ell)$$

is an irreducible middle-extension sheaf on $\mathbf{A}^1/k$, of rank $\deg(f)-1$, pointwise pure of weight 0 and lisse on $\mathbf{A}^1 - S$ with

$$t_{\mathcal{F}_f,k}(x) = |\{y \in C(k) \;\mid\; f(y) = x\}| - 1$$

for $x \in k - S$. This sheaf is also everywhere tamely ramified, so its conductor is $|Z| + \deg(f) - 1$. However, it is not obvious how to count how many sheaves with conductor $\leqslant c$ one may obtain in this manner.

(3) There exists a Fourier transform on middle-extension sheaves on $\mathbf{A}^1/k$, corresponding to the Fourier transform of trace functions, which was defined by Deligne and developed especially by Laumon; precisely, consider a middle-extension sheaf $\mathcal{F}$ which is geometrically irreducible, of weight 0, and not geometrically isomorphic to $\mathcal{L}_\psi$ for some additive character ψ. Fix a non-trivial additive character ψ. Then the Fourier transform $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F})(1/2)$ (where the Tate twist is defined after picking the square root of $|k|$ in $\bar{\mathbf{Q}}_\ell$ mapping to $\sqrt{|k|} > 0$ via our chosen ι) satisfies

$$t_{\mathcal{G},k}(t) = -\frac{1}{\sqrt{|k|}} \sum_{x \in k} t_{\mathcal{F},k}(x)\psi(tx)$$

for $t \in k$, and it is a middle-extension sheaf, geometrically irreducible and pointwise pure of weight 0 (see [17, Section 7] for a survey and details). Moreover, one can show that the conductor of $\mathcal{G}$ is bounded polynomially in terms of the conductor of $\mathcal{F}$ (see, e.g., [12, Prop. 7.2]). However, even without inquiring about possible fixed points of the Fourier transform, its use would at best double any given lower bound for the number of sheaves with bounded ramification.

5. Trace norms and random functions

We describe in this section the proof of Theorem 1.4. The idea is to show that "random" functions defined on k have large trace norms:

Theorem 5.1. *Let X be a complex-valued random variable with $\mathbf{E}(X) = 0$, $\mathbf{E}(|X|^2) > 0$, $|X| \leqslant 1$. For p prime, let φ be random complex-valued functions in $C(k)$ such that the values $\varphi(x)$ are independent and identically distributed like X. For any $N \geqslant 1$, there exists $\alpha \geqslant 1$ depending only on N and on the law of X, such that we have*

$$\mathbf{P}\left(\frac{\sqrt{|k|}}{\alpha \log |k|} \leqslant \|\varphi\|_{\mathrm{tr},s} \leqslant \sqrt{|k|}\right) = 1 + O(|k|^{-N}),$$

for all $s \geqslant 6$, where the implied constant depends only on N and on the law of X.

This result easily implies Theorem 1.4.

Proof of Theorem 1.4. We must show the existence of a non-zero function $\varphi \in C(k)$ such that

$$\|\varphi\|_{\mathrm{tr},s} \gg \frac{\sqrt{|k|}}{\log |k|}\|\varphi\|_1.$$

Since $\|\varphi\|_{\mathrm{tr},s} \geqslant \|\varphi\|_{\mathrm{tr},6}$, it is enough to do this for $s = 6$, and this follows from Theorem 5.1 (for $N = 1$, for instance) and the property (5.2) proved below. □

Theorem 5.1 is a simple probabilistic argument, which uses little knowledge of trace functions in addition to the counting result Theorem 1.1. However, it requires some quantitative upper bound for $|\mathsf{ME}_{\mathbf{A}^1}(k, c)|$, and in fact it requires some control even for c varying with k.

First, we note the following criterion for lower bounds of $\|\varphi\|_{\mathrm{tr},s}$.

Proposition 5.2 (**Lower bounds for trace norms**). *Let k be a finite field and let $\varphi \in C(k)$ be any function. Let $s \geqslant 1$, $\gamma > 0$ and $A \geqslant 0$ be numbers such that*

$$|\varphi(y)| \leqslant A|k|^{1/2-\gamma}$$

for all $y \in k$ and

$$\left|\sum_{x\in k} K(x)\varphi(x)\right| \leqslant A|k|^{1-\gamma}\,\mathbf{c}(K)^s, \quad \sum_{x\in k}|\varphi(x)|^2 \geqslant A^{-1}|k|$$

for all trace functions $K = t_{\mathcal{F},k}$ of sheaves $\mathcal{F} \in \mathsf{ME}(k)$. Then we have

$$\|\varphi\|_{\mathrm{tr},s} \geqslant A^{-2}|k|^{\gamma}.$$

Remark 5.3. This result combined with [12, Cor. 1.6] also allows us to obtain concrete examples of functions with large trace norms. Precisely, if $k = \mathbf{F}_p$ identified with $\{1, \dots, p\}$ and $\varphi(n) = \varrho_f(n)$ for $1 \leqslant n \leqslant p$, where

$$f(z) = \sum_{n\geqslant 1} \varrho_f(n) n^{(\kappa-1)/2} e(nz)$$

is the Fourier expansion of a classical holomorphic cusp form with weight $\kappa \geqslant 2$ and level $N \geqslant 1$ (and trivial nebentypus), then for any $\varepsilon > 0$, we can derive

$$\|\varphi\|_{\mathrm{tr},s} \gg p^{1/8-\varepsilon}$$

for all $s \geqslant s_0$ and p large enough, where s_0 is some absolute constant, and where the implied constant depends on f and ε. The same result holds for the Fourier coefficients of a Maass cusp form. It seems quite conceivable that this estimate should in fact be true with $1/8$ replaced with $1/2$. More generally, it seems to be an interesting de-randomization problem to construct explicit functions $\varphi \in C(k)$ (say bounded by 1) with $\|\varphi\|_{\mathrm{tr},s}$ as large as the value $\approx |k|^{1/2}$ given by Theorem 5.1 for random functions.

We now begin the proof of Theorem 5.1 with some probabilistic preliminaries. We recall that a real-valued random variable X is called *σ-sub-Gaussian*, for some $\sigma > 0$, if

$$\mathbf{E}(e^{tX}) \leqslant \exp\left(\frac{\sigma^2 t^2}{2}\right)$$

for all $t \in \mathbf{R}$. The following properties are easy: (1) if X is σ-sub-Gaussian, then

$$\mathbf{P}(|X| \geqslant \alpha) \leqslant 2\exp\left(-\frac{\alpha^2}{2\sigma^2}\right)$$

for all $\alpha \geqslant 0$, and (2) if $X_1, \dots, X_k$ are σ_i-sub-Gaussian and independent and $a_i \in \mathbf{R}$, then $a_1X_1 + \cdots + a_kX_k$ is σ-sub-Gaussian where

$$\sigma^2 = \sum_{i=1}^{k} a_i^2\sigma_i^2.$$

We will use the following lemma:

Lemma 5.4. *Let k be a finite field. Let $\sigma > 0$, and for $x \in k$, let $\varphi(x)$ be independent complex-valued random variables with the same distribution, such that $|\varphi(x)| \leqslant 1$, $\mathbf{E}(\varphi(x)) = 0$, $\mathbf{E}(|\varphi(x)|^2) = \sigma^2$.*

(1) *The random variables* $\mathrm{Re}(\varphi(x))$ *and* $\mathrm{Im}(\varphi(x))$ *are* 1*-sub-Gaussian.*
(2) *There exists* ν_1, $\nu_2 > 0$ *and* c_1 $c_2 > 0$, *depending only on the common distribution of* $\varphi(x)$, *such that*

$$\mathbf{P}\left(\sum_{x\in k}|\varphi(x)|^2 \geqslant \nu_1|k|\right) \geqslant 1 - e^{-c_1|k|^2}, \tag{5.1}$$

$$\mathbf{P}\left(\sum_{x\in k}|\varphi(x)| \geqslant \nu_2|k|\right) \geqslant 1 - e^{-c_2|k|^2}. \tag{5.2}$$

Proof. (1) Since $|\mathrm{Re}(\varphi(x))| \leqslant |\varphi(x)| \leqslant 1$ and $\mathbf{E}(\mathrm{Re}\,\varphi(x)) = 0$ (and similarly for the imaginary part), this follows from the fact that if X is a real-valued random variable with $\mathbf{E}(X) = 0$ and which satisfies $|X| \leqslant \sigma$, then X is σ-sub-Gaussian (see, e.g., [2, Example 1.2]).
(2) These are elementary instances of concentration of measure (see, e.g., [22, Section 2.1]).

□

The next step shows that a random function is, with very high probability, strongly orthogonal to the trace function of any sheaf with small conductor:

Lemma 5.5. *Let* k *be a finite field,* φ *a random function on* k *as above. Let* $K = t_{\mathcal{F},k}$ *for some* $\mathcal{F} \in \mathsf{ME}(k)$. *We have*

$$\mathbf{P}\left(\left|\sum_{x\in k}K(x)\varphi(x)\right| \geqslant \alpha\,\mathbf{c}(\mathcal{F})^s\sqrt{|k|\log|k|}\right) \leqslant 8|k|^{-\frac{1}{2}\alpha^2\,\mathbf{c}(\mathcal{F})^{2s-2}}$$

for $s \geqslant 2$ *and* $\alpha > 0$.

Proof. We write

$$\varphi(x) = \varphi_1(x) + i\varphi_2(x), \quad K(x) = K_1(x) + iK_2(x)$$

the real and imaginary parts of $\varphi(x)$ and $K(x)$. Expanding the product, we have

$$\mathbf{P}\left(\left|\sum_{x\in k}K(x)\varphi(x)\right| \geqslant \beta\right) \leqslant \sum_{1\leqslant i,j\leqslant 2}\mathbf{P}\left(\left|\sum_{x\in k}K_i(x)\varphi_j(x)\right| \geqslant \beta/4\right)$$

for any $\beta \geqslant 0$. For $i = 1$ or 2, since the real and imaginary parts φ_j of $\varphi(x)$ are 1-sub-Gaussian and independent, we get

$$\mathbf{P}\left(\left|\sum_{x\in k}K_i(x)\varphi_j(x)\right| \geqslant \beta\right) \leqslant 2\exp\left(-\frac{\beta^2}{2\sigma_i^2}\right)$$

for $\beta \geqslant 0$, where

$$\sigma_i^2 = \sum_{x\in k}K_i(x)^2 \leqslant \sigma_K^2 = \sum_{x\in k}|K(x)|^2 \leqslant |k|\,\mathbf{c}(\mathcal{F})^2$$

and we get the result by taking $\beta = \alpha\,\mathbf{c}(K)^s\sqrt{|k|\log|k|}$. □

We now extend this to all sheaves with small enough conductor:

Lemma 5.6. *Let k be a finite field, φ a random function on k as above. For any $\gamma < 1/9$, and any $N \geqslant 1$, there exists $\alpha \geqslant 1$, depending only on γ and N, such that for any finite field k, we have*

$$\mathbf{P}\left(\left|\sum_{x\in k} t_{\mathcal{F},k}(x)\varphi(x)\right| \geqslant \alpha\, \mathbf{c}(\mathcal{F})^4\sqrt{|k|\log|k|},\right.$$
$$\left.\text{for some } \mathcal{F} \text{ with } \mathbf{c}(\mathcal{F}) \leqslant \tfrac{4}{10}|k|^{\gamma}\right) \ll |k|^{-N}.$$

Proof. For any $s \geqslant 2$, let

$$\varpi(c_1,c_2) = \mathbf{P}\left(\left|\sum_{x\in k} t_{\mathcal{F},k}(x)\varphi(x)\right| \geqslant \alpha\, \mathbf{c}(\mathcal{F})^s\sqrt{|k|\log|k|},\right.$$
$$\left.\text{for some sheaf } \mathcal{F} \text{ in } \mathsf{ME}(k) \text{ with } c_1 \leqslant \mathbf{c}(\mathcal{F}) \leqslant c_2\right).$$

We have

$$\varpi \leqslant \sum_{1\leqslant j\leqslant \left\lceil \gamma\frac{\log|k|}{\log 2}\right\rceil} \varpi(2^{j-1},2^j) \leqslant \sum_{j\ll\gamma\log|k|} |\,\mathbf{ME}(k,2^j)| \times 8|k|^{-\alpha^2 2^{(j-1)(2s-2)-1}}$$

by Lemma 5.5. All conductors involved are $\leqslant \frac{4}{10}|k|^{\gamma} < \left(\frac{1}{1265}\right)^{1/9}|k|^{1/9}$ by assumption, so we deduce

$$\varpi \ll \sum_{j\ll\gamma\log|k|} |k|^{B2^{6j}-\alpha^2 2^{(j-1)(2s-2)-1}},$$

for some absolute constant $B \geqslant 1$ by Theorem 1.1. Taking $s = 4$, the exponent of $|k|$ is

$$B2^{6j} - \alpha^2 2^{(j-1)(2s-2)-1} = B2^{6j} - \alpha^2 2^{6j-7} = (B - 2^{-7}\alpha^2)2^{6j} \leqslant -\frac{\alpha^2}{2^8}2^{6j}$$

under the assumption that $\alpha^2 \geqslant 2^8 B$, and we get $\varpi \ll (\log|k|)|k|^{-\alpha^2/4}$, which gives the result by taking $\alpha > 0$ large enough. □

Proof of Theorem 5.1. For any function $\varphi \in C(k)$ with $|\varphi| \leqslant 1$, and any sheaf $\mathcal{F}$ in $\mathsf{ME}(k)$, we have trivially

$$\left|\sum_{x\in k} t_{\mathcal{F},k}(x)\varphi(x)\right| \leqslant 100\,\mathbf{c}(\mathcal{F})^6|k|^{1/2}$$

if $\mathbf{c}(\mathcal{F}) > \frac{4}{10}|k|^{1/10}$. In particular, if we apply the last lemma with $\gamma = \frac{1}{10}$, any fixed $N \geqslant 1$, and the corresponding constant $\alpha \geqslant 1$, we deduce that

$$\mathbf{P}\left(\left|\sum_{x\in k} t_{\mathcal{F},k}(x)\varphi(x)\right| \geqslant \alpha'\,\mathbf{c}(\mathcal{F})^6\sqrt{|k|\log|k|}, \text{for some } \mathcal{F} \text{ in } \mathsf{ME}(k)\right) \ll |k|^{-N}$$

where $\alpha' = \max(\alpha, 100)$. Then taking into account (5.1), we see that if we take

$$s = 6, \quad \gamma = 1/2, \quad A = \alpha\sqrt{\log|k|},$$

then the probability that φ does not satisfy the conditions of Proposition 5.2 for these values is $\ll |k|^{-N}$. Therefore, we obtain our result using the upper-bound (1.2). □

Acknowledgments

We wish to thank N. Katz for discussions surrounding these problems, and H. Esnault for clarifying Deligne's work and its fascinating general context. We also thank the referee for suggesting that we treat the case of sheaves on arbitrary curves over finite fields and for other insightful comments. Finally, thanks to F. Jouve for discussions concerning the issue of lower bounds.

References

[1] A. Beauville, *Les familles stables de courbes elliptiques sur* $\mathbf{P}^1$ *admettant quatre fibres singulires*, C. R. Acad. Sc. Paris **294** (1982), 657–660.
[2] V. Buldygin and Y.V. Kozachenko, *Metric characterization of random variable and random processes*, Translations of Mathematics, Monographs **188**, A.M.S, 2000.
[3] J. Conway and N. Sloane, *Sphere packings, lattices and groups*, Grund. der Math. Wiss. **290**, Springer-Verlag, 1988.
[4] P. Deligne, *Letter to V. Drinfeld*, dated June 18, 2011, 9 p.
[5] ———, *Counting ℓ-adic representations, in the function field case*, lecture at the Newton Institute, July 2009. `http://www.newton.ac.uk/programmes/NAG/seminars/072710001.html`.
[6] ———, *Cohomologie étale, S.G.A* $4\frac{1}{2}$, Lecture Notes in Math. **569**, Springer-Verlag (1977).
[7] ———, *La conjecture de Weil, II*, Publ. Math. IHÉS **52** (1980), 137–252.
[8] P. Deligne and Y. Flicker, *Counting local systems with principal unipotent local monodromy*, Ann. Math. (to appear) `http://www.math.osu.edu/~flicker.1/df.pdf`.
[9] V. Drinfeld, *The number of two-dimensional irreducible representations of the fundamental group of a curve over a finite field*, Funct. Anal. Appl. **15** (1981), 294–295.
[10] H. Esnault and M. Kerz, *A finiteness theorem for Galois representations of function fields over finite fields (after Deligne)*, Acta Math. Vietnam. **37** (2012), 351–362.
[11] É. Fouvry, E. Kowalski and P. Michel, *Algebraic trace functions over the primes*, (2012), `www.math.ethz.ch/~kowalski/weights-over-primes.pdf`.
[12] ———, *Algebraic twists of modular forms and Hecke orbits*, preprint (2012), `www.math.ethz.ch/~kowalski/twists.pdf`.
[13] H. Helfgott and A. Venkatesh, *Integral points on elliptic curves and* 3*-torsion in class groups*, J. Amer. Math. Soc. **19** (2006), 527–559.
[14] P. Jaming and A. Powell, *Uncertainty principles for orthonormal sequences*, J. Funct. Anal. **243** (2007), 611–630.
[15] G. Kabatjanskii and V. Levenshtein, *Bounds for packings on the sphere and in space*, Problem. Peredači Inf. **14** (1978), 3–25.
[16] N. Katz, Gauss sums, *Kloosterman sums and monodromy groups*.
[17] ———, *Exponential sums and differential equations*, Annals of Mathematics Studies **124**, Princeton University Press (1990).
[18] L. Lafforgue, *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. Math. **147** (2002), 1–241.
[19] V. Levenshtein, *Universal bounds for codes and designs*, in 'Handbook of coding theory' (V. Pless and W. Huffman, eds.), Vol 1, North-Holland, 1998, 499–648.
[20] P. Delsarte, J.M. Goethals and J.J. Seidel, *Spherical codes and designs*, Geometriae Dedicata **6** (1977), 363–388.
[21] G. Szegö, *Orthogonal polynomials*, Colloquium Publications **23**, American Mathematical Society, 4th edn., 1975.
[22] T. Tao, *Topics in random matrix theory*, Graduate Studies in Mathematics **132**, American Mathematical Society, 2012.

Université Paris Sud, Laboratoire de Mathématique, Campus d'Orsay, 91405 Orsay Cedex, France
E-mail address: etienne.fouvry@math.u-psud.fr

ETH Zürich – D-MATH, Rämistrasse 101, 8092 Zürich, Switzerland
E-mail address: kowalski@math.ethz.ch

EPFL/SB/IMB/TAN, Station 8, CH-1015 Lausanne, Switzerland
E-mail address: philippe.michel@epfl.ch