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 $\mathbf{A}^1$ 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 combinations of trace functions of sheaves with small complexity. modulo p can not usually be approximated by short linear

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 the affine line 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 [5], as explained by Esnault and Kerz [11, 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 [10] computing the number of unramified 2-dimensional representations for a projective curve, and showing it is of this form; see again the survey in [11, §8] and the paper of Deligne and Flicker [7, §6] (and the lecture [6] of Deligne).

Our goal in this note is very modest. First of all, we will only consider a particularly simple case, and our result will be an explicit upper bound for the size of certain of these sets of étale sheaves. What we prove may not have much interest in the greater scheme of things, 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

Date: January 20, 2013, 9:27.

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.

be present in the literature. We note also that the first version of this note was in fact written "out of curiosity" before the authors were aware of the works of Drinfeld, Deligne, Esnault–Kerz or Deligne–Flicker.

Let p be a prime number and let k be a finite field of characteristic p. Fix an auxiliary prime $\ell \neq p$. We will consider *middle-extension sheaves* on $\mathbf{A}^1/k$, in the sense of [17], i.e., constructible $\bar{\mathbf{Q}}_\ell$-sheaves $\mathcal{F}$ on $\mathbf{A}^1/k$ such that, for any open set U on which $\mathcal{F}$ is lisse, with open immersion $j : U \hookrightarrow \mathbf{A}^1$, 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 [18, §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 $\mathbf{A}^1/k$ 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 $\mathbf{A}^1$.

Let $\mathcal{F}$ be a middle-extension sheaf on $\mathbf{A}^1/k$, of rank $\mathrm{rank}(\mathcal{F})$, with singularities at the finite set $\mathrm{Sing}(\mathcal{F}) \subset \mathbf{P}^1$. We define the analytic conductor (often just called "conductor") of $\mathcal{F}$ to be

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

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

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

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

Theorem 1.1. (1) *We have*

$$|\,\mathrm{ME}(k, c)| \gg |k|^{c-1}$$

with an absolute implied constant.

(2) *There exists an absolute constant B such that we have*

$$|\,\mathrm{ME}(k, c)| \ll |k|^{Bc^6},$$

for all finite fields k with $|k| \geqslant 10^3 c^9$, where the implied constants are absolute. In particular, for fixed c, we have $|\mathrm{ME}(k,c)| \ll |k|^{Bc^6}$.

Here the lower bound (1) is easy and just given for information (see Section 4). The upper bound is our main result, and in fact, we can give fully explicit inequalities, and not just asymptotic statements. Moreover, the constant A can be made explicit, and the c^6 can be refined (see Proposition 3.1 for these more precise results). Although these upper-bounds are probably not sharp, they can be useful for certain purposes, as we will see below.

As far as we know, this theorem 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 correspondance over function fields (as proved by Lafforgue [19]) to reduce to counting automorphic forms or representations, and this is indeed how Deligne and Flicker [7] proceed to obtain a "Lefschetz-type" formula for the counting function for cases where the local monodromy is unipotent (on any smooth projective curve, not only $\mathbf{P}^1$). As far as upper-bounds are concerned, or just asymptotic behavior, one might hope to have some versions of the Weyl Law for the distribution of Laplace eigenvalues, but controlling these 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*

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

(giving the trace of the geometric Frobenius automorphism of k acting on the stalk of $\mathcal{F}$ at a geometric point $\bar{x}$ over $x \in k$, seen as a finite-dimensional representation of the Galois group of k) of $\mathcal{F} \in \mathsf{ME}(k,c)$. We view these trace functions (via some isomorphism $\iota : \bar{\mathbf{Q}}_\ell \longrightarrow \mathbf{C}$) as elements of the finite dimensional Hilbert space of complex-valued functions on 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 trace functions of sheaves in $\mathsf{ME}(k,c)$ is at least $\pi/2 - O(1/\sqrt{|k|})$, i.e., they are what is known as *spherical codes* (sets of points on a sphere with some fixed angular separation property). This 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 [16] (see also [20] 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 Levenstein, as we present in Section 2 (and they might be of independent interest).

In Section 5, we use these estimates to prove that a "random" function $k \longrightarrow \mathbf{C}$ can not be represented by short linear combinations of trace functions of sheaves with small conductor, in some precise quantitative sense. Here it is important to have a quantitative statement on the size of $\mathrm{ME}(k,c)$, and not merely to know that it is finite. We state here an easy corollary that does not involve random functions. First, following [12], we define *trace norms*:

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

Definition 1.2 (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

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

where the infinum 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 element of $\mathsf{ME}(k,c)$ and we denote by δ_a the delta function at a point $a \in k$.

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). We wish to compare this norm with more standard ones, motivated by our results in [12, 13]. 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 the norm $\|i_s\|$ of the identity map

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

(between the finite-dimensional normed vector space $C(k)$ viewed with the L^1-norm and with the trace norm) satisfies $\|i_s\| \leqslant |k|^{1/2}$ for all $s \geqslant 0$. We show that this easy estimate can not be significantly improved:

Theorem 1.3. *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.

Acknowledgements. We wish to thank N. Katz for discussions surrounding these problems, and H. Esnault for clarifying Deligne's work and its fascinating general context.

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

By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geqslant 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. The "implied constant" refers to any value of C for which this holds. It may depend on the set X, which is usually specified explicitly, or clearly determined by the context. We write $f(x) \asymp g(x)$ to mean $f \ll g$ and $g \ll f$.

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. Preliminaries

The range of angles defining spherical codes for which we need bounds is not standard, and we haven't found a direct statement of the exact form we need in the literature. We therefore first explain how to use the Kabatjanskii–Levenshtein bounds [16] to obtain what we want, referring to [20] which is a more accessible reference.

Following the notation in [20], 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 $c > 0$ be a fixed real number. For*

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

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

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

Proof. By [20, (6.24), (6.25)], 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, and furthermore the latter satisfies

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

where h_k is the largest root of the k-th Hermite polynomial H_k (see also [20, Cor. 5.17]). It is known (see, e.g., [21, (6.32.8)]) that

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

in terms of the first zero $i_1 = 4.54564\ldots > 0$ of the Airy function

$$\mathrm{Ai}(x) = \frac{\pi}{3}\sqrt{\frac{x}{3}}\Big\{ J_{1/3}\Big(2\Big(\frac{x}{3}\Big)^{3/2}\Big) + J_{-1/3}\Big(2\Big(\frac{x}{3}\Big)^{3/2}\Big)\Big\},$$

but we prefer to use fully explicit inequalities. For instance, easy arguments (see [21, (6.2.14)]) give the lower bound

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

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

$$\frac{c}{\sqrt{n}} \leqslant \sqrt{\frac{k-1}{2}}\Big(\frac{2(n+k-2)}{(n+2k-2)(n+2k-4)}\Big)^{1/2}.$$

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

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

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

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

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

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

□

Remark 2.2. (1) The point of this result is the polynomial growth of $M(n,\varphi)$ as n tends to infinity for a fixed c, although it may also be interesting in some ranges when c grows with n. When $c < 1$, a bound of this type follows from the early result of Delsarte, Goethals and Seidel [9, 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 ([20, Th. 6.7]), which corresponds to c of size $\alpha n^{1/2}$ for some fixed $\alpha > 0$.

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

(3) See the paper [14] 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 [15] of Jaming and Powell.

3. Proof of the main result

It is more efficient to give estimates for certain subsets of $\mathrm{ME}(k,c)$ and sum the resulting bounds. Indeed, these subsets are of independent interest, and are more closely related to those considered by Drinfeld and Deligne (and Esnault–Kerz, Deligne–Flicker).

Thus let U/k be a dense open subset of $\mathbf{A}^1/k$. 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 their largest open set of lissité in $\mathbf{A}^1/k$, and which satisfy

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

where $j : U \hookrightarrow \mathbf{A}^1$ is the embedding of U in $\mathbf{A}^1$. As before, $\mathrm{L}(U/k,c)$ denotes the set of geometric isomorphism classes of objects in $\mathsf{L}(U/k,c)$. We further denote by $\mathsf{L}_r(U/k,c)$ (resp. $\mathrm{L}_r(U/k,c)$) the subcategory where the rank is $\leqslant r$ (resp. the set of geometric isomorphism classes of this subcategory).

Note that for any such $\mathcal{F}$ on U, the direct image $j_*\mathcal{F}$ is a geometrically irreducible middle-extension sheaf on $\mathbf{A}^1/k$, pointwise of weight 0, i.e., an object in $\mathsf{ME}(k,c)$. Moreover, since 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, we can write

$$|\,\mathrm{ME}(k,c)| \leqslant \sum_{n(U)\leqslant c} |\,\mathrm{L}(U/k,c)| \leqslant \sum_{r\leqslant c}\sum_{n(U)\leqslant c} |\,\mathrm{L}_r(U/k,c)| \tag{3.1}$$

where U/k runs over all open subsets of $\mathbf{A}^1$ which are defined over k and satisfy $n(U) = |\mathbf{P}^1 - U| \leqslant c$. This inner sum can be parameterized by squarefree monic polynomials of degree $\leqslant c$ in $k[X]$, and in particular it involves $\leqslant |k|^c$ terms.

Our basic estimates are the following:

Proposition 3.1 (Counting lisse sheaves)**.** *Let k be a finite field and $c \geqslant 1$. For any open set $U/k \hookrightarrow \mathbf{A}^1/k$ with $n(U) = |\mathbf{P}^1 - U| \leqslant c$ and for $r \leqslant c$, we have*

$$|\,\mathrm{L}_r(U/k,c)| \leqslant \frac{2|k|^{72c^2r^4+12\sqrt{2}cr^2+3}}{\Gamma(72c^2r^4)}$$

provided $|k| \geqslant 782c^3r^6$.

Remark 3.2. Applying the "automorphic side to Galois side" part of the global Langlands correspondance on $\mathbf{P}^1/k$ [19, 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 $F = k(t)$ of $\mathbf{P}^1/k$. Even with automorphic techniques, it is not clear how to prove such a bound.

By (3.1), this proposition implies Theorem 1.1. We now start the proof with a variant of the well-known upper bounds on the dimension of cohomology groups of lisse sheaves on open subsets of $\mathbf{A}^1/k$.

Lemma 3.3. *Let k be a finite field, let $j : U/k \hookrightarrow \mathbf{A}^1/k$ be a dense open subset with $n(U) = |\mathbf{P}^1 - U|$ missing points, and let $\mathcal{F}_1$, $\mathcal{F}_2$ be lisse ℓ-adic sheaves on U/k which are geometrically irreducible. Let $c = \max(\mathbf{c}(j_*\mathcal{F}_1), \mathbf{c}(j_*\mathcal{F}_2))$. We have*

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

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 for 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., [17, Ch. 2]) gives

$$\begin{aligned} -\chi_c(U \times \bar{k}, \mathcal{F}) &= -\chi_c(U \times \bar{k}) \operatorname{rank}(\mathcal{F}) + \sum_{x \in \operatorname{Sing}(\mathcal{F})} \operatorname{Swan}_x(\mathcal{F}) \\ &= (n(U) - 2) r_1 r_2 + \sum_{x \in (\mathbf{P}^1 - U)} \operatorname{Swan}_x(\mathcal{F}). \end{aligned}$$

We have

$$\operatorname{Swan}_x(\mathcal{F}) \leqslant \operatorname{rank}(\mathcal{F}) \lambda_x(\mathcal{F}) = r_1 r_2 \lambda_x(\mathcal{F})$$

at each $x \in \mathbf{P}^1 - U$, 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

$$\begin{aligned} \sum_{x \in (\mathbf{P}^1 - U)} \operatorname{Swan}_x(\mathcal{F}) &\leqslant \operatorname{rank}(\mathcal{F}) \sum_{x \in \mathbf{P}^1 - U} (\lambda_x(\mathcal{F}_1) + \lambda_x(\mathcal{F}_2)) \\ &\leqslant \operatorname{rank}(\mathcal{F})(\mathbf{c}(\mathcal{F}_1) + \mathbf{c}(\mathcal{F}_2)) \leqslant 2c r_1 r_2. \end{aligned}$$

To conclude, we write

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

□

Remark 3.4. (1) 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 $\mathbf{P}^1 - U$ in this statement (i.e., they are not necessarily primitive), in which case an estimate $n(U) \leqslant c$ is not always valid.

(2) The overall order of magnitude of the bound, namely $\approx c r_1 r_2$ (assuming that $n(U) \leqslant c$), can not be significantly improved, since in the tame case we have exactly

$$\dim H_c^1(U \times \bar{k}, \mathcal{F}) = 1 + (n(U) - 2) r_1 r_2.$$

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 be a finite field, let $U \hookrightarrow \mathbf{A}^1$ be an open dense subset of $\mathbf{A}^1/k$. 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*

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

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

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

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

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

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

$$\mathrm{Tr}(\mathrm{Fr}_k \mid H^2_c(\mathbf{A}^1 \times \bar{k}, \mathcal{F})) = \delta(\mathcal{F}_1, \mathcal{F}_2)|k|,$$

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

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

by Deligne's main result on the Rieman Hypothesis over finite fields [8, 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 [11, §5]).

Corollary 3.6. *Let k be a finite field, let $U \hookrightarrow \mathbf{A}^1$ be an open dense subset of $\mathbf{A}^1/k$ and 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, the map $\mathcal{F} \mapsto t_{\mathcal{F},k}$ is injective on any set of representatives of geometric isomorphism classes of objects in $\mathsf{L}(U/k, c)$ under this condition.

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

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

by Lemma 3.5.

For (2), only the "only if" part needs proof (by 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

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

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

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

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 a fixed finite field k and a dense open set $U \hookrightarrow \mathbf{A}^1$ of $\mathbf{A}^1/k$. We now let V denote the vector space of complex-valued functions $U(k) \longrightarrow \mathbf{C}$. We can view it as a complex Hilbert space with the inner product

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

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 the standard inner product denoted $\langle\cdot,\cdot\rangle_{\mathbf{R}}$ on this real Hilbert space. 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*

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

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

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

Since

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

for $0 \leqslant x \leqslant 1/4$, we get the result. □

It follows directly from this lemma and from the definition in Section 2 that

$$|\,\mathrm{L}_r(U/k, c)| \leqslant M\Big(2U(k), \arccos\Big(\frac{6cr^2}{\sqrt{|k|}}\Big)\Big).$$

We can then apply Theorem 2.1 with $n = 2|U(k)| \geqslant 2|k| - 2c$, and c there taken to be $6\sqrt{2}cr^2$. The condition on the dimension in Theorem 2.1 is satisfied provided

$$|k| \geqslant 6\sqrt{2}cr^2((6\sqrt{2}cr^2 + 1)^2 + 1) + c,$$

which certainly holds[2] for $|k| \geqslant 782c^3r^6$ (which is also stronger than the condition on $|k|$ in Lemma 3.7).

4. Comments

The bounds we have obtained are certainly far from the truth. In fact, it would be much more interesting to have decent lower bounds than this type of upper bounds, but lower bounds are much less understood, especially if one restricts more stringently the ramification than by bounding the conductor. This can be seen from 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;

(2) (Pointed out by Katz): Deligne and Flicker [7, 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 [7, §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].

[2] Since $6\sqrt{2} \times ((72 + 12\sqrt{2} + 2) + 1) \leqslant 781$.

4.1. **Examples of sheaves.** We will indicate now some easy lower bounds, which are of much smaller order of magnitude than Proposition 3.1 when bounding only the conductor.

(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., [4, Sommes Trig. (3.5.4)]): if (g_1, g_2) are another pair of functions we have

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

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

$$f_1 - g_1 = h^{|k|} - h + C$$

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 (there is equality if this order is $< |k|$).

In particular, we see that if $c < |k|$, we have

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

by just counting the Artin-Schreier sheaves $\mathcal{L}_{\psi(f)}$ where $f \in k[X]$ has degree c: only polynomials different by a constant give geometrically isomorphic sheaves. This gives the lower bound stated in Theorem 1.1.

(2) The following examples are studied by Katz [18, 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 $|Z| + \deg(f) - 1$.

It is not as easy to count such sheaves as before, especially to understand possible isomorphisms. If we bound uniformly the conductor we might optimistically hope to get as many $\mathcal{F}_f$ as there are curves of genus $\ll c$ over k, which might be of size $|k|^{3c-3}$ as $|k| \to +\infty$, though this is far from being something one can prove today.

(3) There exists a Fourier transform on middle-extension sheaves corresponding to the Fourier transform of trace functions, which was defined by Deligne and developped 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 $\mathcal{G} = \mathrm{FT}_\psi(\mathcal{F})(1/2)$ 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 [18, §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], though the definition of conductor is slightly different there).

However, even without enquiring about possible fixed points of the Fourier transform, its use leads at best to only double the lower bounds for the number of sheaves...

5. Trace norms and random functions

We describe in this section an application of the previous results that leads to Theorem 1.3. Motivated by our results of [12] and [13], which show that trace functions of suitables sheaves on $\mathbf{F}_p$ are uncorrelated with Fourier coefficients of modular forms, or with the Möbius function, one may ask what are functions modulo p which are linear combinations with "small" coefficients of trace functions of sheaves with "small" conductor (the estimates in [12] and [13] extend naturally by linearity to such functions). It is not too surprising that most functions modulo p do not have such representations. We make this precise by considering the trace norms of "random" functions, and showing that the trivial bound (1.2) can usually not be much improved.

Precisely, we will consider the following model of random functions on a finite field k: the values $\varphi(x)$, for $x \in k$, are independent complex-valued random variables (on some fixed probability space $(\Omega, \Sigma, \mathbf{P})$), and they are identically distributed and satisfy $|\varphi(x)| \leqslant 1$ for all x and

$$\mathbf{E}(\varphi(x)) = 0, \qquad \mathbf{E}(|\varphi(x)|^2) > 0.$$

We will show that $\|\varphi\|_{\mathrm{tr},s}$ is close to $\sqrt{|k|}$ with high probability if $s \geqslant 6$. Precisely:

Theorem 5.1. *Let X be a random variable with $\mathbf{E}(X) = 0$, $\mathbf{E}(|X|^2) > 0$, $|X| \leqslant 1$. For p prime, let φ be random functions in $C(k)$ such that the values $\varphi(x)$ are independent and*

identically distributed like X. There exists $\alpha \geqslant 1$, depending only on the law of X, such that we have

$$\mathbf{P}\Big(\frac{\sqrt{|k|}}{\alpha \log |k|} \leqslant \|\varphi\|_{\mathrm{tr},s} \leqslant \sqrt{|k|}\Big) = 1 + O(|k|^{-100}),$$

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

This result easily implies Theorem 1.3.

Proof of Theorem 1.3. 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 $s = 6$. If we pick a fixed random variable X satisfying the assumptions of Theorem 5.1 (e.g., X uniformly distributed on the unit disc), it follows from Theorem 5.1 and the property (5.2) proved below that the corresponding random function has this property with very high probability as $|k| \to +\infty$. In particular, as soon as the probability is > 0, it follows that there exists at least one such function φ (the implied constant is absolute since we fix the distribution X for all $|k|$). □

Theorem 5.1 is a relatively simple probabilistic argument, which uses little knowledge of trace functions in addition to the counting result Theorem 1.1 (and abstract versions can certainly be found in the literature). We use the following criterion to obtain 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*

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

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

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

Proof. The first two assumptions imply by linearity that

$$\Big|\sum_{x\in k} \varphi(x)K(x)\Big| \leqslant A|k|^{1-\gamma}\|K\|_{\mathrm{tr},s}$$

for all $K \in C(k)$. Taking $K = \bar{\varphi}$ and using the last assumption, we get

$$A^{-1}|k| \leqslant A|k|^{1-\gamma}\|K\|_{\mathrm{tr},s},$$

hence the result. □

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-subgaussian, for some $\sigma > 0$, if

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

for all $t \in \mathbf{R}$. The following results are standard and easy:

Lemma 5.3. (1) *If X is σ-subgaussian, then we have*

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

for all $\alpha \geqslant 0$.

(2) *If $X_1, \ldots, X_k$ are σ_i-subgaussian and independent and $a_i \in \mathbf{R}$, then $a_1X_1 + \cdots + a_kX_k$ is σ-subgaussian where*

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

Now we state the properties of our model that we need:

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

(1) *The random variables $\mathrm{Re}(\varphi(x))$ and $\mathrm{Im}(\varphi(x))$ are 1-subgaussian.*

(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*

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

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

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-subgaussian (see, e.g., [2, Example 1.2]).

(2) These are quite standard properties of concentration of measure (see, e.g., [22, §2.1]), but we give the details for completeness. Let $\delta > 0$ be such that

$$t = \mathbf{P}(|\varphi(x)| \geqslant \sqrt{|k|}) > 0.$$

We then have

$$\mathbf{P}\Big(\sum_{x\in k} |\varphi(x)|^2 < \tfrac{1}{2}t\delta|k|\Big) \leqslant \mathbf{P}\Big(\sum_{x\in k} B_x < \tfrac{1}{2}t|k|\Big),$$
$$\mathbf{P}\Big(\sum_{x\in k} |\varphi(x)| < \tfrac{1}{2}t\sqrt{\delta}|k|\Big) \leqslant \mathbf{P}\Big(\sum_{x\in k} B_x < \tfrac{1}{2}t|k|\Big),$$

where B_x is the Bernoulli random variable equal to 1 if $|\varphi(x)| \geqslant \sqrt{\delta}$ and 0 otherwise. The B_x are independent and $\mathbf{P}(B_x = 1) = t > 0$. Consequently, the random variables $C_x = B_x - t$ are centered, independent, and $|C_x| \leqslant 1$. Thus the C_x are also 1-subgaussian and independent, and hence by Lemma 5.3, we have

$$\mathbf{P}\Big(\sum_{x\in k} C_x \leqslant -\alpha\Big) \leqslant \exp\Big(-\frac{\alpha^2}{2|k|}\Big).$$

for any $\alpha \geqslant 0$. Since

$$\mathbf{P}\Big(\sum_{x\in k} B_x < \tfrac{1}{2}t|k|\Big) \leqslant \mathbf{P}\Big(\sum_{x\in k} C_x \leqslant -\tfrac{1}{2}t|k|\Big)$$

we get

$$\mathbf{P}\Big(\sum_{x\in k}|\varphi(x)|^2 < \tfrac{1}{2}t\delta|k|\Big) \leqslant \exp(-c|k|^2)$$

with $c = t/8$, and similarly for the other probability. □

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

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

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

Proof. We write

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

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

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

for any $\beta \geqslant 0$.

Fix i. Since the real and imaginary parts φ_j of $\varphi(x)$ are 1-subgaussian and independent, Lemma 5.3 shows that the random variables

$$X_{i,j} = \sum_{x\in k}K_i(x)\varphi_j(x)$$

satisfy

$$\mathbf{P}(|X_{i,j}| \geqslant \beta) \leqslant 2\exp\Big(-\frac{\beta^2}{2\sigma_i^2}\Big)$$

for $\beta \geqslant 0$, where

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

so that we obtain the result by taking $\beta = \alpha\,\mathbf{c}(K)^s\sqrt{|k|\log|k|}$ and combining these inequalities. □

In order to conclude that φ is, with high probability, almost orthogonal to *all* trace functions of sheaves with small conductor, we now use a union bound and the estimate in Proposition 3.1 for the number of trace functions of sheaves with bounded conductor:

Corollary 5.6. *For any $\gamma < 1/9$, there exists $\alpha \geqslant 1$, depending only on γ, such that for any finite field k, we have*

$$\mathbf{P}\Big(\Big|\sum_{x\in k}t_{\mathcal{F},k}(x)\varphi(x)\Big| \geqslant \alpha\,\mathbf{c}(\mathcal{F})^4\sqrt{|k|\log|k|},\ \textit{for some } \mathcal{F} \textit{ with } \mathbf{c}(\mathcal{F}) \leqslant \frac{4}{10}|k|^{\gamma}\Big) \ll |k|^{-100}.$$

Proof. We combine the previous results with a dyadic subdivision of the conductors $c \leqslant \frac{4}{10}|k|^\gamma$. Let $s \geqslant 2$ be arbitrary. Denoting

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

we need to estimate $\varpi = \varpi(1, \frac{4}{10}|k|^\gamma)$. We write

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

(since the estimate in Lemma 5.5 holds for all sheaves in $\mathsf{ME}(k)$ geometrically isomorphic to a given $\mathcal{F}$ if it holds for $\mathcal{F}$). All conductors involved are $\leqslant \frac{4}{10}|k|^\gamma < \big(\frac{1}{1000}\big)^{1/9}|k|^{1/9}$ by assumption, so we can apply Theorem 1.1 to estimate $|\operatorname{ME}(k,2^j)|$, and 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 $B \geqslant 1$. 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 $\alpha^2 \geqslant 2^8 B$. Then we get

$$\varpi \ll (\log|k|)|k|^{-\alpha^2/4},$$

and for $\alpha > 0$ large enough, we get the desired estimate. □

Proof of Theorem 5.1. We now observe that for any function $\varphi \in C(k)$ with $|\varphi| \leqslant 1$, and any sheaf $\mathcal{F}$, we have

$$\Big|\sum_{x\in k} t_{\mathcal{F},k}(x)\varphi(x)\Big| \leqslant \|t_{\mathcal{F},k}\|_\infty|k| \leqslant \mathbf{c}(\mathcal{F})|k|$$

and hence

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

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

$$\mathbf{P}\Big(\Big|\sum_{x\in k} t_{\mathcal{F},k}(x)\varphi(x)\Big| \geqslant \alpha'\,\mathbf{c}(\mathcal{F})^6\sqrt{|k|\log|k|},\ \text{for } \textit{some } \mathcal{F} \text{ in } \mathsf{ME}(k)\Big) \ll |k|^{-100}$$

where $\alpha' = \max(\alpha, 100)$.

Furthermore, by our choice of random model, we have $|\varphi(x)| \leqslant 1$ for all x. Taking into account (5.1), we see that if we take

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

then the probability that φ does not satisfy the conditions of Proposition 5.2 for these values is $\ll |k|^{-100}$. Therefore, we obtain our result using the upper-bound (1.2) and the monotony of trace norms. □

References

[1] A. Beauville: *Les familles stables de courbes elliptiques sur* $\mathbf{P}^1$ *admettant quatre fibres singulières*, C. R. Acad. Sc. Paris 294 (1982), 657–660.

[2] V.V. Buldygin and Yu. V. Kozachenko: *Metric characterization of random variable and random processes*, Translations of Math. Monographs 188, A.M.S (2000).

[3] J.H. Conway and N.J.A. Sloane: *Sphere packings, lattices and groups*, Grund. der Math. Wiss. 290, Springer–Verlag, 1988.

[4] P. Deligne: *Cohomologie étale*, S.G.A $4\frac{1}{2}$, L.N.M 569, Springer Verlag (1977).

[5] P. Deligne: letter to V. Drinfeld, dated June 18, 2011, 9 pages.

[6] P. Deligne: *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`

[7] P. Deligne and Y. Flicker: *Counting local systems with principal unipotent local monodromy*, preprint (2011), `http://www.math.osu.edu/~flicker.1/df.pdf`

[8] P. Deligne: *La conjecture de Weil, II*, Publ. Math. IHÉS 52 (1980), 137–252.

[9] P. Delsarte, J.M. Goethals and J.J. Seidel: *Spherical codes and designs*, Geometriae Dedicata 6 (1977), 363–388.

[10] V. Drinfeld: *The number of two-dimensional irreducible representations of the fundamental group of a curve over a finite field*, Functional Anal. Appl. 15 (1981), 294–295 (1982).

[11] H. Esnault and M. Kerz: *A finiteness theorem for Galois representations of function fields over finite fields (after Deligne)*, preprint `arXiv:1208.0128v1`.

[12] É. Fouvry, E. Kowalski and Ph. Michel: *Algebraic twists of modular forms and Hecke orbits*, preprint (2012), `www.math.ethz.ch/~kowalski/twists.pdf`.

[13] É. Fouvry, E. Kowalski and Ph. Michel: *Algebraic trace functions over the primes*, preprint (2012), `www.math.ethz.ch/~kowalski/weights-over-primes.pdf`.

[14] H. Helfgott and A. Venkatesh: *Integral points on elliptic curves and* 3*-torsion in class groups*, Journal of the A.M.S 19 (2006), 527–550; `arXiv:math.NT/0405180v2`

[15] P. Jaming and A. Powell: *Uncertainty principles for orthonormal sequences*, J. Funct. Anal. 243 (2007), 611–630.

[16] G.A. Kabatjanskii and V.I. Levenshtein: *Bounds for packings on the sphere and in space*, Problemy Peredači Informacii 14 (1978), 3–25.

[17] N.M. Katz: *Gauss sums, Kloosterman sums and monodromy groups*, Annals of Math. Studies 116, Princeton Univ. Press (1988).

[18] N.M. Katz: *Exponential sums and differential equations*, Annals of Math. Studies 124, Princeton Univ. Press (1990).

[19] L. Lafforgue: *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. math. 147 (2002), 1–241.

[20] V.I. Levenshtein: *Universal bounds for codes and designs*, in "Handbook of coding theory", 499–648, North-Holland, Amsterdam, 1998.

[21] G. Szegö: *Orthogonal polynomials*, A.M.S. Coll. Publ. 23 (1939).

[22] T. Tao: *Topics in random matrix theory*, Grad. Studies in Math. 132, A.M.S (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`