

An inverse theorem for Gowers norms of trace functions over \mathbf{F}_p

BY ÉTIENNE FOUVRY†

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

EMMANUEL KOWALSKI

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

AND PHILIPPE MICHEL‡

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

(Received 29 January 2013)

Abstract

We study the Gowers uniformity norms of functions over $\mathbf{Z}/p\mathbf{Z}$ which are trace functions of ℓ -adic sheaves. On the one hand, we establish a strong inverse theorem for these functions, and on the other hand this gives many explicit examples of functions with Gowers norms of size comparable to that of “random” functions.

1. Introduction

The *Gowers uniformity norms* were introduced by Gowers in his work on Szemerédi’s theorem. As one sees from the definition (see [18, definition 11.2]), these norms (or a suitable power of them) have very algebraic definitions when applied to functions defined over a finite abelian group. In particular, one may consider a finite field k , and attempt to understand the Gowers norm of functions of algebraic nature on k . The most natural definition of such functions seems to be the *trace functions* of suitable sheaves, as we will recall below. Indeed, in recent works [5, 6, 7], we have shown that such functions (in the special case $k = \mathbf{F}_p$) can be exploited powerfully in analytic arguments of various types (amplification method for averages against Fourier coefficients of modular forms, bilinear forms for averages over primes, etc).

In this paper, we consider the Gowers norms of trace functions. Maybe the most crucial issue in the study of these norms has been to understand which bounded functions have “large” Gowers norm, a suitable structural answer being known as an “inverse theorem” for these norms. As it turns out, the rigidity of the structure of trace functions, and especially

† É. F. thanks ETH Zürich, EPF Lausanne and the Institut Universitaire de France for financial support.

‡ Partially supported by the SNF (grant 200021-137488) and the ERC (Advanced Research Grant 228304).

Deligne’s proof of the Riemann Hypothesis, also leads to a rather precise structure theorem for Gowers norms of trace functions over \mathbf{F}_p .

Although this was not anticipated at first,¹ it also turns out that the estimates we obtain give many simple explicit examples of functions with Gowers norms of size comparable to that of “random” functions, in a precise sense recalled below. Since this fact may be of interest to people interested in pseudorandomness measures of various sequences (see also, among others, the papers [17] of Niederreiter and Rivat, [16] of Liu and [9] of Fouvry, Michel, Rivat and Sárközy), we first state a concrete result which does not require any advanced algebraic-geometry language. In the statement, $\|\cdot\|_{U_d}$ is the d th Gowers uniformity norm (normalized as in [18, definition 11.2]), the definition of which is recalled in Section 2.

THEOREM 1.1. *For an odd prime p , and $x \in \mathbf{Z}/p\mathbf{Z}$, let:*

$$\varphi_1(x) = \left(\frac{f(x)}{p}\right); \tag{1.1}$$

$$\varphi_2(x) = e\left(\frac{\bar{x}}{p}\right) \text{ if } x \neq 0 \text{ and } \varphi_2(0) = 0; \tag{1.2}$$

$$\varphi_3(x) = \frac{S(x, 1; p)}{\sqrt{p}} \text{ if } x \neq 0 \text{ and } \varphi_3(0) = -\frac{1}{\sqrt{p}}; \tag{1.3}$$

$$\varphi_4(x) = \frac{1}{\sqrt{p}}(p - |\{(u, v) \in \mathbf{F}_p^2 \mid v^2 = u(u - 1)(u - x)\}|) \text{ if } x \notin \{0, 1\} \text{ and} \tag{1.4}$$

$$\varphi_4(0) = \varphi_4(1) = \frac{1}{\sqrt{p}};$$

where $f \in \mathbf{Z}[X]$ has degree $m \geq 1$ and is not proportional to the square of another polynomial, $(\frac{\cdot}{p})$ is the Legendre symbol, and $S(a, b; c)$ is a classical Kloosterman sum. Then for $d \geq 1$, we have

$$\begin{aligned} \|\varphi_1\|_{U_d}^{2d} &\leq (5m + 10)^{(d+1)2^d} p^{-1}, \\ \|\varphi_2\|_{U_d}^{2d} &\leq 15^{(d+1)2^d} p^{-1}, \\ \|\varphi_3\|_{U_d}^{2d} &\leq 20^{(d+1)2^d} p^{-1}, \\ \|\varphi_4\|_{U_d}^{2d} &\leq 25^{(d+1)2^d} p^{-1}. \end{aligned}$$

Remark 1.1. In [18, exercise 11.1.17], Tao and Vu note that if φ is a random function, in the sense that the values $\varphi(x)$, for $x \in \mathbf{F}_p$, are independent random variables (on some probability space) with $|\varphi(x)| \leq 1$ for all x and with expectation zero, then we have

$$\mathbf{E}(\|\varphi\|_{U_d}^{2d}) \leq p^{-1},$$

where the implied constant depends only on d . Thus this result gives concrete examples of functions which are as uniform as random functions (note that, by Weil’s bound for Kloosterman sums and by Hasse’s bound for the number of points on elliptic curves over finite fields, we have $|\varphi_3|, |\varphi_4| \leq 2$). We are not aware of previous examples with this property in the literature (though the cases of φ_1 and φ_2 are accessible to techniques based only on the Weil bounds for character sums.)

¹ We thank B. Green for pointing out that this application of our result is of interest in combinatorics

We will explain the proof of this result in Section 4. We now discuss the inverse theorems for general trace functions. We first recall the general setup of these functions (further examples are given in Example 1 and in Section 3).

We fix a prime p and a finite field k of characteristic p . Let $\ell \neq p$ be a prime number. 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 $\iota : \bar{\mathbf{Q}}_\ell \rightarrow \mathbf{C}$ 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 $|\iota(t_{\mathcal{F},k}(x))|^2$.

Given any finite field k and any function $\varphi : k \rightarrow \bar{\mathbf{Q}}_\ell$ or $\varphi : k \rightarrow \mathbf{C}$, we denote

$$U_d(\varphi) = \|\varphi\|_{U_d}^{2d}$$

where $\|\cdot\|_{U^d}$ is the d th uniformity norm, and

$$U_d(\mathcal{F}; k) = U_d(t_{\mathcal{F},k})$$

(in fact, we will call $U_d(\varphi)$ the Gowers d -pnorm of φ – the ‘p’ is silent, as in “ptarmigan” or “Psmith” – to avoid confusion.)

We will work mostly with middle-extension sheaves, in the sense of [12], i.e., constructible sheaves \mathcal{F} on \mathbf{A}^1/k such that, for any dense open set U on which \mathcal{F} is lisse, with open immersion $j : U \hookrightarrow \mathbf{A}^1$, we have

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

Given any constructible sheaf \mathcal{F} , lisse on a dense open set $U \subset \mathbf{A}^1$, with $j : U \hookrightarrow \mathbf{A}^1$ the open immersion, the direct image $j_* \mathcal{F}$ is the unique middle-extension sheaf on \mathbf{A}^1 which is isomorphic to \mathcal{F} on U . In particular \mathcal{F} and $j_* \mathcal{F}$ have the same trace functions on U , but those may differ at the singularities $\mathbf{A}^1 - S$. Thus the middle-extension condition can be seen as ensuring that a lisse sheaf on an open set U of \mathbf{A}^1 is extended “optimally” to all of \mathbf{A}^1 .

As in [13, section 7], a middle-extension sheaf as above is called pointwise pure of weight 0, if $j^* \mathcal{F}$ is pointwise pure of weight 0 on U , and it is called arithmetically irreducible (resp. semisimple, resp. geometrically irreducible, geometrically semisimple) if $j^* \mathcal{F}$ corresponds to an irreducible (resp. semisimple) representation of the fundamental group $\pi_1(U, \bar{\eta})$ (resp. of the geometric fundamental group $\pi_1(U \times \bar{k}, \bar{\eta})$), for some geometric generic point $\bar{\eta}$ of U . By the *semisimplification* of \mathcal{F} , we mean the middle-extension sheaf

$$j_* \mathcal{F}^{ss}$$

where \mathcal{F}^{ss} is the semisimplification of the restriction of \mathcal{F} to U .

Note that

$$t_{\mathcal{F},k} = t_{\mathcal{F}^{ss},k},$$

so that for any question involving the trace function of \mathcal{F} , we may assume that the sheaf is arithmetically semisimple.

We measure the complexity of a sheaf on \mathbf{P}^1 over a finite field by its *conductor*: if \mathcal{F} is such a sheaf, of rank $\text{rank}(\mathcal{F})$ with singularities at $\text{Sing}(\mathcal{F}) \subset \mathbf{P}^1$, we define the (*analytic*) *conductor* of \mathcal{F} to be

$$c(\mathcal{F}) = \text{rank}(\mathcal{F}) + \sum_{x \in \text{Sing}(\mathcal{F})} \max(1, \text{Swan}_x(\mathcal{F})). \tag{1.5}$$

An important subclass of sheaves is that of *tamely ramified* sheaves, which by definition are those where $\text{Swan}_x(\mathcal{F}) = 0$ for all x , so that only the rank and number of singularities appear as measures of complexity.

If \mathcal{F} is a sheaf on $U \subset \mathbf{A}^1 \subset \mathbf{P}^1$, the conductor is defined as that of the direct image to \mathbf{P}^1 (i.e., the Swan conductor at any point $x \in \mathbf{P}^1$ is that of the invariants under inertia at x of the fiber of \mathcal{F} over a generic geometric point.)

We now state a first version of our main structural result (see Theorem 4.1 for a more precise form from which it will be deduced; for technical reasons, we are currently only able to treat fully the case of prime fields $k = \mathbf{Z}/p\mathbf{Z}$, which is the most directly relevant to analytic number theory.)

THEOREM 1.2 (Algebraic structure theorem for Gowers norms). *Let p be a prime and let $\ell \neq p$ be an auxiliary prime. Let $d \geq 1$ be an integer such that $p > d$.*

Let \mathcal{F} be a middle-extension ℓ -adic sheaf on $\mathbf{A}^1/\mathbf{F}_p$ which is pointwise pure of weight 0 and arithmetically semisimple.

Then we can write

$$t_{\mathcal{F}, \mathbf{F}_p} = t_1 + t_2$$

where t_1 and t_2 are themselves trace functions and:

(i) *we have*

$$U_d(t_1) \leq (5 \text{c}(\mathcal{F}))^{(d+1)2^d} p^{-1}; \tag{1.6}$$

(ii) *there exists some non-negative integer $j \leq \text{rank}(\mathcal{F}) \leq \text{c}(\mathcal{F})$, polynomials $P_i \in \mathbf{F}_p[X]$ of degree at most $d - 1$ and coefficients β_i bounded by $\text{rank}(\mathcal{F})$ for $1 \leq i \leq j$, such that*

$$t_2(x) = \sum_{i=1}^j \beta_i e\left(\frac{P_i(x)}{p}\right).$$

Note that the condition $p > d$ is certainly not a problem in this horizontal direction, where p is the main variable and we think of having sheaves \mathcal{F}_p for every p with conductor uniformly bounded as p varies (or even growing not too fast).

The more precise structural results will imply a particularly strong inverse theorem if \mathcal{F} is assumed to be geometrically irreducible (and will also imply Theorem 1.1).

COROLLARY 1.3 (Inverse theorem for irreducible sheaves). *Let p, ℓ and \mathcal{F} be as in the theorem, and assume that \mathcal{F} is geometrically irreducible. For $d < p$, exactly one of the following two possibilities holds:*

(i) *there exists $P \in \mathbf{F}_p[X]$ of degree $\leq d - 1$ and a complex number α of modulus 1 such that*

$$t_{\mathcal{F}, \mathbf{F}_p}(x) = \alpha e\left(\frac{P(x)}{p}\right) \tag{1.7}$$

for all $x \in \mathbf{F}_p$;

(ii) *or we have*

$$U_d(\mathcal{F}; \mathbf{F}_p) \leq (5 \text{c}(\mathcal{F}))^{(d+1)2^d} p^{-1}.$$

Remark 1.2. Geometric irreducibility, for sheaves \mathcal{F} with small conductor, is equivalent with approximate L^2 -normality of the trace function over \mathbf{F}_p , i.e., with the condition

$$\frac{1}{p} \sum_{x \in \mathbf{F}_p} |t_{\mathcal{F}, \mathbf{F}_p}(x)|^2 \approx 1$$

(see [6, lemma 3.5] for a precise statement of orthonormality for trace functions.)

The case of tamely ramified sheaves is also simpler since non-trivial Artin–Schreier sheaves are not tame. In fact, the technical difficulty in extending Theorem 1.2 to all finite fields, and the condition $d < p$, are then removed:

COROLLARY 1.4 (Inverse theorem for tame sheaves). *Let k be a finite field of characteristic p , let $\ell \neq p$ be given and let \mathcal{F} be a tamely ramified ℓ -adic middle-extension sheaf on \mathbf{A}_k^1 which does not geometrically contain the trivial sheaf. For $d \geq 1$, we have*

$$U_d(\mathcal{F}; k) \leq (5 c(\mathcal{F}))^{(d+1)2^d} |k|^{-1}.$$

Remark 1.3. Using the triangle inequality, these results of course extend to “small” linear combinations of trace functions, which include the (centered) characteristic functions of sets with algebraic structure (e.g., values of polynomials, or definable sets in the language of rings [1]). We study in [8] some aspects of the norms on functions over finite fields which arise naturally from this point of view.

A number of authors have proved inverse theorems for Gowers norms of functions over finite fields, the most general version being the one of Tao and Ziegler [20] (see also, without exhaustivity, the paper [10] of Green and Tao, and the earlier paper [19] of Tao and Ziegler; note also that, as shown in [10], and independently discovered by Lovett, Meshulam and Samorodnitsky, there do exist counterexamples in large characteristic to the most naive guess for an inverse theorem.) The focus in these papers is different: they consider arbitrary functions on k^n as n grows, and the finite field k is fixed (in [10], the functions involved are themselves polynomials).

The arguments in all these works are much more delicate than the ones of the present paper, and this applies even more to the article [11] of Green, Tao and Ziegler which establishes an inverse theorem for the Gowers norms on (in effect) $\mathbf{Z}/N\mathbf{Z}$, where the main variable is indeed $N \rightarrow +\infty$. There also, polynomial phases do not give the only obstruction to having small Gowers norms, and more general objects related to nilmanifolds are required.

Our proof relies instead on the formalism of algebraic geometry and on the Riemann Hypothesis over finite fields. Thus this note is another illustration of the great power of Deligne’s results, and of the interest in dealing with trace functions of arbitrary sheaves as objects of interest, and tools, in analytic number theory (a point of view which is already apparent in [5, 6, 7]).

Example 1. Possibly the simplest examples of trace functions modulo p are given by

$$\varphi(x) = e\left(\frac{P(x)}{p}\right)$$

where $P \in \mathbf{Z}[X]$ is a polynomial. In that case, the associated sheaf is a so-called Artin–Schreier sheaf, denoted $\mathcal{L}_{\psi(P)}$ for a suitable additive character ψ , and has rank 1. It is therefore geometrically irreducible. Its conductor is $1 + \deg(P)$, hence our theorem states that,

for $p > \text{deg}(P)$, we have

$$\|\varphi\|_{U_d} \leq (5(1 + \text{deg}(P)))^{d+1} p^{-2^{-d}}$$

for all $d \leq \text{deg}(P)$, where the implied constant depends only on $\text{deg}(P)$ (on the other hand, it is easy to check that $\|\varphi\|_{U_d} = 1$ if $d > \text{deg}(P)$). The reader may check that in this special case, our proof can be expressed using only Weil’s theory of character sums in one variable.

In [18, exercise 11.1.12], Tao and Vu observe that one can prove elementarily the estimates

$$\|\varphi\|_{U_d} \leq \left(\frac{d-1}{p}\right)^{2^{-\text{deg}(P)}}$$

for $1 \leq d \leq \text{deg}(P)$, which is weaker in terms of p , except if $d = \text{deg}(P)$.

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 $C \geq 0$ such that $|f(x)| \leq Cg(x)$ 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 a constructible sheaf \mathcal{F} on \mathbf{A}^1/k , and $h \in k$, we write $[+h]^*\mathcal{F}$ for the pullback of \mathcal{F} under the map $x \mapsto x + h$. If \mathcal{F} is a middle-extension sheaf on \mathbf{A}^1/k , we also write $D(\mathcal{F})$ for the middle-extension dual of \mathcal{F} , i.e., given a dense open set $j : U \hookrightarrow \mathbf{A}^1$ where \mathcal{F} is lisse, we have

$$D(\mathcal{F}) = j_*((j^*\mathcal{F})')$$

where the prime denotes the lisse sheaf of U associated to the contragredient of the representation of the fundamental group of U which corresponds to $j^*\mathcal{F}$ (see [13, 7.3.1]). If \mathcal{F} is pointwise pure of weight 0, it is known that

$$t_{D(\mathcal{F}),k'}(x) = \overline{t_{\mathcal{F},k'}(x)}$$

for all finite extensions k'/k and all $x \in k'$ (this property is obvious for $x \in U(k')$ and the point is that this extends to the singularities when the dual is suitably defined.) Note for instance that $c(D(\mathcal{F})) = c(\mathcal{F})$.

2. Preliminaries

We recall the inductive definition of the Gowers norms, as in [18, definition 11.2] (one can sheafify it for trace functions, i.e., one can see the Gowers norm of $t_{\mathcal{F},k}$ as essentially the sum over $x \in k$ of the trace function of a suitable “Gowers sheaf” $\mathcal{U}_d(\mathcal{F})$; it might in fact be interesting to search for some kind of “motivic” inverse theorem for these Gowers sheaves, but we will not pursue this point of view in this paper).

Definition 1 (Gowers norms). Let k be a finite field and $\varphi : k \rightarrow \mathbf{C}$ an arbitrary function. The U_d -norms of φ are defined inductively for $d \geq 1$ by

$$\|\varphi\|_{U_1}^2 = \frac{1}{|k|^2} \sum_{h \in k} \sum_{x \in k} \varphi(x+h) \overline{\varphi(x)}$$

and

$$\|\varphi\|_{U_{d+1}}^{2^{d+1}} = \frac{1}{|k|} \sum_{h \in k} \|\xi_h(\varphi)\|_{U_d}^{2^d}$$

for $d \geq 1$, where

$$\xi_h(\varphi)(x) = \varphi(x + h)\overline{\varphi(x)}.$$

We wish to apply this recursive definition to trace functions. We first observe the trivial bound: recalling that

$$|t_{\mathcal{F},k}(x)| \leq \text{rank}(\mathcal{F})$$

for all $x \in k$ if \mathcal{F} is a middle-extension sheaf on \mathbf{A}^1/k which is pointwise pure of weight 0, we get:

COROLLARY 2.1. *Let \mathcal{F} be pointwise pure of weight 0 and rank $r \geq 1$. Then for $d \geq 1$, we have*

$$0 \leq U_d(\mathcal{F}; k) \leq r^{2^d} \leq c(\mathcal{F})^{2^d}. \tag{2.1}$$

Now we get a sheaf-theoretic interpretation of the recursive definition of Gowers norms. Given a middle-extension sheaf \mathcal{F} and $h \in k$, the trace function of the constructible sheaf

$$\xi_h(\mathcal{F}) = [+h]^*\mathcal{F} \otimes D(\mathcal{F})$$

coincides with

$$\xi_h(t_{\mathcal{F},k}),$$

“almost everywhere”. Precisely it does at any x which is not a singularity of either $[+h]^*\mathcal{F}$ or $D(\mathcal{F})$ (this is clear if x is a singularity for neither of these, and easy to see when x is a singularity of one of them only). In fact, denoting by S the set of singularities of \mathcal{F} in \mathbf{A}^1 , we have

$$t_{\xi_h(\mathcal{F}),k} = \xi_h(t_{\mathcal{F},k})$$

as functions on k provided

$$h \notin E = \{h \in k^\times \mid S \cap (S - h) \neq \emptyset\},$$

and moreover $\xi_h(\mathcal{F})$ is a middle-extension sheaf on \mathbf{A}^1 for $h \notin E$. Note that

$$|E| \leq |S|(|S| - 1) \leq c(\mathcal{F})(c(\mathcal{F}) - 1)$$

since any $h \in E$ is a difference of two (distinct) elements of S , and hence we get:

LEMMA 2.2. *Let k be a finite field, and let \mathcal{F} be an ℓ -adic middle-extension sheaf on \mathbf{A}^1/k which is pointwise pure of weight 0. Denote*

$$\xi_h(\mathcal{F}) = [+h]^*\mathcal{F} \otimes D(\mathcal{F})$$

for given \mathcal{F} and $h \in k$. Then $\xi_h(\mathcal{F})$ is a constructible sheaf, which is tame if \mathcal{F} is tame. Further, let

$$E = \{h \in k^\times \mid S \cap (S - h) \neq \emptyset\}, \quad \text{where } S = \{\text{singularities of } \mathcal{F}\}.$$

Then each $\xi_h(\mathcal{F})$ with $h \notin E$ is a middle-extension sheaf on \mathbf{A}^1/k , pointwise pure of weight 0, and we have

$$U_{d+1}(\mathcal{F}; k) = \frac{1}{|k|} \sum_{h \in k-E} U_d(\xi_h(\mathcal{F}); k) + \theta \frac{|E| \text{rank}(\mathcal{F})^{2^{d+1}}}{|k|} \tag{2.2}$$

for any $d \geq 1$, where $|\theta| \leq 1$.

Proof. Since it is clear that $\xi_h(\mathcal{F})$ is indeed tame if \mathcal{F} is, the only thing that remains is to justify the error term in (2.2). But if $\varphi = t_{\mathcal{F},k}$, we have a trivial bound

$$\frac{1}{|k|} U_d(\xi_h(\varphi)) \leq \text{rank}(\mathcal{F})^{2 \cdot 2^d} |k|^{-1}$$

for any $h \in k$ (similar to the previous corollary), hence the result.

We now state the essential result that allows us to get optimal bounds, which is a general version of the Riemann Hypothesis, for sums in one variable. The version we use is as follows:

THEOREM 2.3 (Deligne). *Let p be a prime number and \mathcal{F} an ℓ -adic middle-extension sheaf on \mathbf{A}^1/k , pointwise pure of weight 0, such that $H_c^2(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) = 0$. Then we have*

$$\left| \sum_{x \in k} t_{\mathcal{F},k}(x) \right| \leq 2 c(\mathcal{F})^2 \sqrt{|k|}.$$

Proof. By the Grothendieck–Lefschetz trace formula and the Riemann Hypothesis, we have

$$\left| \sum_{x \in k} t_{\mathcal{F},k}(x) \right| \leq \dim H_c^1(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) \sqrt{|k|}$$

since $H_c^0(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) = H_c^2(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) = 0$.

By the Euler–Poincaré formula of Grothendieck–Ogg–Shafarevich (see, e.g., [15, chapter 14]), we also know that, under our assumptions, we have

$$\begin{aligned} \dim H_c^1(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) &= -\chi_c(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) \\ &= \sum_{x \in \text{Sing}(\mathcal{F})} \text{Swan}_x(\mathcal{F}) + \sum_{x \in \text{Sing}(\mathcal{F}) \cap \mathbf{A}^1} (\text{rank}(\mathcal{F}) - \dim \mathcal{F}_x) - \text{rank}(\mathcal{F}) \\ &\leq c(\mathcal{F}) + \text{rank}(\mathcal{F}) |\text{Sing}(\mathcal{F})| \\ &\leq 2c(\mathcal{F})^2 \end{aligned}$$

hence the result.

3. Further examples

In this section, we will simply give a few examples of trace functions of various kinds. The remainder of the proof of Theorem 1.2 is found in Section 5, after a statement of a stronger structural result in Section 4.

Example 2 (Mixed characters). If $U \hookrightarrow \mathbf{A}^1$ is a dense open subset (defined over k), and f_1 (resp. f_2) is a regular function $f_1 : U \rightarrow \mathbf{A}^1$ (resp. a non-zero regular function $f_2 : U \rightarrow \mathbf{G}_m$) 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 $\psi : k \rightarrow \bar{\mathbf{Q}}_\ell^\times$ and multiplicative character $\chi : k^\times \rightarrow \bar{\mathbf{Q}}_\ell^\times$, 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., [2, Sommes trigonométriques (3.5.4)]): if (g_1, g_2) is 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 $d \geq 2$ 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 $\mathbf{P}^1 \rightarrow \mathbf{P}^1$) at x (there is equality if this order is $< |k|$).

In particular, if $f_1 = 0$ and f_2 is not a d th power, then \mathcal{F} is tamely ramified everywhere, geometrically irreducible and non-trivial, so that Corollary 1.4 applies (over arbitrary finite fields).

Example 3 (Families of Kloosterman sums). Deligne proved that, for any p and $\ell \neq p$, and any non-trivial additive character ψ , there exists a middle-extension sheaf $\mathcal{K}\ell$ on $\mathbf{P}^1/\mathbf{F}_p$ which is pointwise pure of weight 0, geometrically irreducible, lisse on \mathbf{G}_m , and satisfies

$$t_{\mathcal{K}\ell,k}(a) = -\frac{1}{\sqrt{|k|}} \sum_{x \in k^\times} \psi(ax + x^{-1})$$

for any finite extension k/\mathbf{F}_p and $a \in k$. This sheaf is of rank 2, tamely ramified at 0 and wildly ramified at ∞ with Swan conductor 1, so that $c(\mathcal{K}\ell) = 2 + 1 + 1 = 4$.

Example 4 (Point-counting functions). The following examples have been studied by Katz [13, example 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 of degree $d < p$. 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 . Then, denoting by

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

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

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

is a 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 $|Z| + \deg(f) - 1$.

In many cases, \mathcal{F}_f is also geometrically irreducible. For instance, this happens when f is *supermorse*, defined to mean that $\deg(f) < p$, that all zeros of df are simple, and that f separates these zeros (i.e., $|S| = |Z|$).

Example 5 (Further formalism). There exists a Fourier transform on middle-extension sheaves 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}_ψ for some additive character ψ . Fix a non-trivial additive character ψ . Then the Fourier transform $\mathcal{G} = \text{FT}_\psi(\mathcal{F})(1/2)$ 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 [13, 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., [5, proposition 7.2], though the definition of conductor is slightly different there).

In particular, applying the Fourier transform to the previous examples, we find many examples of one-parameter families of exponential sums arising as trace functions with bounded conductor, namely

$$x \mapsto -\frac{1}{\sqrt{|k|}} \sum_{y \in (C-D)(k)} e\left(\frac{xf(y)}{p}\right)$$

for the sheaves \mathcal{F}_f , and

$$x \mapsto -\frac{1}{\sqrt{|k|}} \sum_{y \in k} \chi(f_2(y)) \psi(f_1(y) + xy)$$

for Artin–Schreier–Kummer sheaves (for instance, the Kloosterman sums $\mathcal{K}\ell$ of Example 3 can be seen as the Fourier transform of the Artin–Schreier sheaf $\mathcal{L}_{\psi(x^{-1})}$.)

4. Refined structural results

We will deduce Theorem 1.2 from the following result which gives stronger structural information concerning the Gowers norms of trace functions of middle-extension sheaves.

THEOREM 4.1 (Structure theorem for Gowers norms, II). *Let p be a prime and let $\ell \neq p$ be an auxiliary prime. Let $d \geq 1$ be an integer such that $p > d$.*

Let \mathcal{F} be a middle-extension ℓ -adic sheaf on $\mathbf{A}^1/\mathbf{F}_p$ which is pointwise pure of weight 0 and arithmetically semisimple. Then one of the following two conditions holds:

- (i) *there exists an additive character ψ of \mathbf{F}_p , possibly trivial, and a polynomial $P \in \mathbf{F}_p[X]$ of degree at most $d - 1$ such that \mathcal{F} geometrically contains the Artin–Schreier sheaf $\mathcal{L}_{\psi(P)}$;*

(ii) or else we have

$$U_d(\mathcal{F}; \mathbf{F}_p) \leq (5 c(\mathcal{F}))^{(d+1)2^d} p^{-1}. \tag{4.1}$$

In this section, before proving this result, we check that it implies all our previous statements.

Proof of Theorem 1.2. Let \mathcal{F} satisfy the assumptions of Theorem 1.2. Since it is arithmetically semisimple, we can write

$$\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_2,$$

where \mathcal{F}_2 is the sum of all irreducible components of \mathcal{F} which are geometrically isomorphic to an Artin–Schreier sheaf $\mathcal{L}_{\psi(P)}$ for some polynomial P of degree $\leq d - 1$. We then have

$$t_{\mathcal{F}, \mathbf{F}_p} = t_1 + t_2, \text{ with } t_i = t_{\mathcal{F}_i, \mathbf{F}_p}.$$

Now we apply Theorem 4.1 to \mathcal{F}_1 and \mathcal{F}_2 separately. By construction, the first part of the dichotomy can not hold for \mathcal{F}_1 , and hence we get the desired estimate

$$U_d(t_1) = U_d(\mathcal{F}_1; \mathbf{F}_p) \leq (5 c(\mathcal{F}))^{(d+1)2^d} p^{-1},$$

by (4.1).

Now for t_2 , we write \mathcal{F}_2 as a direct sum of geometrically isotypic components, which are all of the form $\mathcal{F}_{\psi(P_i)}$ for some $P_i \in \mathbf{F}_p[X]$ of degree $\leq d - 1$. There are at most $\text{rank}(\mathcal{F})$ such components, and the trace function for each of them is of the form

$$x \mapsto \beta_i \psi(P_i(x)),$$

where β_i is the sum of the twisting factors α of all the arithmetic subsheaves of \mathcal{F}_2 which are geometrically isomorphic to $\mathcal{L}_{\psi(P_i)}$. Since \mathcal{F}_2 is pointwise pure of weight 0, each α is (under ι) of modulus 1, and hence $|\beta_i| \leq \text{rank}(\mathcal{F})$. Thus t_2 is of the form claimed in Theorem 1.2.

It is also clear that Theorem 4.1 implies Corollary 1.3, since if \mathcal{F} is geometrically irreducible, the only possibility for the first case of the dichotomy is that \mathcal{F} be geometrically isomorphic to a sheaf $\mathcal{L}_{\psi(P)}$ with $\text{deg}(P) \leq d - 1$, which immediately implies (1.7).

As for Corollary 1.4, it follows for $d < p$ and $k = \mathbf{F}_p$ because if \mathcal{F} is tamely ramified, the only Artin–Schreier sheaf it may geometrically contain is the trivial sheaf. The general case of Corollary 1.4 follows by inspection of the following argument (we will make remarks indicating the relevant points).

Finally, we explain how this structure result implies Theorem 1.1; this will show that many more explicit functions with small Gowers norms can be constructed from the examples in Section 3.

Proof of Theorem 1.1. We note first that because of Corollary 2.1, we can assume that $d < p$ for the functions $\varphi_1, \varphi_2, \varphi_3$ and φ_4 (the respective ranks of the sheaves will be 1, 1, 2, 2), the bounds being trivial for $d \geq p$.

(1) The function φ_1 arises as the case of Example 2 for U the affine line itself, χ the Legendre character modulo p , $f_1 = 0$ and $f_2 = f$. The corresponding sheaf \mathcal{F}_1 has rank 1 so is necessarily geometrically irreducible. It is tame and not geometrically trivial if f is not proportional to the square of another polynomial, and the singularities are ∞ and the zeros of f , so the conductor of \mathcal{F}_1 is at most $2 + m$. Hence the first alternative of Theorem 4.1 can not hold (alternatively, we can apply Corollary 1.3 here, since the sheaf is tame).

(2) The function φ_2 is the case of Example 2 for $U = \mathbf{A}^1 - \{0\}$, $\chi = 1$, $f_1(x) = x^{-1}$. The corresponding sheaf \mathcal{F}_2 is of rank 1 so geometrically irreducible. It is tamely ramified at ∞ and wildly ramified with Swan conductor 1 at 0, so the conductor is 3. The classification of Artin–Schreier sheaves shows that the first alternative of Theorem 4.1 does not hold, so we obtain the desired bound.

(3) The function $-\varphi_3$ is Example 3, where it is explained that the conductor is 4. The Kloosterman sheaf is geometrically irreducible (for instance, because it is the sheaf-theoretic Fourier transform of the previous sheaf \mathcal{F}_2 , and the Fourier transform sends geometrically irreducible sheaves to irreducibles sheaves.) Since it is of rank 2, the first alternative of Theorem 4.1 is also impossible here, and we get the stated estimate.

(4) Let

$$\mathcal{E} : v^2 = u(u - 1)(u - x)$$

denote the Legendre family of elliptic curves over \mathbf{F}_p , viewed as an affine algebraic surface over $\mathbf{A}^1 - \{0, 1\}$ by the projection

$$\pi : \begin{cases} \mathcal{E} \longrightarrow \mathbf{A}^1 - \{0, 1\} \\ (u, v, x) \longmapsto x. \end{cases}$$

The function φ_4 arises from the middle-extension to \mathbf{P}^1 of the sheaf $\mathcal{F}_4 = R^1\pi_!\bar{\mathbf{Q}}_\ell(1/2)$. This is a tame geometrically irreducible sheaf of rank 2, ramified at $\{0, 1, \infty\}$, so the conductor is 5 and we obtain the result as before.

5. Proof of the inverse theorem

We will now prove Theorem 4.1. As can be expected, the argument is by induction on d , and the base case $d = 1$ is an easy consequence of the Riemann Hypothesis, for any finite field:

PROPOSITION 5.1 (Inverse theorem for $d = 1$). *Let k be a finite field and let \mathcal{F} be a middle-extension sheaf on \mathbf{A}^1/k which is pointwise pure of weight 0. If $\mathcal{F} \otimes \bar{k}$ does not contain a trivial subsheaf, then we have*

$$U_1(\mathcal{F}; k) \leq 4c(\mathcal{F})^4|k|^{-1}. \tag{5.1}$$

Proof. We have by definition

$$\begin{aligned} U_1(\mathcal{F}; k) &= \frac{1}{|k|^2} \sum_{(h,x) \in k^2} t_{\mathcal{F},k}(x+h) \overline{t_{\mathcal{F},k}(x)} \\ &= \left| \frac{1}{|k|} \sum_{x \in k} t_{\mathcal{F},k}(x) \right|^2, \end{aligned}$$

and hence the estimate (5.1) follows immediately from Theorem 2.3, unless

$$H_c^2(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) \neq 0.$$

But, if \mathcal{F} is lisse on the dense open subset U of \mathbf{A}^1 , we have

$$H_c^2(\mathbf{A}^1 \times \bar{k}, \mathcal{F}) = H_c^2(U \times \bar{k}, \mathcal{F}) = (\mathcal{F}_{\bar{\eta}})_{\pi_1(U \times \bar{k}, \bar{\eta})}(-1)$$

by birational invariance and the coinvariant formula for the topmost cohomology of a lisse sheaf. Since \mathcal{F} is pointwise pure of weight 0 on U , it corresponds to a representation of $\pi_1(U \times \bar{k}, \bar{\eta})$ which is geometrically semisimple (by results of Deligne [3]), and therefore

$$(\mathcal{F}_{\bar{\eta}})_{\pi_1(U \times \bar{k}, \bar{\eta})} \neq 0$$

implies that \mathcal{F} contains a trivial summand.

We will now deal with U_d -pnorms, $d \geq 2$, using an induction on d based on (2.2). Precisely, consider the following statement, for a given integer $d \geq 1$:

Inverse(d). For any prime p with $p > d$, for any $\ell \neq p$, for any middle extension ℓ -adic sheaf \mathcal{F} on $\mathbb{A}^1/\mathbb{F}_p$, pointwise pure of weight 0 and arithmetically semisimple, either there exists an additive character ψ of \mathbb{F}_p , possibly trivial, and a polynomial $P \in \mathbb{F}_p[X]$ of degree at most $d - 1$ such that \mathcal{F} contains geometrically a summand isomorphic to $\mathcal{L}_{\psi(P)}$, or else we have

$$U_d(\mathcal{F}; \mathbb{F}_p) \leq (5 c(\mathcal{F}))^{(d+1)2^d} p^{-1}.$$

Note that Proposition 5.1 implies that **Inverse(1)** is valid, and that Theorem 4.1 simply states that **Inverse(d)** holds for all $d \geq 1$. Hence we will be done by induction once we show:

PROPOSITION 5.2 (Induction step). Let $d \geq 1$ be such that **Inverse(d)** holds. Then so does **Inverse(d + 1)**.

For the proof of Proposition 5.2, we will use two lemmas. Before stating the first, we introduce some terminology. Given a finite field k and an open dense subset U/k of \mathbb{A}^1/k , a lisse sheaf \mathcal{F} on U is called *induced* if it is arithmetically irreducible, and the corresponding representation of $\pi_1(U, \bar{\eta})$ is isomorphic to an induced representation $\text{Ind}_H^{\pi_1(U, \bar{\eta})} \varrho_0$, for some proper normal finite-index subgroup H of $\pi_1(U, \bar{\eta})$ containing $\pi_1(U \times \bar{k}, \bar{\eta})$ and some irreducible representation ϱ_0 . We need the following corollary of elementary representation theory: if \mathcal{F} is arithmetically irreducible on U , and is not induced, then it is geometrically isotypic.

LEMMA 5.3. Let k be a finite field of characteristic p , and let \mathcal{F} be a middle-extension ℓ -adic sheaf on \mathbb{A}^1/k , which is arithmetically irreducible and lisse on some dense open set $U \hookrightarrow \mathbb{A}^1$.

(1) Either the sheaf \mathcal{F} is geometrically isotypic on U , or its trace function is identically zero on $U(k)$.

(2) Suppose that \mathcal{F} is geometrically isotypic, and let ϱ denote the geometrically irreducible representation of $\pi_1(\bar{U}, \bar{\eta})$ which corresponds to the isotypic component of \mathcal{F} . Suppose further that, for some $h \in k$, some polynomial $P \in k[X]$ and ℓ -adic character ψ , we have a geometric summand

$$\mathcal{L}_{\psi(P)} \hookrightarrow [+h]^* \mathcal{F} \otimes D(\mathcal{F})$$

on U . Then we have a geometric isomorphism

$$[+h]^* \mathcal{F} \simeq \mathcal{F} \otimes \mathcal{L}_{\psi(P)}.$$

Proof. (1) follows from the remark before the statement: if \mathcal{F} is not geometrically isotypic, then it is induced so that, on U , the corresponding representation ϱ is given by

$$\varrho \simeq \text{Ind}_H^{\pi_1(U, \bar{\eta})} \varrho_0.$$

It is however elementary that, in this situation, the character of ϱ is identically zero on the non-trivial cosets of H , and all Frobenius $\text{Fr}_{x,k}$ corresponding to $x \in U(k)$ have this property since we have

$$H = \{g \in \pi_1(U, \bar{\eta}) \mid \text{deg}(g) \equiv 0 \pmod{m}\}$$

for some $m \geq 2$, where deg is the degree which gives an isomorphism

$$\text{deg} : \pi_1(U, \bar{\eta})/\pi_1(U \times \bar{k}, \bar{\eta}) \longrightarrow \hat{\mathbf{Z}},$$

and since $\text{deg}(\text{Fr}_{x,k}) = -1$ for all $x \in U(k)$.

(2) We have a geometric isomorphism $\mathcal{F} \simeq n\varrho$ on U , for some $n \geq 1$. Then the assumption gives

$$\mathcal{L}_{\psi(P)} \hookrightarrow [+h]^*\mathcal{F} \otimes D(\mathcal{F}) \simeq n^2([+h]^*\varrho \otimes \varrho'),$$

on U , and since the right-hand side is isotypic and the left-hand side irreducible, we derive the existence of a geometric injection

$$\mathcal{L}_{\psi(P)} \hookrightarrow [+h]^*\varrho \otimes \varrho',$$

and therefore of a geometric isomorphism

$$[+h]^*\varrho \simeq \varrho \otimes \mathcal{L}_{\psi(P)},$$

and hence

$$[+h]^*\mathcal{F} \simeq \mathcal{F} \otimes \mathcal{L}_{\psi(P)}$$

by taking copies of this, first on U , and then on \mathbf{A}^1 because the sheaves involved are middle-extensions.

The next lemma gives some properties of lisse sheaves on $\mathbf{A}_{\mathbf{F}_p}^1$ which are (geometrically) “almost” invariant under some non-trivial translations. It complements certain results of [5] (where the invariance under homographies in PGL_2 acting on the projective line is a crucial issue, and where only the base field $k = \mathbf{F}_p$ is considered.) This is also where the restriction to $k = \mathbf{F}_p$ occurs; roughly speaking, to extend Theorem 1.2 to any finite field of characteristic p , we would need a similar statement as the second part of this lemma to be valid when G is an arbitrary finite subgroup of $\bar{\mathbf{F}}_p$. However, if \mathcal{F} is tame, the statement is vacuously true (with no assumption on d in (2)), simply because there is no non-trivial tame sheaf which is lisse on \mathbf{A}^1 .

LEMMA 5.4. *Let \bar{k} be an algebraic closure of \mathbf{F}_p , $\ell \neq p$ an auxiliary prime. Let \mathcal{F} be a lisse ℓ -adic sheaf on \mathbf{A}^1/\bar{k} such that \mathcal{F} is irreducible and non-trivial.*

(1) *We have $\text{Swan}_\infty(\mathcal{F}) \geq \text{rank}(\mathcal{F})$, with equality if and only if \mathcal{F} is isomorphic to \mathcal{L}_ψ for some non-trivial ℓ -adic additive character.*

(2) *Let $d < p - 1$ be given. Suppose there exists a cyclic subgroup $G \subset \bar{k}$ of order p such that we have isomorphisms*

$$[+h]^*\mathcal{F} \simeq \mathcal{F} \otimes \mathcal{L}_{\psi(P_h)} \tag{5.2}$$

on \mathbf{A}^1 for all $h \in G$, where $P_h \in \bar{k}[X]$ has degree $\leq d$. Then \mathcal{F} is either isomorphic to $\mathcal{L}_{\psi(Q)}$ for some non-trivial additive character ψ and polynomial Q of degree $\leq d + 1$, or it satisfies

$$\text{Swan}_\infty(\mathcal{F}) \geq p + \text{rank}(\mathcal{F}).$$

Proof. (1) Since the geometric fundamental group of \mathbf{A}^1 is topologically generated by the inertia subgroups and \mathcal{F} is lisse on \mathbf{A}^1 , we see first that \mathcal{F} is irreducible as representation of the inertia group $I(\infty)$ at ∞ .

Since \mathcal{F} is lisse on \mathbf{A}^1 and non-trivial, we have $H_c^0(\mathbf{A}^1, \mathcal{F}) = H_c^2(\mathbf{A}^1, \mathcal{F}) = 0$, and by the Euler–Poincaré formula, we get

$$\dim H_c^1(\mathbf{A}^1, \mathcal{F}) = -\chi_c(\mathbf{A}^1, \mathcal{F}) = \text{Swan}_\infty(\mathcal{F}) - \text{rank}(\mathcal{F}),$$

since the Euler–Poincaré characteristic of \mathbf{A}^1 is 1. Now, the left-hand side is a non-negative integer, and we therefore deduce

$$\text{Swan}_\infty(\mathcal{F}) \geq \text{rank}(\mathcal{F}),$$

which is the first claim.

Now suppose there is equality. Since \mathcal{F} is irreducible as an $I(\infty)$ representation, it has a unique break λ at ∞ such that $\text{Swan}_\infty(\mathcal{F}) = \lambda \text{rank}(\mathcal{F})$. We therefore have equality if and only if $\lambda = 1$.

We can now apply the “break-lowering lemma” in [12, theorem 8.5.7] (it is applicable because \mathcal{F} is already $I(\infty)$ -irreducible). This shows that there exists a non-trivial additive ℓ -adic character ψ of k such that $\mathcal{G} = \mathcal{F} \otimes \mathcal{L}_{\psi(X)}$ has all breaks < 1 . But \mathcal{G} is lisse on \mathbf{A}^1 and still irreducible as $I(\infty)$ representation. We claim that \mathcal{G} is (geometrically) trivial. Indeed, otherwise the inequality above would be applicable to \mathcal{G} and would give

$$\text{rank}(\mathcal{F}) = \text{rank}(\mathcal{G}) \leq \text{Swan}_\infty(\mathcal{G}) < \text{Swan}_\infty(\mathcal{F}),$$

which is a contradiction. Hence \mathcal{G} is geometrically trivial, and we get a geometric isomorphism $\mathcal{F} \simeq \mathcal{L}_{\bar{\psi}}$.

(An alternative proof of the equality case goes as follows: if \mathcal{F} were not of this form, it would be a Fourier sheaf in the sense of [13, section 7.3.5]; since it is lisse on \mathbf{A}^1 with all breaks at ∞ larger than 1, denoting by \mathcal{G} its Fourier transform, the latter would be lisse at 0 by [13, lemma 7.3.9 (3)] and we would get

$$\text{Swan}_\infty(\mathcal{F}) = \text{rank}(\mathcal{F}) + \text{rank}(\mathcal{G}) > \text{rank}(\mathcal{F}),$$

by [13, lemma 7.3.9, (2)], since \mathcal{G} is also irreducible by [13, theorem 7.3.8 (3)], hence has non-zero rank.)

(2) The finite subgroup $G \subset \bar{k}$ is cyclic, hence generated by some $0 \neq h \in \bar{k}$. Since $d < p - 1$, we can find a polynomial $Q \in \bar{k}[X]$ of degree $\leq d + 1$ such that

$$Q(X + h) - Q(X) = P_h.$$

We now form the sheaf $\mathcal{F}_1 = \mathcal{F} \otimes \mathcal{L}_{\psi(Q)}$. It is lisse on \mathbf{A}^1 , and we have

$$[+x]^* \mathcal{F}_1 \simeq \mathcal{F}_1$$

for any $x \in G = \mathbf{F}_p h$. Denoting

$$\phi : \mathbf{A}^1 \longrightarrow \mathbf{A}^1/G \simeq \mathbf{A}^1$$

the quotient map for the action of G on \mathbf{A}^1 , the fact that G is cyclic of order p implies that there exists a sheaf \mathcal{F}_2 on \mathbf{A}^1/G such that

$$\mathcal{F}_1 \simeq \phi^*(\mathcal{F}_2).$$

We then use the invariance of Swan conductors under pushforward for virtual representations of degree 0 (see references in [14, p. 286, line 3]), i.e., the formula

$$\text{Swan}_\infty(\phi^*\mathcal{F}_2 - \text{rank}(\mathcal{F}_2)\bar{\mathcal{Q}}_\ell) = \text{Swan}_\infty(\phi_*(\phi^*\mathcal{F}_2 - \text{rank}(\mathcal{F}_2)\bar{\mathcal{Q}}_\ell)),$$

where $-$ refers to the Grothendieck ring of lisse sheaves on \mathbf{A}^1 . The left-hand side is equal to

$$\text{Swan}_\infty(\phi^*\mathcal{F}_2) = \text{Swan}_\infty(\mathcal{F}_1),$$

while the right-hand side is equal to

$$\begin{aligned} \text{Swan}_\infty(\phi_*(\phi^*\mathcal{F}_2 - \text{rank}(\mathcal{F}_2)\bar{\mathcal{Q}}_\ell)) &= \sum_{\eta \in \hat{G}} (\text{Swan}_\infty(\mathcal{F}_2 \otimes \mathcal{L}_\eta) - \text{rank}(\mathcal{F}_2) \text{Swan}_\infty(\mathcal{L}_\eta)) \\ &= \sum_{\eta \in \hat{G}} (\text{Swan}_\infty(\mathcal{F}_2 \otimes \mathcal{L}_\eta) - \text{rank}(\mathcal{F}_2)) + \text{rank}(\mathcal{F}_2), \end{aligned} \tag{5.3}$$

where η runs over ℓ -adic characters of G , and the \mathcal{L}_η are the corresponding lisse sheaves on \mathbf{A}^1 .

Since \mathcal{F} is irreducible, so is \mathcal{F}_2 , and the twists $\mathcal{F}_2 \otimes \mathcal{L}_\eta$ in the sum. If one term in this sum is zero, we get

$$\text{Swan}_\infty(\mathcal{F}_2 \otimes \mathcal{L}_\eta) = \text{rank}(\mathcal{F}_2 \otimes \mathcal{L}_\eta)$$

and therefore, by the equality case of (1), we have

$$\mathcal{F}_2 \simeq \mathcal{L}_{\bar{\eta}} \otimes \mathcal{L}_{\psi'}$$

for some additive character ψ' . Pulling back under ϕ , it follows that \mathcal{F}_1 is also an Artin-Scheier sheaf $\mathcal{L}_{\psi(aX)}$ for some a , and hence

$$\mathcal{F} \simeq \mathcal{L}_{\psi(aX)} \otimes \mathcal{L}_{\psi(-Q)}$$

in that case.

On the other hand, if none of the terms in the sum vanishes, we get

$$\text{Swan}_\infty(\mathcal{F}_1) = \text{Swan}_\infty(\phi^*\mathcal{F}_2) \geq p + \text{rank}(\mathcal{F}_1).$$

In particular, by assumption, this is $> d$, and hence

$$\text{Swan}_\infty(\mathcal{F}) = \text{Swan}_\infty(\mathcal{F}_1 \otimes \mathcal{L}_{\psi(-Q)}) = \text{Swan}_\infty(\mathcal{F}_1) \geq p + \text{rank}(\mathcal{F}).$$

The final lemma gives an upper-bound for the conductor of $\xi_h(\mathcal{F})$.

LEMMA 5.5. *Let \mathcal{F} be a middle-extension sheaf on $\mathbf{A}^1/\bar{\mathbf{F}}_p$ and $h \in \bar{\mathbf{F}}_p$ such that the set of singularities of \mathcal{F} and $[+h]^*\mathcal{F}$ in \mathbf{A}^1 are distinct. Then the conductor of $\xi_h(\mathcal{F})$ satisfies*

$$c(\xi_h(\mathcal{F})) \leq 5c(\mathcal{F})^2.$$

Proof. Indeed, since the singularities are disjoint, we have

$$c(\xi_h(\mathcal{F}) \leq \text{rank}(\mathcal{F})^2 + 2 \text{rank}(\mathcal{F}) \sum_{x \in S} \text{Swan}_x(\mathcal{F}) + \text{Swan}_\infty(\xi_h(\mathcal{F})).$$

But from known properties of Swan conductors [4, (3.2)], we have

$$\text{Swan}_\infty(\xi_h(\mathcal{F})) \leq \text{rank}(\mathcal{F}) \text{Swan}_\infty([+h]^* \mathcal{F}) + \text{rank}(\mathcal{F}) \text{Swan}_\infty(D(\mathcal{F})) \leq 2c(\mathcal{F})^2,$$

hence the result.

We are now able to conclude the inductive proof of the inverse theorem. The reader is encouraged to check the tame case, for an arbitrary finite field and with no assumption on d compared with the characteristic p .

Proof of Proposition 5.2. We start with the data for a case of **Inverse**($d + 1$): p is a prime number $> d + 1$, \mathcal{F} is a middle-extension sheaf of weight 0 on $\mathbf{A}^1/\mathbf{F}_p$ which is pointwise pure of weight 0 and arithmetically semisimple. We will show that one of the two conditions in **Inverse**($d + 1$) holds. For notational simplicity, we write $c = c(\mathcal{F})$ and $S = \text{Sing}(\mathcal{F}) \cap \mathbf{A}^1$.

Let U/\mathbf{F}_p be the complement of the singularities S of \mathcal{F} in $\mathbf{A}^1/\mathbf{F}_p$, so that \mathcal{F} is lisse on U/\mathbf{F}_p . Let

$$\mathcal{F} = \bigoplus_{1 \leq i \leq r} \mathcal{F}_i$$

be a decomposition of \mathcal{F} into direct sum of arithmetically irreducible middle-extension sheaves. Note that $r \leq \text{rank}(\mathcal{F}) \leq c$ and each \mathcal{F}_i also has conductor $\leq c$, and hence we have

$$U_{d+1}(\mathcal{F}; \mathbf{F}_p) \leq c^{2^{d+1}} \sum_{i=1}^r U_{d+1}(\mathcal{F}_i; \mathbf{F}_p). \tag{5.4}$$

We now consider a fixed i , and the arithmetically irreducible sheaf \mathcal{F}_i . If \mathcal{F}_i is induced, its trace function is zero on U , and is bounded by $\text{rank}(\mathcal{F}_i) \leq c$ on the complement, which contains at most c points, so that a trivial estimate gives

$$U_{d+1}(\mathcal{F}_i; \mathbf{F}_p) \leq \frac{c^{1+2^{d+1}}}{p}. \tag{5.5}$$

Now we assume that \mathcal{F}_i is not induced. By Lemma 2.2, noting that the singularities of \mathcal{F}_i are among those of \mathcal{F} , we have the inductive formula

$$U_{d+1}(\mathcal{F}_i; \mathbf{F}_p) = \frac{1}{p} \sum_{h \in \mathbf{F}_p - E} U_d(\xi_h(\mathcal{F}_i); \mathbf{F}_p) + \theta \frac{c^{2+2^{d+1}}}{p} \tag{5.6}$$

with $|\theta| \leq 1$, where

$$E = \{h \in \mathbf{F}_p^\times \mid S \cap (S - h) \neq \emptyset\}.$$

Each term in the sum can be trivially bounded by

$$\frac{1}{p} U_d(\xi_h(\mathcal{F}_i); \mathbf{F}_p) \leq \text{rank}(\xi_h(\mathcal{F}_i))^{2^d} p^{-1} = \text{rank}(\mathcal{F}_i)^{2 \cdot 2^d} p^{-1} \leq c^{2^{d+1}} p^{-1} \tag{5.7}$$

(which we can therefore use for some exceptional h , provided their number is not too large in terms of c).

Furthermore, we know that for each $h \in \mathbf{F}_p^\times - E$, the sheaf $\xi_h(\mathcal{F}_i)$ is a middle-extension sheaf, lisse on $U_h = U \cap (U - h)$ and pointwise pure of weight 0. By Lemma 5.5, its conductor is $\leq 5c^2$.

We can therefore apply the induction assumption **Inverse**(d). We obtain the bound

$$U_d(\xi_h(\mathcal{F}_i); \mathbf{F}_p) \leq (5c(\xi_h \mathcal{F}_i))^{(d+1)2^d} p^{-1} \leq (5c)^{(d+1)2^{d+1}} p^{-1}, \tag{5.8}$$

for all those $h \in \mathbf{F}_p^\times - E$ such that there does *not* exist some $P_h \in \mathbf{F}_p[X]$ with $\deg(P_h) \leq d - 1$ with a geometric embedding

$$\mathcal{L}_{\psi(P)} \hookrightarrow \xi_h(\mathcal{F}_i) = [+h]^* \mathcal{F}_i \otimes D(\mathcal{F}_i).$$

We denote by $F_i \subset \mathbf{F}_p - E$ the set of exceptional h for which this last property holds (including $h = 0$). By Lemma 5.3, (2), if $h \in F_i$, we have a geometric isomorphism

$$[+h]^* \mathcal{F}_i \simeq \mathcal{F}_i \otimes \mathcal{L}_{\psi(P_h)}$$

for some polynomial P_h of degree $\leq d - 1$, and hence

$$F_i \subset G = \{h \in \mathbf{F}_p \mid [+h]^* \mathcal{F}_i \text{ is geometrically isomorphic to } \mathcal{F}_i \otimes \mathcal{L}_{\psi(P)} \text{ for some } P \text{ of degree } \leq d - 1\}.$$

This subset G is an additive subgroup of \mathbf{F}_p , hence either trivial or equal to \mathbf{F}_p . In the former case, we are done. Otherwise, we first note that if \mathcal{F}_i has a singularity $a \in \mathbf{A}^1$, all elements in its orbit under the action of G are also singularities, i.e., $|G| \leq c$. We can apply (5.7) for all $h \in G$, getting a contribution

$$\leq |G|c^{2^{d+1}} p^{-1} \leq c^{1+2^{d+1}} p^{-1} \tag{5.9}$$

for these terms.

The other possibility is that \mathcal{F}_i is lisse on \mathbf{A}^1 . We can then apply Lemma 5.4, (2) (to the geometrically irreducible component of the arithmetically irreducible but non-induced sheaf \mathcal{F}_i) and two possibilities arise: either \mathcal{F}_i is geometrically isomorphic to a direct sum of copies of $\mathcal{L}_{\psi(Q)}$ for some polynomial Q of degree $\leq d$, or otherwise we have

$$c \geq \text{Swan}_\infty(\mathcal{F}_i) \geq |G| = p,$$

in which case we also get the bound (5.9) for this contribution.

Combining (5.4), (5.5), (5.9) and the average of the inductive bounds (5.8), we get

$$U_{d+1}(\mathcal{F}; \mathbf{F}_p) \leq Ap^{-1},$$

where

$$A = c^{2^{d+1}} \left\{ c^{1+2^{d+1}} + c^{2+2^{d+1}} + (5c)^{(d+1)2^{d+1}} \right\},$$

and in order to finish the induction, we must check that $A \leq (5c)^{(d+2)2^{d+1}}$, for $d \geq 1$, which is easily done, e.g., using the bound

$$c^{2^{d+1}} \times \left\{ c^{1+2^{d+1}} + c^{2+2^{d+1}} \right\} \leq 2c^{(d+2)2^{d+1}}.$$

Acknowledgements. Thanks to R. Pink for help with questions concerning ℓ -adic cohomology, and to J. Wolf for interesting discussions concerning Gowers norms. Thanks to F. Jouve for his remarks and comments concerning the manuscript, and thanks also to B. Green for suggesting the inclusion of a concrete statement like Theorem 1.1.

REFERENCES

- [1] Z. CHATZIDAKIS, L. VAN DEN DRIES and A. MACINTYRE. Definable sets over finite fields. *J. Reine Angew. Math.* **427** (1992), 107–135.
- [2] P. DELIGNE. Cohomologie étale, S.G.A 4 $\frac{1}{2}$. *Lecture Notes in Math.* **569** (Springer Verlag, 1977).
- [3] P. DELIGNE. La conjecture de Weil, II. *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252.
- [4] 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; arXiv:1208.0128v3.
- [5] É. FOUVRY, E. KOWALSKI and PH. MICHEL. Algebraic twists of modular forms and Hecke orbits. preprint (2012); arXiv:1210.0617v4.
- [6] É. FOUVRY, E. KOWALSKI and PH. MICHEL. Counting sheaves using spherical codes, preprint (2012); arXiv:1210.0851v2.
- [7] É. FOUVRY, E. KOWALSKI and PH. MICHEL. Algebraic trace functions over the primes, preprint (2012); arXiv:1211.6043v1.
- [8] É. FOUVRY, E. KOWALSKI and PH. MICHEL. Trace norms over finite fields, in preparation.
- [9] É. FOUVRY, P. MICHEL, J. RIVAT and A. SÁRKÖZY. On the pseudorandomness of the signs of Kloosterman sums. *J. Australian Math. Soc.* **77** (December 2004), 425–436.
- [10] B. J. GREEN and T. TAO. The distribution of polynomials over finite fields, with applications to the Gowers norms. *Contrib. Discr. Math.* **4** (2009), 1–36; arXiv:0711.3191.
- [11] B. J. GREEN, T. TAO and T. ZIEGLER. An inverse theorem for the Gowers $U^{s+1}[N]$ -norm. *Annals of Math.* **176** (2012), 1231–1372; arXiv:1009.3998.
- [12] N. M. KATZ. Gauss sums, Kloosterman sums and monodromy groups. *Annals of Math. Studies* **116** (Princeton University Press, 1988).
- [13] N. M. KATZ. Exponential sums and differential equations. *Annals of Math. Studies* **124** (Princeton University Press, 1990).
- [14] N. M. KATZ. Moments, monodromy and perversity. *Annals of Math. Studies* **159** (Princeton University Press, 2005).
- [15] N. M. KATZ. Convolution and equidistribution: Sato–Tate theorems for finite-field Mellin transforms. *Annals of Math. Studies* **180** (Princeton University Press, 2011).
- [16] H. LIU. Gowers uniformity norm and pseudorandom measures of the pseudorandom binary sequences. *Internat. J. Number Theory* **7** (2005), 1279–1302.
- [17] H. NIEDERREITER and J. RIVAT. On the Gowers norms of pseudorandom binary sequences. *Bull. Aust. Math. Soc.* **79** (2009), 259–271.
- [18] T. TAO and V. VU. Additive Combinatorics. *Cambridge Studies in Advanced Math.* **105** (Cambridge University Press, 2006).
- [19] T. TAO and T. ZIEGLER. The inverse conjecture for the Gowers norm over finite fields via the correspondence principle. *Anal. PDE* **3** (2010), 1–20; arXiv:0810.5527.
- [20] T. TAO and T. ZIEGLER. The inverse conjecture for the Gowers norm over finite fields in low characteristics. *Ann. Comb.* **16** (2012), 121–188; arXiv:1101.1469.