GEOMETRIC NON-VANISHING

DOUGLAS ULMER

Abstract. We consider L-functions attached to representations of the Galois group of the function field of a curve over a finite field. Under mild tameness hypotheses, we prove non-vanishing results for twists of these L-functions by characters of order prime to the characteristic of the ground field and more generally by certain representations with solvable image. We also allow local restrictions on the twisting representation at finitely many places. Our methods are geometric, and include the Riemann-Roch theorem, the cohomological interpretation of L-functions, and monodromy calculations of Katz. As an application, we prove a result which allows one to deduce the conjecture of Birch and Swinnerton-Dyer for non-isotrivial elliptic curves over function fields whose L-function vanishes to order at most 1 from a suitable Gross-Zagier formula.

1. Introduction

Non-vanishing results have long played an important role in the application of L-functions to arithmetic, beginning with Dirichlet's 1837 proof of the infinitude of primes in an arithmetic progression. The area remains active and there is a vast literature. We refer to [BFH96], [MM97], [Gol00], and their bibliographies for an overview of some recent work in the area.

Over number fields, one typically considers *automorphic* L-functions, since only these are known to have good analytic properties. Here, proofs of non-vanishing results necessarily use automorphic methods such as modular symbols, Fourier coefficients of half-integral weight forms, metaplectic Eisenstein series, or average value computations based on character sum estimates. Over function fields, similar automorphic ideas can be applied (see for instance [HR92] and [Gup97]), but the theory is much less developed.

On the other hand, in the function field case, one has a much better understanding of *motivic* L-functions, i.e., those attached to Galois representations, because of Grothendieck's analysis of L-functions. This powerful cohomological interpretation allows one to apply geometric methods to the study of these L-functions.

The goal of this paper is to use geometric methods to prove a very general non-vanishing result for twists of motivic L-functions over a function field. Because Lafforgue has proven the Langlands correspondence for GL_n over function fields [Laf02], our results apply to many automorphic L-functions as well.

To state the result more precisely, let $\mathcal{C}$ be a smooth, proper, geometrically irreducible curve over a finite field $\mathbb{F}_q$ of characteristic p, $F = \mathbb{F}_q(\mathcal{C})$, and $\overline{F}$ a separable closure of F. Let $\mathbb{F}_{q^n} \subset \overline{F}$ be the subfield of q^n elements, $\overline{\mathbb{F}}_q = \cup_{n\geq 1}\mathbb{F}_{q^n}$, and set $F_n = \mathbb{F}_{q^n}(\mathcal{C})$ $(n \geq 1)$ and $F_\infty = \overline{\mathbb{F}}_q(\mathcal{C})$. Let ρ be a continuous, absolutely

Date: May 13, 2004.

This paper is based upon work supported by the National Science Foundation under Grant No. DMS 0070839.

irreducible ℓ-adic representation of $\mathrm{Gal}(\overline{F}/F)$ for some $\ell \neq p$. We assume that ρ is unramified outside a finite set of places of F and that it is geometrically absolutely irreducible, i.e., that it is absolutely irreducible when restricted to $\mathrm{Gal}(\overline{F}/F_\infty)$. We write $L(\rho, F, s)$ for the L-function attached to ρ (see 3.1.7 for the definition) and $L(\rho, K, s)$ for the L-function of $\rho|_{\mathrm{Gal}(\overline{F}/K)}$ for any finite extension K of F contained in $\overline{F}$.

Fix a positive integer d not divisible by p and a complex number s_0. We seek elements $f \in F^\times$ such that $F(f^{1/d})$ has degree d over F and the ratio

$$\frac{L(\rho, F(f^{1/d}), s)}{L(\rho, F, s)}$$

is non-vanishing at $s = s_0$. We can find such f if we first replace F with F_n for sufficiently large n. More precisely, here is the statement of a very weak version of our main result:

1.1. **Theorem.** *Assume that $d|q-1$ and that ρ is everywhere at worst tamely ramified or that $p > \deg \rho + 2$. Then for infinitely many integers n, there exists an element $f \in F_n^\times$ such that the extension $F_n(f^{1/d})$ of F_n has degree d and*

$$\frac{L(\rho, F_n(f^{1/d}), s)}{L(\rho, F_n, s)} \text{ does not vanish at } s = s_0.$$

Before discussing the strengthenings of this result which are our goal, let us remark on the difference between it and what one might expect from analogy with the classical case. Fix F as above and consider extensions of the form $K = F(f^{1/d})$ partially ordered by the degree of their conductors. Then one might expect that for sufficiently large conductor, there exists an extension K of this type such that the non-vanishing conclusion of the theorem holds. More optimistically, one might hope that as the degree of the conductor goes to infinity, the proportion of the extensions K that satisfy the non-vanishing conclusion is positive and bounded away from 0. This may well be true, but the methods of this paper lead to a slightly different point of view (for reasons explained in Section 2). Namely, we consider extensions $K = F_n(f^{1/d})$ of *bounded conductor* for varying n. We show that for large n there exist extensions for which the non-vanishing conclusion holds. Our methods also show that the density of extensions for which we have non-vanishing is positive and bounded away from 0 as $n \to \infty$. (We do not, however, state explicitly the densities. If needed, they may easily be extracted from the proofs of Proposition 6.3.1 and Corollary 9.6.)

The first strengthening of Theorem 1.1 concerns the hypothesis $d|q-1$. Because of it, the ratio in the conclusion of the theorem is a product of twists $L(\rho \otimes \chi, F_n, s)$ where χ runs through the non-trivial characters of $\mathrm{Gal}(F_n(f^{1/d})/F_n) \cong \mathbb{Z}/d\mathbb{Z}$. Thus Theorem 1.1 is about the non-vanishing of abelian twists of $L(\rho, F_n, s)$. In our main theorem, we drop the condition that $d|q-1$ and so the extension $F_n(f^{1/d})/F_n$ may not be Galois. This means that we have to consider twists of ρ by certain non-abelian representations of $\mathrm{Gal}(\overline{F}/F_n)$.

The second strengthening is that we are able to impose local conditions (splitting, inertness, ramification) on the extension $F_n(f^{1/d})/F_n$ at finitely many places.

The third strengthening is that we make a statement for all sufficiently large n. It turns out that for certain data (ρ, d, local conditions, and points s_0), the ratio $L(\rho, F_n(f^{1/d}), s)/L(\rho, F_n, s)$ vanishes at $s = s_0$ for arbitrarily large n and all

$f \in F_n^\times$ satisfying the local conditions. (Think for example of a situation where the local conditions force the sign in a functional equation to be -1.) In these "exceptional situations" our result will assert simple vanishing, rather than non-vanishing. The analysis of the exceptional situations is somewhat intricate. From a monodromy point of view, their cause is clear enough (it is related to the fact that every odd dimensional orthogonal matrix has 1 or -1 as an eigenvalue), but we have gone to some pains to describe the exceptional situations in terms of *easily computable* (essentially local) data, like local root numbers and conductors. This yields criteria which are well-suited to applications. The precise result is stated as Theorem 5.2.

Another strengthening is that we allow the point s_0 to vary with n. I do not know of any application of this generalization, but it is natural from a certain point of view and it does not make the proof any harder.

The case of the theorem where $d|q-1$ and we do not impose local conditions follows fairly easily from the monodromy calculations [Kat02] of Katz. The motivation for considering degrees d that do not divide $q-1$ and local conditions comes from an application to elliptic curves which was the genesis of this project. The result says roughly that any non-isotrivial elliptic curve over F whose L-function vanishes to order ≤ 1 can be put into position to apply a Gross-Zagier formula. More precisely:

1.2. **Theorem.** *Assume that $F = \mathbb{F}_q(\mathcal{C})$ has characteristic $p > 3$ and let E be an elliptic curve over F with $j(E) \notin \mathbb{F}_q$. Then there exists a finite separable extension F' of F and a quadratic extension K of F' such that the following conditions hold:*

- *(a) E is semi-stable over F'.*
- *(b) There is a place of F', call it ∞, where E has split multiplicative reduction.*
- *(c) The place ∞ of F' is not split in K.*
- *(d) Every other place of F' where E has bad reduction is split in K.*
- *(e) $\mathrm{ord}_{s=1} L(E/F', s) = \mathrm{ord}_{s=1} L(E/F, s)$ and $\mathrm{ord}_{s=1} L(E/K, s)$ is odd and $\leq \mathrm{ord}_{s=1} L(E/F', s) + 1$. In particular, if $\mathrm{ord}_{s=1} L(E/F, s) \leq 1$, then $\mathrm{ord}_{s=1} L(E/K, s) = 1$.*

As we have explained elsewhere [Ulm04, 3.8], this result together with a suitably general Gross-Zagier formula implies that the conjecture of Birch and Swinnerton-Dyer holds for elliptic curves E over function fields F of characteristic $p > 3$ with $\mathrm{ord}_{s=1} L(E/F, s) \leq 1$.

The plan of the paper is as follows. In the next section we consider the simplest case of Theorem 1.1, in which we take $\mathcal{C} = \mathbb{P}^1$, ρ the trivial representation, $d = 2$, and $s_0 = 1/2$. The result in this case can easily be proven by elementary methods, but we give a proof which already contains the main ideas of the general case. This section is meant for motivation and none of the rest of the paper relies on it. In Sections 3 and 4 we discuss some preliminaries on the factorization of the ratio $L(\rho, F_n(f^{1/d}), s)/L(\rho, F_n, s)$ into twists of $L(\rho, F_n, s)$ and on local root numbers and conductors and then use them to analyze the exceptional situations mentioned above. Then we are ready to state the main theorem in Section 5. The main body of the proof begins in Section 6 where we define a variety X parameterizing extensions $F_n(f^{1/d})/F_n$ and study the set of points of X satisfying local conditions of splitting, inertness, and ramification. In Section 7 we review the cohomological interpretation of L-functions and construct a sheaf $\mathcal{G}$ on X whose stalks give the twisted L-functions we are studying. In Section 8 we calculate the monodromy

groups of $\mathcal{G}$, using crucially the results of [Kat02]. In Sections 9-10 we apply a variant of Deligne's equidistribution theorem and the monodromy calculations to prove our non-vanishing results. The application to elliptic curves is given in Section 11.

This paper relies heavily on the difficult work of Katz [Kat02]. Fortunately, we are able to treat his results as a "black box" for most of the argument (one important exception being the proof of Proposition 7.2.10.) We hope that this paper may serve as an introduction to some of the powerful ideas in [Kat02].

Acknowledgements: It is a pleasure to thank Nick Katz for making a preliminary version of [Kat02] available to me and for some helpful remarks at an early stage of the project. I also thank Minhyong Kim for encouraging me to think about the problem in its natural generality and the referee for making several comments and corrections.

2. The simplest case

In this section we consider the simplest case of Theorem 1.1, namely that where $\mathcal{C} = \mathbb{P}^1$, ρ is the trivial representation, $d = 2$, and $s_0 = 1/2$. (For brevity, we use certain notational conventions which are not spelled out until later, but which are standard and should be clear.) Since we assume as always that $p \nmid d$, we have $p > 2$. If $f \in F_n^\times$ is not a square, then on one hand, $L(\rho, F_n(\sqrt{f}), s)$ is the zeta function of the hyperelliptic curve $\mathcal{C}_f$ over $\mathbb{F}_{q^n}$ with function field $F_n(\sqrt{f})$, and on the other hand,

$$L(\rho, F_n(\sqrt{f}), s) = L(\rho, F_n, s)L(\rho \otimes \chi_f, F_n, s) = \frac{L(\rho \otimes \chi_f, F_n, s)}{(1 - q^{-ns})(1 - q^{-n(1-s)})}$$

where χ_f is the quadratic character of $\mathrm{Gal}(\overline{F}/F_n)$ associated to the extension $F_n(\sqrt{f})/F_n$. This means that

$$\frac{L(\rho, F_n(\sqrt{f}), s)}{L(\rho, F_n, s)} = L(\rho \otimes \chi_f, F_n, s)$$

is the numerator of the zeta function of $\mathcal{C}_f$.

Thus Theorem 1.1 asserts that for infinitely many n, there exists a hyperelliptic curve over $\mathbb{F}_{q^n}$ whose zeta function does not vanish at the center point of the functional equation, namely at $s_0 = 1/2$. This in fact holds for all sufficiently large n and it is possible to give elementary proofs of this fact, but we need a proof that will work in a much more general situation. In the rest of this section we give such a proof in order to illustrate the main ideas of the proof of Theorem 5.2.

The first point is to note that

$$L(\rho \otimes \chi_f, F_n, s) = \det\left(1 - Fr^n\, q^{-ns} \,\middle|\, H^1(\mathcal{C}_f \times \operatorname{Spec} \overline{\mathbb{F}}_q, \mathbb{Q}_\ell\right)$$

by Grothendieck's analysis of L-functions. Here Fr is the endomorphism of $H^1(\mathcal{C}_f \times \operatorname{Spec} \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$ induced by the identity on $\mathcal{C}_f$ and the geometric (q^{-1}-power) Frobenius on $\overline{\mathbb{F}}_q$. Thus we need to study the distribution of eigenvalues of Frobenius on H^1 of hyperelliptic curves and in particular to find an f such that $q^{n/2}$ is not an eigenvalue of Fr^n on $H^1(\mathcal{C}_f \times \operatorname{Spec} \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$.

To that end, we construct a large family of hyperelliptic curves. More precisely, fix an odd integer $D \geq 3$. Let X be the variety over $\mathbb{F}_q$ whose $\mathbb{F}_{q^n}$ points are the monic polynomials of degree D over $\mathbb{F}_{q^n}$ with distinct roots. I.e., X is obtained from affine space $\mathbb{A}^D$ by removing a discriminant hypersurface. Over X we construct a

family $\pi : Y \to X$ of hyperelliptic curves of genus $g = (D-1)/2$ in such a way that the fiber over $f \in X(\mathbb{F}_{q^n})$ is the curve $\mathcal{C}_f$. Explicitly, we view polynomials as rational functions on $\mathbb{P}^1$. We have a rational function f_{univ} on $\mathbb{P}^1 \times X$, namely $f_{univ} = x^D + a_1 x^{D-1} + \cdots + a_D$ where x is the standard coordinate on $\mathbb{P}^1$ and $a_1, \ldots, a_D$ are the natural coordinates on X. Taking the square root of f_{univ} gives a surface Y with a map $Y \to \mathbb{P}^1 \times X \to X$ with the desired property.

Next we consider the sheaf $\mathcal{G} = R^1\pi_*\mathbb{Q}_\ell$ on X which is lisse because π is smooth and proper. The stalk of $\mathcal{G}$ at a geometric point over $f \in X(\mathbb{F}_{q^n})$ is canonically isomorphic to $H^1(\mathcal{C}_f \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$ and so we have united the cohomology groups we wish to study in one object. Let $\overline{\eta}$ be a geometric generic point of X and consider the natural monodromy representation of $\pi_1(X, \overline{\eta})$ on the stalk $\mathcal{G}_{\overline{\eta}}$, which is a $2g$-dimensional $\mathbb{Q}_\ell$ vector space. (See Section 7 for more on lisse sheaves and monodromy representations.) Let us assume for convenience that q is a square in $\mathbb{Q}_\ell$ and fix a square root. Then we twist the representation of $\pi_1(X, \overline{\eta})$ by the unique character which sends a geometric Frobenius element at a place v of X to $q^{-\deg(v)/2}$. Call the resulting representation τ.

The key input is a calculation of the monodromy group of τ. More precisely, write π_1^{arith} for $\pi_1(X, \overline{\eta})$ and π_1^{geom} for $\pi_1(X \times \overline{\mathbb{F}}_q, \overline{\eta})$. Then we define G^{arith}, the arithmetic monodromy group of τ, as the Zariski closure of $\tau(\pi_1^{\text{arith}})$ in $\mathrm{GL}(\mathcal{G}_{\overline{\eta}})$. Similarly, G^{geom} is the Zariski closure of $\tau(\pi_1^{\text{geom}})$. By [Del80, 1.3.9], G^{geom} is a (not necessarily connected) semisimple algebraic group over $\mathbb{Q}_\ell$. Note that $\mathcal{G}$ carries a natural alternating form (the cup product on cohomology) with values in $\mathbb{Q}_\ell(-1)$. This form is respected by the action of π_1^{arith} and so the arithmetic monodromy group lies *a priori* in a symplectic group. (This is why we introduced the twist by $Fr_v \mapsto q^{-\deg v/2}$; otherwise, π_1^{arith} would act by symplectic similitudes.) Theorem 10.1.18.3 of [KS99] is a calculation of this monodromy group. Namely, Katz and Sarnak show that G^{geom} is the full symplectic group Sp_{2g}, and therefore so is the *a priori* larger group G^{arith}.

At this point we could apply Deligne's equidistribution result, which says roughly that Frobenius elements are equidistributed in the monodromy group. (This is what we will do in the general case.) But in the current simple context, it is more efficient to proceed as follows. Let $E_1 \subset \mathrm{Sp}_{2g}(\mathbb{Q}_\ell) \subset \mathrm{GL}(\mathcal{G}_{\overline{\eta}})$ be the subset of matrices which have 1 as an eigenvalue. This is a proper Zariski closed subset and so there exists an element $c \in \pi_1^{\text{arith}}$ such that $\tau(c) \notin E_1$.

Since π_1^{arith} is compact, choosing a suitable basis, we may assume that the image of τ lies in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ and then we may form the reduced representations $\tau_m : \pi_1^{\text{arith}} \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^m\mathbb{Z})$. For large enough m we have that $\det(1 - \tau_m(c)) \neq 0$. If $f \in X(\mathbb{F}_{q^n})$ we write $Fr_{n,f} \in \pi_1^{\text{arith}}$ for the corresponding geometric Frobenius element (induced by the map $\mathrm{Spec}\,\mathbb{F}_{q^n} \to X$); it is well-defined up to conjugacy. By the Cebotarev density theorem, for all sufficiently large n there exist elements $f \in X(\mathbb{F}_{q^n})$ such that $\tau_m(Fr_{n,f})$ and $\tau_m(c)$ are in the same conjugacy class. This implies that 1 is not an eigenvalue of $Fr_{n,f}$ on $\mathcal{G}_{\overline{\eta}}$ and so $q^{n/2}$ is not an eigenvalue of Fr^n on $H^1(\mathcal{C}_f \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$. Therefore $s = 1/2$ is not a zero of $L(\rho \otimes \chi_f, F_n, s)$ which is the desired result.

It is clear from this argument why we need to use the extensions F_n in the main theorem. Indeed, if we consider extensions of F_n (for varying n) of the form $F_n(f^{1/d})$ and of bounded conductor, then there is a scheme X of finite type whose $\mathbb{F}_{q^n}$ points parameterize the extensions under consideration and there is a lisse sheaf

$\mathcal{G}$ on X whose stalks are the cohomology groups related to twisted L-functions. On the other hand, if we were to consider only extensions of F of the form $F(f^{1/d})$ then the set of extensions under consideration would naturally be the $\mathbb{F}_q$ points of an inductive limit of schemes of finite type, with components of arbitrarily large dimension. Moreover, the relevant sheaf on this ind-scheme would have stalks of arbitrarily large rank. It is not at all clear how to handle this situation.

3. Preliminaries on L-functions

3.1. **Input data and hypotheses.** The notation and hypotheses the following paragraphs (3.1.1 through 3.1.10) will be in force for the rest of the paper.

3.1.1. Let $\mathcal{C}$ be a smooth, proper, geometrically irreducible curve over the finite field $\mathbb{F}_q$ of characteristic p and let $F = \mathbb{F}_q(\mathcal{C})$ be its field of functions. Choose an algebraic closure F^{alg} of F and let $\overline{F} \subset F^{\text{alg}}$ be the separable closure of F. Let $G = \text{Gal}(\overline{F}/F)$ be the absolute Galois group of F. For each place v of F we choose a decomposition group $D_v \subset G$ and we let I_v and Fr_v be the corresponding inertia group and geometric Frobenius class. We write $\deg v$ for the degree of v and $q_v = q^{\deg v}$ for the cardinality of the residue field at v.

For positive integers n we write $\mathbb{F}_{q^n}$ for the subfield of $\overline{F}$ of cardinality q^n, F_n for the compositum $\mathbb{F}_{q^n}F$, and $G_n \subset G$ for $\text{Gal}(\overline{F}/F_n)$. We write F_∞ for $\overline{\mathbb{F}}_q F$ and G_∞ for $\text{Gal}(\overline{F}/F_\infty)$.

3.1.2. Fix a prime $\ell \neq p$ and let $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$, the field of ℓ-adic numbers. Fix also imbeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ and a compatible isomorphism $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. Whenever a square root of q is needed in $\overline{\mathbb{Q}}_\ell$, we take the one mapping to the positive square root of q in $\mathbb{C}$. Having made this choice, we can define Tate twists by half integers.

3.1.3. Fix a continuous, absolutely irreducible representation $\rho : \text{Gal}(\overline{F}/F) \to \text{GL}_r(E)$ where E is a finite extension of $\mathbb{Q}_\ell$ in $\overline{\mathbb{Q}}_\ell$. (We may extend the coefficient field E as necessary below.) We assume that ρ remains absolutely irreducible when restricted to G_∞ and that it is unramified outside a finite set of places, so that it factors through $\pi_1(U, \overline{\eta})$ for some non-empty open subscheme $j : U \hookrightarrow \mathcal{C}$. (Here $\overline{\eta}$ is the geometric point of $\mathcal{C}$ defined by the fixed embedding $F \hookrightarrow F^{\text{alg}}$.) By [Laf02, VII.6] and [Del80, 1.2.8-10], ρ is ι-pure of some weight w, i.e., for every place v where ρ is unramified, each eigenvalue α of $\rho(Fr_v)$ satisfies $|\iota(\alpha)| = q_v^{w/2}$. For convenience, we assume that w is an integer.

3.1.4. We say that a representation τ of G_n is self-dual if it is isomorphic to its contragredient. This is equivalent to saying that there is a non-degenerate G_n-equivariant bilinear pairing on the underlying space. If this pairing is symmetric, we say τ is "orthogonally self-dual" and that τ "has sign $+1$". If it is alternating, we say τ is "symplectically self-dual" and that τ "has sign -1". Schur's lemma implies that if an irreducible representation is self-dual, then it is either orthogonally or symplectically self-dual. Also, if a representation is symplectically self-dual, then its degree is even.

If τ is self-dual, then the weight w of τ is 0. To generalize slightly, we say that τ is symplectically (orthogonally) self-dual of weight w if τ has weight w and the Tate twist $\tau(w/2)$ is symplectically (orthogonally) self-dual. (Here $\tau(w/2)$ is characterized by the equation $\tau(w/2)(Fr_v) = \tau(Fr_v)q_v^{-w/2}$.)

3.1.5. Since ρ is absolutely irreducible when restricted to G_∞, Schur's lemma implies that if ρ is self-dual when restricted to G_∞, then for any integer w there is a character of $G/G_\infty \cong \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ such that $\rho \otimes \chi$ is self-dual of weight w.

We always assume that if ρ is self-dual when restricted to G_∞, then it is already self-dual of some integer weight w as a representation of G. In light of the above, this is not a serious restriction.

3.1.6. For each place v of F we write $\mathrm{Cond}_v \rho$ for the exponent of the Artin conductor of ρ at v. (See [Ser79, Chap. VI] for definitions.) We let $\mathfrak{n} = \sum_v (\mathrm{Cond}_v \rho)[v]$ be the global Artin conductor of ρ, viewed as an effective divisor on $\mathcal{C}$. We write $|\mathfrak{n}|$ for the support of $\mathfrak{n}$, i.e., for the set of places of F where ρ is ramified.

3.1.7. Attached to ρ we have an L-function, defined formally by the product

$$L(\rho, F, T) = \prod_v \det\left(1 - \rho(Fr_v)T^{\deg v} \,\middle|\, (E^r)^{\rho(I_v)}\right)^{-1}.$$

The Grothendieck-Lefschetz trace formula implies that $L(\rho, F, T)$ is actually a rational function of T. More precisely, if ρ is the trivial representation, $L(\rho, F, T)$ is just the Z-function of F (so $L(\rho, F, q^{-s}) = \zeta(\mathcal{C}, s)$) and if ρ is geometrically non-trivial, i.e., non-trivial when restricted to G_∞, then $L(\rho, F, T)$ is a polynomial in T of degree $N = (2g_{\mathcal{C}} - 2)(\deg \rho) + \deg \mathfrak{n}$.

Writing the numerator of $L(\rho, F, T)$ as $\prod(1 - \beta_i T)$, we call the β_i the inverse roots of $L(\rho, F, T)$. Deligne's purity result [Del80, 3.2.3] says that the inverse roots of $L(\rho, F, T)$ have ι-weight $w + 1$, i.e., $|\iota(\beta_i)| = q^{w+1}$ for all i.

If K is a finite extension of F contained in $\overline{F}$, we abbreviate $L(\rho|_{\mathrm{Gal}(\overline{F}/K)}, K, T)$ to $L(\rho, K, T)$.

Using the embedding $E \hookrightarrow \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ we may view $L(\rho, F, T)$ as a rational function in T with complex coefficients. Then the L-function appearing in the Introduction is $L(\rho, F, q^{-s})$.

3.1.8. Fix a positive integer d prime to p. We let $a = [\mathbb{F}_q(\mu_d) : \mathbb{F}_q]$ where μ_d denotes the d-th roots of unity. If necessary, we expand the coefficient field E so that it contains the d-th roots of unity and a square root of q.

Fix also three finite sets of places of F called S_s, S_i, S_r, which are pairwise disjoint.

We will be considering extensions of F_n of the form $K = F_n(f^{1/d})$ where $f \in F_n^\times$ and where the places of F_n over S_s, S_i, and S_r are split, inert, or ramified in K. More precisely:

3.1.9. **Definition.** We say that f *satisfies the local conditions* or $K = F_n(f^{1/d})$ *satisfies the local conditions* if the following hold:

(a) for every place v of F_n over S_s, there is a place of K over v unramified and of residue degree 1;
(b) for every place v of F_n over S_i, there is a place of K over v unramified and of largest possible residue degree, namely $\gcd(d, q_v - 1)$;
(c) every place of F_n over S_r is totally ramified in K; and
(d) every place of F_n over $|\mathfrak{n}| \setminus S_r$ is unramified in K.

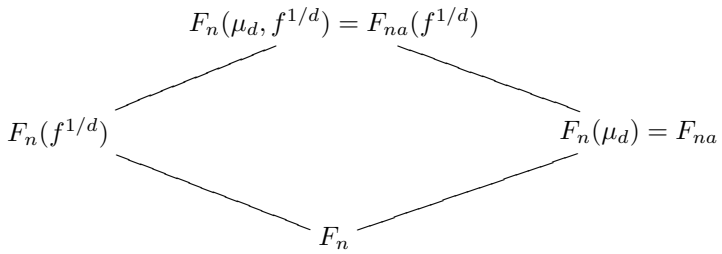
3.1.10. The last piece of data we need is a sequence of algebraic numbers α_n, indexed by positive integers n, which we view as elements of $\overline{\mathbb{Q}}_\ell$ via the fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. We assume that the image of α_n under $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$ has absolute value $q^{n(w+1)/2}$.

3.2. **Base change and twisting.** Our main theorem is a statement about the existence of $f \in F_n^\times$ such that $L(\rho, F_n(f^{1/d}), T)$ has no higher order of zero at $T = \alpha_n^{-1}$ than $L(\rho, F_n, T)$ does. If F_n contains the d-th roots of unity then $F_n(f^{1/d})$ is a Kummer extension of F_n and we have a factorization

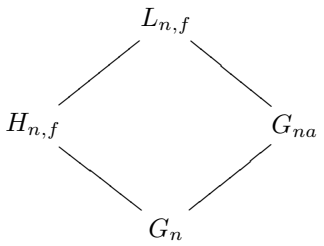
$$L(\rho, F_n(f^{1/d}), T) = \prod_{i=0}^{d-1} L(\rho \otimes \chi_f^i, F_n, T)$$

where χ_f is a character of order d of G_n trivial on $\mathrm{Gal}(\overline{F}/F_n(f^{1/d}))$. (Here and elsewhere we write $\rho \otimes \chi_f^i$ for what should properly be denoted $\rho|_{G_n} \otimes \chi_f^i$.) Thus in this case the main theorem is a non-vanishing statement for abelian twists of ρ. The purpose of this subsection is to record a similar factorization valid without the assumption that F_n contains the d-th roots of unity. This will relate the main theorem to a statement about non-vanishing of certain non-abelian twists.

3.2.1. Let f be an element of $F_n^\times$ which is not an e-th power for any divisor $e > 1$ of d and choose a d-th root $f^{1/d}$ of f in $\overline{F}$. Set $G_n = \mathrm{Gal}(\overline{F}/F_n)$, $H_{n,f} = \mathrm{Gal}(\overline{F}/F_n(f^{1/d}))$, $G_{na} = \mathrm{Gal}(\overline{F}/F_n(\mu_d))$, and $L_{n,f} = \mathrm{Gal}(\overline{F}/F_n(\mu_d, f^{1/d}))$. Here is the diagram of fields:



and the corresponding diagram of Galois groups:



Clearly G_{na} and $L_{n,f}$ are normal subgroups of G_n and $H_{n,f}$ is a (possibly non-normal) subgroup of G_n of index d. Moreover, $G_n/L_{n,f}$ is a semi-direct product:

$$G_n/L_{n,f} = G_{na}/L_{n,f} \rtimes H_{n,f}/L_{n,f} \cong G_{na}/L_{n,f} \rtimes G_n/G_{na}.$$

Fix an isomorphism $\mu_d(\overline{F}) \tilde{\to} \mu_d(E)$ and let χ_f be the E-valued character of G_{na} of order d given by the natural isomorphism $G_{na}/L_{n,f} \tilde{\to} \mu_d(\overline{F})$ (namely $\sigma \mapsto \sigma(f^{1/d})/f^{1/d}$) followed by $\mu_d(\overline{F}) \tilde{\to} \mu_d(E)$. Note that χ_f^i is in fact well-defined on the possibly larger group $\mathrm{Gal}(\overline{F}/F_n(\mu_{d/\gcd(d,i)}))$.

3.2.2. **Lemma.** *If $\Phi \in G$ lies over the geometric Frobenius in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ and $(\chi_f^i)^\Phi$ is defined by $(\chi_f^i)^\Phi(h) = \chi_f^i(\Phi h \Phi^{-1})$, then $(\chi_f^i)^\Phi = \chi_f^{iq}$.*

Proof. This is an easy consequence of the definitions. □

3.2.3. Our notational convention in 3.1.7 says that

$$L(\rho, F_n(f^{1/d}), T) = L(\mathrm{Res}^{G_n}_{H_{n,f}} \rho, F_n(f^{1/d}), T)$$

and by standard properties of L-functions (e.g., [Del73, 3.8.2]),

$$L(\mathrm{Res}^{G_n}_{H_{n,f}} \rho, F_n(f^{1/d}), T) = L(\mathrm{Ind}^{G_n}_{H_{n,f}} \mathrm{Res}^{G_n}_{H_{n,f}} \rho, F_n, T).$$

Also, $\mathrm{Ind}^{G_n}_{H_{n,f}} \mathrm{Res}^{G_n}_{H_{n,f}} \rho \cong \rho \otimes \mathrm{Ind}^{G_n}_{H_{n,f}} \mathbf{1}$ where we write $\mathbf{1}$ for the trivial representation with coefficients in E of $H_{n,f}$ ([Ser77, 3.3 Example 5]). It is well-known that $\mathrm{Ind}^{G_n}_{H_{n,f}} \mathbf{1}$ is the linear representation associated to the permutation action of G_n on the coset space $G_n/H_{n,f}$. We need to know how this representation factors into irreducibles.

3.2.4. **Lemma.** *Let $\sigma_f = \mathrm{Ind}^{G_n}_{H_{n,f}} \mathbf{1}$. Then the irreducible constituents of σ_f are in bijection with the orbits of multiplication by q^n on $\mathbb{Z}/d\mathbb{Z}$. For each orbit $o \subset \mathbb{Z}/d\mathbb{Z}$, set $d_o = d/gcd(d,i)$ for any $i \in o$ and set $a_o = [F_n(\mu_{d_o}) : F_n] = \#o$. Then the representation $\sigma_{o,f}$ corresponding to the orbit o has dimension a_o and the restriction of $\sigma_{o,f}$ to $G_{na_o} = \mathrm{Gal}(\overline{F}/F_n(\mu_{d_o}))$ splits into lines; more precisely, $\sigma_{o,f}|_{G_{na_o}} \cong \oplus_{i \in o} \chi_f^i$.*

For example, when $\mu_d \subset F_n$, i.e., $q^n \equiv 1 \pmod d$, all the orbits o are singletons and we have $\sigma_f \cong \oplus_{i \in \mathbb{Z}/d\mathbb{Z}} \chi_f^i$ as representations of G_n.

Proof. This is a standard exercise in representation theory. Indeed, by [Ser77, 7.3], the restriction of σ_f to G_{na} is $\mathrm{Ind}^{G_{na}}_{L_{n,f}} \mathbf{1}$ which is easily seen to be $\oplus_{i \in \mathbb{Z}/d\mathbb{Z}} \chi_f^i$. (To apply [Ser77], we should note that all the representations in question are trivial on $L_{n,f}$ and so we are really working with subgroups of the finite group $G_n/L_{n,f}$.) The factors χ_f^i are permuted by G_n and Lemma 3.2.2 shows that under the right action $(\chi_f^i)^g(h) = \chi_f^i(ghg^{-1})$, we have $(\chi_f^i)^g = \chi_f^{iq^{n(g)}}$ where $q^{n(g)}$ is the image of g under the natural map $G_n \to G_n/G_{na} \subset (\mathbb{Z}/d\mathbb{Z})^\times$; the image of this map is the cyclic subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by q^n. This proves that $\sigma_{o,f} = \oplus_{i \in o} \chi_f^i$ is an irreducible constituent of σ_f and it is clear that $\sigma_{o,f}$ splits into lines when restricted to G_{na_o}. □

Thus, the general analogue of the factorization at the beginning of this section is

$$L(\rho, F_n(f^{1/d}), T) = \prod_{o \subset \mathbb{Z}/d\mathbb{Z}} L(\rho \otimes \sigma_{o,f}, F_n, T) \tag{3.2.4.1}$$

where the product is over the orbits of q^n on $\mathbb{Z}/d\mathbb{Z}$. If we assume that n is relatively prime to $a = [\mathbb{F}_q(\mu_d) : \mathbb{F}_q]$ then the orbits for multiplication by q^n are the same as the orbits for multiplication by q.

It will be useful to know that $\sigma_{o,f}$ is itself induced. Recall that $d_o = d/\gcd(i,d)$ for any $i \in o$ and $a_o = [F_n(\mu_{d_o}) : F_n] = \#o$.

3.2.5. **Lemma.** *$\sigma_{o,f} \cong \mathrm{Ind}^{G_n}_{G_{na_o}} \chi_f^i$ for any $i \in o$.*

Proof. This is immediate from the facts that $\sigma_{o,f}|_{G_{na_o}} \cong \oplus_{i\in o}\chi_f^i$ and that G_n/G_{na_o} permutes the factors χ_f^i simply transitively. □

Here is a criterion for $\sigma_{o,f}$ to be self-dual.

3.2.6. **Lemma.** *$\sigma_{o,f}$ admits a non-degenerate G_n-invariant pairing if and only if $-o = o$, i.e., if and only if $\{-i \,|\, i \in o\} = o$. In this case, the pairing is symmetric.*

Proof. If $-o = o$ it is easy to write down explicitly a G_n-invariant symmetric pairing. Indeed, this is obvious if $o = \{d/2\}$ and so $\sigma_{o,f} = \chi_f^{d/2}$. Otherwise, $a_o = \#o$ is even and by the previous lemma $\sigma_{o,f}$ can be realized as

$$\{\phi : G_n \to E \,|\, \phi(gh) = \chi_f^i(h)\phi(g) \text{ for all } h \in G_{na_o}\}$$

for any fixed $i \in o$. The G_n action is given by $(g\phi)(g') = \phi(g^{-1}g')$. Let g be a generator of $\mathrm{Gal}(F_n(\mu_{d_o})/F_n) \cong \mathbb{Z}/a_o\mathbb{Z}$. A suitable pairing is then given by

$$\langle \phi_1, \phi_2 \rangle = \sum_{j=0}^{a_o-1} \phi_1(g^j)\phi_2(g^{j+a_o/2}).$$

(To check the G_n-invariance, one uses that $\mathrm{Gal}(F_n(\mu_{d_o}, f^{i/d})/F_n)$ is the semi-direct product

$$\mathrm{Gal}(F_n(\mu_{d_o}, f^{i/d})/F_n(\mu_{d_o})) \rtimes \mathrm{Gal}(F_n(\mu_{d_o})/F_n)$$

and that $g^{a_o/2}$ acts by inversion on $\mathrm{Gal}(F_n(\mu_{d_o}, f^{i/d})/F_n(\mu_{d_o})) = G_{na_o}/\ker(\chi_f^i)$.) Since $\sigma_{o,f}$ is irreducible, any other G_n-invariant pairing is a scalar multiple of this one, so is symmetric.

Conversely, if $-o \neq o$, then $\sigma_{o,f}$ is visibly not self-dual when restricted to G_{na_o} (where it is isomorphic to $\oplus_{i\in o}\chi_f^i$). Thus it cannot be self-dual as a representation of G_n. □

4. Forced zeroes

4.1. **Functional equations and forced zeroes.** As a step toward stating a more precise version of the main theorem, we review some well-known facts about the functional equations satisfied by $L(\rho, F, T)$ and its twists.

4.1.1. Let $\tau : G_n \to \mathrm{GL}_r(E)$ be an absolutely irreducible representation of G_n which is unramified outside a finite set of places and is ι-pure of some weight w. (In the applications, τ will be ρ or one of its twists $\rho \otimes \sigma_{o,f}$.)

4.1.2. The L-functions $L(\tau, F_n, T)$ satisfy functional equations. If τ has weight w, then we have

$$L(\tau, F_n, T) = W(\tau, F_n)q^{n\frac{(w+1)}{2}N}T^N L(\tau^\vee, F_n, (q^{n(w+1)}T)^{-1}) \tag{4.1.2.1}$$

where $W(\tau, F_n)$ is an algebraic number of weight 0, $N = (2g_{\mathcal{C}} - 2)(\dim\tau) + \deg \mathrm{Cond}(\tau)$, and $\tau^\vee$ is the contragredient of τ. (If $n(w+1)N$ is odd, we take the positive square root of q, or more precisely, the square root of q in E which maps to the positive square root of q under ι. Although we have omitted it from the notation, in general $W(\tau, F_n)$ depends on ι, via the choice of square root of q.)

If τ is the trivial representation, $W(\tau, F_n) = 1$. If τ is geometrically non-trivial and the inverse roots of $L(\tau, F_n, T)$ are $\beta_1, \ldots, \beta_N$, then $W(\tau, F_n)q^{n\frac{(w+1)}{2}N}$ can be described succinctly (and independently of ι) as $\prod_{i=1}^N(-\beta_i)$. This implies that $W(\tau, F_{nm}) = (-1)^{N(m+1)}W(\tau, F_n)^m$.

4.1.3. As is well-known, functional equations sometimes force zeroes of L-functions at certain values of s or $T = q^{-s}$. In the remainder of this subsection, we explain how this works out in the function field situation (where the functional equation has *two* fixed points).

As usual, let τ be an absolutely irreducible representation of G_n of weight w and consider the functional equation 4.1.2.1. Note that the involution $T \mapsto (q^{n(w+1)}T)^{-1}$ has two fixed points, namely $T = \pm q^{-n(w+1)/2}$. Thus, when τ is self-dual the functional equation may force $\pm q^{n(w+1)/2}$ as inverse roots of $L(\tau, F_n, T)$. Here is the precise statement, which we leave as a simple exercise for the reader.

4.1.4**. Lemma.** *Suppose that τ is geometrically non-trivial and self-dual of weight w and let N be the degree, as a polynomial in T, of $L(\tau, F_n, T)$.*

(1) If N is even and $W(\tau, F_n) = -1$, then $\pm q^{n(w+1)/2}$ are both inverse roots of $L(\tau, F_n, T)$.
(2) If N is odd, then $-W(\tau, F_n)q^{n(w+1)/2}$ is an inverse root of $L(\tau, F_n, T)$.

The lemma applies only if τ is symplectically self-dual. Indeed, when τ is orthogonally self-dual, $W(\tau, F_n) = 1$ and N is even (see 7.1.9) and when τ is not self-dual, the functional equation does not force any inverse roots since in that case the functional equation relates two different L-functions.

4.1.5. Let $\Psi_n \subset F_n^\times$ be the set of functions f such that the quadratic extension $F_n(\sqrt{f})/F_n$ satisfies the local conditions (i.e., it is split at places of F_n over S_s, inert at places of F_n over S_i, totally ramified at places of F_n over S_r, and is unramified at all places of F_n over $|\mathfrak{n}| \setminus S_r$). Note that we make no restrictions at places not over $S_s \cup S_i \cup S_r \cup |\mathfrak{n}|$ and so Ψ_n is an infinite set.

If $f \in F_n^\times$ we write ψ_f for the character of $\mathrm{Gal}(\overline{F}/F_n)$ corresponding to the quadratic extension $F_n(\sqrt{f})/F_n$. (In the notation of the previous section, this would be $\sigma_{\{d/2\},f} = \chi_f^{d/2}$.)

As we have seen, functional equations can force certain numbers α to be inverse roots of the twisted L-functions $L(\rho \otimes \psi_f, F_n, T)$ for many ψ_f. In order to control this situation, we need to analyze when the signs $W(\rho \otimes \psi_f, F_n)$ are fixed as f varies over Ψ_n. To do so, we need to collect some facts about the signs W.

4.1.6. It will be important for us that the sign $W(\tau, F_n)$ in the functional equation admits an expression as a product of local factors. (See [Del73, 9.9], [Tat79, 3.4], or [Lau87, 3.2.1.1] for more details; [Lau87] treats the case where the representation ρ need not *a priori* be part of a compatible family.) In general, one must make auxiliary choices of a measure and an additive character to define these local factors, but in case τ is symplectically self-dual, the local factors are independent of these choices. Since this is the only case we need, we assume for the rest of this subsection that τ is symplectically self-dual.

Under that assumption, there are local factors $W_v(\tau, F_n) = \pm 1$ which depend only on the restriction of τ to D_v (and ι) and which are 1 wherever τ is unramified. The global sign is then given by $W(\tau, F_n) = \prod_v W_v(\tau, F_n)$. We need to know how these local factors behave under quadratic twists.

4.1.7**. Lemma.** *Suppose that $p = char(F)$ is odd, τ is a symplectically self-dual representation of G of some weight w, and ψ is a quadratic character of G_n.*

(1) If τ is unramified at v and ψ is ramified at v, then

$$\begin{aligned} W_v(\tau\otimes\psi, F_n) &= (-1)^{(q_v-1)(\dim\tau)/4} \\ &= (-1)^{(\deg v)(q^n-1)(\dim\tau)/4}. \end{aligned}$$

(2) If τ is ramified at v and ψ is unramified and non-trivial at v, then

$$W_v(\tau\otimes\psi, F_n) = (-1)^{\mathrm{Cond}_v(\tau)} W_v(\tau, F_n).$$

Proof. In case 1, $\tau\otimes\psi|_{D_v}$ is a direct sum of 1-dimensional representations and we can compute the value of W_v using classical results on Gauss sums. We leave the details as an exercise.

In case 2, [Del73, 5.5.1] or [Tat79, 3.4.6] says that

$$W_v(\tau\otimes\psi, F_n) = \psi(\pi_v)^{\mathrm{Cond}_v(\tau)} W_v(\tau, F_n).$$

(Here we use that τ is symplectic and so $\deg(\tau)$ is even.) But our assumptions imply that $\psi(\pi_v) = -1$. □

4.1.8. For the rest of this subsection, we assume:

ρ is symplectically self-dual of some weight w

This hypothesis implies that the dimension of ρ is even and using this, it is not hard to check that the parity of the degree of $\mathrm{Cond}(\rho\otimes\psi_f)$ is the same for all $f\in\Psi_n$. Since the degree in T of $L(\rho\otimes\psi_f, F_n, T)$ is $N = (2g_{\mathcal{C}}-2)(\deg\rho)+\deg\mathrm{Cond}(\rho\otimes\psi_f)$, the parity of N is independent of the choice of $f\in\Psi_n$.

We now discuss a (local) hypothesis which determines whether the sign $W(\rho\otimes\psi_f, F_n)$ is the same for all $f\in\Psi_n$ or whether it varies. Note that for all v over $|\mathfrak{n}|$, $\mathrm{Cond}_v(\rho\otimes\psi_f)$ is independent of the choice of $f\in\Psi_n$.

(4.1.8.1) For every place v of F_n over $|\mathfrak{n}|\setminus(S_s\cup S_i)$, $\mathrm{Cond}_v(\rho\otimes\psi_f)$ is even for one (and thus every) $f\in\Psi_n$.

4.1.9. **Lemma.** *If hypothesis 4.1.8.1 is satisfied then the signs $W(\rho\otimes\psi_f, F_n)$ for $f\in\Psi_n$ are all the same. On the other hand, if hypothesis 4.1.8.1 fails then $W(\rho\otimes\psi_f, F_n)$ takes both values ±1 as f varies through Ψ_n.*

Proof. Recall that we have assumed that ρ is symplectically self-dual. If $f\in\Psi_n$ then for places v of F_n not over $|\mathfrak{n}|$, part 1 of Lemma 4.1.7 tells us that

$$W_v(\rho\otimes\psi_f, F_n) = \begin{cases} 1 & \text{if } \psi_f \text{ is unramified at } v \\ (-1)^{(\deg v)(q-1)(\deg\rho)/4} & \text{if } \psi_f \text{ is ramified at } v. \end{cases}$$

But the sum of $\deg v$ over places of F_n which are not over $|\mathfrak{n}|$ and where ψ_f is ramified has fixed parity independent of f. Indeed

$$\sum_{v \text{ over } |\mathrm{Cond}(\psi_f)|\setminus|\mathfrak{n}|} \deg v \equiv \sum_{v \text{ over } |\mathfrak{n}|\cap S_r} \deg v \pmod 2$$

since $\mathrm{Cond}(\psi_f)$ has even degree. Thus the sign $\prod_{v \text{ not over } |\mathfrak{n}|} W_v(\rho\otimes\psi_f, F_n)$ is independent of $f\in\Psi_n$.

Now take f and f' in Ψ_n. If v is over $|\mathfrak{n}|$, then $\psi'' = \psi_{f'}/\psi_f$ is unramified at v and it is trivial on D_v if v is over $S_s\cup S_i$. Applying part 2 of Lemma 4.1.7 at those

places v over $|\mathfrak{n}| \setminus (S_s \cup S_i)$ where ψ'' is non-trivial (with τ replaced by $\rho \otimes \psi$ and ψ replaced by ψ''), we conclude that

$$\frac{W(\rho \otimes \psi_f, F_n)}{W(\rho \otimes \psi_{f'}, F_n)} = \prod_{\substack{v \text{ over } |\mathfrak{n}| \setminus (S_s \cup S_i) \\ \psi'' \text{ non-trivial on } D_v}} (-1)^{\mathrm{Cond}_v(\rho \otimes \psi_f)}$$

Hypothesis 4.1.8.1 implies that this quantity is 1. If 4.1.8.1 fails, by the Riemann-Roch theorem, we can choose f and f' in Ψ_n so that this quantity takes both values ± 1. (See Section 6 for more details and a quantitative statement about the density of such f'.) □

4.1.10. A common situation where $\tau = \rho \otimes \sigma_{o,f}$ is symplectically self-dual is when ρ is symplectically self-dual and $-o = o$, so that $\sigma_{o,f}$ is orthogonally self-dual and the tensor product is symplectically self-dual. In particular, the results of the preceding subsections are relevant to the special case where $\sigma_{o,f}$ is a quadratic character ψ_f, i.e., when $o = \{d/2\}$.

Recall that N, the degree of $L(\rho \otimes \psi_f, F_n, T)$ as a polynomial in T, is given by

$$N = (2g_{\mathcal{C}} - 2)(\deg \rho) + \deg \mathrm{Cond}(\rho \otimes \psi_f).$$

Lemma 4.1.9 and Lemma 4.1.4 imply that $L(\rho \otimes \psi_f, F_n, T)$ has certain predictable inverse roots, as f varies over the set Ψ_n, in the following two situations:

(i) if ρ is symplectically self-dual, the hypothesis 4.1.8.1 is satisfied, N is even, and $W(\rho \otimes \psi_f, F_n) = -1$ for one (and thus all) $f \in \Psi_n$, then $\alpha = \pm q^{n(w+1)/2}$ are both inverse roots of $L(\rho \otimes \psi_f, F_n, T)$

(ii) if ρ is symplectically self-dual, the hypothesis 4.1.8.1 is satisfied, and N is odd, then $\alpha = -W(\rho \otimes \psi_f, F_n) q^{n(w+1)/2}$ is an inverse root of $L(\rho \otimes \psi_f, F_n, T)$ for all $f \in \Psi_n$.

4.2. **Zeroes forced by induction.** It turns out that there is another source of forced inverse roots of L-functions, not visible via functional equations, coming from the fact that $\sigma_{o,f}$ is an induced representation. Here is the precise statement:

4.2.1. **Proposition.** *Let F, ρ, d, and $n > 0$ be as in 3.1. Fix an orbit o of multiplication by q^n on $\mathbb{Z}/d\mathbb{Z}$ and set as usual $d_o = d/\gcd(d, i)$ for any $i \in o$ and $a_o = \#o = [F_n(\mu_{d_o}) : F_n]$. Assume that $-o = o$ and $a_o > 1$. Fix $f \in F_n^\times$ and assume that the degree of $\mathrm{Cond}(\rho \otimes \chi_f^i)$ is odd for one (and thus every) $i \in o$. Then*

(1) if ρ is symplectically self-dual of weight w, then $1 - \left(Tq^{n\frac{w+1}{2}}\right)^{a_o}$ divides $L(\rho \otimes \sigma_{o,f}, F_n, T)$.

(2) if ρ is orthogonally self-dual of weight w, then $1 + \left(Tq^{n\frac{w+1}{2}}\right)^{a_o}$ divides $L(\rho \otimes \sigma_{o,f}, F_n, T)$.

Note that the asserted inverse roots of the L-function are not fixed points of the involution $T \mapsto (q^{n(w+1)}T)^{-1}$ in part (2), and not all of them are fixed points in part (1) as soon as $a_o > 2$.

We delay the proof of the proposition until 7.1.11 below, where it can be most naturally explained in terms of cohomology. For the moment, we just check the assertion that $\mathrm{Cond}(\rho \otimes \chi_f^i)$ is odd for all $i \in o$ if it is so for one $i \in o$. In fact, if Φ

denotes an element of $\mathrm{Gal}(\overline{F}/F)$ which induces the q-power Frobenius on $\overline{\mathbb{F}}_q$ and $(\rho\otimes\chi_f^i)^{\Phi^n}$ is defined by

$$(\rho\otimes\chi_f^i)^{\Phi^n}(g)=(\rho\otimes\chi_f^i)(\Phi^n g\Phi^{-n})$$

then

$$\mathrm{Cond}(\rho\otimes\chi_f^{iq^n})=\mathrm{Cond}\left((\rho\otimes\chi_f^i)^{\Phi^n}\right)$$

and so $\mathrm{Cond}(\rho\otimes\chi_f^i)$ and $\mathrm{Cond}(\rho\otimes\chi_f^{iq^n})$ have the same degree.

4.2.2. Here is an example of forced zeroes "in nature" which can be treated by elementary means.

Let q be a prime power with $q\equiv 2 \pmod 3$ and let X be a smooth projective curve over $\mathbb{F}_q$ given as a 3-fold cover of the projective line by the equation

$$y^3=f(x)$$

where $f(x)$ is a rational function on the line. Suppose that X has odd genus. (This can be arranged, for example, by assuming that f has d simple zeroes and $d-1$ poles, one of which is double, the others simple.) Note that as we vary f we get a large family of curves.

The claim then is that the numerator of the zeta function (or rather Z-function) $Z(X,T)$ is divisible by $1+qT^2$, i.e., it has $\pm\sqrt{-q}$ as inverse zeroes. (In terms of $\zeta(X,s)=Z(X,q^{-s})$, we are claiming that there are zeroes at $s=\frac{1}{2}+\frac{\pi i}{2\ln q}$ and $s=\frac{1}{2}+\frac{3\pi i}{2\ln q}$.) Note that these inverse zeroes are *not* at fixed points of the functional equation.

The claim can be seen by an elementary argument: observe that since $q\equiv 2 \pmod 3$, every element of $\mathbb{F}_q$ has a unique cube root and so the number of points on X over $\mathbb{F}_q$ is $q+1$. A similar statement applies for all odd degree extensions of $\mathbb{F}_q$. This implies that the set of inverse roots of the numerator of the Z-function is invariant under $\alpha\mapsto -\alpha$. It is also invariant under $\alpha\mapsto q/\alpha$ and the product of the inverse roots is q^g. Since there are $2g$ inverse roots and g is odd, it follows that for some inverse root α we have $\alpha=-q/\alpha$, as claimed. (Thanks to Mike Zieve for supplying this argument.)

4.2.3. We now return to the general analysis of forced zeroes. We want to give a simple local criterion which determines whether the condition "$\mathrm{Cond}(\rho\otimes\chi_f^i)$ is odd for $i\in o$" holds for a fixed o and all f satisfying the local conditions. Consider the following hypothesis:

(4.2.3.1) For all places v of F_n over $|\mathfrak{n}|\cap S_r$, $\mathrm{Cond}_v(\rho\otimes\chi_v)$ has fixed parity as χ_v varies over totally ramified characters of D_v of order exactly $d_o=d/\gcd(i,d)$. Moreover,

$$\sum_{v\in|n|\cap S_r}\mathrm{Cond}_v(\rho\otimes\chi_v)\deg v+\sum_{v\in|n|\setminus S_r}\mathrm{Cond}_v(\rho)\deg v$$

is odd for some (and thus any) choice of totally ramified local characters χ_v.

4.2.4. **Proposition.** *Fix an orbit $o\neq\{d/2\}$, an $i\in o$, and an integer n prime to a_o. Then $\deg\mathrm{Cond}(\rho\otimes\chi_f^i)$ is odd for all $f\in F_n^\times$ satisfying the local conditions if and only if ρ is even dimensional and hypothesis 4.2.3.1 is satisfied.*

Proof. The degree of the Artin conductor is

$$\sum_{v \text{ over } |\mathfrak{n}|} \mathrm{Cond}_v(\rho \otimes \chi_f^i) \deg v + \sum_{v \text{ not over } |\mathfrak{n}|} \mathrm{Cond}_v(\rho \otimes \chi_f^i) \deg v$$

and we have

$$\sum_{v \text{ over } |\mathfrak{n}|} \mathrm{Cond}_v(\rho \otimes \chi_f^i) \deg v$$
$$= \sum_{v \text{ over } |\mathfrak{n}| \cap S_r} \mathrm{Cond}_v(\rho \otimes \chi_f^i) \deg v + \sum_{v \text{ over } |\mathfrak{n}| \setminus S_r} \mathrm{Cond}_v(\rho) \deg v$$

and

$$\sum_{v \text{ not over } |\mathfrak{n}|} \mathrm{Cond}_v(\rho \otimes \chi_f^i) \deg v = \sum_{\substack{v \text{ not over } |\mathfrak{n}| \\ v(f) \not\equiv 0 \pmod{d_0}}} \deg \rho \deg v.$$

It is thus clear that if ρ is even dimensional and hypothesis 4.2.3.1 is satisfied, then $\deg \mathrm{Cond}(\rho \otimes \chi_f^i)$ is odd for all f satisfying the local conditions.

For the converse, first assume that $\deg \rho$ is even and hypothesis 4.2.3.1 fails. Choose local characters χ_v of order exactly d_o at each v over $|\mathfrak{n}| \cap S_r$ so that the sum appearing in 4.2.3.1 is even. Then there is an element $f \in F_n^\times$ satisfying the local conditions such that the local component at v of χ_f^i is the fixed χ_v for all v over $|\mathfrak{n}| \cap S_r$. (This is an easy consequence of the Riemann-Roch theorem; we just need to fix (modulo d_o) the valuation of f at v over $|\mathfrak{n}| \cap S_r$. See Section 6 below for a more precise version of this result.) For such f, it is clear that $\deg \mathrm{Cond}(\rho \otimes \chi_f^i)$ is even.

Finally, assume that $\deg \rho$ is odd. Fix a divisor D which is the sum of the places over S_r, each with multiplicity one, plus a sum of places of odd degree not over $S_s \cup S_i \cup S_r \cup |\mathfrak{n}|$ also with multiplicity one; we insist that there should be at least 2 such places and that the degree of D be sufficiently large, namely greater than $2g-2$ plus the sum of the degrees of all places over $S_s \cup S_i$. Let f be an element of $F_n^\times$ satisfying the local conditions and such that the divisor of f is $-D$ plus an effective square free divisor. (I.e., f has polar divisor D and its zeroes are distinct.) The existence of such an f again follows easily from the Riemann-Roch theorem. We note that $\deg \mathrm{Cond}(\rho \otimes \chi_f^i)$ only depends on D, not on the specific f chosen. If, for this D, $\deg \mathrm{Cond}(\rho \otimes \chi_f^i)$ is even, we are finished. If not, modify D as follows: drop one place (of odd degree) not over $S_s \cup S_i \cup S_r \cup |\mathfrak{n}|$ and change the coefficient of another place not over $S_s \cup S_i \cup S_r \cup |\mathfrak{n}|$ from 1 to 2. Calling the resulting divisor D', choose $f' \in F_n^\times$ with polar divisor D' and distinct zeroes which satisfies the local conditions. Then we have removed one term $\deg \rho \deg v$ from the last displayed sum and not changed anything else (here we use that $i \neq d/2$) and so

$$\deg \mathrm{Cond}(\rho \otimes \chi_{f'}^i) = \deg \mathrm{Cond}(\rho \otimes \chi_f^i) - \deg \rho \deg v$$

which is even. □

4.2.5. *Remark.* In general it is not possible to find one f which makes $\deg \mathrm{Cond}(\rho \otimes \chi_f^i)$ even for all i in several different orbits o. By the proposition, we can always arrange this for one orbit. If $\deg \rho$ is odd, we can find one f which makes this true for at least half of the orbits in any fixed collection of orbits (for a fixed d).

4.2.6. The upshot of this subsection is that $L(\rho\otimes\sigma_{o,f},F_n,T)$ has certain predictable inverse roots for all f satisfying the local conditions in the following two situations:

(i) if ρ is symplectically self-dual of weight w, $o=-o$, $a_o=\#o>1$, and hypothesis 4.2.3.1 is satisfied, then the solutions α of $\alpha^{a_o}=q^{n(w+1)/2}$ are inverse roots of $L(\rho\otimes\sigma_{o,f},F_n,T)$.
(ii) if ρ is orthogonally self-dual of weight w and of even degree, $o=-o$, $a_o=\#o>1$, and hypothesis 4.2.3.1 is satisfied, then the solutions α of $\alpha^{a_o}=-q^{n(w+1)/2}$ are inverse roots of $L(\rho\otimes\sigma_{o,f},F_n,T)$.

5. Statement of the main technical theorem

5.1. **Exceptional situations.** It will turn out that 4.1.10 and 4.2.6 exhaust the supply of "forced zeroes" in our situation. The following definitions give a convenient terminology for when forced zeroes occur:

5.1.1. **Definitions.** We say that ρ, d, S_s, S_i, S_r, n, $o\subset\mathbb{Z}/d\mathbb{Z}$, and α_n are "exceptional" (or more briefly "n is exceptional") if one of the following conditions holds:

(i) ρ is symplectically self-dual of weight w, $o=\{d/2\}$, the hypothesis 4.1.8.1 is satisfied, $\deg\operatorname{Cond}(\rho\otimes\chi_f)$ is even and $W(\rho\otimes\chi_f,F_n)=-1$ for one (and thus all) $f\in\Phi_n$, and $\alpha_n=\pm q^{n(w+1)/2}$
(ii) ρ is symplectically self-dual of weight w, $o=\{d/2\}$, the hypothesis 4.1.8.1 is satisfied, $\deg\operatorname{Cond}(\rho\otimes\chi_f)$ is odd and $\alpha_n=-W(\rho\otimes\chi_f,F_n)q^{n(w+1)/2}$ for one (and thus all) $f\in\Phi_n$
(iii) ρ is symplectically self-dual of weight w, $-o=o$ and $a_o=\#o>1$, hypothesis 4.2.3.1 holds for $i\in o$, and $\alpha_n^{a_o}=q^{n\frac{w+1}{2}a_0}$
(iv) ρ is even dimensional and orthogonally self-dual of weight w, $-o=o$ and $a_o=\#o>1$, hypothesis 4.2.3.1 holds for $i\in o$, and $\alpha_n^{a_o}=-q^{n\frac{w+1}{2}a_0}$
(v) ρ is symplectically self-dual of weight w, $-o=o$ and $a_o=\#o>1$, and $\alpha_n^{a_o}=q^{n\frac{w+1}{2}a_0}$
(vi) ρ is orthogonally self-dual of weight w, $-o=o$ and $a_o=\#o>1$, and $\alpha_n^{a_o}=-q^{n\frac{w+1}{2}a_0}$

The exceptional situation (i) and (ii) arise in the context of elliptic curves and "Heegner conditions" as we will see in Section 11 below. Situations (iii) and (iv) are related to the "exotic" forced zeroes of Subsection 4.2 and are also needed for the application to elliptic curves.

Note that exceptional situations (iii) and (iv) are subsets of situations (v) and (vi) respectively. When we consider several orbits o at once, we will find that there is always a forced zero (of multiplicity one) in situations (iii) and (iv), whereas in situations (v) and (vi), we will only be able to assert that the multiplicity of a zero at α_n is at most one.

We can now state the main theorem:

5.2. **Theorem.** *Suppose that F, ρ, d, S_s, S_i, S_r, (α_n) satisfy the hypotheses of 3.1. Suppose also either that ρ is at worst tamely ramified at every place v of F or that $p\geq\deg\rho+2$ and ρ is tamely ramified at all places $v\in|\mathfrak{n}|\cap S_r$.*

(1) Fix an orbit $o\subset\mathbb{Z}/d\mathbb{Z}$ for multiplication by q and set $d_o=d/\gcd(d,i)$ for any $i\in o$ and $a_o=\#o=[F(\mu_{d_o}):F]$. Then for all sufficiently large n

relatively prime to a_o, there exists $f \in F_n^\times$ such that every place of F_n over S_s (resp. S_i, S_r) splits (resp. is "as inert as possible", is totally ramified) in $F_n(f^{1/d})$ and

- *if n is exceptional of type (i)-(iv), $L(\rho\otimes\sigma_{o,f}, F_n, T)$ has α_n as a simple inverse root*
- *in all other cases, α_n is not an inverse root of $L(\rho \otimes \sigma_{o,f}, F_n, T)$*

(2) *Set $a = [F(\mu_d) : F]$. Then for all sufficiently large n relatively prime to a, there exists $f \in F_n^\times$ such that every place of F_n over S_s (resp. S_i, S_r) splits (resp. is "as inert as possible", is totally ramified) in $F_n(f^{1/d})$ and for each orbit $o \subset \mathbb{Z}/d\mathbb{Z}$ for multiplication by q:*

- *if n is exceptional of type (i)-(iv), $L(\rho\otimes\sigma_{o,f}, F_n, T)$ has α_n as a simple inverse root*
- *if n is exceptional of type (v) or (vi), $L(\rho \otimes \sigma_{o,f}, F_n, T)$ has α_n as an inverse root of multiplicity at most 1*
- *in all other cases, α_n is not an inverse root of $L(\rho \otimes \sigma_{o,f}, F_n, T)$*

It is possible to get somewhat better control of the type (v) and (vi) exceptional situations in various contexts. For example, if $\deg\rho$ is odd, we can find an f so that $L(\rho\otimes\sigma_{o,f}, F_n, T)$ does not vanish at α_n for at least half of the orbits o of type (vi). These improvements do not seem likely to be of much use, so we omit them.

5.3. **Twisting.** Note that the truth of the theorem is invariant under twisting in the following sense: the theorem holds for F, ρ, d, S_s, S_i, S_r, (α_n) if and only if it holds for F, $\rho(t)$, d, S_s, S_i, S_r, $(q^{-tn}\alpha_n)$. (Here as in 3.1.4, $\rho(t)$ is the Tate twisted representation, characterized by $\rho(t)(Fr_v) = \rho(Fr_v)q_v^{-t}$.) Thus by twisting we may assume that ρ has weight $w = -1$ and the α_n all have ι-weight 0, i.e., satisfy $|\iota\alpha_n| = 1$. We make this assumption for the rest of the paper.

6. Local conditions

6.1. **Notational conventions.** The rest of this article will use more algebraic geometry. We set the following notations and conventions.

All schemes considered will be of finite type over $\operatorname{Spec}\mathbb{F}_q$. If X is such a scheme and k is an extension field of $\mathbb{F}_q$, we write $X\times k$ for $X\times_{\operatorname{Spec}\mathbb{F}_q}\operatorname{Spec} k$. Let $\overline{\mathbb{F}}_q$ denote an algebraic closure of $\mathbb{F}_q$. We will often use a bar to denote the base change to $\overline{\mathbb{F}}_q$, so for example $\overline{\mathcal{C}} = \mathcal{C}\times\overline{\mathbb{F}}_q$.

We write Fr for the geometric (q^{-1}-power) Frobenius of $\overline{\mathbb{F}}_q$ and its subfields, and also for the automorphism of $\overline{X} = X\times\overline{\mathbb{F}}_q$ which is the identity on X and Fr on $\overline{\mathbb{F}}_q$, and for its action on cohomology.

Suppose that X is reduced and irreducible and let $\overline{\eta}$ be a geometric generic point of X with residue field $\kappa(\overline{\eta})$. To fix ideas, we take $\overline{\eta}$ to be the spectrum of an algebraic closure of the field of rational functions on X. Let $\pi_1(X,\overline{\eta})$ be the fundamental group of X with base point $\overline{\eta}$. (See [SGA1, Exp. V].)

Let k be a finite extension of $\mathbb{F}_q$ and $x \in X(k)$ be a k-valued point of X, i.e., a morphism $\operatorname{Spec} k \to X$. Choosing an algebraic closure $\overline{k}$ of k yields a geometric point $\overline{x} : \operatorname{Spec}\overline{k} \to X$ over x, from which we deduce an embedding

$$\operatorname{Gal}(\overline{k}/k) \cong \pi_1(\operatorname{Spec} k, \operatorname{Spec}\overline{k}) \hookrightarrow \pi_1(X,\overline{x}) \cong \pi_1(X,\overline{\eta}).$$

where the last isomorphism is a non-canonical "path" isomorphism. We write $Fr_{k,x}$ for the image of the geometric Frobenius. The conjugacy class of $Fr_{k,x}$ is

well-defined independently of the choices. When k is a field with q^n elements, we also write $Fr_{n,x}$ for $Fr_{k,x}$.

Similarly, if x is a closed point of X with residue field $\kappa(x)$, we may view x as a $\kappa(x)$-valued point of X and form a Frobenius element $Fr_x = Fr_{\kappa(x),x} \in \pi_1(X, \overline{\eta})$ which is well-defined up to conjugation. We will use this notation mostly in the case where X is a curve and x is the closed point associated to a place of the function field of X.

6.2. **The parameter space X.** We now introduce an effective $\mathbb{F}_q$-rational divisor D on $\mathcal{C}$, say $D = \sum_v a_v[v]$ where v runs over places of F and the coefficients a_v are non-negative. As usual, $\deg(D) = \sum_v a_v \deg v$ denotes the degree of D and $|D|$ denotes the support of D, i.e., the set of places where $a_v \neq 0$. We consider D as a divisor on the curves $\mathcal{C} \times \mathbb{F}_{q^n}$ in the natural way. In the course of the discussion we may enlarge D so that its degree is "sufficiently large" in a sense which will be made precise as needed.

Let L be the scheme representing the functor on $\mathbb{F}_q$-algebras

$$R \mapsto H^0(\mathcal{C} \times_{\operatorname{Spec} \mathbb{F}_q} \operatorname{Spec} R, \mathcal{O}(D)) = H^0(\mathcal{C}, \mathcal{O}(D)) \otimes_{\mathbb{F}_q} R.$$

In concrete terms, this just means that L is an affine space over $\operatorname{Spec} \mathbb{F}_q$ of dimension $\dim_{\mathbb{F}_q} H^0(\mathcal{C}, \mathcal{O}(D))$. Note as well that the set of $\mathbb{F}_q$ points $L(\mathbb{F}_q)$ is what would classically be denoted $L(D)$.

Now let X be the scheme which represents the functor $R \mapsto$ "the set of elements of $L(R)$ whose zeroes (as section of $\mathcal{O}(D)$) are distinct and disjoint from $|D| \cup |\mathfrak{n}| \cup S_s \cup S_i$." It is clear what the quoted phrase means when R is a field; the precise meaning for a general scheme and a very detailed proof of the existence of X is explained in [Kat02, 5.0.6, 6.0, and 6.1]. Among other things it is proven there that X is an open subscheme of L. (Essentially, X is obtained from L by removing the hyperplanes corresponding to sections of $\mathcal{O}(D)$ vanishing at some point in $|D| \cup |\mathfrak{n}| \cup S_s \cup S_i$ and a discriminant locus corresponding to sections with multiple zeroes.)

6.3. **General local conditions.** In this subsection we make some general definitions which will allow us to identify those points of $X(\mathbb{F}_{q^n})$ which satisfy various local conditions needed in the proof of the main theorem.

Let us fix for each n a finite set of places S_n of F_n and for each place $w \in S_n$ a non-empty subset of $C_{n,w} \subset F_{n,w}^\times / F_{n,w}^{\times d}$. We define the degree of S_n by $\deg(S_n) = \sum_{w \in S_n} \deg(w)$ and we say that the collection $(S_n, C_{n,w})$ is *compatible with* D if the following condition is satisfied: for every every w in S_n, there exists an element $f \in F_n^\times$ such that the order of pole $-w(f)$ is equal to the coefficient of w in D and the class of f in $F_{n,w}^\times / F_{n,w}^{\times d}$ lies in the subset $C_{n,w}$.

We say that $f \in F_n^\times$ *satisfies the local conditions imposed by* $(S_n, C_{n,w})$ if for every $w \in S_n$, the class of f in $F_{n,w}^\times / F_{n,w}^{\times d}$ lies in the subset $C_{n,w}$. It is a consequence of the Riemann-Roch theorem that if the degree of D is sufficiently large (namely $> 2g_{\mathcal{C}} - 2 + \deg(S_n)$) and $(S_n, C_{n,w})$ is compatible with D, then there are elements of $L(\mathbb{F}_{q^n}) \subset F_n$ which satisfy the local conditions imposed by $(S_n, C_{n,w})$. The next proposition tells us that the set of such elements which also lie in $X(\mathbb{F}_{q^n})$ has a positive density, bounded away from 0.

Fix an effective divisor D and a set of local conditions $(S_n, C_{n,w})$ for each n which are compatible with D. Define

$$Y_n = \{f \in X(\mathbb{F}_{q^n}) |\ f \text{ satisfies the local conditions imposed by } (S_n, C_{n,w})\}.$$

6.3.1. **Proposition.** *Assume that* $\deg(D) > 2g_{\mathcal{C}} - 2 + \deg(S_n)$ *for all* n. *Then there exists a constant* $C > 0$, *independent of* n, *such that*

$$\frac{\#Y_n}{\#X(\mathbb{F}_{q^n})} > C$$

for all sufficiently large n.

Proof. Let $B = \sup_n \deg(S_n)$, which is finite by hypothesis. For each n, introduce an auxiliary effective divisor defined by $D'_n = \sum_{w \in S_n} [w]$. Note that $\deg(D'_n) = \deg(S_n) \leq B$.

Define $L(\mathbb{F}_{q^n})^{\text{good}}$ to be those elements of $L(\mathbb{F}_{q^n})$ which satisfy the local conditions imposed by $(S_n, C_{n,w})$. Whether an element $f \in L(\mathbb{F}_{q^n})$ lies in $L(\mathbb{F}_{q^n})^{\text{good}}$ is determined by the leading terms in the expansion of f at places in $|D'_n| = S_n$. More precisely, note that for each $w \in S_n$ there is a well-defined map

$$\frac{\mathcal{O}(D)_w}{\mathcal{O}(D - D'_n)_w} \setminus 0 \to F_{n,w}^{\times} / F_{n,w}^{\times d}$$

where $\mathcal{O}(D)_w$ and $\mathcal{O}(D - D'_n)_w$ are the stalks of $\mathcal{O}(D)$ and $\mathcal{O}(D - D'_n)$ at w. This map is not surjective, but its image does meet $C_{n,w}$ (this is the definition of compatible) and its non-empty fibers all have cardinality

$$\frac{(q_w - 1)}{\gcd(q_w - 1, d)} \geq \frac{(q_w - 1)}{d}.$$

Let $C'_{n,w}$ be the subset of $\mathcal{O}(D)_w / \mathcal{O}(D - D'_n)_w$ consisting of non-zero elements which map to $C_{n,w}$. Then $C'_{n,w}$ is non-empty and its "density" (i.e., its cardinality divided by that of $\mathcal{O}(D)_w / \mathcal{O}(D - D'_n)_w$) is positive and bounded away from 0 for all $n \gg 0$. (Indeed, it is bounded below by $(q_w - 1)/dq_w = 1/d - 1/dq_w$.) Now let C'_n be the subset $\prod_{w \in S_n} C'_{n,w}$ of

$$H^0(\mathcal{C} \times \mathbb{F}_{q^n}, \mathcal{O}(D)/\mathcal{O}(D - D'_n)) = \prod_{w \in S_n} \mathcal{O}(D)_w / \mathcal{O}(D - D'_n)_w.$$

Again C'_n has positive density which is bounded away from 0 for all n. Moreover, $f \in L(\mathbb{F}_{q^n})$ is in $L(\mathbb{F}_{q^n})^{\text{good}}$ if and only if its image under the natural homomorphism

$$L(\mathbb{F}_{q^n}) = H^0(\mathcal{C} \times \mathbb{F}_{q^n}, \mathcal{O}(D)) \to H^0(\mathcal{C} \times \mathbb{F}_{q^n}, \mathcal{O}(D)/\mathcal{O}(D - D'_n))$$

lies in C'_n.

By the Riemann-Roch theorem, this homomorphism is surjective because

$$\deg D > 2g_{\mathcal{C}} - 2 + B \geq 2g_{\mathcal{C}} - 2 + \deg D'_n.$$

Also, the fibers of this homomorphism all have the same cardinality, so the density of $L(\mathbb{F}_{q^n})^{\text{good}}$ in $L(\mathbb{F}_{q^n})$ is bounded away from 0 for all n: there is an explicit constant $C' > 0$ such that

$$\frac{\#L(\mathbb{F}_{q^n})^{\text{good}}}{\#L(\mathbb{F}_{q^n})} > C'$$

for all n.

On the other hand, X contains the complement of a hypersurface in L and so there is a constant C'' such that we have a Lang-Weil type estimate

$$\frac{\#(L(\mathbb{F}_{q^n}) \setminus X(\mathbb{F}_{q^n}))}{\#L(\mathbb{F}_{q^n})} < \frac{C''}{q^{n/2}}.$$

Thus

$$\begin{aligned}\frac{\#Y_n}{\#X(\mathbb{F}_{q^n})} &\geq \frac{\#Y_n}{\#L(\mathbb{F}_{q^n})} \\ &= \frac{\#\left(L(\mathbb{F}_{q^n})^{\mathrm{good}} \cap X(\mathbb{F}_{q^n})\right)}{\#L(\mathbb{F}_{q^n})} \\ &\geq \frac{\#L(\mathbb{F}_{q^n})^{\mathrm{good}} - \#\left(L(\mathbb{F}_{q^n}) \setminus X(\mathbb{F}_{q^n})\right)}{\#L(\mathbb{F}_{q^n})} \\ &> C' - \frac{C''}{q^{n/2}}\end{aligned}$$

and this proves the proposition. □

6.4. **Typical D and local conditions.** Now we discuss the local conditions to be used in the proof of the main theorem. In this subsection we give the "typical" conditions, then in the next subsection we explain how they should be modified in certain special circumstances. The point is that the proofs of 4.1.9 and 4.2.1 give conditions under which certain zeroes can be avoided and we need to insure that these conditions are satisfied.

Here are the typical conditions on D. We require that the effective divisor $D = \sum_v a_v[v]$ satisfies:

(a) a_v is relatively prime to d for all $v \in S_r$.
(b) $a_v = 0$ for all $v \in S_s \cup S_i \cup (|\mathfrak{n}| \setminus S_r)$.
(c) $a_v = 1$ for at least one $v \notin S_s \cup S_i \cup S_r$.
(d) $\deg(D) > 2g_{\mathcal{C}} - 2 + \deg(S_s \cup S_i)$.
(e) $\deg(D) > \max(12g_{\mathcal{C}} + 9, 6\deg(\mathfrak{n}) + 11, 72\deg(\rho) - (2g_{\mathcal{C}} - 2))$.

The reason for the requirements on $\deg D$ will become clear later in the proof. Less stringent requirements are needed in many cases, but we have chosen to simplify by making a uniform hypothesis.

Our typical local conditions are as follows: S_n will be the set of places of F_n over $S_s \cup S_i$. If $w \in S_n$ lies over S_s, then $C_{n,w} = \{1\} \subset F_{n,w}^\times / F_{n,w}^{\times d}$. If $w \in S_n$ lies over S_i, then $C_{n,w} \subset F_{n,w}^\times / F_{n,w}^{\times d}$ is the set of generators of the cyclic subgroup $\mathcal{O}_{n,w}^\times / \mathcal{O}_{n,w}^{\times d}$.

It is clear that the local conditions $(S_n, C_{n,w})$ are compatible with D and that an element $f \in F_n^\times$ which satisfies the local conditions imposed by $(S_n, C_{n,w})$ satisfies the local conditions in the sense of 3.1.8.

6.5. **Three special situations.** First suppose we are considering part (1) of the main theorem, $o = \{d/2\}$, ρ is symplectically self-dual (of weight $w = -1$), and for some n the condition 4.2.3.1 fails and $\alpha_n = \pm 1$. Then we need to impose additional local conditions $C_{n,w}$ at places w over $|\mathfrak{n}| \setminus (S_s \cup S_i)$. So we replace condition (d) above with

(d) $\deg(D) > 2g_{\mathcal{C}} - 2 + \deg(S_s \cup S_i) + \deg(|\mathfrak{n}| \setminus (S_s \cup S_i))$.

Note that the right hand side of this inequality is independent of n and so we may fix one D which works for all n. The proof of 4.1.9 shows that by imposing local conditions at places over $|\mathfrak{n}|\setminus(S_s\cup S_i)$, we may fix the sign in the functional equation of $L(\rho\otimes\psi_f, F_n, T)$ where ψ_f is the quadratic character of G_n corresponding to the extension $F_n(f^{1/2})/F_n$. We choose such local conditions so that the sign is $+1$ when the degree of the L-function is even and so that the sign is equal to that of α_n when the degree of the L-function is odd. (Cf. 4.1.4.) It is clearly possible to do this in such a way that the new local conditions $(S_n, C_{n,w})$ are still compatible with D.

The second special situation is when we consider part (2) of the main theorem, d is even (so that one of the orbits considered is $o = \{d/2\}$), ρ is symplectically self-dual (of weight $w = -1$), and for some n the condition 4.2.3.1 fails and $\alpha_n = \pm 1$. Again we replace condition (d) above with

(d) $\deg(D) > 2g_{\mathcal{C}} - 2 + \deg(S_s \cup S_i) + \deg(|\mathfrak{n}| \setminus (S_s \cup S_i))$

and we add local conditions at places w over $|\mathfrak{n}| \setminus (S_s \cup S_i)$ to force the sign in the functional equation of the quadratic twist $L(\rho \otimes \psi_f, F_n, T)$ to take a certain value depending on N and α_n. It is clearly possible to do this in such a way that the new local conditions $(S_n, C_{n,w})$ are still compatible with D.

The third special situation is when we consider part (1) of the main theorem, $o = -o$, $a_o = \#o > 1$, and either (a) ρ is symplectically self-dual (of weight $w = -1$) and for some n $\alpha_n^{a_o} = 1$; or (b) ρ is orthogonally self-dual (of weight $w = -1$) and for some n $\alpha_n^{a_o} = -1$. By Propositions 4.2.4 and 4.2.1 we have forced zeroes if $\deg \rho$ is even and hypothesis 4.2.3.1 holds. If one of these conditions fails, the proof of Proposition 4.2.4 tells us how to avoid forced zeroes and we must build this into the definition of D. More precisely, if ρ is odd-dimensional we choose D so that the sum of the degrees of places in $|D|$ and not over $S_s \cup S_i \cup S_r \cup |\mathfrak{n}|$ is either odd or even, as required to make the degree of $\mathrm{Cond}(\rho \otimes \chi_f^i)$ even. On the other hand, if ρ is even dimensional and hypothesis 4.2.3.1 fails, then we choose the coefficients a_v of D at places $v \in |\mathfrak{n}| \cap S_r$ so as to make the conclusion of 4.2.3.1 false. Note that fixing the integer a_v (modulo d) is the same as fixing the local character of inertia χ_f^i. Note also that the conditions on D are independent of n so there is one D which works for all n. In this third special situation, the new conditions are all on the coefficients of D away from the places in S_n, so the new D and the local conditions $(S_n, C_{n,w})$ are clearly compatible.

6.6. **Summary.** For the rest of the paper, we fix a divisor D and compatible local conditions $(S_n, C_{n,w})$ according to the recipe in Subsections 6.4-6.5. (This data depends of course on the data F, ρ, d, S_s, S_i, S_r, and (α_n) fixed in Subsection 3.1 and, when we are considering part (1) of the theorem, on a fixed orbit $o \subset \mathbb{Z}/d\mathbb{Z}$ for multiplication by q.)

The divisor D determines a parameter space X of functions, and the conditions $(S_n, C_{n,w})$ determine a subset $Y_n \subset X(\mathbb{F}_{q^n})$ of functions which satisfy the local conditions imposed by $(S_n, C_{n,w})$. Because we assumed the degree of D is large (specifically, because of the first hypothesis on $\deg(D)$ in 6.4 above), the density of Y_n in $X(\mathbb{F}_{q^n})$ is positive and bounded away from 0 for all sufficiently large n. Moreover, by our choice of local conditions $(S_n, C_{n,w})$ the functions $f \in Y_n$ satisfy the local conditions in the sense of Definition 3.1.9.

7. Twisted L-functions and sheaves on X

In this section, we relate the twisted L-functions $L(\rho \otimes \sigma_{o,f}, F_n, T)$ to certain sheaves on the parameter space X. We assume familiarity with the basic formalism and techniques of étale sheaves and their cohomology, as explained for example in [SGA4$\frac{1}{2}$, [Arcata] and [Rapport]] or [Mil80], and in much more detail in [SGA4] and [SGA5].

7.1. L-functions and cohomology.

We begin in this subsection by reviewing Grothendieck's cohomological expression for the L-functions $L(\rho\otimes\sigma_{o,f}, F_n, T)$, "one f at a time."

7.1.1. Let $\tau : G \to \mathrm{GL}_r(E)$ be a continuous Galois representation such that there exists a non-empty Zariski open subset $j : U \hookrightarrow \mathcal{C}$ with τ unramified at all places in U, i.e., such that τ factors through $\pi_1(U, \overline{\eta})$. Then there is a twisted constant constructible (i.e., lisse) sheaf of E vector spaces $\mathcal{F}_U$ on U corresponding to τ. (Briefly, since G and $\pi_1(U, \overline{\eta})$ are compact we may conjugate τ so that its image lies in $\mathrm{GL}_r(\mathcal{O}_E)$. If $\mathfrak{m}$ denotes the maximal ideal of $\mathcal{O}_E$, reducing modulo powers of $\mathfrak{m}$ gives representations $\pi_1(U, \overline{\eta}) \to \mathrm{GL}_r(\mathcal{O}_E/\mathfrak{m}^n)$ into finite groups. These correspond to étale sheaves of $\mathcal{O}_E/\mathfrak{m}^n$-modules, free of rank r. For varying n, these finite sheaves collate into a $\mathfrak{m}$-adic system and tensoring with E gives $\mathcal{F}_U$. Here of course we are using the standard abuse of terminology, according to which a "lisse sheaf of E vector spaces" is actually an inverse system of twisted constant, constructible sheaves of $\mathcal{O}_E/\mathfrak{m}^n$-modules, up to torsion.)

Conversely, given a lisse sheaf of E vector spaces on some non-empty open subset U of $\mathcal{C}$, taking the stalk at $\overline{\eta}$ yields a continuous representation of G. These constructions set up an equivalence of categories between lisse sheaves of E vector spaces on U and continuous representations of $\pi_1(U, \overline{\eta})$ on finite dimensional E vector spaces. (We refer to [SGA4$\frac{1}{2}$, [Rapport] §2] or [Mil80, I.5, II.1, and V.1] for more details, and [SGA4, VII, VIII, IX] plus [SGA5, V, VI] for many more details.)

Given τ as above, form $\mathcal{F}_U$ and set $\mathcal{F}_\tau = j_*\mathcal{F}_U$. Note that $j^*\mathcal{F}_\tau = \mathcal{F}_U$. If $j' : V \hookrightarrow U$ is a smaller Zariski open set, then it follows easily from the definitions that $j'_*\mathcal{F}_V \cong \mathcal{F}_U$ and so $\mathcal{F}_\tau$ is independent of the choice of U.

7.1.2. A "middle extension" sheaf of E vector spaces on $\mathcal{C}$ is a constructible sheaf $\mathcal{F}$ of E vector spaces for the étale topology such that: (i) there exists a non-empty Zariski open $j : U \hookrightarrow \mathcal{C}$ such that $j^*\mathcal{F}$ is lisse; and (ii) for one (and thus any) such U, $j_*j^*\mathcal{F} \cong \mathcal{F}$. The preceding subsection describes a functor from the category of finite dimensional continuous representations of G on vector spaces over E ramified only at a finite set of places to the category of middle extension sheaves of E vector spaces on $\mathcal{C}$. This functor is an equivalence of categories whose quasi-inverse sends a sheaf $\mathcal{F}$ to its geometric generic stalk $\mathcal{F}_{\overline{\eta}}$ equipped with the natural action of G.

7.1.3. Suppose $\mathcal{C}' \to \mathcal{C}$ is an étale Galois cover and $\mathcal{F}$ is the middle extension sheaf on $\mathcal{C}'$ corresponding to a representation τ of the fundamental group of $\mathcal{C}'$. If $g \in \pi_1(\mathcal{C}, \overline{\eta})$, then g induces an automorphism $g : \mathcal{C}' \to \mathcal{C}'$. We have that $g^*\mathcal{F}$ is the middle extension sheaf corresponding to the representation τ^g, defined by $\tau^g(h) = \tau(ghg^{-1})$. We will apply this remark below in the case where $\mathcal{C}' = \mathcal{C} \times \mathbb{F}_{q^n}$ and g is a lift of the geometric Frobenius under $\pi_1(\mathcal{C}, \overline{\eta}) \twoheadrightarrow \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

7.1.4. Some caution is required when applying standard constructions of linear algebra (such as $\otimes$ and Hom) in the category of middle extension sheaves. For example, it is not true in general that $\mathcal{F}_{\tau_1\otimes\tau_2} \cong \mathcal{F}_{\tau_1}\otimes\mathcal{F}_{\tau_2}$. What is true is that if $j : U \hookrightarrow \mathcal{C}$ is a Zariski open such that τ_1 and τ_2 factor through $\pi_1(U,\overline{\eta})$, then $\mathcal{F}_{\tau_1\otimes\tau_2} \cong j_*\left(j^*(\mathcal{F}_{\tau_1})\otimes j^*(\mathcal{F}_{\tau_2})\right)$. In what follows we will be explicit about constructions like this one.

7.1.5. If $\mathcal{F}$ is a constructible ℓ-adic sheaf on a scheme X we write $H^i(X,\mathcal{F})$ and $H^i_c(X,\mathcal{F})$ for the cohomology and cohomology with compact supports of X with coefficients in $\mathcal{F}$. There is a natural "forget supports" morphism $H^i_c(X,\mathcal{F}) \to H^i(X,\mathcal{F})$ which in general is neither injective nor surjective.

If $\mathcal{F}_\tau$ is the middle extension sheaf on $\mathcal{C}$ attached to a representation τ of G unramified over U and $\overline{U} = U\times\overline{\mathbb{F}}_q$, then one has that $H^0(\overline{\mathcal{C}},\mathcal{F}_\tau) = H^0(\overline{U},\mathcal{F}_U)$ is the $G_\infty = \mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_qF)$-invariants in the representation space of τ. If U is affine (i.e., a proper subset of X), then $H^2(\overline{U},\mathcal{F}_U) = 0$. By Poincaré duality, $H^0_c(\overline{U},\mathcal{F}_U) = 0$ and $H^2_c(\overline{U},\mathcal{F}_U)$ is the G_∞-coinvariants of τ, with $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ action twisted by $E(-1)$.

The following lemma is well-known but I know of no convenient reference for the proof.

7.1.6. **Lemma.** *Let τ be a representation of G as above which is unramified over the open $j : U \hookrightarrow \mathcal{C}$. Form the sheaves $\mathcal{F}_U$ and $\mathcal{F}_\tau = j_*\mathcal{F}_U$. Then $j^* : H^1(\overline{\mathcal{C}},\mathcal{F}_\tau) \to H^1(\overline{U},\mathcal{F}_U)$ is injective and*

$$j^*\left(H^1(\overline{\mathcal{C}},\mathcal{F}_\tau)\right) = \mathrm{Im}\left(H^1_c(\overline{U},\mathcal{F}_U) \to H^1(\overline{U},\mathcal{F}_U)\right).$$

Proof. Consider the Leray spectral sequences for j with and without compact supports. The exact sequences of low degree terms and the "forget supports" maps yield a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(\overline{\mathcal{C}},\mathcal{F}_\tau) & \xrightarrow{a=j^*} & H^1(\overline{U},\mathcal{F}_U) & \longrightarrow & H^0(\overline{\mathcal{C}},R^1\mathcal{F}_\tau) \\
 & & \uparrow{\scriptstyle b} & & \uparrow{\scriptstyle c} & & \\
0 & \longrightarrow & H^1_c(\overline{\mathcal{C}},R^0_c\mathcal{F}_\tau) & \xrightarrow{d=j^*} & H^1_c(\overline{U},\mathcal{F}_U) & \longrightarrow & H^0_c(\overline{\mathcal{C}},R^1_cj_*\mathcal{F}_U).
\end{array}$$

In particular, $j^* : H^1(\overline{\mathcal{C}},\mathcal{F}_\tau) \to H^1(\overline{U},\mathcal{F}_U)$ is injective. Since j is quasi-finite and separated, $R^1_cj_*\mathcal{F}_U = 0$ and so d is an isomorphism. On the other hand, we have an exact sequence of constructible sheaves on $\overline{\mathcal{C}}$

$$0 \to j_!\mathcal{F}_U \to \mathcal{F}_\tau \to i_*i^*\mathcal{F}_\tau \to 0$$

where $i : Z \hookrightarrow \mathcal{C}$ is the complement of U. Since j is étale, $R^0_cj_*\mathcal{F}_U = j_!\mathcal{F}_U$ and so taking cohomology with compact supports yields an exact sequence

$$H^1_c(\overline{\mathcal{C}},j_!\mathcal{F}) \to H^1_c(\overline{\mathcal{C}},\mathcal{F}_\tau) \to H^1_c(\overline{\mathcal{C}},i_*i^*\mathcal{F}_\tau).$$

But $i_*i^*\mathcal{F}_\tau$ is a skyscraper sheaf and so $H^1_c(\overline{\mathcal{C}},i_*i^*\mathcal{F}_\tau) = 0$. This shows that b is surjective. Thus we have $\mathrm{Im}(a) = \mathrm{Im}(ab) = \mathrm{Im}(cd) = \mathrm{Im}(c)$, as desired. □

7.1.7. It follows from the lemma and Poincaré duality that if τ is self-dual of some weight w then $H^1(\overline{\mathcal{C}},\mathcal{F}_\tau)$ is self-dual of weight $w+1$, i.e., we have a perfect pairing of representations of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$

$$H^1(\overline{\mathcal{C}},\mathcal{F}_\tau)\times H^1(\overline{\mathcal{C}},\mathcal{F}_\tau) \to E(-w-1).$$

If τ is orthogonally (resp. symplectically) self-dual, then $H^1(\overline{\mathcal{C}}, \mathcal{F}_\tau)$ is symplectically (resp. orthogonally) self-dual.

7.1.8. Let $\mathcal{F} = \mathcal{F}_\rho$ be the middle extension sheaf on $\mathcal{C}$ corresponding to the representation ρ fixed in Subsection 3.1. The Grothendieck-Lefschetz trace formula computes the L function of the representation ρ in terms of the cohomology of the sheaf $\mathcal{F}$. More precisely,

$$L(\rho, F, T) = \prod_{i=0}^{2} \det\left(1 - Fr\, T | H^i(\overline{\mathcal{C}}, \mathcal{F}_\rho)\right)^{(-1)^{i+1}}$$

where as usual Fr is the geometric (q^{-1}-power on $\overline{\mathbb{F}}_q$) Frobenius endomorphism of $\overline{\mathcal{C}}$. The cohomology groups are finite dimensional E vector spaces and so the L-function is a rational function in T. When ρ is irreducible and geometrically non-trivial (or more generally a direct sum of geometrically non-trivial irreducibles), the groups $H^i(\overline{\mathcal{C}}, \mathcal{F}_\rho)$ vanish for $i = 0, 2$ and the L-function is a polynomial in T.

7.1.9. Now assume that o is an orbit of multiplication by q^n on $(\mathbb{Z}/d\mathbb{Z})^\times$ and $f \in X(\mathbb{F}_{q^n}) \subset F_n^\times$. Then $\rho \otimes \sigma_{o,f}$ is semisimple as a representation of G_n and also semisimple when restricted to G_∞. By our choice of D defining X, $\sigma_{o,f}$ is totally ramified at at least one place where $\mathcal{F}$ is lisse and so $\rho \otimes \sigma_{o,f}$ does not contain the trivial representation when restricted to G_∞. Thus we have

$$L(\rho \otimes \sigma_{o,f}, F_n, T) = \det\left(1 - Fr^n\, T | H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\sigma_{o,f}})\right).$$

As we saw in Lemma 3.2.6, if $o = -o$, then $\sigma_{o,f}$ is orthogonally self-dual and so if ρ is self-dual, then so is $\rho \otimes \sigma_{o,f}$, with the same sign as ρ. In particular, if ρ is orthogonally self-dual (of weight $w = -1$), then $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\sigma_{o,f}})$ is symplectically self-dual and so the L-function has even degree in T and satisfies the functional equation

$$L(\rho \otimes \sigma_{o,f}, F_n, T) = L(\rho \otimes \sigma_{o,f}, F_n, 1/T)$$

in other words, the root number $W(\rho \otimes \sigma_{o,f}, F_n) = 1$.

7.1.10. Recall from Lemma 3.2.4 that if $f \in F_n^\times$, o is an orbit of multiplication by q^n on $(\mathbb{Z}/d\mathbb{Z})^\times$, and $a_o = \#o$, then when restricted to G_{na_o}, $\sigma_{o,f} \cong \oplus_{i\in o}\chi_f^i$. This implies that as sheaves on $\mathcal{C} \times \mathbb{F}_{q^{na_o}}$

$$\mathcal{F}_{\rho\otimes\sigma_{o,f}} \cong \oplus_{i\in o}\mathcal{F}_{\rho\otimes\chi_f^i}$$

Similarly, since $\sigma_{o,f} \cong \mathrm{Ind}_{G_{na_o}}^{G_n} \chi_f^i$ for any $i \in o$ (Lemma 3.2.5), we have

$$\mathcal{F}_{\rho\otimes\sigma_{o,f}} \cong b_*\mathcal{F}_{\rho\otimes\chi_f^i}$$

where $b : \mathcal{C} \times \mathbb{F}_{q^{na_o}} \to \mathcal{C}$ is the natural projection.

By the remark in 7.1.3 and Lemma 3.2.2, if Φ is an element of G lifting the geometric Frobenius of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, then

$$\Phi^*\mathcal{F}_{\rho\otimes\chi_f^i} \cong \mathcal{F}_{(\rho\otimes\chi_f^i)^\Phi} \cong \mathcal{F}_{\rho\otimes\chi_f^{iq}}.$$

7.1.11. We can now give the proof of Proposition 4.2.1. In light of 7.1.9 and our assumption that ρ has weight $w = -1$, what is to be proven is that all of the a_o-th roots of $-\operatorname{sgn}(\rho)$ appear as eigenvalues of Fr^n on $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\sigma_{o,f}})$. (Here $\operatorname{sgn}(\rho)$ is 1 if ρ is orthogonally self-dual and -1 if it is symplectically self-dual.) Since

$$H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\sigma_{o,f}}) \cong \oplus_{i\in o} H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^i})$$

and $(\chi_f^i)^{Fr^n} = \chi_f^{iq^n}$, the matrix of Fr^n is a block permutation matrix, i.e., has the form

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & A_{iq^{n(a_o-1)}} \\ A_i & 0 & 0 & \cdots & 0 \\ 0 & A_{iq^n} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{7.1.11.1}$$

where A_j is the matrix of $Fr^n : H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^j}) \to H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^{jq^n}})$. This implies that the eigenvalues of Fr^n are all of the a_o-th roots of the eigenvalues of Fr^{na_o}. (I.e., if $P_{Fr^n}(T)$ and $P_{Fr^{na_o}}(T)$ are the characteristic polynomials of Fr^n and Fr^{na_o} on $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\sigma_{o,f}})$ and $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^i})$, then $P_{Fr^n}(T) = P_{Fr^{na_o}}(T^{a_o})$.) Thus we must show that $-\operatorname{sgn}(\rho)$ is an eigenvalue of Fr^{na_o} on $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^i})$.

We assumed that ρ is self-dual of weight $w = -1$. Since $\sigma_{o,f}$ is orthogonally self-dual, $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\sigma_{o,f}})$ is literally self-dual (i.e., self-dual of weight 0), of sign opposite to that of ρ. Moreover, the subspaces $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^i})$ and $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^{-i}})$ are put in duality by the restriction of the form.

Let us fix bases of each $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^i})$ such that for all i the chosen basis of $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^i})$ is dual to that of $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^{-i}})$. Then in the matrix 7.1.11.1, the self-duality implies that $A_{iq^{j+a_o/2}} = (A_{iq^j})^\vee$ for $0 \le j < a_o/2$ and $A_i = -\operatorname{sgn}(\rho)(A_{iq^{a_o/2}})^\vee$ where $A^\vee$ denotes the inverse transpose of A.

Thus, the matrix of Fr^{na_o} on $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho\otimes\chi_f^i})$ is

$$-\operatorname{sgn}(\rho)(A^\vee_{iq^{a_o/2-1}} \cdots A_i^\vee)(A_{iq^{a_o/2-1}} \cdots A_i) = -\operatorname{sgn}(\rho) B^\vee B$$

where $B = A_{iq^{a_o/2-1}} \cdots A_i$. The first part of the following lemma then finishes the proof.

7.1.12. **Lemma.** *Consider invertible $N \times N$ matrices B over an infinite field and let $B^\vee$ denote the inverse transpose of B. If N is odd then for every B, $B^\vee B$ has 1 as an eigenvalue; moreover, given $\alpha \neq 1$ in the ground field, there exists a B such that the multiplicity of 1 as an eigenvalue of $B^\vee B$ is 1 and α is not an eigenvalue of $B^\vee B$. If N is even, for any α there exists a B such that α is not an eigenvalue of $B^\vee B$. All of the above remains true of we restrict to matrices B having any fixed non-zero determinant.*

Proof. First, note that $(B^\vee B)^t = B^t B^{-1}$ and $(B^\vee B)^{-1} = B^{-1} B^t$. This implies that $(B^\vee B)^{-1}$ is conjugate to $(B^\vee B)^t$, which, by the Jordan form, is conjugate to $B^\vee B$. Thus the set of eigenvalues of $B^\vee B$ is invariant under $\lambda \mapsto \lambda^{-1}$. On the other hand, the product of the eigenvalues of $B^\vee B$ is $\det(B^\vee B) = 1$. If N is odd, this implies that at least one of the eigenvalues must be 1.

For the existence assertions, we may build up a suitable B using 2×2 blocks of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

Indeed, these matrices have determinant a and the eigenvalues of

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{\vee} \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b/a \\ -b & 1 - b^2/a \end{pmatrix}$$

vary with b and avoid 1 and α for suitable b. □

7.2. **Globalization.** Our next task is to define for each orbit o of multiplication by q on $(\mathbb{Z}/d\mathbb{Z})^{\times}$ a sheaf $\mathcal{G}_o$ on X whose stalk at a geometric point over $f \in X(\mathbb{F}_{q^n})$ is the cohomology group $H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho \otimes \sigma_{o,f}})$. We will use several constructions and results from [Kat02, Chaps. 5 and 6]. There are some errors in Chapter 5, which Katz has addressed. We refer to his web site (`http://www.math.princeton.edu/~nmk`) for a corrected version.

7.2.1. Consider the product $X \times \mathcal{C}$ with its two projections π_1 and π_2 to X and $\mathcal{C}$ respectively. On the product $X \times \mathcal{C}$ we have a "universal rational function" F_{univ}, characterized by the formula $F_{univ}(f, p) = f(p)$. The divisor of poles of F_{univ} is $D \times \mathcal{C}$, its divisor of zeroes is finite étale over X (via π_1) of degree equal to $\deg D$ and the divisor of zeroes of F_{univ} is disjoint from its divisor of poles.

Let $\mathcal{D} \subset X \times \mathcal{C}$ be the reduced divisor whose support is the union of the divisor of F_{univ} and $X \times (\mathcal{C} \setminus U)$ where $j : U \hookrightarrow \mathcal{C}$ is a Zariski open subset over which ρ is unramified. Also let $\tilde{j} : V = (X \times \mathcal{C}) \setminus \mathcal{D} \hookrightarrow X \times \mathcal{C}$ be the inclusion.

7.2.2. Let $\lambda : \mathcal{X} \to X \times \mathcal{C}$ be the normalization of $X \times \mathcal{C}$ in the field extension $\mathbb{F}_q(X \times \mathcal{C})(F_{univ}^{1/d})$ of $\mathbb{F}_q(X \times \mathcal{C})$. Clearly λ has degree d and is étale over $V \subset X \times \mathcal{C}$.

7.2.3. Let $\underline{E}$ denote the constant sheaf on $\mathcal{X}$ with stalk E and consider $\lambda_* \underline{E}$ and its restriction $\tilde{j}^* \lambda_* \underline{E}$ to V. Since λ is étale of degree d over V, $\tilde{j}^* \lambda_* \underline{E}$ is lisse of rank d. The argument of Lemma 3.2.4 applies in this situation and we have a factorization

$$\tilde{j}^* \lambda_* \underline{E} \cong \bigoplus_{o \subset \mathbb{Z}/d\mathbb{Z}} \Sigma_o$$

where the sum is over orbits of multiplication by q on $\mathbb{Z}/d\mathbb{Z}$ and Σ_o is a lisse sheaf of E-vector spaces on V of rank $\#o$.

7.2.4. After a small base extension, Σ_o becomes isomorphic to a sum of rank 1 lisse sheaves. More precisely, the base change of λ to $\mathbb{F}_q(\mu_d)$, i.e.,

$$\mathcal{X} \times \mathbb{F}_q(\mu_d) \to X \times \mathcal{C} \times \mathbb{F}_q(\mu_d),$$

is Galois with Galois group naturally identified with $\mu_d(\overline{F})$ by $\sigma \mapsto \sigma(F_{univ}^{1/d})/F_{univ}^{1/d}$. Composing with an isomorphism $\mu_d(\overline{F}) \to \mu_d(E)$ (the same one we used in 3.2.1), we get a character $\chi_{F_{univ}}$ which is unramified over V. We let $\mathcal{L}_{univ}^i$ be the rank 1 lisse sheaf on $V \times \mathbb{F}_q(\mu_d)$ corresponding to $\chi_{F_{univ}}^i$. We note that $\mathcal{L}_{univ}^i$ in fact descends to $V \times \mathbb{F}_q(\mu_{d_o})$ where as before $d_o = d/\gcd(d, i)$ for any $i \in o$.

With these notations, we have a factorization

$$\Sigma_o|_{V \times \mathbb{F}_q(\mu_{d_o})} \cong \bigoplus_{i \in o} \mathcal{L}_{univ}^i$$

of lisse sheaves of E-vector spaces on $V \times \mathbb{F}_q(\mu_{d_o})$. (This is the global version of the factorization at the end of Lemma 3.2.4.)

Similarly, globalizing Lemma 3.2.5, we have

$$\Sigma_o = b_*(\mathcal{L}^i_{univ})$$

for any $i \in o$, where b is the projection $X \times \mathbb{F}_q(\mu_{d_o}) \to X$.

Globalizing Lemma 3.2.2 and 7.1.3, we have $Fr^*(\mathcal{L}^i_{univ}) \cong \mathcal{L}^{iq}_{univ}$.

Globalizing Lemma 3.2.6, we have that Σ_o is self-dual if and only if $-o = o$, in which case it is orthogonally self-dual of weight 0.

7.2.5. Recall that π_1 and π_2 denote the projections from $X \times \mathcal{C}$ to X and $\mathcal{C}$ respectively. Let μ be the restriction of π_1 to V. We define

$$\mathcal{G}_{o,*} = R^1\mu_* \left((\tilde{j}^* \pi_2^* \mathcal{F}_\rho) \otimes \Sigma_o \right)$$

and

$$\mathcal{G}_{o,!} = R^1\mu_! \left((\tilde{j}^* \pi_2^* \mathcal{F}_\rho) \otimes \Sigma_o \right).$$

Since $\deg(D) > 2g+1$, the arguments of [Kat02, 5.2.1 and 6.2.10] show that these are lisse sheaves on X whose formation is compatible with arbitrary change of base.

7.2.6. There is a natural "forget supports" morphism $\mathcal{G}_{o,!} \to \mathcal{G}_{o,*}$ and we define $\mathcal{G}_o$ to be the image of this morphism. Again by [Kat02, 5.2.1 and 6.2.10], $\mathcal{G}_o$ is lisse of formation compatible with arbitrary change of base and by Deligne [Del80, 3.2.3], it is ι-pure of weight 0.

By standard base change results, the stalk of $\mathcal{G}_o$ at a geometric point $\overline{f}$ over $f \in X(\mathbb{F}_{q^n})$ is

$$\mathcal{G}_{o,\overline{f}} \cong \mathrm{Im}\left(H^1_c(\overline{U}, j^*\mathcal{F}_\rho \otimes j^*\mathcal{F}_{\sigma_{o,f}}) \to H^1(\overline{U}, j^*\mathcal{F}_\rho \otimes j^*\mathcal{F}_{\sigma_{o,f}}) \right)$$

where $j : U \hookrightarrow \mathcal{C}$ is a Zariski open over which ρ is unramified and f is regular and non-zero. By Lemma 7.1.6, this is

$$H^1(\overline{\mathcal{C}}, j_*(j^*\mathcal{F}_\rho \otimes j^*\mathcal{F}_{\sigma_{o,f}})) = H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho \otimes \sigma_{o,f}}).$$

7.2.7. By 7.1.9,

$$\begin{aligned} L(\rho \otimes \sigma_{o,f}, F_n, T) &= \det\left(1 - Fr^n T \,|\, H^1(\overline{\mathcal{C}}, \mathcal{F}_{\rho \otimes \sigma_{o,f}})\right) \\ &= \det\left(1 - Fr_{n,f} T \,|\, \mathcal{G}_{o,\overline{f}}\right). \end{aligned}$$

Thus we may study the L-functions $L(\rho \otimes \sigma_{o,f}, F_n, T)$ for every $f \in X(\mathbb{F}_{q^n})$ by studying the sheaf $\mathcal{G}_o$.

7.2.8. We have variants of $\mathcal{G}_o$ over a small base extension of X. More precisely, if $i \in o$ and we work over $\mathbb{F}_q(\mu_{d_o})$ then we can define

$$\begin{aligned} \mathcal{G}_{i,*} &= R^1\mu_* \left((\tilde{j}^* \pi_2^* \mathcal{F}_\rho) \otimes \mathcal{L}^i_{univ} \right), \\ \mathcal{G}_{i,!} &= R^1\mu_! \left((\tilde{j}^* \pi_2^* \mathcal{F}_\rho) \otimes \mathcal{L}^i_{univ} \right), \end{aligned}$$

and

$$\mathcal{G}_i = \mathrm{Im}\left(\mathcal{G}_{o,!} \to \mathcal{G}_{o,*} \right).$$

(Here we are abusing abusing notation slightly by using μ, $\tilde{j}$ and π_2 to denote various maps to and from $X \times \mathcal{C} \times \mathrm{Spec}\, \mathbb{F}_q(\mu_{d_o})$.) By arguments similar to those

mentioned above, we have that $\mathcal{G}_i$ is lisse and its stalk at a geometric point over $f \in X(\mathbb{F}_{q^n})$ is $H^1(\mathcal{C} \times \overline{\mathbb{F}}_q, \mathcal{F}_{\rho \otimes \chi_f^i})$.

The Grothendieck-Ogg-Shafarevitch formula says that the rank of $\mathcal{G}_i$ is

$$(2g_{\mathcal{C}} - 2)(\deg \rho) + \deg \operatorname{Cond}(\rho \otimes \chi_f^i).$$

Because we assumed $\deg(D)$ is large (cf. 6.4 (e)), [Kat02, 5.3.6] says that $\mathcal{G}_i$ is irreducible and [Kat02, 5.5.1 and 5.7.1] say that $\mathcal{G}_i$ is self-dual on $\overline{X}$ if and only if $\mathcal{F}$ is self dual and $i = d/2$, in which case its sign is the opposite of that of $\mathcal{F}$.

7.2.9. Over $X \times \mathbb{F}_q(\mu_d)$, $\mathcal{G}_o$ factors. More precisely, we have

$$b^* \mathcal{G}_o = \oplus_{i \in o} \mathcal{G}_i$$

and

$$\mathcal{G}_o = b_* \mathcal{G}_i$$

for any $i \in o$, where $b : X \times \mathbb{F}_q(\mu_{d_o}) \to X$ is the projection. Also, $Fr^*(\mathcal{G}_i) \cong \mathcal{G}_{iq}$.

7.2.10. **Proposition.** *Write $\overline{X}$ for $X \times \overline{\mathbb{F}}_q$. Then we have*

(1) $\mathcal{G}_i \cong \mathcal{G}_j$ on $\overline{X}$ if and only if $i \equiv j \pmod{d}$
(2) $\mathcal{G}_i \cong \mathcal{G}_j^\vee$ on $\overline{X}$ if and only if $\mathcal{F}$ is self-dual (of weight $w = -1$) and $i \equiv -j \pmod{d}$.

More generally, if $f : Y \to \overline{X}$ is a connected, finite, étale cover, then $f^*\mathcal{G}_i$ and $f^*\mathcal{G}_j$ are isomorphic (resp. dual) if and only if $i \equiv j \pmod{d}$ (resp. $\mathcal{F}$ is self-dual (of weight $w = -1$) and $i \equiv -j \pmod{d}$).

7.3. **Corollary.** *The lisse sheaf $\mathcal{G}_o$ on X is irreducible. It is self-dual if and only if $o = -o$ and $\mathcal{F}$ is self-dual (of weight $w = -1$) on $\overline{X}$ (and thus by our assumptions self-dual on X). In this case $\mathcal{G}_o$ is orthogonally self-dual if $\mathcal{F}$ is symplectically self-dual and $\mathcal{G}_o$ is symplectically self-dual if $\mathcal{F}$ is orthogonally self-dual.*

Proof of Corollary 7.3. We have $\mathcal{G}_o = b_* \mathcal{G}_i$ where $b : X \times \mathbb{F}_q(\mu_{d_o}) \to X$ is the natural projection. But $\mathcal{G}_i$ is irreducible (see 7.2.8) and $Fr^{j*}(\mathcal{G}_i) \ncong \mathcal{G}_i$ unless $iq^j \cong i$ (by Proposition 7.2.10), so it follows from Mackey's criterion that $\mathcal{G}_o$ is irreducible.

It is also clear that if $\mathcal{F}$ is self-dual (of weight $w = -1$) and $-o = o$, then $\mathcal{G}_o$ is self-dual on X with the asserted sign.

Suppose then that $\mathcal{G}_o$ is self-dual on X. On $\overline{X}$ we have $\mathcal{G}_o \cong \oplus_{i \in o} \mathcal{G}_i$ and $\mathcal{G}_o^\vee \cong \oplus_{j \in o} \mathcal{G}_j^\vee$. Since each $\mathcal{G}_i$ is irreducible we must have $\mathcal{G}_i \cong \mathcal{G}_j^\vee$ for some $j \in o$. Then by Proposition 7.2.10, $\mathcal{F}$ is self-dual and $j = -i$. This holds for every $i \in o$, so $-o = o$. □

Proof of Proposition 7.2.10. The "if" parts of both statements are trivial. The proofs of the converses rely heavily on the details of the proofs in [Kat02], especially those in Chapter 5, not just the results themselves.

We work throughout on $\overline{\mathcal{C}} = \mathcal{C} \times \operatorname{Spec} \overline{\mathbb{F}}_q$ and $\overline{X} = X \times \operatorname{Spec} \overline{\mathbb{F}}_q$. Since we have assumed that the degree of D is large (cf. hypothesis (e) on $\deg(D)$ in 6.4), by [Kat02, 5.4.8], we may write $D = D_1 + D_2$ where the D_i satisfy several conditions. If $p > 2$, the conditions are:

- $\deg(D_1) \geq 2g + 2$
- $\deg(D_2) \geq 2g + 1$
- the coefficients of D_2 are invertible modulo p

- If $D = \sum a_i P_i$ (where the P_i are distinct $\overline{\mathbb{F}}_q$ points of $\mathcal{C}$) and $a_i > 2$, then $P_i \in |D_2|$
- if $4|d$ then $2\deg(D_1) < 2g_{\mathcal{C}} - 2 + \deg(D) - 2\deg(|\mathfrak{n}| \setminus |D_2|)$
- if $4|d$ and $g_{\mathcal{C}} = 0$ then in addition $\deg(D_2) \geq 2$.

If $p = 2$, the conditions are:

- $\deg(D_i) \geq 6g_{\mathcal{C}} + 3$
- the coefficients of D_2 are odd
- If $D = \sum a_i P_i$ (where the P_i are distinct $\overline{\mathbb{F}}_q$ points of $\mathcal{C}$) and $a_i > 2$, then $P_i \in |D_2|$.

We write $L(D_i)$ for $H^0(\overline{\mathcal{C}}, \mathcal{O}_{\overline{\mathcal{C}}}(D_i))$. Fix a function $f_1 \in L(D_1)$ which has distinct zeroes, all of which are disjoint from $|\mathfrak{n}| \cup |D|$. (It is elementary that the set of such functions f_1 is dense in $L(D_1)$; cf. [Kat02, 5.0.6].) Consider functions $f_2 \in L(D_2)$ which satisfy the following conditions: (i) f_2 has distinct zeroes, all of which are disjoint from $|\mathfrak{n}| \cup |D| \cup f_1^{-1}(0)$; (ii) the ramification of f_2 is minimal in the following strong sense: if $p > 2$ then all of the zeroes of the differential df are simple zeroes and if $p = 2$, then all of the zeroes of df have multiplicity exactly 2; and (iii) f_2 separates the points in

$$S = \left(\{\text{zeroes of } df_2\} \cup f_1^{-1}(0) \cup |D| \cup |\mathfrak{n}|\right) \setminus |D_2|$$

i.e., each $s \in S$ is the only element of S in its fiber $f_2^{-1}(f_2(s))$. Theorems 2.2.6 and 2.4.2 of [Kat02] guarantee that the set of f_2 satisfying these restrictions is a dense open subset of $L(D_2)$.

The map F defined by $F(t) = f_1(t - f_2)$ defines a morphism from the open subset $U = \mathbb{A}^1 \setminus S$ of the affine line over $\overline{\mathbb{F}}_q$ (with coordinate t) to $\overline{X}$. Proposition 5.3.7 of [Kat02] says that we can almost recover $\mathcal{F}$ from $\mathcal{G}_i$ via F and [Kat02, Thm. 5.4.9] gives a reasonably complete description of the ramification of $F^*(\mathcal{G}_i)$ on $\mathbb{P}^1 \setminus U$. More precisely, we have an isomorphism of perverse sheaves on U

$$F^*(\mathcal{G}_i)[1] \cong \left(f_{2*}j_{2*}j_1^*(\mathcal{F} \otimes \mathcal{L}_{\chi^i(f_1)})\right)[1] *_{mid,+} j_*\mathcal{L}_{\chi^i}[1]$$

where $j_i : \overline{\mathcal{C}} \setminus |D| \hookrightarrow \overline{\mathcal{C}} \setminus |D_i|$ and $j : \mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} \hookrightarrow \mathbb{A}^1$ are the natural inclusions and $*_{mid,+}$ is the middle additive convolution (for which we refer to [Kat02, Chapter 4]). If $\mathcal{G}_i \cong \mathcal{G}_j$ and $i \not\equiv j \pmod d$ we deduce an isomorphism

$$\left(f_{2*}j_{2*}j_1^*(\mathcal{F} \otimes \mathcal{L}_{\chi^i(f_1)})\right)[1] \cong \left(f_{2*}j_{2*}j_1^*(\mathcal{F} \otimes \mathcal{L}_{\chi^j(f_1)})\right)[1] *_{mid,+} j_*\mathcal{L}_{\chi^{j-i}}[1].$$

Now if $p > 2$ there is a point t of $\mathbb{A}^1$ so that $f_2 : \overline{\mathcal{C}} \to \mathbb{A}^1$ is ramified, with ramification index $e = 2$ at exactly one point over t and is unramified at the others and so that $\mathcal{F} \otimes \mathcal{L}_{\chi^i(f_1)}$ and $\mathcal{F} \otimes \mathcal{L}_{\chi^j(f_1)}$ are unramified at all points over t. Let $\mathcal{H}_i \cong f_{2*}j_{2*}j_1^*(\mathcal{F} \otimes \mathcal{L}_{\chi^i(f_1)})$, viewed as a representation of $I(t)$, the inertia group at t, and similarly for $\mathcal{H}_j$. Then, using a superscript to denote invariants, $\mathcal{H}_i/\mathcal{H}_i^{I(t)} \cong \mathcal{H}_j/\mathcal{H}_j^{I(t)}$ and these representations are spaces of dimension $\operatorname{Rank}\mathcal{F}$ on which $I(t)$ acts by a non-trivial character of order 2. But $\mathcal{H}_j$ is in the class $\mathcal{P}_{conv}$ (see [Kat02, 4.0]) and so by [Kat02, 4.1.10(1a)] we have

$$\mathcal{H}_i/\mathcal{H}_i^{I(t)} \cong \mathcal{H}_j/\mathcal{H}_j^{I(t)} \otimes \mathcal{L}_{\chi^{j-i}(x-t)}$$

as $I(t)$ representations. This obviously contradicts the assumption $i \not\equiv j \pmod d$ which concludes the proof of part (1) when $p > 2$.

The argument for $p = 2$ is similar, but we have to contend with wild ramification. In this case, there is a point t of $\mathbb{A}^1$ so that $f_2 : \overline{\mathcal{C}} \to \mathbb{A}^1$ is ramified, with

ramification index $e = 2$ and df_2 vanishing to order exactly 2 at exactly one point over t and is unramified at the others and so that $\mathcal{F} \otimes \mathcal{L}_{\chi^i(f_1)}$ and $\mathcal{F} \otimes \mathcal{L}_{\chi^j(f_1)}$ are unramified at all points over t. Then, with $\mathcal{H}_i$ and $\mathcal{H}_j$ defined as before, we have that $\mathcal{H}_i/\mathcal{H}_i^{I(t)}$ has dimension $\operatorname{Rank}\mathcal{F}$ and $I(t)$ acts through a character of Swan conductor 1 (see [Kat02, 2.7.1]); moreover, the character only depends on f_2, not on i. Applying [Kat02, 4.1.10 and 4.2.1], we have that $F^*(\mathcal{G}_i)/F^*(\mathcal{G}_i)^{I(t)} \cong \chi^{2i}\rho$ as $I(t)$ representations, where ρ is a character of 2-power order and Swan conductor 1. Thus if $\mathcal{G}_i \cong \mathcal{G}_j$ we have $\chi^{2i}\rho \cong \chi^{2j}\rho'$ where ρ and ρ' have 2-power order. Since d is prime to $p = 2$, we conclude that $i \equiv j \pmod{d}$.

We now turn to the proof of part (2) of the proposition. Let us temporarily denote the sheaf $\mathcal{G}_i$ constructed from $\mathcal{F}$ as $\mathcal{G}(\mathcal{F}, i)$, so that our hypothesis is that $\mathcal{G}(\mathcal{F}, i) \cong \mathcal{G}(\mathcal{F}, j)^\vee$. Since $\mathcal{G}(\mathcal{F}, j)^\vee \cong \mathcal{G}(\mathcal{F}^\vee, -j)$, our hypothesis is equivalent to $\mathcal{G}(\mathcal{F}, i) \cong \mathcal{G}(\mathcal{F}^\vee, -j)$. The argument proving the first part of the proposition does not use much about $\mathcal{F}$; more precisely, the only information about $\mathcal{F}$ we use is the support of its Artin conductor. Since $\mathcal{F}$ and $\mathcal{F}^\vee$ have the same Artin conductor, the argument generalizes immediately to prove that $i \cong -j \pmod{d}$. Thus it remains to show that $\mathcal{G}(\mathcal{F}, i) \cong \mathcal{G}(\mathcal{F}^\vee, i)$ implies that $\mathcal{F} \cong \mathcal{F}^\vee$. To that end, we choose functions f_1 and f_2 satisfying the same hypotheses as before. Let

$$\mathcal{H} = j_{2*}j_1^*(\mathcal{F} \otimes \mathcal{L}_{\chi^i(f_1)})$$

and

$$\mathcal{H}' = j_{2*}j_1^*(\mathcal{F}^\vee \otimes \mathcal{L}_{\chi^i(f_1)}).$$

As representations $\operatorname{Gal}(\overline{F}/F)$, $\mathcal{H}$ and $\mathcal{H}'$ are irreducible and by assumption we have

$$f_{2*}\mathcal{H}[1] *_{mid,+} j_*\mathcal{L}_{\chi^i}[1] \cong f_{2*}\mathcal{H}'[1] *_{mid,+} j_*\mathcal{L}_{\chi^i}[1]$$

which implies $f_{2*}\mathcal{H} = f_{2*}\mathcal{H}'$.

Choose a point $t \in \mathbb{A}^1$ such that $f_2 : \mathcal{C} \to \mathbb{A}^1$ is unramified at every point over t, $\mathcal{F}$ is unramified at every point over t, and exactly one point of $f_1^{-1}(0)$, call it s_0, lies over t. Then $\mathcal{H}$ is ramified at s_0 and unramified at the other points over t; more precisely, as a representation of $I(s_0)$, the inertia group at s_0, $\mathcal{H}$ is isomorphic to a direct sum of $\operatorname{Rank}\mathcal{F}$ copies of $\mathcal{L}_{\chi^i(f_1)}$, on which $I(s_0)$ acts by a non-trivial character of finite order. The same is true of $\mathcal{H}'$. Now we have inclusions

$$\mathcal{H} \hookrightarrow f_2^*f_{2*}\mathcal{H} \cong f_2^*f_{2*}\mathcal{H}' \hookleftarrow \mathcal{H}'$$

Since the sheaves $\mathcal{H}$ and $\mathcal{H}'$ are irreducible, their images in the middle either coincide or are linearly independent. But we can see that the latter is impossible by noting that as a representation of $I(s_o)$, $f_2^*f_{2*}\mathcal{H}$ has an unramified subspace of codimension $\operatorname{Rank}\mathcal{F}$. Since, as representations of $I(s_0)$, $\mathcal{H}$ and $\mathcal{H}'$ are both totally ramified of dimension $\operatorname{Rank}\mathcal{F}$, there is not enough room in $f_2^*f_{2*}\mathcal{H}$ for them to be linearly independent. Thus we have an isomorphism $\mathcal{H} \cong \mathcal{H}'$. Since j_1 and j_2 are open immersions and $\mathcal{F}$ is a middle extension, it follows immediately that $\mathcal{F} \cong \mathcal{F}^\vee$. This completes the proof of part (2) of the proposition.

For the "more generally," suppose $f : Y \to \overline{X}$ is a connected, finite, étale cover such that $f^*\mathcal{G}_i$ is isomorphic to $f^*\mathcal{G}_j$. Choose functions f_1 and f_2 and define S as above, let $F : U = \mathbb{A}^1 \setminus S \to \overline{X}$ be defined by $F(t) = f_2(t - f_1)$, and let $g : V \to U$ be the pull back of $f : Y \to \overline{X}$ to U. We may choose the f_i so that V is connected. The proofs of [Kat02, 1.5.1 and 1.7.1] (applied in the context of [Kat02, 5.4.9 or 5.6.2]) show that each $F^*\mathcal{G}_i$ is "Lie irreducible" i.e., it remains irreducible when restricted to any connected, finite, étale cover of U. Considering the action

of $\pi_1(U)$ on $\mathrm{Hom}_V(g^*F^*\mathcal{G}_i, g^*F^*\mathcal{G}_j)$, which is 1-dimensional by Schur's lemma, we see that there exists a rank 1 lisse sheaf $\mathcal{L}_\psi$ (with associated character ψ of $\pi_1(U)$) such that $F^*\mathcal{G}_i \cong F^*\mathcal{G}_j \otimes \mathcal{L}_\psi$.

We are going to use the nature of the ramification of $\mathcal{G}_i$ and $\mathcal{G}_j$ to show that such a ψ must be trivial. First of all, ψ is unramified on $U = \mathbb{A}^1 \setminus S$. Since we assumed that $\mathcal{F}$ is tame at all places in $|D|$, $F^*\mathcal{G}_i$ and $F^*\mathcal{G}_j$ are tame at $\infty \in \mathbb{P}^1$ and so ψ must be tame there as well. At each place in S, the stalk of $F^*\mathcal{G}_i$, viewed as representation of the local inertia group, is the direct sum of a ramified representation of some dimension e and some copies of the trivial representation and we always have the inequality $e \leq r = \mathrm{Rank}\,\mathcal{F}$. But $N_i = \mathrm{Rank}\,\mathcal{G}_i$ is large (at least $(2g-2+\deg(D))\,\mathrm{Rank}\,\mathcal{F}$) and so $N_i > 2e$. Similarly for $F^*\mathcal{G}_j$. This implies that ψ must be unramified at every place in S. Thus ψ is a character of $\pi_1(U)$ which is unramified at every place of $S = \mathbb{P}^1 \setminus (U \cup \{\infty\})$ and which is tame at ∞. Since $\mathbb{A}^1$ is "tamely simply connected" (i.e., $\pi_1^{\mathrm{tame}}(\mathbb{A}^1) = 0$), we must have that ψ is trivial. This means that $F^*\mathcal{G}_i$ and $F^*\mathcal{G}_j$ are already isomorphic on U which implies, by the argument of part (1), that $i \cong j \pmod d$.

The argument when $f^*\mathcal{G}_i$ is dual to $f^*\mathcal{G}_j$ is quite similar and will be omitted. This completes the proof of the proposition. □

8. Monodromy groups

8.1. **Definitions.** As usual, we write $\overline{X}$ for $X \times \overline{\mathbb{F}}_q$. If $i \in \mathbb{Z}/d\mathbb{Z}$, set $X_i = X \times \mathbb{F}_q(\mu_{d/(d,i)})$. In the previous section we defined sheaves $\mathcal{G}_o$ on X for each orbit $o \subset \mathbb{Z}/d\mathbb{Z}$ of multiplication by q and $\mathcal{G}_i$ on X_i for each $i \in \mathbb{Z}/d\mathbb{Z}$ and we proved that $\mathcal{G}_o \cong \oplus_{i\in o}\mathcal{G}_i$ on X_i and that $Fr^*(\mathcal{G}_i) \cong \mathcal{G}_{iq}$.

These sheaves can be viewed as representations of various fundamental groups. More precisely, fix a geometric generic point $\overline{\eta}$ of $\overline{X}$; we also write $\overline{\eta}$ for the induced geometric generic points of X_i and X. Consider the arithmetic and geometric fundamental groups

$$\pi_1(\overline{X}, \overline{\eta}) \subset \pi_1(X_i, \overline{\eta}) \subset \pi_1(X, \overline{\eta}).$$

All three groups act on the stalk at $\overline{\eta}$ of $\mathcal{G}_o$ and the two smaller groups act on the stalk at $\overline{\eta}$ of $\mathcal{G}_i$, so we have homomorphisms

$$\tau_o : \pi_1(X, \overline{\eta}) \to \mathrm{Aut}(\mathcal{G}_{o,\overline{\eta}})$$

and

$$\tau_i : \pi_1(X_i, \overline{\eta}) \to \mathrm{Aut}(\mathcal{G}_{i,\overline{\eta}}).$$

Here $\mathrm{Aut}(\mathcal{G}_{o,\overline{\eta}})$ is viewed as the set of E points of an algebraic group over E, isomorphic of course to $\mathrm{GL}_{\mathrm{Rank}\,\mathcal{G}_o}$, and similarly with $\mathrm{Aut}(\mathcal{G}_{i,\overline{\eta}})$. The isomorphism $Fr^*(\mathcal{G}_i) \cong \mathcal{G}_{iq}$ implies that if $\Phi \in \pi_1(X, \overline{\eta})$ is an element inducing the geometric (q^{-1}-power) Frobenius automorphism of $\overline{\mathbb{F}}_q$, then $\tau_i^\Phi \cong \tau_{iq}$.

We define the arithmetic monodromy group G_o^{arith} to be the Zariski closure of the image of τ_o and the geometric monodromy group G_o^{geom} to be the Zariski closure of $\tau_0(\pi(\overline{X}, \overline{\eta}))$. Similarly, G_i^{arith} is by definition the Zariski closure of the image of τ_i and G_i^{geom} is by defintion the Zariski closure of $\tau_i(\pi(\overline{X}, \overline{\eta}))$. Deligne proved [Del80, 1.3.9] that G_o^{geom} and G_i^{geom} are (not necessarily connected) semisimple algebraic groups over E. We will prove below that (after a suitable twist) the indices of $G_o^{\mathrm{geom}} \subset G_o^{\mathrm{arith}}$ and $G_i^{\mathrm{geom}} \subset G_i^{\mathrm{arith}}$ are finite, so the arithmetic groups are also semisimple.

8.2. **Katz' monodromy calculation.** The main theorem of [Kat02] is a calculation of the groups G_i^{geom}. Under the hypotheses of Sections 3.1 and 6.4-6.5 and Theorem 5.2 (in particular, ρ is everywhere tame or tame at places in S_r and $p > \deg\rho + 2$, and $\deg(D)$ is large), we have that G_i^{geom} is isomorphic to:

$$\begin{cases} \mathrm{Sp}(N_i) & \text{if } d/i = 2 \text{ and } \mathcal{F} \text{ is orthogonally self-dual} \\ \mathrm{O}(N_i) \text{ or } \mathrm{SO}(N_i) & \text{if } d/i = 2 \text{ and } \mathcal{F} \text{ is symplectically self-dual} \\ \mathrm{SL}^{(\nu_i)}(N_i) & \text{if } d/i \neq 2 \text{ or } \mathcal{F} \text{ is not self-dual.} \end{cases}$$

([Kat02, 5.5.1 case (1b) and 5.7.1] Here N_i is the rank of $\mathcal{G}_i$, $\mathrm{GL}(N_i)$, $\mathrm{Sp}(N_i)$, $\mathrm{O}(N_i)$, and $\mathrm{SO}(N_i)$ refer to the standard general linear, symplectic, orthogonal, and special orthogonal groups over E, and

$$\mathrm{SL}^{(\nu_i)}(N_i) = \{g \in \mathrm{GL}(N_i) | (\det g)^{\nu_i} = 1\}.$$

In the second case, if N_i is odd, then $G_i^{\mathrm{geom}} = \mathrm{O}(N_i)$. Note that the connected component of G_i^{geom} is either $\mathrm{Sp}(N_i)$, $\mathrm{SO}(N_i)$, or $\mathrm{SL}(N_i)$.

8.3. **Structure of $G_o^{\mathbf{geom},0}$.** In this subsection we apply the results of Katz to determine the connected component of the algebraic group G_o^{geom}. If $o = \{i\}$, then G_o^{geom} was already determined by Katz, as in the previous subsection. So for the rest of this subsection we assume that $\#o > 1$ and thus $d_o > 2$. Because of the decomposition $\mathcal{G}_o \cong \prod_{i\in o} \mathcal{G}_i$ on $\overline{X}$, we have

$$G_o^{\mathrm{geom}} \subset \prod_{i\in o} \mathrm{Aut}(\mathcal{G}_i) \cong \prod_{i\in o} \mathrm{GL}(N_i).$$

Let $p_i : G_o^{\mathrm{geom}} \to \mathrm{Aut}(\mathcal{G}_i)$ be the projection onto the i-th factor. It is elementary from the definitions that $p_i(G_o^{\mathrm{geom}})$ is contained in G_i^{geom}. Since this image is Zariski dense and the image of a morphism of algebraic groups is closed [Bor91, I.1.4a], we have $p_i(G_o^{\mathrm{geom}}) = G_i^{\mathrm{geom}}$. It follows from [Bor91, I.1.4b] that $p_i(G_o^{\mathrm{geom},0}) = G_i^{\mathrm{geom},0} \cong \mathrm{SL}(N_i)$ where the superscript 0 indicates the connected component of the identity.

8.3.1. **Proposition.** *Let o be an orbit of multiplication by q on $\mathbb{Z}/d\mathbb{Z}$.*

(1) If $\mathcal{F}$ is not self-dual on $\overline{X}$ or if $o \neq -o$ then the projections p_i induce an isomorphism

$$G_o^{geom,0} \cong \prod_{i\in o} G_i^{geom,0} \cong \prod_{i\in o} \mathrm{SL}(N_i).$$

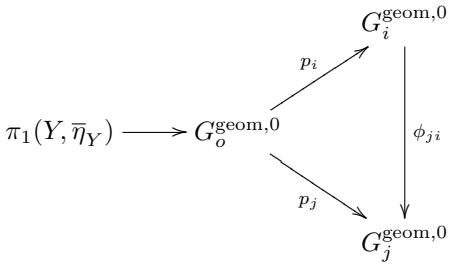
(2) If $\mathcal{F}$ is self dual on $\overline{X}$ and $o = -o$, let $S \subset o$ be a set of representatives for o modulo ± 1. Then the projections p_i induce an isomorphism

$$G_o^{geom,0} \cong \prod_{i\in S} G_i^{geom,0} \cong \prod_{i\in S} \mathrm{SL}(N_i).$$

If $j \notin S$ then in terms of suitable bases, the projection $p_j : G_o^{geom,0} \to G_i^{geom,0}$ sends a tuple of matrices $(A_i)_{i\in S}$ to $A_{-j}^{\vee} = {}^t(A_{-j})^{-1}$.

Proof. Let $\mathfrak{g}_o$ and $\mathfrak{g}_i$ denote the Lie algebras of $G_o^{\mathrm{geom},0}$ and $G_i^{\mathrm{geom},0}$, which are semisimple. The projections p_i induce surjections $dp_i : \mathfrak{g}_o \to \mathfrak{g}_i \cong sl(N_i)$. Let $\mathfrak{h}_i' = \ker dp_i$. Since $\mathfrak{g}_o$ is semisimple, we have a decomposition $\mathfrak{g}_o = \mathfrak{h}_i \oplus \mathfrak{h}_i'$ where $\mathfrak{h}_i$ is an ideal mapping isomorphically onto $\mathfrak{g}_i$. Now take $j \in o$, $j \not\equiv i \pmod d$ and consider dp_j restricted to $\mathfrak{h}_i$, so that $dp_j|_{\mathfrak{h}_i} : \mathfrak{h}_i \to \mathfrak{g}_j$. The source and target of

this homomorphism are both simple (they are both isomorphic to $sl(N_i)$) so $p_j|_{\mathfrak{h}_i}$ is either 0 or an isomorphism. Let us suppose for a moment that it is an isomorphism and define $d\phi_{ji} = dp_j \circ (dp_i|_{\mathfrak{h}_i})^{-1} : \mathfrak{g}_i \tilde{\to} \mathfrak{g}_j$. Since $\mathrm{SL}(N_i)$ is simply connected we may integrate $d\phi_{ji}$ to an isomorphism $\phi_{ji} : G_i^{\mathrm{geom},0} \to G_j^{\mathrm{geom},0}$. Let $Y \to \overline{X}$ be the finite étale cover which trivializes $\det \mathcal{G}_i$ for all $i \in o$ and let $\overline{\eta}_Y$ be a geometric generic point of Y. Then we have a commutative diagram



Now it is well known that the only automorphisms of SL are inner or inner composed with $A \mapsto A^\vee = {}^tA^{-1}$. (This follows easily from the Lie algebra version, which is [Jac79, Chap. IX, Thm. 5, p. 283].) Thus if $dp_j|_{\mathfrak{h}_i}$ is an isomorphism, then τ_i and τ_j become isomorphic or contragredient over Y; equivalently, $\mathcal{G}_i$ and $\mathcal{G}_j$ become isomorphic or dual on Y. But Proposition 7.2.10, the first case is impossible ($j \not\equiv i$) and the second is impossible unless $j \equiv -i$ and $\mathcal{F}$ is self-dual. Thus, under the hypotheses of (1), $p_j|_{\mathfrak{h}_i}$ must be zero for all $i \not\equiv j$. From this we easily conclude that $\mathfrak{g}_o \cong \prod_{i\in o} \mathfrak{g}_i$. This implies that the projections p_i induce a local isomorphism $G_o^{\mathrm{geom},0} \to \prod_{i\in o} G_i^{\mathrm{geom},0}$ and since the target is simply connected, they in fact induce an isomorphism. This concludes the proof of (1).

Under the hypotheses of (2), $dp_j|_{\mathfrak{h}_i}$ is zero if $j \not\equiv -i$ and we know (by the trivial part of Proposition 7.2.10) that if $j \equiv -i$ then $dp_j|_{\mathfrak{h}_i}$ is an isomorphism. As in part (1), we easily conclude that the dp_i induce an isomorphism $\mathfrak{g}_o \cong \prod_{i\in S} \mathfrak{g}_i$ and thus the p_i induce an isomorphism $G_o^{\mathrm{geom},0} \cong \prod_{i\in S} G_i^{\mathrm{geom},0}$. Also, there is an isomorphism ϕ_{ji} as in the displayed equation above, and since $i \not\equiv j$, this isomorphism is not inner, so in terms of suitable bases it is $A_i \mapsto A_i^\vee$. This completes the proof of the proposition. □

The last sentence of the proposition can also be deduced by explicit matrix calculations, as in 8.6 below.

8.4. **Structure of G_o^{geom}.** Let Φ_o^{geom} and Φ_i^{geom} denote the groups of connected components of G_o^{geom} and G_i^{geom} respectively. By Katz' monodromy calculation, we have $\Phi_i^{\mathrm{geom}} \cong \mu_{\nu_i}$, the roots of unity of order ν_i for some integer ν_i. The isomorphism $\tau_i^\Phi \cong \tau_{iq}$ and the fact that $\pi_1(\overline{X}, \overline{\eta})$ is a normal subgroup of $\pi_1(X, \overline{\eta})$ imply that ν_i is independent of i for i running through a fixed orbit o; let ν_o denote the common value of the ν_i. Thus Φ_o^{geom} is a subgroup of $\prod_{i\in o} \Phi_i^{\mathrm{geom}} = \mu_{\nu_o}^{a_o}$; the isomorphism $\tau_i^\Phi \cong \tau_{iq}$ implies that this subgroup is invariant under cyclic permutation ($i \mapsto iq$) of the factors. Also, since $p_i(G_o^{\mathrm{geom}}) = G_i^{\mathrm{geom}}$, the projection p_i induces a surjection $\Phi_o^{\mathrm{geom}} \to \Phi_i^{\mathrm{geom}}$ for each i. So in all, we have that Φ_o^{geom} is a subgroup of $\prod_{i\in o} \mu_{\nu_o}^{a_o}$ which maps surjectively onto each factor and which is invariant under cyclic permutation of the factors.

8.5. **Arithmetic monodromy groups.** Our next goal is to determine the structure of the arithmetic monodromy group G_o^{arith} or rather of a twisted version of it. This will amount to determining its component group.

8.5.1. Given an ℓ-adic unit $\beta \in \mathcal{O}_E^\times$ there is a continuous Galois representation $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \to E^\times$ which sends Fr to β. We denote the corresponding lisse sheaf on $\operatorname{Spec}\mathbb{F}_q$, as well as its pull back to various schemes over $\mathbb{F}_q$, by $\beta^{\deg}$.

If we write $\mathcal{G}(\mathcal{F}, o)$ for the sheaf on X defined above using the sheaf $\mathcal{F}$ on $\mathcal{C}$ and the orbit $o \subset \mathbb{Z}/d\mathbb{Z}$, then the projection formula implies that we have a canonical isomorphism $\mathcal{G}(\mathcal{F} \otimes \beta^{\deg}, o) \cong \mathcal{G}(\mathcal{F}, o) \otimes \beta^{\deg}$ of sheaves on X. Define $G^{\mathrm{geom}}(\beta)$ and $G^{\mathrm{arith}}(\beta)$ to be the geometric and arithmetic monodromy groups associated to $\mathcal{G}(\mathcal{F}, o) \otimes \beta^{\deg}$. Since $\beta^{\deg}$ is trivial on $\overline{X}$ we have $G^{\mathrm{geom}}(\beta) = G^{\mathrm{geom}}$. On the other hand, $G^{\mathrm{arith}}(\beta)$ will in general differ from G^{arith}.

The connection with L-functions also changes: we have

$$\begin{aligned}\det\left(1 - T\,Fr_{n,f}\,\middle|\,(\mathcal{G}(\mathcal{F}, o) \otimes \beta^{\deg})_{\overline{f}}\right) &= \det\left(1 - \beta T\,Fr_{n,f}\,\middle|\,\mathcal{G}(\mathcal{F}, o)_{\overline{f}}\right)\\ &= L(F_n, \rho \otimes \sigma_{o,f}, \beta T)\end{aligned}$$

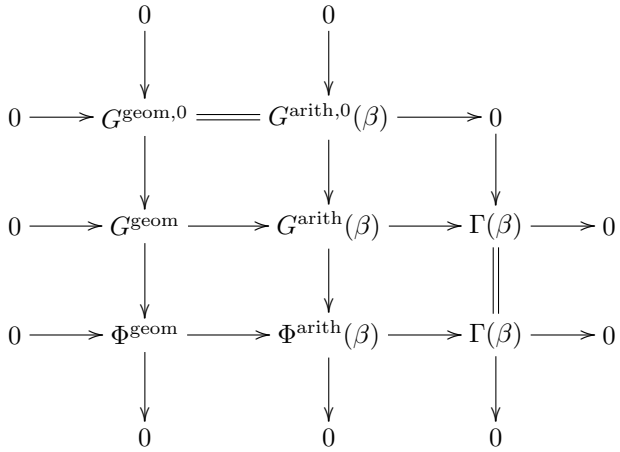
for all $f \in X(\mathbb{F}_{q^n})$.

8.5.2. For the rest of this section, we view $\mathcal{F}$ and o as being fixed and we drop them from the notation. Let $\Gamma(\beta)$ be defined as $G^{\mathrm{arith}}(\beta)/G^{\mathrm{geom}}(\beta)$ and consider the following commutative diagram, where the columns and rows are exact by definition.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & G^{\mathrm{geom},0} & \longrightarrow & G^{\mathrm{arith},0}(\beta) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & G^{\mathrm{geom}} & \longrightarrow & G^{\mathrm{arith}}(\beta) & \longrightarrow & \Gamma(\beta) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
 & & \Phi^{\mathrm{geom}} & \longrightarrow & \Phi^{\mathrm{arith}}(\beta) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

The next proposition says that for a suitable β, G^{geom} has finite index in $G^{\mathrm{arith}}(\beta)$ and so $G^{\mathrm{geom},0} = G^{\mathrm{arith},0}(\beta)$. Thus for such a β we can complete the diagram into

the following, where all rows and columns are exact:



8.5.3. **Proposition.** *Expanding E if necessary, there exists a $\beta \in \mathcal{O}_E^\times$ such that the conditions below hold.*

- *(a) The arithmetic monodromy group associated to $\mathcal{G}(\mathcal{F}, o) \otimes \beta^{deg}$ contains G_o^{geom} as a finite index subgroup, i.e., $\Gamma(\beta)$ is finite.*
- *(b) $\Gamma(\beta)$ is cyclic of order a_o or $2a_o$. Its order is $2a_o$ if and only if either (i) $a_o > 1$, $o = -o$, $\mathcal{F}$ is orthogonally self-dual, N_i is odd and ν_i is odd; or (ii) $o = \{d/2\}$, $\mathcal{F}$ is symplectically self-dual, $G^{geom} = \mathrm{SO}(N_{d/2})$ and $G^{arith} = \mathrm{O}(N_{d/2})$.*
- *(c) $\Phi^{arith}(\beta)$ is the semi-direct product $\Phi^{geom} \rtimes \Gamma(\beta)$ where the action of $\Gamma(\beta)$ on $\Phi^{geom} \subset \prod \mu_{\nu_o}$ is by cyclic permutation of the factors.*

If $\mathcal{F}$ is self-dual (of weight $w = -1$) on X and $o = -o$, then we may take $\beta = 1$.

Proof. First suppose that $\mathcal{F}$ is self-dual (of weight $w = -1$) and $o = \{d/2\}$. Then $\mathcal{G}(\mathcal{F}, o)$ self-dual and so G_o^{arith} is *a priori* contained in an orthogonal or symplectic group. But as we have seen, G_o^{geom} is the full symplectic group or contains the special orthogonal group, so (a), (b), and (c) are clear in this case.

Next, we make an observation about determinants. Let Φ be an element of $\pi_1(X, \overline{\eta})$ inducing the geometric Frobenius on $\overline{\mathbb{F}}_q$. Then since $\tau_i^\Phi \cong \tau_{iq}$, we have that $\det \tau_i(\Phi^{a_o}) = \det \tau_{iq}(\Phi^{a_o})$ and so $\det \tau_i(\Phi^{a_o})$ is independent of $i \in o$. This means that there is a $\beta \in \mathcal{O}_E^\times$ such that $\det\left(\tau_i \otimes \beta^{\deg}\right)(\Phi^{a_o}) = 1$ for all $i \in o$.

Now assuming that $o \neq \{d/2\}$ or $\mathcal{F}$ is not self-dual, we have seen that the groups $G^{\mathrm{geom},0}$ are all $\mathrm{SL}(N_i)$ and so $\left(\tau_o \otimes \beta^{\deg}\right)(\Phi^{a_o})$ lies in G^{geom}. Since $\left(\tau_o \otimes \beta^{\deg}\right)(\Phi)$ generates $\Gamma(\beta)$, this proves that $\Gamma(\beta)$ is finite cyclic of order dividing a_o, indeed of order exactly a_o since $\tau_o(\Phi)$ permutes the factors of $\mathcal{G}_o \cong \oplus_{i \in o} \mathcal{G}_i$ cyclically. It also shows that $\Phi^{\mathrm{arith}}(\beta)$ is a semi-direct product, i.e., the lower row of our diagram is split exact. That the action of $\Gamma(\beta)$ on Φ^{geom} is as asserted follows easily from the formula $\tau_i^\Phi \cong \tau_{iq}$.

This completes the proof of the proposition except in the case where $\mathcal{F}$ is self-dual (of weight $w = -1$), $a_o > 1$, and $o = -o$, in which case we insist that $\beta = 1$ and we have to show that Γ is finite of order a_o or $2a_o$. But under these hypotheses, $\mathcal{G}(\mathcal{F}, i)$ and $\mathcal{G}(\mathcal{F}, -i)$ are dual on X_i and so $\det \tau_i(\Phi^{a_o}) = (\det \tau_{-i}(\Phi^{a_o}))^{-1}$. Since $\det \tau_i(\Phi^{a_o})$ is independent of $i \in o$, this implies that these determinants are ± 1.

A matrix calculation (see 8.6 below) shows that this determinant is in fact 1 if $\mathcal{F}$ is symplectically self-dual, and it is $(-1)^{N_i}$ if $\mathcal{F}$ is orthogonally self-dual. In light of Proposition 8.3.1, this implies that $\tau_o(\Phi^{2a_o})$ lies in G_o^{geom} and $\tau_o(\Phi^{a_o})$ lies in G_o^{geom} except in the cases mentioned in part (2). This completes the proof of the proposition. □

Note that for β as in the proposition, the twisted sheaf $\mathcal{G}(\mathcal{F}\otimes\beta^{\deg}, o)$ is again ι-pure of weight 0.

8.6. **Reduced characteristic polynomials.** Let $\mathrm{GL}(N)$ denote the general linear group over some field and let $G\subset\mathrm{GL}(N)$ be a closed algebraic subgroup. We define the reduced characteristic polynomial function as follows. For each irreducible component of G, let $P_0(T)$ be the gcd of the (reversed) characteristic polynomials of the elements of that component. Then define $P_g^{\mathrm{red}}(T)$, the reduced characteristic polynomial of $g\in G$, to be the usual (reversed) characteristic polynomial, divided by the gcd P_0 for the component in which g lies. The key property of the reduced characteristic polynomial is that if α is any element of the ground field, then the set of $g\in G$ such that $P_g^{\mathrm{red}}(\alpha)=0$ is a Zariski closed subset which contains no irreducible components of G. In particular, if the field is $\mathbb{C}$, this set has Haar measure zero.

Now we compute the reduced characteristic polynomials (or rather the gcd's P_0) for various components of the groups $G_o^{\mathrm{arith}}(\beta)\subset\mathrm{GL}(\mathcal{G}_o\otimes\beta^{\deg})$.

8.6.1. If $o=\{d/2\}$ and $\mathcal{F}$ is orthogonally self-dual, then $G^{\mathrm{arith}}=\mathrm{Sp}(N_{d/2})$ and $P_0(T)=1$.

8.6.2. If $o=\{d/2\}$ and $\mathcal{F}$ is symplectically self-dual, then G^{arith} is either $\mathrm{SO}(N_{d/2})$ or $\mathrm{O}(N_{d/2})$. In the former case $N_{d/2}$ is necessarily even (see 8.2) and so $P_0(T)=1$. In the latter, there are two cases depending on the parity of $N_{d/2}$. If $N_{d/2}$ is even, $P_0(T)$ is 1 on $\mathrm{SO}(N_{d/2})$ and $1-T^2$ on $\mathrm{O}_-(N_{d/2})$. If $N_{d/2}$ is odd, $P_0(T)$ is $1-T$ on $\mathrm{SO}(N_{d/2})$ and $1+T$ on $\mathrm{O}_-(N_{d/2})$.

8.6.3. Next we consider the case where $o\neq -o$ or $\mathcal{F}$ is not self-dual. Here we claim that $P_0(T)=1$ on every component of G_o^{arith}. Recall that components of G_o^{arith} are indexed by tuples $((\zeta_i)_{i\in o}, b)$ where $(\zeta_i)\in\prod_{i\in S}\mu_{\nu_o}$ and $b\in\mathbb{Z}/a_o\mathbb{Z}$. For convenience, we prove the assertion only for components where b is a generator of a_o; the other cases are similar but would require more notational complexity. Let us fix $j\in o$ and a basis of $\mathcal{G}_{j,\overline{\eta}}$. We extend this to a basis of $\mathcal{G}_{o,\overline{\eta}}$ by applying $\tau_o(\Phi^b), \tau_o(\Phi^{2b}), \dots$ to the original basis. In terms of this basis, the matrix of an element g of the component indexed by $((\zeta_i)_{i\in o}, b)$ is a "block cyclic permutation matrix," i.e., it has the form

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & A_{jq^{a_o-1}} \\ A_j & 0 & 0 & \cdots & 0 \\ 0 & A_{jq} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

where the blocks are $N_o\times N_o$ and $\det A_i=\zeta_i$ for all $i\in o$. Moreover, as g varies through the component, the matrices A_i vary (independently) over all matrices with these determinants. (This comes from Proposition 8.3.1 above.) It follows easily that $P_0(T)=1$.

8.6.4. Finally, we consider the case where $o = -o$, $a_o > 1$, and $\mathcal{F}$ is self-dual (of weight $w = -1$) and we restrict to components indexed by $((\zeta_i)_{i\in o}, b)$ where b is prime to a_o. In this case, we claim that if N_o is even, then $P_0(T) = 1$ on every such component whereas if N_o is odd, $P_0(T) = (1 - T^{a_o})$ if $\mathcal{F}$ is symplectically self-dual and $P_0(T) = (1 + T^{a_o})$ if $\mathcal{F}$ is orthogonally self-dual.

It will be convenient to argue with matrices. (This is essentially the same argument as in 7.1.11.) Choosing a basis as above, elements g of the component indexed by $((\zeta_i)_{i\in o}, b)$ are block cyclic permutation matrices, as above, but as we will see, there are relations among the A_i. To see this, note that the matrix of the form on $\mathcal{G}_{o,\overline{\eta}}$) (which is orthogonal resp. symplectic if $\mathcal{F}$ is symplectically resp. orthogonally self-dual) is

$$\begin{pmatrix} 0 & I_{N_o a_0/2} \\ \epsilon I_{N_o a_0/2} & 0 \end{pmatrix}$$

where $I_{N_o a_0/2}$ denotes the identity matrix of size $N_o a_o/2$ and $\epsilon = -\operatorname{sgn}(\rho)$, i.e., $\epsilon = 1$ if ρ is symplectically self-dual and -1 if it is orthogonally self-dual. Writing out the condition that g respects the form, we find that $A_{-jq^{kb}} = A^{\vee}_{jq^{kb}}$ for $k = 0, \dots, a_o/2 - 2$ and $A_{-q^{(a_o/2-1)b}} = \epsilon A^{\vee}_{-q^{(a_o/2-1)b}}$. By Proposition 8.3.1, other than these restrictions, the matrices vary freely among those with determinants (ζ_i).

Now since the matrix of g is block cyclic permutation, its eigenvalues are all of the a_o-th roots of those of g^{a_o}. The matrix calculation above shows that the matrix of g^{a_o} is block diagonal with blocks of the form

$$\epsilon A^{\vee}_{jq^{(a_o/2-1)b}} A^{\vee}_{jq^{(a_o/2-2)b}} \cdots A^{\vee}_{j} A_{jq^{(a_o/2-1)b}} A_{jq^{(a_o/2-2)b}} \cdots A_j$$

which is of the form $\epsilon B^{\vee} B$. (To tie up a loose end in Proposition 8.5.3, note that these blocks have determinant ϵ^{N_o}.) By Lemma 7.1.12, if N is odd, all the matrices $B^{\vee}B$ have 1 as an eigenvalue, generically of multiplicity 1 and have no other shared eigenvalues. If N is even then there are no shared eigenvalues. This completes the proof of our claims about $P_0(T)$.

9. Equidistribution

In this section we fix the sheaf $\mathcal{F}$ and the orbit o and then choose a β as in Proposition 8.5.3. We will drop this data from the notation and so just write G^{arith} and G^{geom} for the arithmetic and geometric monodromy groups attached to $\mathcal{G}(\mathcal{F}, o) \otimes \beta^{\deg}$. Also, Γ will denote $G^{\mathrm{arith}}/G^{\mathrm{geom}}$.

9.1. **Maximal compact subgroups.** Using the embedding $E \hookrightarrow \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ we may extend scalars and define semisimple algebraic groups $G^{\mathrm{arith}}_{/\mathbb{C}}$ and $G^{\mathrm{geom}}_{/\mathbb{C}}$ over $\mathbb{C}$. Let $G^{\mathrm{arith}}(\mathbb{C})$ and $G^{\mathrm{geom}}(\mathbb{C})$ denote their complex points, which we regard as complex semisimple Lie groups.

We will denote by K^{arith} and K^{geom} maximal compact subgroups of $G^{\mathrm{arith}}(\mathbb{C})$ and $G^{\mathrm{geom}}(\mathbb{C})$. By Weyl's "unitarian trick," K^{arith} is Zariski dense in $G^{\mathrm{arith}}_{/\mathbb{C}}$ and so $K^{\mathrm{arith}}/K^{\mathrm{geom}} \cong G^{\mathrm{arith}}/G^{\mathrm{geom}} \cong \Gamma$ is a finite cyclic group. Also, the group of components of K^{arith} and K^{geom} are the same as those of G^{arith} and G^{geom}.

We define the reduced characteristic polynomials $P^{\mathrm{red}}_k(T)$ for $k \in K^{\mathrm{arith}}$ as in 8.6 above (dividing the usual reversed characteristic polynomial by the gcd of the characteristic polynomials over each connected component). Again because K^{arith} is Zariski dense in $G^{\mathrm{arith}}_{/\mathbb{C}}$, the reduced characteristic polynomials for K^{arith} are

just the restrictions of the reduced characteristic polynomials from G^{arith} (via the embedding ι).

9.2. **Haar measures.** Fix an element $\gamma \in \Gamma \cong K^{\mathrm{arith}}/K^{\mathrm{geom}}$ and let $K^{\mathrm{arith}}_\gamma$ denote the inverse image of γ in K^{arith}. We denote the set of conjugacy classes of K^{arith} which meet $K^{\mathrm{arith}}_\gamma$ by $K^{\mathrm{arith},\#}_\gamma$; since Γ is abelian, this is just the quotient of $K^{\mathrm{arith}}_\gamma$ by the conjugation action of K^{geom}.

Let $d\mu_{\mathrm{Haar},\gamma}$ be the K^{geom}-translation invariant measure on $K^{\mathrm{arith}}_\gamma$ of total mass 1. (We may take the left or right invariant measure as either is bi-invariant.) Let $d\mu^{\#}_{\mathrm{Haar},\gamma}$ be its push-forward onto $K^{\mathrm{arith},\#}_\gamma$. The main equidistribution statement will be that a suitably normalized sum of point masses corresponding to Frobenius elements converges to the measure $d\mu^{\#}_{\mathrm{Haar},\gamma}$.

9.3. **Frobenius classes.** Let f be an element of $X(\mathbb{F}_{q^n})$ and denote as usual a corresponding Frobenius element (defined up to conjugacy) by $Fr_{n,f} \in \pi_1(X, \overline{\eta})$. The monodromy representation τ_o gives us an element (up to conjugacy) $\tau_o(Fr_{n,f}) \in G^{\mathrm{arith}}(E) \hookrightarrow G^{\mathrm{arith}}(\mathbb{C})$ and we denote its "semi-simple part" (obtained from a Jordan form by throwing away the off-diagonal terms) by $\tau_o(Fr_{n,f})^{ss}$. Because $\mathcal{G}(\mathcal{F}, o) \otimes \beta^{\deg}$ is ι-pure of weight 0, the eigenvalues of $\tau_o(Fr_{n,f})^{ss}$ lie on the unit circle, and so $\tau_o(Fr_{n,f})^{ss}$ is conjugate to an element of K^{arith}. The K^{arith}-conjugacy class of this element is well-defined and we denote it by $\theta(f, n)$.

Note that the image of $\tau_o(Fr_{n,f})$ in $\Gamma = G^{\mathrm{arith}}/G^{\mathrm{geom}}$ (which we have seen is $\mathbb{Z}/a_o\mathbb{Z}$ or $\mathbb{Z}/2a_o\mathbb{Z}$) is just the class γ of n. Thus as f varies through $X(\mathbb{F}_{q^n})$, the classes $\theta(f, n)$ all lie in the set of classes of K^{arith} over a fixed element $\gamma \in \Gamma$, i.e., in $K^{\mathrm{arith},\#}_\gamma$.

9.4. **Equidistribution.** For each integer n we have the finite set of points $X(\mathbb{F}_{q^n})$ and the corresponding conjugacy classes $\theta(f, n)$ in $K^{\mathrm{arith},\#}$. We define a measure $d\mu_n$ on the set of conjugacy class $K^{\mathrm{arith},\#}$ by averaging the point masses at the various classes $\theta(f, n)$ for $f \in X(\mathbb{F}_{q^n})$. Thus, if ϕ is a class function on K^{arith},

$$\int_{K^{\mathrm{arith},\#}} \phi \, d\mu_n = \frac{1}{\#X(\mathbb{F}_{q^n})} \sum_{f \in X(\mathbb{F}_{q^n})} \phi(\theta(f, n)).$$

Note that this measure is supported on $K^{\mathrm{arith},\#}_\gamma$ where γ is the class of n in Γ.

The basic equidistribution statement is that the measures $d\mu_n$ converge weakly to $d\mu^{\#}_{\mathrm{Haar},\gamma}$ as $n \to \infty$ through a fixed class in Γ. In other words, if ϕ is a continuous class function on K^{arith}, we have

$$\lim_{\substack{n\to\infty \\ [n]=\gamma}} \int_{K^{\mathrm{arith},\#}} \phi \, d\mu_n = \int_{K^{\mathrm{arith},\#}} \phi \, d\mu^{\#}_{\mathrm{Haar},\gamma} \tag{9.4.1}$$

This result is [KS99, 9.7.10] (with $S = \operatorname{Spec} \mathbb{F}_q$) which is a mild generalization of [Del80, 3.5.3].

9.5. **Good test functions.** We will apply the equidistribution statement 9.4.1 to a well-chosen test function to conclude that for large enough n, there are many $f \in X(\mathbb{F}_{q^n})$ such that a given α is not a root of the reduced characteristic polynomial $P^{\mathrm{red}}_{\theta(f,n)}$.

Let $K^{\mathrm{arith}}_\alpha$ denote the subset of elements $k \in K^{\mathrm{arith}}$ where $P^{\mathrm{red}}_k(\alpha) = 0$. This is a Zariski closed subset which is a proper subset of each component of K^{arith}.

9.5.1. **Proposition.** *For every $\epsilon > 0$ there exist smooth class functions $f_\alpha : K^{arith} \to \mathbb{R}$ indexed by $\alpha \in S^1$ such that*

(a) $0 \leq f_\alpha(k) \leq 1$ for all $k \in K^{arith}$, all $\alpha \in S^1$.
(b) For all $\alpha \in S^1$, $f_\alpha(k) = 1$ for all $k \in K^{arith}_\alpha$.
(c) There exists n_0 such that for each $\gamma \in \Gamma$ and all $n > n_0$ in the class of γ, $\int_{K^{arith,\#}_\gamma} f_\alpha \, d\mu_n < \epsilon$ for all $\alpha \in S^1$.

Proof. Let f_α be defined by the formula

$$f_\alpha(k) = e^{-C\left|P_k^{\mathrm{red}}(\alpha)\right|^2}$$

where P_k^{red} is the reduced characteristic polynomial of k and C is a positive real number. Clearly f_α is a smooth class function of k which satisfies the first two requirements of the proposition.

Because f_α vanishes on a proper Zariski closed subset of each component of K^{arith} (i.e., on a set of Haar measure zero) and S^1 is compact, we can choose one C so that

$$\int_{K^{\mathrm{arith},\#}_\gamma} f_\alpha \, d\mu^{\#}_{\mathrm{Haar},\gamma} < \epsilon/2$$

for all $\alpha \in S^1$.

Next, we claim that for sufficiently large n,

$$\left| \int_{K^{\mathrm{arith},\#}_\gamma} f_\alpha \, d\mu_n - \int_{K^{\mathrm{arith},\#}_\gamma} f_\alpha \, d\mu^{\#}_{\mathrm{Haar},\gamma} \right| < \epsilon/2$$

for all $\alpha \in S^1$. For a fixed α, this is just our equidistribution statement 9.4.1. Again by the compactness of S^1, there is one n_0 so that the displayed inequaltiy holds for all $n > n_0$ in the class of γ and all $\alpha \in S^1$. Since Γ is finite, there is one n_0 that works for all γ.

Combining the two displayed inequalities shows that the functions f_α also satisfy the third requirement of the proposition. □

9.6. **Corollary.** *Let $X(\mathbb{F}_{q^n})_\alpha$ be the set of elements $f \in X(\mathbb{F}_{q^n})$ where $P^{red}_{\theta(f,n)}(\alpha)$ vanishes. Then for every $\epsilon > 0$ there exists an integer n_0 such that for $n > n_0$*

$$\frac{\#X(\mathbb{F}_{q^n})_\alpha}{\#X(\mathbb{F}_{q^n})} < \epsilon$$

Proof. Indeed, the fraction on the left hand side is bounded above by $\int_{K^\#} f_\alpha \, d\mu_n$ where f_α is the function appearing in the proposition. □

10. End of the proof of the main theorem

We are now in a position to prove the main technical theorem, Theorem 5.2. We first give the basic structure of the argument, then adapt it to the various cases, considering one orbit o at a time (i.e., part (1) of the theorem). Then we discuss the case of several orbits at once (i.e., part (2) of the theorem).

10.1. **The basic argument.** We are given data $\mathcal{C}$, ρ, d, S_s, S_i, S_r, and $(\alpha_n)_{n\geq 1}$ satisfying the hypotheses of 3.1. By twisting, we may assume that ρ has weight $w=-1$ and that the α_n all have ι-weight 0. The representation ρ gives rise to a middle extension sheaf $\mathcal{F}$ on $\mathcal{C}$. Fix $o\subset\mathbb{Z}/d\mathbb{Z}$, an orbit for multiplication by q. Then we choose a divisor D and local conditions $(S_n, C_{n,w})$ as described in 6.4-6.5. Using $\mathcal{C}$ and D, we construct the space X parameterizing certain degree d covers of $\mathcal{C}$ and the sheaf $\mathcal{G}(\mathcal{F},o)$. Then we choose an ℓ-adic unit β as in 8.5.3 and consider $\mathcal{G}(\mathcal{F}\otimes\beta^{\deg},o)$, as well as its arithmetic monodromy group G^{arith} and its compact form K^{arith}.

Proposition 6.3.1 guarantees that for all sufficiently large n, the density of points $f\in X(\mathbb{F}_{q^n})$ satisfying the local conditions imposed by $(S_n, C_{n,w})$ is bounded below by some positive constant C independent of n. Applying Corollary 9.6 with $\alpha=(\beta\alpha_n)^{-1}$ guarantees that for any $\epsilon>0$, for all sufficiently large n relatively prime to a_o, the density of points $f\in X(\mathbb{F}_{q^n})$ such that $P^{\text{red}}_{\theta(f,n)}((\beta\alpha_n)^{-1})\neq 0$ is at least $1-\epsilon$. Since

$$L(\rho\otimes\sigma_{f,o},F_n,T)=P_{\theta(f,n)}(\beta^{-1}T)=P^{\text{red}}_{\theta(f,n)}(\beta^{-1}T)\left(\frac{P_{\theta(f,n)}(\beta^{-1}T)}{P^{\text{red}}_{\theta(f,n)}(\beta^{-1}T)}\right)$$

the remainder of the argument consists of relating the exceptional situations to the specific choices of local conditions and the "forced zeroes," i.e., the inverse roots of $P_k(T)/P^{\text{red}}_k(T)$ for $k=\theta(f,n)\in K^{\text{arith}}$.

10.2. **The case where $o\neq -o$ or ρ is not self-dual.** In this case, by 8.6.3, $P_k(T)=P^{\text{red}}_k(T)$ for all $k\in K^{\text{arith}}$. Thus there are no "forced zeroes" and so the basic argument already proves part (1) of the theorem in this case.

10.3. **The case where $o=-o$, $a_o>1$, and ρ is self-dual.** In this case, by Proposition 8.5.3 we may take $\beta=1$. Let N_o be the rank of $\mathcal{G}_i$ for any $i\in o$. Then we have seen in 8.6.4 that if N_o is even then $P_k(T)=P^{\text{red}}_k(T)$ for all $k\in K^{\text{arith}}$, whereas if N_o is odd, then $P_k(T)=P^{\text{red}}_k(T)(1+\text{sgn}(\rho)T^{a_o})$ where $\text{sgn}(\rho)$ is -1 if ρ is symplectic and 1 if it is orthogonal. In particular, if N_o is even or if $\alpha_n^{a_o}\neq-\text{sgn}(\rho)$ then the basic argument already suffices.

If hypothesis 4.2.3.1 fails or if ρ has odd degree, then we have chosen D and (S_n, C_w) so that N_o is even. (These are the choices we made in 6.5.)

So let us assume that hypothesis 4.2.3.1 holds, ρ has even degree, and that $\alpha_n^{a_o}=-\text{sgn}(\rho)$, i.e., that we are in the exceptional situation of type (iii) or (iv). In these cases, $P_k(T)/P^{\text{red}}_k(T)=(1+\text{sgn}(\rho)T^{a_o})$ has α_n as inverse root to order exactly one.

This completes the proof of the theorem in the case appearing in the section title.

10.4. **The case where $o=\{d/2\}$ and $\mathcal{F}$ is self-dual.** The argument is quite similar to that in the previous subsection, with different adjustments for the exceptional cases.

If ρ is orthogonally self-dual, then the monodromy group G^{arith} is symplectic and so by 8.6.1, the ratio $P_k(T)/P^{\text{red}}_k(T)$ is 1.

From now on we assume that ρ is symplectically self-dual so that the monodromy group is an orthogonal group. By Proposition 8.5.3 we may assume $\beta=1$. If hypothesis 4.1.8.1 fails, then by 4.1.9 the signs in the functional equation vary as f varies. This implies that the arithmetic and geometric monodromy groups are both

$\mathrm{O}(N_o)$. But then our choice of local conditions in 6.5 forces $k = \theta(f, n)$ into the component ($\mathrm{SO}(N_o)$ or $\mathrm{O}_-(N_o)$) where α_n is not an inverse root of $P_k(T)/P_k^{\mathrm{red}}(T)$.

From now on, we also assume that hypothesis 4.1.8.1 holds, so that the sign in the functional equation is fixed for a fixed n and all $f \in X(\mathbb{F}_{q^n})$ satisfying the local conditions. Then there are four cases, depending on the parity of $N = N_o$ and the sign $W = W(\rho \otimes \chi_f, F_n)$ in the functional equation. More precisely, if N is even and $W = 1$, then $P_k(T)/P_k^{\mathrm{red}}(T) = 1$. If N is even and $W = -1$, then $P_k(T)/P_k^{\mathrm{red}}(T) = (1-T^2)$ and so if $\alpha_n = \pm 1$ (i.e., we are in an exceptional situation of type (i)), then α_n is a simple inverse root of $P_k(T)/P_k^{\mathrm{red}}(T)$. If N is odd then $P_k(T)/P_k^{\mathrm{red}}(T) = (1 + WT)$ and so if $\alpha_n \neq -W$, then α_n is not an inverse root of $P_k(T)/P_k^{\mathrm{red}}(T)$, whereas if $\alpha_n = -W$ (i.e., we are in an exceptional situation of type (ii)), then α_n is a simple inverse root of $P_k(T)/P_k^{\mathrm{red}}(T)$.

This completes the proof of the theorem in the case appearing in the section title, and thus the proof of all of part (1) of the theorem.

10.5. **Part (2) of Theorem 5.2.** The argument is similar to that for part (1). We choose D and local conditions $(S_n, C_{n,w})$ according to the recipe in 6.4 and the second paragraph of 6.5 and construct X and a sheaf $\mathcal{G}_o = \mathcal{G}(\mathcal{F}, o)$ on X for each orbit $o \subset \mathbb{Z}/d\mathbb{Z}$. Then we choose ℓ-adic units β_o as in 8.5.3 and consider $\mathcal{G}(\mathcal{F} \otimes \beta_o^{\deg}, o)$, its arithmetic monodromy group G_o^{arith}, and its compact form K_o^{arith}.

Applying Proposition 6.3.1 and Corollary 9.6, we find that for all sufficiently large n, there exists an element $f \in X(\mathbb{F}_{q^n})$ satisfying the local conditions imposed by $(S_n, C_{n,w})$ and such that for all o, $\beta_o \alpha_n$ is not an inverse root of $P_{\theta(f,n)}^{\mathrm{red}}(T)$. Thus we are reduced to considering the zeroes of $P_k(T)/P_k^{\mathrm{red}}(T)$ where $k = \theta(f, n)$.

In the exceptional situations of type (i)-(iv) and in the non-exceptional situations, the analysis is exactly as for part (1). The exceptional situations of type (v) and (vi) are like those of type (iii) and (iv), except that in the former, we assume that hypothesis 4.2.3.1 fails. We used this hypothesis to show, in Proposition 4.2.4, that *for one orbit* o, if 4.2.3.1 fails, we can choose local conditions so that the rank of $\mathcal{G}_o$ is even, and so $P_k(T)/P_k^{\mathrm{red}}(T) = 1$. But as we already remarked after 4.2.4, it is not possible in general to do this for several orbits o at once. In 6.5 we chose local conditions to handle possible trouble with the orbit $o = \{d/2\}$ (when d is even) and so we have no control over the orbits appearing in exceptional situations of types (v) and (vi). So in these situations, the rank of $\mathcal{G}_o$ may be odd or even, and $P_k(T)/P_k^{\mathrm{red}}(T)$ may be 1, so that we have non-vanishing of the L-function, or it may be $1 + \mathrm{sgn}(\rho) T^{a_o}$, so that we have simple vanishing (if $\alpha_n^{a_o} = -\mathrm{sgn}(\rho)$) or non-vanishing (if not) of the L-function. Thus the conclusion is that we have vanishing to order at most 1, as desired. This completes the proof of part (2) of Theorem 5.2.

10.6. **Proof of Theorem 1.1.** We want to apply Theorem 5.2, part (2), to the data F, ρ, and d, setting $S_s = S_i = S_r = \emptyset$ and $\alpha_n = q^{-ns_0}$. The hypotheses of 3.1 are satisfied, except possibly 3.1.5. But if χ is a character of G/G_∞, then the truth of Theorem 1.1 for $\rho \otimes \chi$ and all s_0 implies the truth of Theorem 1.1 for ρ and all s_0. Thus we may legitimately apply Theorem 5.2.

Since we assume that $d|q-1$, all the orbits $o \subset \mathbb{Z}/d\mathbb{Z}$ are singletons. In particular, the exceptional situations of types (iii)-(vi) do not occur. Exceptional situations of types (i) or (ii) can occur only if d is even, ρ is symplectically self-dual and the exponent of the local Artin conductor $\mathrm{Cond}_v(\rho)$ is even for all v. (This is

what 4.1.8.1 says when $S_s = S_i = S_r = \emptyset$.) If no exceptional situations occur, then Theorem 1.1 follows immediately from Theorem 5.2, and we may even replace "infinitely many n" with "all sufficiently large n."

So let us assume that d is even, ρ is symplectically self-dual, and 4.1.8.1 is satisfied. Then $\deg(\mathrm{Cond}(\rho \otimes \chi_f^{d/2}))$ is even for all f satisfying the local conditions and so exceptional situation (ii) is in fact impossible. Exceptional situation (i) occurs only if the root number $W(\rho \otimes \chi_f^{d/2}, F_n) = -1$. But if this happens then for any even multiple m of n, $W(\rho \otimes \chi_f^{d/2}, F_m) = 1$ (cf. 4.1.2) and so we avoid all exceptional situations. Thus there are infinitely many values of n for which there exists a good f. This completes the proof of Theorem 1.1.

With slightly more work, one can prove that Theorem 1.1 holds with "infinitely many n" replaced by "all sufficiently large even n," and in many cases by "all sufficiently large n."

11. Application to elliptic curves

The goal of this section is to prove the following two theorems.

11.1. **Theorem.** *Let $\mathcal{C}$ be a geometrically irreducible curve over a finite field $\mathbb{F}_q$ of characteristic $p > 3$ and let $F = \mathbb{F}_q(\mathcal{C})$. Let E be a non-isotrivial elliptic curve over F. Then there exists a finite separable extension F'/F such that:*

- *(a) E has split multiplicative reduction at some place of F'*
- *(b) E is semistable over F', i.e., it has good or multiplicative reduction at every place of F'*
- *(c) $\mathrm{ord}_{s=1} L(E/F', s) = \mathrm{ord}_{s=1} L(E/F, s)$*

11.2. **Theorem.** *Let $\mathcal{C}$ be a geometrically irreducible curve over a finite field $\mathbb{F}_q$ of characteristic $p > 3$ and let $F = \mathbb{F}_q(\mathcal{C})$ and $F_n = \mathbb{F}_{q^n}(\mathcal{C})$. Let E be a non-isotrivial elliptic curve over F of conductor $\mathfrak{n}$.*

- *(1) Fix three finite, pairwise disjoint sets of places S_s, S_i, S_r of F. Then for all sufficiently large n relatively prime to some integer B, there is a quadratic extension K/F_n such that*

$$\mathrm{ord}_{s=1} L(E/K, s) \leq \mathrm{ord}_{s=1} L(E/F, s) + 1$$

  and such that the places of F_n over S_s (resp. S_i, S_r) are split (resp. inert, ramified).
- *(2) If E has split multiplicative reduction at some place ∞ of F and we let $S_s = |\mathfrak{n}| \setminus \{\infty\}$, $S_i = \emptyset$ and $S_r = \{\infty\}$, then for all sufficiently large n prime to B there exists K as above so that $\mathrm{ord}_{s=1} L(E/K, s)$ is odd. In particular, if $\mathrm{ord}_{s=1} L(E/F, s) = 1$, then $\mathrm{ord}_{s=1} L(E/K, s) = 1$. The same conclusion holds if we take $S_s = |\mathfrak{n}| \setminus \{\infty\}$, $S_i = \{\infty\}$ and $S_r = \emptyset$.*

Theorem 1.2 of the introduction is an immediate consequence. Indeed, we first apply 11.1 to find a suitable F', then apply the second part of 11.2, with F' playing the role of F, to find K.

To prove these two theorems, we will apply Theorem 5.2 to the representation ρ of $\mathrm{Gal}(\overline{F}/F)$ on the Tate module $V_\ell(E)$ for some $\ell \neq p$. Note that ρ is symplectically self-dual of weight 1 and it satisfies the hypotheses of Subsection 3.1. We have $L(E/F, s) = L(\rho, F, q^{-s})$.

11.3. **Proof of 11.2.** We begin with an easy lemma.

11.3.1. **Lemma.** *If E is an elliptic curve over $F = \mathbb{F}_q(\mathcal{C})$ and if $F_n = \mathbb{F}_{q^n}(\mathcal{C})$, then there exists an integer b such that $\mathrm{ord}_{s=1} L(E/F_n, s) = \mathrm{ord}_{s=1} L(E/F, s)$ for all n relatively prime to b.*

Proof. First assume that E is non-constant, so that $L(E/F, s)$ is a polynomial in q^{-s}. Writing $L(E/F, s) = \prod_{i=1}^{N}(1 - \alpha_i q^{-s})$ we have that $\mathrm{ord}_{s=1} L(E/F, s)$ is the number of α_i which are equal to q. On the other hand, $L(E/F_n, s) = \prod_{i=1}^{N}(1-\alpha_i^n q^{-ns})$ and so $\mathrm{ord}_{s=1}(L(E/F_n, s)$ is equal to the number of α_i satisfying $\alpha_i^n = q^n$. Thus we may take b to be the least common multiple of the orders of all roots of unity appearing in the set $\{\alpha_i/q | i = 1, \ldots, N\}$.

If E is constant, the argument is similar, except that $L(E/F, s)$ is now a polynomial in q^{-s} divided by $(1 - q^{-s})(1 - q^{2-s})$. □

11.3.2. The first part of Theorem 11.2 is an easy consequence of the main Theorem 5.2. Indeed, Lemma 11.3.1 says that for all n prime to b, $\mathrm{ord}_{s=1} L(E/F_n, s) = \mathrm{ord}_{s=1} L(E/F, s)$. On the other hand, Theorem 5.2, applied with $d = 2$, the given S_s, S_i, and S_r, and $\alpha_n = q^n$, says that for all sufficiently large n (prime to $a_o = 1$) there exists an $f \in F_n^\times$ such that the quadratic extension $K = F_n(\sqrt{f})$ satisfies the local conditions imposed by S_s, S_i, and S_r and with

$$\mathrm{ord}_{s=1} \frac{L(E/K, s)}{L(E/F_n, s)} = L(E/F_n, \chi_f, s) \leq 1$$

where χ_f is the quadratic character of F_n associated to K. Moreover, we can conclude that $\mathrm{ord}_{s=1} L(E/F_n, \chi_f, s) = 0$ unless we are in one of the exceptional situations (i) or (ii).

For the second part of Theorem 11.2, we take $B = b \deg \infty$, so that if n is prime to B, then there is a unique place of F_n over ∞. The assertion is that the sign in the functional equation of $L(E/K, s)$ is -1, and this follows easily from the factorization of the sign into a product of local factors. Indeed, over each place of F_n in $|\mathfrak{n}| \setminus \infty$ there are two places of K and the local root number there are equal and so cancel. The only remaining contribution is at the unique place of K over ∞ (which is unique because we have assumed ∞ is inert or ramified in K). There E is split multiplicative and the local contribution is -1. This means that the sign in the functional equation of $L(E/K, s)$ is -1, i.e., the L-function vanishes to odd order.

This completes the proof of Theorem 11.2. □

11.4. **Proof of Theorem 11.1.** For brevity, we say that an extension F' of F is "good" if $\mathrm{ord}_{s=1} L(E/F', s) = \mathrm{ord}_{s=1} L(E/F, s)$. Theorem 5.2 guarantees the existence of good extensions $F' = F_n(f^{1/d})$ satisfying various local conditions for n sufficiently large and prime to $a = [\mathbb{F}_q(\mu_d) : \mathbb{F}_q]$ and the b of Lemma 11.3.1.

We proceed in three main steps. First we find a good extension F' of F such that E has a place of split multiplicative reduction over F'. Then we replace F with F' and eliminate places of reduction types II, II^*, IV and IV^* (i.e., we replace F with a good extension such that there are no places of these types). Lastly we eliminate places of reduction types III, III^*, and I_0^*.

11.4.1. *Step 1:* Since E is assumed to be non-isotrivial, its j-invariant is non-constant and thus has a pole at some place v_0 of F. Thus E is potentially multiplicative at this place. There are three possibilities: (i) E is split multiplicative at v_0; (ii) E is non-split multiplicative at v_0; (iii) E has reduction type I_n^* for some $n > 0$.

In case (i) there is nothing to do for the first step and we set $F' = F$.

In case (ii) we need a quadratic extension in which v_0 is inert. If the integer b appearing in Lemma 11.3.1 is odd, we may take $F' = F_2 = \mathbb{F}_{q^2}F$. If b is even, we need a geometric extension. For the rest of step 1, we set $d = 2$ and $\alpha_n = q^n$. Set $S_s = S_r = \emptyset$ and $S_i = \{v_0\}$. If the hypothesis 4.1.8.1 fails, or if it holds and the signs appearing in Lemma 4.1.9 are $+1$ then we are not in an exceptional situation and so for large enough n prime to b Theorem 5.2 supplies us with a good quadratic extension F' of F_n such that v_0 is inert. In the case where hypothesis 4.1.8.1 holds and the signs appearing in Lemma 4.1.9 are -1 then we are in an exceptional situation and we proceed in two substeps. First we set $S_r = S_i = \emptyset$ and $S_s = \{v_0\}$. By Lemma 4.1.7(2) the signs appearing in Lemma 4.1.9 are now $+1$ and we can find a good quadratic extension F' of F_n for some large n prime to b where v_0 is split. Replacing F with F' we now have two places of multiplicative reduction, call them v_0 and v_1. Setting $S_s = S_r = \emptyset$ and $S_i = \{v_0\}$ we see that hypothesis 4.1.8.1 fails (because of v_1) and so we are not in an exceptional situation. The argument in the first part of case (ii) gives us a quadratic extension F' of F where v_0 is inert and so E has split multiplicative reduction at the place of F' over v_0. This completes the analysis in case (ii).

In case (iii) we will find a quadratic extension in which v_0 is ramified. We set $S_s = S_i = \emptyset$ and $S_r = \{v_0\}$. For any ramified local character χ_{v_o} at v_0, we have $\mathrm{Cond}_{v_0}(\rho \otimes \chi_{v_0}) = 1$ which is odd, so the hypothesis 4.1.8.1 fails and we are not in an exceptional situation. Then for n large and prime to b Theorem 5.2 supplies a good quadratic extension F' of F_n in which every place over v_0 is ramified. Then E will have multiplicative reduction at each place of F' over v_0. If necessary, i.e., if the reduction is not split multiplicative, then we replace F with F' and apply the argument of case (ii) again to find a good extension over which E is split multiplicative.

We now replace F with F' and so we may assume that E has a place of split multiplicative reduction over F. This property is preserved in arbitrary finite extensions of F so we may forget about it for the rest of the proof.

11.4.2. *Step 2:* For a finite extension F' of F and an integer m, we let $S_m(F')$ be the set of places v of F' where E has additive reduction and $m = 12/gcd(v(\Delta_v), 12)$ where Δ_v is the discriminant of a minimal model of E at v. Thus S_m consists of places of reduction type I_0^* for $m = 2$, types IV and IV^* for $m = 3$, types III and III^* for $m = 4$, and types II and II^* for $m = 6$, and S_m is empty for other values of m. We need to find a good extension F' of F such that $S_m(F')$ is empty for all m. To do this we use the well-known fact that E obtains good reduction over any place of $S_m(F)$ which is ramified of index a multiple of m. (Here we use crucially that $p > 3$.)

In step 2, we will find a good extension F' so that $S_3(F')$ and $S_6(F')$ are empty. For the rest of this step (except the very end) we let $d = 3$ and $\alpha_n = q^n$. Theorem 5.2 will supply us with good cubic extensions of F_n in which the places over $S_3(F) \cup S_6(F)$ are totally ramified. If F' is such an extension, then places of F'

over $S_6(F)$ are in $S_2(F')$ and places of F' over $S_3(F)$ are places of good reduction. Thus replacing F with F' we will reduce to the case where $S_3(F)$ and $S_6(F)$ are empty.

To start, let $S_r = S_3(F) \cup S_6(F)$, and $S_s = S_i = \emptyset$. If $q \equiv 1 \pmod 3$, the extensions $F_n(f^{1/3})/F_n$ are Galois and we are in a non-exceptional situation. Theorem 5.2 supplies us with good cubic extensions in which the places of $S_3(F)$ and $S_6(F)$ are totally ramified.

If $q \equiv 2 \pmod 3$ but the integer b of Lemma 11.3.1 is odd, then we may replace F with F_2 and then proceed as in the previous paragraph.

If $q \equiv 2 \pmod 3$ and b is even, we again set $S_r = S_3(F) \cup S_6(F)$, and $S_s = S_i = \emptyset$ and consider the integer N_o where $o \subset (\mathbb{Z}/3\mathbb{Z})$ is the orbit of multiplication by q not containing 0. If N_o is even, we are not in an exceptional situation and we obtain a good cubic extension as above. If N_o is odd, then we are in an exceptional situation of type (iii) and so we will modify our input data. Note that the parity of N_o is the same as the parity of

$$\sum_{v \text{ over } |\mathfrak{n}| \cap S_r} \mathrm{Cond}_v(\rho \otimes \chi_f) \deg v + \sum_{v \text{ over } |\mathfrak{n}| \setminus S_r} \mathrm{Cond}_v(\rho) \deg v$$

for any $f \in X(\mathbb{F}_{q^n})$ satisfying the local conditions. Thus one of these sums is odd. If the second sum is odd, then E must have a place of multiplicative reduction of odd degree. If v is such a place, then $\mathrm{Cond}_v(\rho) = 1$ but $\mathrm{Cond}_v(\rho \otimes \chi_f) = 2$, and so if we change S_r to $S_3(F) \cup S_6(F) \cup \{v\}$, then N_o is now even and we may proceed as in the first part of this paragraph. If the first sum is odd, we make a preliminary quadratic extension using Theorem 5.2. More precisely, we set $d = 2$, $S_s = S_r = \emptyset$, $S_i = S_3(F) \cup S_6(F)$, and $\alpha_n = q^n$. Because we have a place of split multiplicative reduction, this is not an exceptional situation and we find a good quadratic extension F' of F_n for n large and relatively prime to b. Now every place of $S_3(F') \cup S_6(F')$ has even degree. Replacing F with F' we return to the setup with $d = 3$, $S_r = S_3(F) \cup S_6(F)$, $S_s = S_i = \emptyset$, and $\alpha_n = q^n$. Now we have that every place in S_r has even degree and so either N_o is even or the second displayed sum is odd and we may proceed as in the first part of this paragraph.

Applying step 2 iteratively, replacing F with F' at each iteration, we may now aassume that $S_3(F)$ and $S_6(F)$ are empty.

11.4.3. *Step 3:* Now we use quadratic extensions to eliminate $S_2(F)$ and $S_4(F)$. Let $d = 2$, $S_s = S_i = \emptyset$, $S_r = S_2(F) \cup S_4(F)$, and $\alpha_n = q^n$. Since we have a place of multiplicative reduction, hypothesis 4.1.8.1 fails and so we are in a non-exceptional situation. Theorem 5.2 gives us a good quadratic extension F' of F_n for some large n prime to b in which every place of F_n over S_r is ramified. This means that E acquires good reduction at every place over $S_2(F)$, $S_4(F')$ is empty and $S_2(F')$ consists of precisely the places over $S_4(F)$. Replacing F with F' and repeating this construction once more yields a good extension F' where $S_m(F')$ is empty for all m. This F' is an extension of the original F with all the required properties and this completes the proof of Theorem 11.1. □

References

[BFH96] D. Bump, S. Friedberg, and J. Hoffstein, *On some applications of automorphic forms to number theory*, Bull. Amer. Math. Soc. (N.S.) **33** (1996), 157–175.

[Bor91] A. Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Del73] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 501–597. Lecture Notes in Math., Vol. 349.

[Del80] ———, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. (1980), no. 52, 137–252.

[Gol00] D. Goldfeld, *Review of* [MM97], Bull. Amer. Math. Soc. (N.S.) **37** (2000), 155–159.

[Gup97] S. Dutta Gupta, *Mean values of L-functions over function fields*, J. Number Theory **63** (1997), no. 1, 101–131.

[HR92] J. Hoffstein and M. Rosen, *Average values of L-series in function fields*, J. Reine Angew. Math. **426** (1992), 117–150.

[Jac79] N. Jacobson, *Lie algebras*, Dover Publications Inc., New York, 1979, Republication of the 1962 original.

[Kat02] N. M. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002, See the web site `http://www.math.princeton.edu/~nmk` for corrections.

[KS99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[Laf02] L. Lafforgue, *Chtoucas de Drinfeld et correspondance de Langlands*, Invent. Math. **147** (2002), no. 1, 1–241.

[Lau87] G. Laumon, *Transformation de Fourier, constantes d'équations fonctionnelles et conjecture de Weil*, Inst. Hautes Études Sci. Publ. Math. (1987), no. 65, 131–210.

[Mil80] J. S. Milne, *Etale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[MM97] M. Ram Murty and V. Kumar Murty, *Non-vanishing of L-functions and applications*, Progress in Mathematics, vol. 157, Birkhäuser Verlag, Basel, 1997.

[Ser77] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[SGA1] A. Grothendieck, *Revêtments étales et groupe fondamental*, Lecture Notes in Mathematics, vol. 224, Springer-Verlag, New York, 1971.

[SGA4] A. Grothendieck et. al., *Théorie des topos et cohomologie étale des schémas*, Lecture Notes in Mathematics, vol. 269, 270, 305, Springer-Verlag, New York, 1972.

[SGA4$\frac{1}{2}$] P. Deligne et. al., *Cohomologie étale*, Lecture Notes in Mathematics, vol. 569, Springer-Verlag, New York, 1977.

[SGA5] A. Grothendieck et. al., *Cohomologie ℓ-adique et fonctions L*, Lecture Notes in Mathematics, vol. 589, Springer-Verlag, New York, 1977.

[Tat79] J. T. Tate, *Number theoretic background*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–26.

[Ulm04] D. L. Ulmer, *Elliptic curves and analogies between number fields and function fields*, Heegner points and Rankin L-series (MSRI Publications 49), Cambridge Univ. Press, 2004, pp. 285–315.

Department of Mathematics, University of Arizona, Tucson, AZ 85721
E-mail address: `ulmer@math.arizona.edu`