REPORT ON THE IRREDUCIBILITY OF L-FUNCTIONS

NICHOLAS M. KATZ

Abstract. In this paper, in honor of the memory of Serge Lang, we apply ideas of Chavdarov and work of Larsen to study the $\mathbb{Q}$-irreducibility, or lack thereof, of various orthogonal L-functions, especially L-functions of elliptic curves over function fields in one variable over finite fields. We also discuss two other approaches to these questions, based on work of Matthews, Vaserstein, and Weisfeller, and on work of Zalesskii-Serezkin.

1. Introduction

By the pioneering work of Dwork [Dw-Rat] and Grothendieck [Gr-Rat], we know that zeta functions of varieties over finite fields, as well as L-functions attached to quite general algebro-geometric situations over finite fields, are rational functions. In many cases, either this function or its "interesting part" is a polynomial with $\mathbb{Q}$-coefficients. In such cases, it is natural to wonder about the factorization properties of this $\mathbb{Q}$-polynomial. This question was first investigated by Chavdarov [Chav, Theorems 2.1, 2.3, 2.5], who used monodromy techniques to show that for a fixed genus $g \geq 1$, most genus g curves over a large finite field $\mathbb{F}_q$ have the numerator of their zeta function $\mathbb{Q}$-irreducible, i.e., the fraction of the genus g curves over $\mathbb{F}_q$ with this irreducibility property tends to 1 as q grows. [Strictly speaking, Chavdarov's literal result requires q to be a power of a fixed prime p.] Recently Kowalski [Kow-LSM] combined Chavdarov's monodromy methods with large sieve techniques to give quantitative refinements of Chavdarov's results.

It occurred to the author in the Fall of 2001 that one might apply Chavdarov's ideas to study the irreducibility properties of L-functions of elliptic curves E over one-variable function fields K over finite fields $\mathbb{F}_q$. Here one knows that, so long as the j-invariant is non-constant, the L-function is a polynomial with $\mathbb{Z}$-coefficients, of known degree d, of the form

$$L(T) = det(1 - qTA)$$

Date: April 14, 2010.

for a (necessarily unique up to conjugacy) element A in the compact real orthogonal group $O(d,\mathbb{R})$. The unitarized L-function,

$$L_u(T) := L(T/q) = det(1 - TA)$$

thus has coefficients in $\mathbb{Z}[1/q]$. Being the reversed characteristic polynomial of an element A in $O(d,\mathbb{R})$, it satisfies the functional equation

$$T^d L_u(1/T) = det(-A) L_u(T).$$

Here $det(-A) = \pm 1$ is the "sign in the functional equation". With this normalization, the point $T = 1$ is the Birch and Swinnerton-Dyer point. The Birch and Swinnerton-Dyer conjecture states that the Mordell-Weil rank of E/K, $MWrk.(E/k)$, is equal to the multiplicity of $T = 1$ as a zero of $L_u(T)$ (which has come to be called the "analytic rank" of E/K, $an.rk.(E/k)$). One has (in the function field case) the a priori inequality

$$MWrk.(E/k) \leq an.rk.(E/k).$$

The analytic rank is odd if and only if the sign in the functional equation is -1, in which case the analytic rank, being odd, is at least 1. On the other hand, if the sign in the functional equation is $+1$, then the analytic rank, being even, has "no reason" to be nonzero. There is a general expectation that, in any reasonable enumeration sense, "most" elliptic curves will have the lowest possible analytic rank, i.e. 0 or 1, that is compatible with the sign in their functional equations. We refer the reader to [deJ-Ka, 9.7], [Ka-TLFM, 8.3, 9.11, 10.3] and [Ka-MMP, 13.1.7] for one approach to this sort of question.

One knows that, depending on the parity of d and on the sign in the functional equation, either 1 or -1 or both or neither necessarily occur as "imposed" eigenvalues of an element A in $O(d,\mathbb{R})$. More precisely, for d odd, $-det(-A)$ is always an eigenvalue of A. For d even and $det(-A) = -1$, both ± 1 are always eigenvalues of A. So it is natural to introduce the "reduced" polynomial

$$Rdet(1 - TA) := det(1 - TA)/(1 - T); \quad d \text{ odd}, \ \text{sign} - 1,$$

$$Rdet(1 - TA) := det(1 - TA)/(1 + T); \quad d \text{ odd}, \ \text{sign} + 1,$$

$$Rdet(1 - TA) := det(1 - TA)/(1 - T^2); \quad d \text{ even}, \ \text{sign} - 1,$$

$$Rdet(1 - TA) := det(1 - TA); \quad d \text{ even}, \ \text{sign} + 1,$$

and the reduced (unitarized) L-function

$$L_{u,red}(T) := Rdet(1 - TA)$$

We propose to show that in various settings, "most" elliptic curves have their reduced L-functions $\mathbb{Q}$-irreducible. The relevance to the Birch and Swinnerton-Dyer Conjecture is simply this: so long as the reduced L-function has degree ≥ 2, if it is $\mathbb{Q}$-irreducible then it cannot have $T = 1$ as a root, and hence its analytic rank is as low as possible. This consequence for analytic rank gives nothing better than the already cited results [deJ-Ka, 9.7], [Ka-TLFM, 8.3, 9.11, 10.3] and [Ka-MMP, 13.1.7], the only interest is in the methods. [Work of Emmanuel Kowalski [Kow-RQT], Chris Hall [Ha], and Florent Jouve [Jo], using related ideas together with large sieve technology, allows one to do better.] It would be interesting to understand what is the analogue, if any, in the number field case, of the irreducibility of the reduced L-function.

To end this introduction, let us mention briefly a natural question that we do not discuss at all; given that "most" elliptic curves have their reduced L-functions $\mathbb{Q}$-irreducible, what are the galois groups (of the splitting fields, over $\mathbb{Q}$, of) the $\mathbb{Q}$-irreducible polynomials which arise? A natural guess is that for d odd, say $d = 2n + 1$, we should "usually" get the Weyl group of the root system B_n, independent of the sign in the functional equation. For d even and sign $+1$, say $d = 2n$, we should "usually" get the Weyl group of the root system D_n. But for d even and sign -1, say $d = 2n + 2$, we should "usually" get[1] the Weyl group of the root system C_n. The analogous question for families of curves of genus g, where we have symplectic monodromy, was posed and answered by Chavdarov [Chav] and made more quantitative by Kowalski [Kow-LSM]; here the galois group is "usually" the Weyl group of the root system C_g.

These results were worked out in the author's Princeton graduate courses of Fall, 2001 and of 2004-2005, and were presented in lectures at the University of Minnesota (2001), NYU (2001), the Newton Institute (2004), the University of Tokyo (2004), and Brown University (2005). It is a pleasure to thank the listeners for their stimulating questions.

2. The general setup, and the basic examples

We work over an integral domain R which is normal, finitely generated as a $\mathbb{Z}$-algebra, and whose fraction field has characteristic zero. Typically, R will simply be $\mathbb{Z}[1/N]$ for some integer $N \geq 1$. Over R, we are given a smooth R-scheme M/R of relative dimension $\nu \geq 1$ with geometrically connected fibres. Over M, we are given a proper smooth

[1] The reason we expect this Weyl group is the fact [Weyl, (9.15) on p. 226] that in the compact orthogonal group $O(2n + 2, \mathbb{R})$, the space of conjugacy classes of sign (here sign = determinant) -1 is, with its "Hermann Weyl measure" of total mass one, isomorphic to the space of conjugacy classes in the compact symplectic group $USp(2n)$, with its "Hermann Weyl measure" of total mass one.

curve C/M and a closed subscheme $D \subset C$ which is finite etale over M. We denote by U/M the open curve

$$U := C - D.$$

Finally, over U we are given a relative elliptic curve E/U.

Before going further, let us give the two basic examples we have in mind.

The first example is the universal family of good degree d polynomial twists of the Legendre curve. Here R is $\mathbb{Z}[1/2]$. We fix an integer $d \geq 3$, and take for M the open set $Twist_d$ in the affine space $\mathbb{A}^d_R$ of all monic, degree d polynomials in one variable λ consisting of those polynomials $f(\lambda)$ for which the product $f(0)f(1)Discrim(f)$ is invertible. Over this $Twist_d$ we have the universal such polynomial, f_{univ}, and we have the constant curve $\mathbb{P}^1/Twist_d$, with coordinate λ, in which we take for D the disjoint union of the sections $\infty, 0, 1$ and the zero locus of f_{univ}. So D is finite etale over $Twist_d$ of degree d+3. Here we have

$$U = \mathbb{A}^1_{Twist_d}[1/\lambda(\lambda - 1)(f_{univ}(\lambda)].$$

Over this U, we take for E/U the twisted Legendre curve in $\mathbb{P}^2_U$ whose affine equation is

$$y^2 = f_{univ}(\lambda)x(x-1)(x-\lambda).$$

For each finite field k of odd characteristic, and for each k-valued point f in $Twist_d(k)$, we obtain a relative elliptic curve $E_{k,f}$ over the punctured λ-line $\mathbb{A}^1_k[1/\lambda(\lambda-1)f(\lambda)]$, namely the twisted Legendre curve $y^2 = f(\lambda)x(x-1)(x-\lambda)$. Its L-function is a polynomial of degree $2d$ if d is even, and of degree $2d-1$ if d is odd.We will show that as $\#k$ grows, the fraction of twisting polynomials f in $Twist_d(k)$ for which the reduced L-function of the twisted Legendre curve is $\mathbb{Q}$-irreducible tends to 1. On the other hand, we have at present no means of addressing the following extremely natural question. Fix a finite field k of odd characteristic, and consider, as the integer d grows, the fraction of twisting polynomials f in $Twist_d(k)$ for which the reduced L-function of the twisted Legendre curve is $\mathbb{Q}$-irreducible. Does this fraction tend to 1 as d grows but k stays fixed? To some other nonzero limit (cf. [Poonen] for an analogous situation)? To any limit?

The second example is the universal family of good Weierstrass curves with g_2 and g_3 of at most specified degrees d_2 and d_3 respectively. Here R is $\mathbb{Z}[1/6]$. We fix integers $d_2 \geq 3$ and $d_3 \geq 3$, and we suppose that either $d_2 \geq 5$ or that $d_3 \geq 7$. We take for M the open set $W(d_2, d_3)$ in the affine space $\mathbb{A}^{1+d_2}_R \times \mathbb{A}^{1+d_3}_R$ consisting of those pairs of polynomials

$(g_2(t), g_3(t))$ of degrees at most (d_2, d_3), for which the auxiliary polynomial $\Delta(g_2, g_3) := g_2(t)^3 - 27g_3(t)^2$ has degree exactly $Max(3d_2, 2d_3)$ and has *its* discriminant invertible. Over $W(d_2, d_3)$ we have the universal pair $(g_{2,univ}(t), g_{3,univ}(t))$, the constant curve $\mathbb{P}^1/W(d_2, d_3)$ with coordinate t, and the divisor D which is the disjoint union of the section ∞ and the zero locus of $\Delta(g_{2,univ}(t), g_{3,univ}(t))$. So D is finite etale over $W(d_2, d_3)$ of degree $1 + Max(3d_2, 2d_3)$. Here we have

$$U = \mathbb{A}^1_{W(d_2,d_3)}[1/\Delta(g_{2,univ}(t), g_{3,univ}(t))].$$

Over this U, we take for E/U the relative elliptic curve given in $\mathbb{P}^2_U$ whose affine equation is the universal Weierstrass equation

$$y^2 = 4x^3 - g_{2,univ}(t)x - g_{3,univ}(t).$$

For each finite field k in which 6 is invertible, and for each k-valued point $(g_2(t), g_3(t))$ in $W(d_2, d_3)(k)$, we obtain the relative elliptic curve E_{k,g_2,g_3} over the punctured t-line $\mathbb{A}^1_k[1/\Delta(g_2, g_3)]$, namely the Weierstrass curve $y^2 = 4x^3 - g_2(t)x - g_3(t)$. Its L-function is a polynomial of degree $Max(3d_2, 2d_3) - 2$ if 12 divides $Max(3d_2, 2d_3)$, otherwise of degree $Max(3d_2, 2d_3) - 4$. We will show that as $\#k$ grows, the fraction of points $(g_2(t), g_3(t))$ in $W(d_2, d_3)(k)$ for which the reduced L-function of the corresponding Weierstrass curve is $\mathbb{Q}$-irreducible tends to 1. Just as in the first example, if we fix a finite field k in which 6 is invertible, and vary the integers (d_2, d_3) in such a way that, say, $Min(d_2, d_3)$ grows, we have no understanding of the limiting behavior, if any, of the fraction of of points in $W(d_2, d_3)(k)$ whose reduced L-function is $\mathbb{Q}$-irreducible.

3. Back to the general setup; axiomatics

We return to the general setup. Thus R is an integral domain which is normal, finitely generated as a $\mathbb{Z}$-algebra, and whose fraction field has characteristic zero, and M/R is smooth of relative dimension $\nu \geq 1$ with geometrically connected fibres. Over M, we are given a proper smooth curve C/M and a closed subscheme $D \subset C$ which is finite etale over M. U/M is the open curve

$$U := C - D,$$

and over U we are given a relative elliptic curve E/U. So our picture is

$$E \to U \subset C \to M \to Spec(R).$$

Let us name these morphisms, say

$$f : E \to U,$$

$$j : U \subset C,$$

$$\pi : C \to M.$$

If k is a finite field and $m \in M(k)$ is a k-valued point of M, then by base change we obtain from $E/U/M$ an open curve $U_{k,m}/k$ and a relative elliptic curve $E_{k,m}/U_{k,m}/k$. Let us recall the cohomological genesis of its unitarized L-function.

For a prime number ℓ, and A any of the rings $\mathbb{F}_\ell$, $\mathbb{Z}_\ell$, $\mathbb{Q}_\ell$ or $\overline{\mathbb{Q}_\ell}$, consider the lisse sheaf on $U[1/\ell]$ given by

$$\mathcal{F}_A := R^1 f_\star A.$$

It is a sheaf of free A-modules of rank 2, whose determinant is canonically the Tate-twisted constant sheaf $A(-1)$. So we have a canonical symplectic autoduality paring

$$\mathcal{F}_A \times \mathcal{F}_A \to A(-1).$$

Because R and hence M are normal and connected of generic characteristic zero, any lisse A-sheaf on $U[1/\ell]$ (here $\mathcal{F}_A$) is tamely ramified along the finite etale divisor $D[1/\ell]$. We next consider its extension by direct image,

$$\mathcal{G}_A := j_\star \mathcal{F}_A,$$

on $C[1/\ell]$. The autoduality pairing on $\mathcal{F}_A$ extends by direct image to a pairing

$$\mathcal{G}_A \times \mathcal{G}_A \to j_\star A(-1) \cong A(-1).$$

The formation of $\mathcal{G}_A$ on $C[1/\ell]$ commutes with arbitrary base change on $M[1/\ell]$, and its restriction to $D[1/\ell]$ is a lisse sheaf of free A-modules on $D[1/\ell]$. We then form the Tate-twisted higher direct image sheaf

$$\mathcal{H}_A := R^1 \pi_\star \mathcal{G}_A(1)$$

on $M[1/\ell]$. This is a lisse sheaf of (not necessarily free, when A is $\mathbb{Z}_\ell$) A-modules of finite type. Its formation commutes with arbitrary base change on $M[1/\ell]$. It is endowed with an A-linear cup product pairing

$$\mathcal{H}_A \times \mathcal{H}_A \to R^2 \pi_\star A(1) \cong A.$$

When A is a field, this pairing makes $\mathcal{H}_A$ orthogonally self-dual. When A is $\mathbb{Q}_\ell$ or $\overline{\mathbb{Q}_\ell}$, then $\mathcal{H}_A$ is, in addition, pure of weight zero. We view the lisse sheaf $\mathcal{H}_A$ as a representation of $\pi_1(M[1/\ell])$.

Theorem 3.1. *In the general setup $E/U/M/R$ as above, there exist integers $d \geq 0$ and $N \geq 1$ such that for ℓ not dividing N, $\mathcal{H}_{\mathbb{Z}_\ell}$ is a lisse sheaf of free $\mathbb{Z}_\ell$-modules of rank d on $M[1/\ell]$ which, by the cup product pairing*

$$\mathcal{H}_{\mathbb{Z}_\ell} \times \mathcal{H}_{\mathbb{Z}_\ell} \to \mathbb{Z}_\ell,$$

is orthogonally self dual over $\mathbb{Z}_\ell$.

Proof. Pick an embedding of R into $\mathbb{C}$, and make the extension of scalars from R to $\mathbb{C}$. We denote the superscript an the corresponding analytic objects. Thus we have the locally constant sheaf $\mathcal{H}^{an}_{\mathbb{Z}}$ of finitely generated abelian groups on M^{an}, endowed with the cup product pairing to $\mathbb{Z}^{an}$. If we tensor it with $\mathbb{Q}$, we obtain the locally constant sheaf $\mathcal{H}^{an}_{\mathbb{Q}}$ on M^{an}, which by cup product is orthogonally self-dual. We take for d the rank of $\mathcal{H}^{an}_{\mathbb{Q}}$. If we invert a suitable integer $N \geq 1$, and tensor $\mathcal{H}^{an}_{\mathbb{Z}}$ with $\mathbb{Z}[1/N]$ to obtain (by the flatness of $\mathbb{Z}[1/N]$ over $\mathbb{Z}$) $\mathcal{H}^{an}_{\mathbb{Z}[1/N]}$, we find that $\mathcal{H}^{an}_{\mathbb{Z}[1/N]}$ is a locally constant sheaf of free $\mathbb{Z}[1/N]$-modules of rank d which under cup product is orthogonally self-dual over $\mathbb{Z}[1/N]$. We can take this N to be the N of the theorem. Indeed, for any ℓ not dividing N, we can make the flat extension of scalars from $\mathbb{Z}[1/N]$ to $\mathbb{Z}_\ell$ and infer that $\mathcal{H}^{an}_{\mathbb{Z}_\ell}$ is a lisse sheaf of free $\mathbb{Z}_\ell$-modules of rank d on M^{an} which is orthogonally self dual over $\mathbb{Z}_\ell$. By the comparison theorem, the restriction to $M_{\mathbb{C}}$ of $\mathcal{H}_{\mathbb{Z}_\ell}$ is therefore a lisse sheaf of free $\mathbb{Z}_\ell$-modules on $M_{\mathbb{C}}$ which is orthogonally self dual over $\mathbb{Z}_\ell$. It follows that the lisse sheaf $\mathcal{H}_{\mathbb{Z}_\ell}$ on $M[1/\ell]$ itself is torsion-free and $\mathbb{Z}_\ell$-autodual under the cup product pairing. Indeed, it suffices to check both the torsion-freeness of the lisse sheaf in question, namely $\mathcal{H}_{\mathbb{Z}_\ell}$, and the $\mathbb{Z}_\ell$-nondegeneracy of the pairing, at a single geometric point of $M[1/\ell]$. □

We now consider two fibrewise conditions that may or may not hold in our general setup. Both of these conditions do hold in both of the examples given above (Legendre twists and Weierstrass families), cf. [Ka-MMP, 8.2.3 and 10.2.13] respectively for these two cases.

(1) For every finite field k, and for every k-valued point m in $M(k)$, the relative elliptic curve $E_{k,m}/U_{k,m}/k$ has non-constant j-invariant.

(2strong) For every finite field k and every ring homomorphism $\phi : R \to k$, denote by $M_{k,\phi}/k$ the fibre of M/R above (k, ϕ). For every ℓ invertible in k, consider the restriction to $M_{k,\phi}$ of the lisse sheaf $\mathcal{H}_{\mathbb{Q}_\ell}$ on $M[1/\ell]$. View this lisse sheaf as a representation $\rho_{k,\phi,\ell} : \pi_1(M_{k,\phi}) \to O(d, \mathbb{Q}_\ell)$. Under every such homomorphism $\rho_{k,\phi,\ell}$, the image in $O(d, \mathbb{Q}_\ell)$ of the geometric fundamental group

$$\pi_1^{geom}(M_{k,\phi}) := \pi_1(M_{k,\phi} \otimes_k \overline{k}) \lhd \pi_1(M_{k,\phi})$$

is Zariski dense in $O(d, \overline{\mathbb{Q}}_\ell)$.

In certain applications, cf. [Ka-MMP, 7.2.7, 8.2.5, 10.2.15] and [Ka-TLFM, 8.5.7, 8.6.7], one knows only that the following weaker version of the second condition holds.

(2weak) For every finite field k and every ring homomorphism $\phi : R \to k$, denote by $M_{k,\phi}/k$ the fibre of M/R above (k, ϕ). For every ℓ invertible in k, consider the restriction to $M_{k,\phi}$ of the lisse sheaf $\mathcal{H}_{\mathbb{Q}_\ell}$ on $M[1/\ell]$. View this lisse sheaf as a representation $\rho_{k,\phi,\ell} : \pi_1(M_{k,\phi}) \to O(d, \mathbb{Q}_\ell)$. Under each such homomorphisms $\rho_{k,\phi,\ell}$, the image in $O(d, \mathbb{Q}_\ell)$ of the geometric fundamental group

$$\pi_1^{geom}(M_{k,\phi}) := \pi_1(M_{k,\phi} \otimes_k \overline{k}) \lhd \pi_1(M_{k,\phi})$$

is Zariski dense in *either* $SO(d, \overline{\mathbb{Q}}_\ell)$ *or in* $O(d, \overline{\mathbb{Q}}_\ell)$.

If the first condition holds, then for every ℓ invertible in k, the lisse sheaf $\mathcal{F}_{\mathbb{Q}_\ell}$ on $U_{k,m}/k$ is geometrically irreducible, and (hence) the unitarized L-function is given by the action of the Frobenius conjugacy class $Frob_{k,m}$ in $\pi_1(M[1/\ell])$ on the lisse sheaf $\mathcal{H}_{\mathbb{Q}_\ell}$:

$$L_u(E_{k,m}/U_{k,m}, T) = det(1 - TFrob_{k,m}|\mathcal{H}_{\mathbb{Q}_\ell}).$$

[If we do not impose the first condition, the lisse sheaf $\mathcal{F}_{\mathbb{Q}_\ell}$ on $U_{k,m}/k$ could be geometrically constant (e.g., if E/U were a constant elliptic curve), in which case the unitarized L-function would not be a polynomial, but rather a rational function whose numerator is given by the right hand side.] Since these unitarized L-function have rational coefficients which "do not know about ℓ", we see that the sheaves $\mathcal{H}_{\mathbb{Q}_\ell}$ on $M[1/\ell]$ form, as ℓ varies, a "compatible system of orthogonal ℓ-adic representations" on M. Moreover, and this is the import of the previous theorem, there exists a single orthogonal group $O(d)/\mathbb{Z}[1/N]$, corresponding to a quadratic form over $\mathbb{Z}[1/N]$ in d variables whose discriminant is invertible in $\mathbb{Z}[1/N]$, such that for every ℓ we land in its $\mathbb{Q}_\ell$-points, and such that for ℓ prime to N, we land in its $\mathbb{Z}_\ell$ points. What is essential here is"only" the following (apparently weak) consequence of this last fact: for almost all ℓ (namely those ℓ prime to N), we are landing in the $\mathbb{Z}_\ell$ points of an orthogonal group over $\mathbb{Z}_\ell$ corresponding to a quadratic form over $\mathbb{Z}_\ell$ in d variables whose discriminant is invertible in $\mathbb{Z}_\ell$.

For each finite field k and each homomorphism $\phi : R \to k$, denote by $IrrFrac(k, \phi) \in \mathbb{Q}$ the fraction of the k-valued points m in the fibre $M_{k,\phi}/k$ for which the reduced unitarized L-function $L_{u,red}(E_{k,m}/U_{k,m}, T)$ is $\mathbb{Q}$-irreducible.

4. Statement of the main theorem

Theorem 4.1. *In the general setup $E/U/M/R$, suppose that the fibrewise conditions* (1) *and* (2weak) *of the previous section hold. Suppose also that d, the common degree of the L-functions, is ≥ 3. Given a real number $\epsilon > 0$, there exists a real constant $X = X(\epsilon, E/U/M/R)$*

such that for any finite field k with $\#k > X$, and any homomorphism $\phi : R \to k$, we have

$$IrrFrac(k, \phi) \geq 1 - \epsilon.$$

5. Statement of an abstract version of the main theorem

Let us now consider an abstract version of our situation. We are given a finitely generated $\mathbb{Z}$-algebra R. Over R, we are given a smooth R-scheme M/R of relative dimension $\nu \geq 1$ with geometrically connected fibres. We are given an integer $d \geq 3$. For every prime ℓ such that $M[1/\ell]$ is nonempty, we are given a lisse $\mathbb{Q}_\ell$-sheaf $\mathcal{H}_{\mathbb{Q}_\ell}$ on $M[1/\ell]$ of rank d, together with a symmetric autoduality pairing

$$\mathcal{H}_{\mathbb{Q}_\ell} \times \mathcal{H}_{\mathbb{Q}_\ell} \to \mathbb{Q}_\ell.$$

These sheaves are assumed to form a compatible system of ℓ-adic representations on M (in the sense that each characteristic polynomial of Frobenius has rational coefficients which are independent of the auxiliary choice of allowed ℓ). Each sheaf $\mathcal{H}_{\mathbb{Q}_\ell}$ is assumed pure of weight zero. For all but finitely many ℓ, say for all ℓ outside a finite set S of primes, we are given a lisse $\mathbb{Z}_\ell$-sheaf $\mathcal{H}_{\mathbb{Z}_\ell}$ on $M[1/\ell]$ of free $\mathbb{Z}_\ell$ modules of rank d, together with a symmetric autoduality pairing over $\mathbb{Z}_\ell$,

$$\mathcal{H}_{\mathbb{Z}_\ell} \times \mathcal{H}_{\mathbb{Z}_\ell} \to \mathbb{Z}_\ell,$$

which is an integral form of $\mathcal{H}_{\mathbb{Q}_\ell}$ with its autoduality pairing.

For each finite field k and each homomorphism $\phi : R \to k$, denote by $IrrFrac(k, \phi) \in \mathbb{Q}$ the fraction of the k-valued points m in the fibre $M_{k,\phi}/k$ for which the reduced characteristic polynomial $Rdet(1 - TFrob_{k,m}|\mathcal{H})$ is $\mathbb{Q}$-irreducible.

Theorem 5.1. *In the abstract version given above, with $d \geq 3$, suppose that the fibrewise condition* (2weak) *of the previous section holds. Given a real number $\epsilon > 0$, there exists a real constant $X = X(\epsilon, R)$ such that for any finite field k with $\#k > X$, and any homomorphism $\phi : R \to k$, we have*

$$IrrFrac(k, \phi) \geq 1 - \epsilon.$$

We will fix $\epsilon > 0$, and prove the theorem for this value of ϵ. We reduce immediately to the case when R is reduced. If we have a finite decomposition of $Spec(R)$ as the disjoint union of finitely many locally closed, reduced affine subschemes $Spec(R_i)$, it suffices to prove the theorem (for our fixed $\epsilon > 0$), over each $Spec(R_i)$ separately. Indeed, then we can take $X(\epsilon, R)$ to be $Max_i(X(\epsilon, R_i))$. So by noetherian induction on $Spec(R)$, it suffices to prove that the theorem holds, for our fixed $\epsilon > 0$, in some affine open neighborhood of some maximal point of $Spec(R)$. Any sufficiently small such open neighborhood is of the form $Spec(R_1)$, with R_1 a normal integral domain which is a finitely generated $\mathbb{Z}$-algebra. Making the extension of scalars from R to R_1, we are reduced to proving the following "generic" version of the theorem.

Theorem 5.2. *In the abstract version given above, with $d \geq 3$, suppose that the fibrewise condition* (2weak) *of the previous section holds. Suppose in addition that R is a normal integral domain which is a finitely generated $\mathbb{Z}$-algebra. Given a real number $\epsilon > 0$, there exists a real constant $X = X(\epsilon, R)$ and a nonzero element $r = r(\epsilon) \in R$, such that for any finite field k with $\#k > X$, and any homomorphism $\phi : R \to k$ for which $\phi(r) \neq 0$, we have*

$$IrrFrac(k, \phi) \geq 1 - \epsilon.$$

6. Interlude: Review of orthogonal groups over finite fields of odd characteristic

In this section, we fix an integer $d \geq 1$, a finite field $E = \mathbb{F}_q$ of odd characteristic, and a nondegenerate quadratic form in d variables over E, i.e., a d-dimensional E vector space V endowed with a symmetric E-bilinear form $\Psi : V \times V \to E$ which makes V autodual. We denote by $O(V, \Psi) := Aut_E(V, \Psi)$ the corresponding finite orthogonal group.

One knows that for fixed d and E, there are precisely two isomorphism classes of nondegenerate quadratic form, distinguished by whether or not the discriminant is a square in $E^\times$. When d is odd, the two isomorphism classes give rise to the same orthogonal group; indeed if (V, Ψ) represents one class, then for any nonsquare $\alpha \in E^\times$, $(V, \alpha\Psi)$ represents the other, while visibly their orthogonal groups coincide. So we may speak unambiguously of the group $O(d, E)$ when d is odd.

When $d = 2n$ is even, then the two cases are called the split case and the nonsplit case. The standard model for the split case is given by the quadratic form $\sum_{i=1}^n x_i x_{n+i}$ (so here $(-1)^n$Discriminant is a square), which we will denote $(split_{2n}, std)$. A convenient model for the nonsplit case is to take $V := \mathbb{F}_{q^{2n}}$ as our $\mathbb{F}_q$ vector space, endowed with the symmetric bilinear form

$$\Psi(x, y) := (1/2)Trace_{\mathbb{F}_{q^{2n}}/\mathbb{F}_q}(xy^{q^n}),$$

and quadratic form

$$\Psi(x, x) = Trace_{\mathbb{F}_{q^n}/\mathbb{F}_q}(Norm_{\mathbb{F}_{q^{2n}}/\mathbb{F}_{q^n}}(x)).$$

For ease of later reference, we will refer to this model as the standard nonsplit model, and denote it $(\mathbb{F}_{q^{2n}}, std)$. The split and nonsplit orthogonal groups are *not* isomorphic, they even have different orders. We will denote them $O_{spl}(d, E)$ and $O_{nonspl}(d, E)$ respectively when we need to distinguish them.

On the Clifford algebra $Cl := Cl(V, \Psi)$ attached to (V, Ψ), we have the E-algebra involution I which is $v \mapsto -v$ on V, and the E-algebra anti-automorphism $x \mapsto t(x)$ which is the identity on V. We have its unit group $Cl^\times$. The unit group acts on the Clifford algebra by the sign-twisted conjugation action: $u \in Cl^\times$ acts as $x \mapsto I(u)xu^{-1}$. Inside $Cl^\times$ we have the (twisted) Clifford group, namely the subgroup $C^\times$ consisting of those elements which map V to itself. Every nonisotropic $v \in V$ lies in $C^\times$, for the map $x \mapsto I(v)xv^{-1}$ is then, for $x \in V$, reflection in v. Moreover, one knows that every element of $C^\times$ is a nonzero scalar times a (possibly empty) product of nonisotropic vectors $v \in V$; this corresponds to the fact that in the orthogonal group $O(V, \Psi)$, every element is a product of reflections in nonisotropic vectors. For $u \in C^\times$, its "norm" $N(u) := t(u)u$ lies in $E^\times$, and $x \mapsto N(x)$ is a group homomorphism. Its kernel is the group $Pin(V, \Psi)$:

$$Pin(V, \Psi) := Ker(N : C^\times \to E^\times).$$

The subgroup of $Pin(V, \Psi)$ consisting of the elements fixed by the involution I is the group $Spin(V, \Psi)$.

Remark 6.1. The reader should be warned of a possible source of serious confusion. In the older literature, e.g., [Artin-GA], [Bour-AlgIX] and [Chev-Spin], the unit group is made to act on the Clifford algebra by the literal conjugation action: $u \in Cl^\times$ acts as $x \mapsto uxu^{-1}$, and one takes the (untwisted) Clifford group, denoted Γ in [Chev-Spin, 2.3], accordingly. This leads to unpleasant difficulties, centered on the fact that when V is odd-dimensional, there are nonscalar elements of Γ which act trivially on V, and the "norm" of an element of Γ need not be a scalar. Contorsions are adopted to get around these difficulties; one obtains the group $Spin(V, \Psi)$, but there is no $Pin(V, \Psi)$ in the older theory. The sign-twisted approach, and the group Pin, first appeared in [AtBS-Clif, 1.7, 3.1], cf. also [Kar-Clif, 1.1.4-8].

We have an exact sequence

$$\{1\} \to \pm 1 \to Pin(V, \Psi) \to O(V, \Psi) \to \pm 1,$$

in which the last map is the spinor norm, denoted

$$sp : O(V, \Psi) \to \pm 1.$$

The spinor norm is determined by its value on reflections Rfl_v in nonisotropic vectors $v \in V$ (since these elements generate $O(V, \Psi)$). For these, we have the explicit formula

$$sp(Rfl_v) = \text{the class of } \Psi(v, v) \text{ in } E^\times/(E^\times)^2 \cong \pm 1.$$

If $d \geq 2$, the spinor norm is surjective, and we have a short exact sequence

$$\{1\} \to \pm 1 \to Pin(V, \Psi) \to O(V, \Psi) \to \pm 1 \to \{1\},$$

under which the inverse image of $SO(V, \Psi)$ in $Pin(V, \Psi)$ is $Spin(V, \Psi)$. So we also have the more standard short exact sequence

$$\{1\} \to \pm 1 \to Spin(V, \Psi) \to SO(V, \Psi) \to \pm 1 \to \{1\}.$$

We also have the determinant homomorphism

$$det : O(V, \Psi) \to \pm 1.$$

The simultaneous kernel of these two homomorphisms, sp and det, is denoted $\Omega(V, \Psi)$.

When $d \geq 5$, or when $d = 4$ and we are in the nonsplit case, or when $d = 3$ and the characteristic is ≥ 5, the group $\Omega(V, \Psi)$ is, modulo its center, a nonabelian simple group, cf. [Artin-GA, Theorems 4.9, 5.20, 5.21, 5.27]. Moreover, in these cases, the only proper normal subgroups of $\Omega(V, \Psi)$ are subgroups of its center, and consequently $\Omega(V, \Psi)$ is its own commutator subgroup. The center of $\Omega(V, \Psi)$ is trivial if either d is odd or if the discriminant is a nonsquare, otherwise it is ± 1. When $d = 4$ and the characteristic is ≥ 5 and we are in the split case, then $\Omega(V, \Psi)/\pm 1$ is the product $PSL(2, E) \times PSL(2, E)$ of the simple group $PSL(2, E)$ with itself, cf. [Artin-GA, Theorem 5.22], and $\Omega(V, \Psi)$ is its own commutator subgroup [being a quotient of $Spin(V, \Psi) \cong SL(2, E) \times SL(2, E)$, which is its own commutator subgroup].

One knows [Artin-GA, Theorems 5.14, 5.17] that $\Omega(V, \Psi)$ is the commutator subgroup of $O(V, \Psi)$, indeed this was its *definition* before Chevalley introduced the use of Clifford algebras in these questions, cf. [Die-GC, Chpt. III, section 12, p. 23]. For $d \geq 2$, the quotient group $O(V, \Psi)/\Omega(V, \Psi)$ is, by the pair of maps (det, sp) the group $\{\pm 1\} \times \{\pm 1\}$. We will need to know, in each of the four cosets of $\Omega(V, \Psi)$ in $O(V, \Psi)$, lower bounds for the numbers of elements A whose reduced reversed characteristic polynomials $Rdet(1 - TA)$ have, as E-polynomials, certain imposed factorization patterns. For each $(\alpha, \beta) \in \{\pm 1\} \times \{\pm 1\}$, we denote by

$$O(V, \Psi)(det = \alpha, sp = \beta)$$

the corresponding coset.

There is a further cautionary remark we need to make at this point. Suppose $d \geq 2$, we are given a subgroup H of $GL(V) := Aut_E(V)$, and we are told that $H = O(V, \Psi)$ for some symmetric autoduality Ψ. Then the subgroup $\Omega(V, \Psi)$ is an intrinsic subgroup of H, namely its commutator subgroup. The *det* homomorphism

$$det : H \to \pm 1$$

is intrinsic on H as a subgroup of $GL(V)$. However, the spinor norm homomorphism

$$sp : H \to \pm 1$$

depends on the choice of Ψ. Indeed, if we replace Ψ by a nonzero scalar multiple $\alpha\Psi$ with α a nonsquare, the orthogonal group does not change, but the two spinor norms are related by

$$sp_{(V,\alpha\Psi)}(h) = det(h) sp_{(V,\Psi)}(h).$$

On the other hand, since the quotient group $H/\Omega(V, \Psi)$ is of type $(2, 2)$, with *det* and $sp_{(V,\Psi)}$ an $\mathbb{F}_2$-basis of its character group, we see that for any Ψ_1 on V with $O(V, \Psi) = O(V, \Psi_1)$, we have either $sp_{(V,\Psi_1)}(h) = sp_{(V,\Psi)}(h)$ for every $h \in H$, or we have $sp_{(V,\Psi_1)}(h) = det(h) sp_{(V,\Psi)}(h)$ for every $h \in H$. Thus each of the two cosets of $\Omega(V, \Psi)$ in $H \cap SL(V) = SO(V, \Psi)$ is intrinsic, e.g., one is a subgroup and one isn't, but the two cosets of $\Omega(V, \Psi)$ in $H \setminus H \cap SL(V) = O(V, \Psi) \setminus SO(V, \Psi)$ may be interchanged by different choices of Ψ. In the discussion below, we work with particular models of our orthogonal groups, i.e., we make specific choices of Ψ. But we prove only statements which are invariant under replacing *sp* by $det \times sp$.

Lemma 6.2. *Fix $d = 2n \geq 2$. Suppose $q := \#E \geq 7$. In each of the two cosets of $\Omega(d, E)$ in $SO_{nonspl}(d, E)$, the fraction of elements A for which $Rdet(1 - TA)$ is E-irreducible is at least $1/2n$.*

Proof. In the standard nonsplit model $(\mathbb{F}_{q^{2n}}, std)$, the group $\mu_{1+q^n} := \mu_{1+q^n}(\mathbb{F}_{q^{2n}})$, acting by homothety on $\mathbb{F}_{q^{2n}}$, lies in $SO_{nonspl}(2n, E)$. Moreover, we know [Saito-sign, Lemma 1, parts 4 and 5] that the spinor norm, restricted to μ_{1+q^n}, is trivial precisely on the subgroup $\mu_{(1+q^n)/2}$ of squares. We also remark that every $\mathbb{F}_{q^{2n}}$-homothety which lies in the orthogonal group lies in μ_{1+q^n}. It follows that if $\zeta \in \mu_{1+q^n}$ is an element such that the field $\mathbb{F}_q(\zeta)$ is $\mathbb{F}_{q^{2n}}$, then its characteristic polynomial is an $\mathbb{F}_q$-irreducible palindromic polynomial, and its centralizer in $O_{nonspl}(2n, E)$ is the subgroup μ_{1+q^n} [simply because any $\mathbb{F}_q$-linear endomorphism A of $\mathbb{F}_{q^{2n}}$ which commutes with ζ is $\mathbb{F}_{q^{2n}}$-linear, so an $\mathbb{F}_{q^{2n}}$-homothety]. So for any such ζ, its conjugacy class in $O_{nonspl}(2n, E)$

contains $\#O_{nonspl}(2n,E)/(1+q^n)$ elements, all of which have the same $\mathbb{F}_q$-irreducible palindromic characteristic polynomial as ζ, as well as the same spinor norm and determinant as ζ. If we take a second such element ζ_1 which is not one of the $2n$ Galois conjugates of ζ, then its characteristic polynomial is a different $\mathbb{F}_q$-irreducible palindromic polynomial, so certainly its conjugacy class in $O_{nonspl}(2n,E)$ is disjoint from that of ζ. [Conversely, Galois conjugate elements of μ_{1+q^n} are $O_{nonspl}(2n,E)$-conjugate, since the Galois automorphisms of $\mathbb{F}_{q^{2n}}/\mathbb{F}_q$ lie in the orthogonal group, and their conjugation action on elements of μ_{1+q^n} is the same as their Galois action.] Denote temporarily by $N_\pm$ the number of elements $\zeta \in \mu_{1+q^n}$ of spinor norm ± 1 such that the field $\mathbb{F}_q(\zeta)$ is $\mathbb{F}_{q^{2n}}$. Taking the union of their conjugacy classes, we obtain $\#O_{nonspl}(2n,E)N_\pm/2n(1+q^n)$ elements in $O_{nonspl}(2n,E)(det = 1, sp = \pm 1)$ with an E-irreducible palindromic characteristic polynomial.

One sees easily if $\zeta \in \mu_{1+q^n}$ is such that $\mathbb{F}_q(\zeta)$ is a proper subfield of of $\mathbb{F}_{q^{2n}}$, then either $\zeta = \pm 1$, or $\mathbb{F}_q(\zeta)$ is $\mathbb{F}_{q^{2a}}$ for some divisor $a < n$ of n, $\zeta \in \mu_{1+q^a}$ and n/a is odd. Thus, denoting $[x] := Floor(x)$, at most $2 + [n/3]q^{[n/3]}$ of the elements in μ_{1+q^n} fail to generate $\mathbb{F}_{q^{2n}}$ over $\mathbb{F}_q$. So we have the estimates

$$N_\pm \geq (1+q^n)/2 - 2 - [n/3]q^{[n/3]}.$$

Treating separately the cases $[n/3] = 0$ and $[n/3] \geq 1$, we see that so long as $q \geq 7$, we have

$$N_\pm \geq (1+q^n)/4.$$

Thus we obtain at least

$$\#O_{nonspl}(2n,E)/8n = \#O_{nonspl}(2n,E)(det = 1, sp = \pm 1)/2n$$

elements in $O_{nonspl}(2n,E)(det = 1, sp = \pm 1)$ with an E-irreducible palindromic characteristic polynomial. □

Lemma 6.3. *Fix $d = 2n \geq 4$. Suppose $q := \#E \geq 7$. In each of the two cosets $O(d,E)(det = -1, sp = \pm 1)$, the fraction of elements A for which $Rdet(1 - TA)$ is E-irreducible is at least $1/4(2n-2)$.*

Proof. We take as model of our quadratic space

$$(\mathbb{F}_{q^{2n-2}}, std) \oplus (\mathbb{F}_{q^2}, std)$$

in the *split* case, and

$$(\mathbb{F}_{q^{2n-2}}, std) \oplus (split_2, std)$$

in the *nonsplit* case. Corresponding to these direct sum decompositions, we have inclusions of the corresponding orthogonal groups

$$O(2n-2,E)\times O(2,E)\subset O(2n,E).$$

In the orthogonal group of the first factor, take an element $\zeta\in\mu_{1+q^{n-1}}$ which generates $\mathbb{F}_{q^{2n-2}}$ over $\mathbb{F}_q$. In the orthogonal group of the second factor, take a reflection R of spinor norm one, e.g., take the reflection in a vector of square length one. The centralizer in $O(2n,E)$ of the element (ζ,R) is the product group $\mu_{1+q^{n-1}}\times\{\pm1,\pm R\}$. [Indeed, if an element A in an orthogonal group over a field of characteristic not 2 has a (reversed or not, the two agree up to sign) characteristic polynomial which is a product $\prod_i f_i(T)$ of pairwise prime polynomials, each of which has its roots stable by $x\mapsto 1/x$, then the decomposition of the ambient vector space V as the direct sum of the spaces $V_i:=Ker(f_i(A))$ is an orthogonal decomposition. Any endomorphism B of V which commutes with A preserves this decomposition, say $B=\oplus_i(B_i\ on\ V_i)$, and on each V_i, B_i commutes with $A|V_i$. Moreover, if B is orthogonal, then so is each B_i.] The counting argument used to prove the lemma above then gives the asserted result. □

Lemma 6.4. *Fix $d=2n+1\geq 3$. Suppose $q:=\#E\geq 7$. In each of the four cosets $O(d,E)(det=\pm1,sp=\pm1)$, the fraction of elements A for which $Rdet(1-TA)$ is E-irreducible is at least $1/4n$.*

Proof. We take as model of our quadratic space

$$(\mathbb{F}_{q^{2n}},std)\oplus(\mathbb{F}_q,x^2),$$

and repeat the previous argument, now using elements of the form $(\zeta,\pm1)$. □

Lemma 6.5. *Fix $d=2n\geq 6$. Suppose $q:=\#E\geq 7$. Fix a partition of n as $n=a+b$ with $1\leq a<b$. In each of the two cosets of $\Omega(d,E)$ in $SO_{spl}(d,E)$, the fraction of elements A for which $Rdet(1-TA)$ is of the form*

$$(\mathrm{E-irreducible\ of\ degree\ 2a})(\mathrm{E-irreducible\ of\ degree\ 2b})$$

is at least $1/32ab$.

Proof. We take as model of our quadratic space

$$(\mathbb{F}_{q^{2a}},std)\oplus(\mathbb{F}_{q^{2b}},std),$$

and repeat the previous argument, now using elements of the form $(\zeta_a\in\mu_{1+q^a},\zeta_b\in\mu_{1+q^b})$. If ζ_a (respectively ζ_b) has full degree $2a$ (respectively $2b$) over $\mathbb{F}_q$, the centralizer of this element in $O(2n,E)$

is the product group $\mu_{1+q^a} \times \mu_{1+q^b}$, and the argument concludes as before. □

Lemma 6.6. *Fix $d = 2n \geq 4$. Suppose $q := \#E \geq 7$. In each of the two cosets of $\Omega(d, E)$ in $SO_{spl}(d, E)$, the fraction of elements A for which $Rdet(1 - TA)$ is of the form*

$$(\mathrm{E-irreducible}\ P(T)\ \mathrm{of\ degree\ n})(\mathrm{E-irreducible}\ Q(T)\ \mathrm{of\ degree\ n}),$$

with P and Q relatively prime, and with

$$Q(T) = (\mathrm{some\ constant\ in\ E}^\times)T^n P(1/T),$$

is at least $1/2n$.

Proof. We take as model

$$V := \mathbb{F}_{q^n} \oplus \mathbb{F}_{q^n},$$

with the split quadratic form

$$\Psi(x \oplus y, x \oplus y) := Trace_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xy).$$

The group $\mathbb{F}_{q^n}^\times$ is then a subgroup of $SO(V, \Psi)$, with $\zeta \in \mathbb{F}_{q^n}^\times$ acting as

$$(\zeta, \zeta^{-1}) : x \oplus y \mapsto \zeta x \oplus \zeta^{-1} y.$$

By [Saito-sign, Lemma 1.1, part 2], the spinor norm, restricted to this $\mathbb{F}_{q^n}^\times$ subgroup, is trivial precisely on the squares. Take an element (ζ, ζ^{-1}) such that ζ has full degree n over $\mathbb{F}_q$, and such that ζ and ζ^{-1} have different irreducible polynomials over $\mathbb{F}_q$ (i.e., such that ζ and ζ^{-1} are not Galois conjugate). Then the centralizer of (ζ, ζ^{-1}) in $O(V, \Psi)$ is precisely the subgroup $\mathbb{F}_{q^n}^\times$. Moreover, knowing the characteristic polynomial of (ζ, ζ^{-1}) determines ζ up to replacing it by either one of its n conjugates or by one of the n conjugates of ζ^{-1}.

The ζ's which fail the first condition are those which lie in a proper subfield $\mathbb{F}_{q^a}$ for some divisor $a < n$ of n. Those which fail the second condition are those which lie in some subgroup μ_{1+q^a}, with $2a|n$. For $q \geq 7$, a routine counting shows that the number of ζ's which fail one or both of the two conditions is at most $(q^n - 1)/4$. The argument now concludes as before. □

With these preliminary lemmas established, we get the following product theorems.

Theorem 6.7. *Fix an odd integer $d = 2n + 1 \geq 3$, an integer $r \geq 1$, and a list of r primes*

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

Denote by G the subgroup of the product group $\prod_i O(d, \mathbb{F}_{\ell_i})$ consisting of those elements $(A_1, ..., A_r)$ all of whose determinants, viewed in ± 1, coincide. In any coset of $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ in G, the fraction of elements $(A_1, ..., A_r)$ such that $Rdet(1 - TA_i)$ is $\mathbb{F}_{\ell_i}$-irreducible for some i is at least

$$1 - (1 - 1/4n)^r.$$

Proof. The point is that the quotient $G/\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ is naturally the product of $r + 1$ copies of ± 1, by means of the common value of the determinant and the spinor norms of the factors. So any coset is a product, either of cosets $O(d, \mathbb{F}_{\ell_i})(det = 1, sp = \alpha_i)$, or of cosets $O(d, \mathbb{F}_{\ell_i})(det = -1, sp = \alpha_i)$. The assertion is now immediate from Lemma 6.4. □

Theorem 6.8. *Fix an even integer $d = 2n \geq 4$, an integer $r \geq 1$, and a list of r primes*

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

Denote by G the subgroup of the product group $\prod_i O_{nonspl}(d, \mathbb{F}_{\ell_i})$ consisting of those elements $(A_1, ..., A_r)$ all of whose determinants, viewed in ± 1, coincide. In any coset of $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ in G, the fraction of elements $(A_1, ..., A_r)$ such that $Rdet(1 - TA_i)$ is $\mathbb{F}_{\ell_i}$-irrreducible for some i is at least

$$1 - (1 - 1/8n)^r.$$

Proof. By the product structure of the coset, the assertion is immediate from Lemmas 6.2 and 6.3. □

Theorem 6.9. *Fix an even integer $d = 2n \geq 4$, an integer $r \geq 1$, and a list of r primes*

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

Denote by G the subgroup of the product group $\prod_i O(d, \mathbb{F}_{\ell_i})$ consisting of those elements $(A_1, ..., A_r)$ all of whose determinants, viewed in ± 1, coincide; the factor groups may be separately split or nonsplit at will. In any coset of $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ in G for which the common value of the determinant is -1, the fraction of elements $(A_1, ..., A_r)$ such that $Rdet(1 - TA_i)$ is $\mathbb{F}_{\ell_i}$-irrreducible for some i is at least

$$1 - (1 - 1/8n)^r.$$

Proof. By the product structure of the coset, the assertion is immediate from Lemma 6.3. □

Theorem 6.10. *Fix an even integer $d = 2n \geq 6$, an integer $r \geq 1$, and a list of r primes*

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

Choose a partition of n, say $n = a + b$ with $1 \leq a < b$. Denote by G the subgroup of the product group $\prod_i O_{spl}(d, \mathbb{F}_{\ell_i})$ consisting of those elements $(A_1, ..., A_r)$ all of whose determinants, viewed in ± 1, coincide. In any coset of $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ in G for which the common value of the determinant is $+1$, the fraction of elements $(A_1, ..., A_r)$ such that $Rdet(1 - TA_i)$ is of the form

$$(\mathrm{E-irreducible\ of\ degree\ 2a})(\mathrm{E-irreducible\ of\ degree\ 2b})$$

for some i, AND such that $Rdet(1 - TA_j)$ is of the form

$$(\mathrm{E-irreducible\ of\ degree\ n})(\mathrm{a\ different\ E-irreducible\ of\ degree\ n})$$

for some j, is at least

$$1 - (1 - 1/32ab)^r - (1 - 1/2n)^r.$$

Proof. By the product structure of the coset, the assertion is immediate from Lemmas 6.5 and 6.6 □

Theorem 6.11. *Fix $d = 4$, an integer $r \geq 1$, and a list of r primes*

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

Denote by G the subgroup of the product group $\prod_i O_{spl}(4, \mathbb{F}_{\ell_i})$ consisting of those elements $(A_1, ..., A_r)$ all of whose determinants, viewed in ± 1, coincide. In any coset of $\prod_i \Omega(4, \mathbb{F}_{\ell_i})$ in G for which the common value of the determinant is $+1$, the fraction of elements $(A_1, ..., A_r)$ such that $Rdet(1 - TA_i)$ is, for some i, of the form

$$P(T)Q(T)$$

with $P(T)$ and $Q(T)$ relatively prime $\mathbb{F}_{\ell_i}$-irreducibles of degree 2, neither of which is palindromic, and such that

$$Q(T) = (\text{some constant in E}^\times)T^2P(1/T),$$

is at least

$$1 - (1 - 1/4)^r.$$

Proof. If we omitted the requirement that neither $P(T)$ nor $Q(T)$ be palindromic, the assertion would be immediate from the product structure of the coset, and Lemma 6.6. But the nonpalindromicity is automatic. Indeed, the fact that

$$Q(T) = (\text{some constant in E}^\times)T^2P(1/T),$$

tells us that if $\zeta \in \mathbb{F}_{\ell_i^2}^\times$ is a root of $P(T)$, then $1/\zeta$ is a root of $Q(T)$, hence cannot be a root of $P(T)$, since $P(T)$ and $Q(T)$ are relatively prime. But the two roots of a palindromic polynomial of degree two are reciprocals. Thus $P(T)$ is not palindromic, and similarly for $Q(T)$ □

7. Proof of Theorem 5.2, via a theorem of Larsen

Let us put ourselves in the situation which Theorem 5.2 purports to treat. Choose a finite field k and a ring homomorphism $\phi : R \to k$ (for instance, take a maximal ideal $\mathcal{I}$ of R, take k to be $R/\mathcal{I}$, and take ϕ to be canonical map of R onto $R/\mathcal{I}$). Making the extension of scalars $\phi : R \to k$, we get the space $M_{k,\phi}$. On $M_{k,\phi}$, we have the restrictions of the sheaves $\mathcal{H}_{\mathbb{Q}_\ell}$, for all ℓ invertible in k, as well as of the restrictions of the sheaves $\mathcal{H}_{\mathbb{Z}_\ell}$, for all such ℓ not in the finite set S. For each ℓ invertible in k, let us denote by Γ_ℓ the image in $O(d, \mathbb{Q}_\ell)$ of the arithmetic fundamental group $\pi_1(M_{k,\phi})$ under the homomorphism which "is" $\mathcal{H}_{\mathbb{Q}_\ell}|M_{k,\phi}$. Meanwhile, consider the composite map

$$Spin(d, \mathbb{Q}_\ell) \to SO(d, \mathbb{Q}_\ell) \subset O(d, \mathbb{Q}_\ell).$$

According to a striking theorem of Larsen [Lar-Max, 3.17], the inverse image of Γ_ℓ in $Spin(d, \mathbb{Q}_\ell)$ is, for a set of primes ℓ of Dirichlet density one, a "hyperspecial" maximal compact subgroup of $Spin(d, \mathbb{Q}_\ell)$. Now for all ℓ invertible in k and not in S, Γ_ℓ lies in $O(d, \mathbb{Z}_\ell)$, and so its inverse image lies in $Spin(d, \mathbb{Z}_\ell)$. Whenever this inverse image is a maximal compact subgroup of $Spin(d, \mathbb{Q}_\ell)$, it must, by its maximality, be equal to the possibly larger compact subgroup $Spin(d, \mathbb{Z}_\ell)$. Thus we infer that among the primes ℓ invertible in k and not in S, there is a set of Dirichlet density one, the "good primes" over (k, ϕ), for which the inverse image of Γ_ℓ in $Spin(d, \mathbb{Z}_\ell)$ is the entire group $Spin(d, \mathbb{Z}_\ell)$.

For each of these good ℓ, which we may take to all be ≥ 5, let us denote by $\Gamma_{mod\ \ell}$ the image in $O(d, \mathbb{F}_\ell)$ of the arithmetic fundamental group $\pi_1(M_{k,\phi})$ under the homomorphism which "is" $\mathcal{H}_{\mathbb{Z}_\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell|M_{k,\phi}$. Then by Larsen's theorem, $\Gamma_{mod\ \ell}$ contains $\Omega(d, \mathbb{F}_\ell)$ for these good ℓ. Thus we have

$$\Omega(d, \mathbb{F}_\ell) \subset \Gamma_{mod\ \ell} \subset O(d, \mathbb{F}_\ell).$$

Let us denote by $\Gamma_{geom,mod\ \ell}$ the image in $O(d, \mathbb{F}_\ell)$ of the geometric fundamental group $\pi_1^{geom}(M_{k,\phi})$. Then

$$\Gamma_{geom,mod\ \ell} \lhd \Gamma_{mod\ \ell},$$

and the quotient is cyclic, being a quotient of $Gal(\overline{k}/k)$. We claim that for each good ℓ, we have

$$\Omega(d, \mathbb{F}_\ell) \subset \Gamma_{geom,mod\ \ell}.$$

Indeed, the intersection $\Omega(d, \mathbb{F}_\ell) \cap \Gamma_{geom,mod\ \ell}$ inside $\Gamma_{mod\ \ell}$ is a normal subgroup of $\Omega(d, \mathbb{F}_\ell)$ with cyclic quotient. As $d \geq 3$, $\Omega(d, \mathbb{F}_\ell)$ is its own commutator subgroup, so it has no proper normal subgroup which gives a cyclic quotient. Thus for each good ℓ we have

$$\Omega(d, \mathbb{F}_\ell) \subset \Gamma_{geom, mod\ \ell} \subset \Gamma_{mod\ \ell} \subset O(d, \mathbb{F}_\ell).$$

Suppose we are given an integer $r \geq 1$, and a list of r good primes

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

Denote by G the subgroup of the product group $\prod_i O(d, \mathbb{F}_{\ell_i})$ consisting of those elements $(A_1, ..., A_r)$ all of whose determinants, viewed in ± 1, coincide. Denote by

$$\Gamma_{geom, mod\ \ell_1, \ell_2, ... \ell_r} \subset G \subset \prod_i O(d, \mathbb{F}_{\ell_i})$$

the image of the geometric fundamental group $\pi_1^{geom}(M_{k,\phi})$ under the direct sum of the various *mod* ℓ_i representations.

A key point is the following result of Goursat-Ribet type, cf. [Ribet-Gal, 5.2.2].

Lemma 7.1. *The group* $\Gamma_{geom, mod\ \ell_1, \ell_2, ... \ell_r}$ *contains* $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$*:*

$$\prod_i \Omega(d, \mathbb{F}_{\ell_i}) \subset \Gamma_{geom, mod\ \ell_1, \ell_2, ... \ell_r} \subset G \subset \prod_i O(d, \mathbb{F}_{\ell_i}).$$

Proof. The projection of $\Gamma_{geom, mod\ \ell_1, \ell_2, ... \ell_r} \subset \prod_i O(d, \mathbb{F}_{\ell_i})$ to each $O(d, \mathbb{F}_{\ell_i})$ factor contains $\Omega(d, \mathbb{F}_{\ell_i})$, as we have noted above. Now consider the commutator subgroup $D := D\Gamma_{geom, mod\ \ell_1, \ell_2, ... \ell_r}$ of $\Gamma_{geom, mod\ \ell_1, \ell_2, ... \ell_r}$. As each group $\Omega(d, \mathbb{F}_{\ell_i})$ is its own commutator subgroup, D is a subgroup of $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ which maps onto each factor.

Suppose first that either $d \neq 4$, or that $d = 4$ and all our groups are nonsplit. Then the individual groups $\Omega(d, \mathbb{F}_{\ell_i})$ are simple modulo their centers, and the corresponding simple groups are pairwise nonisomorphic. So by Goursat's Lemma [Ribet-Gal, 5.2.1], D maps onto each pair of factors $\Omega(d, \mathbb{F}_{\ell_i}) \times \Omega(d, \mathbb{F}_{\ell_j}), i < j$. Since each $\Omega(d, \mathbb{F}_{\ell_i})$ has no nontrivial abelian quotients, Ribet's Lemma [Ribet-Gal, 5.2.2] shows that D is the full product $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$.

In the remaining case, when $d = 4$ and all the groups are split, each $\Omega(4, \mathbb{F}_{\ell_i}) / \pm 1$ is $PSL(2, \mathbb{F}_{\ell_i}) \times PSL(2, \mathbb{F}_{\ell_i})$. We first note that as $PSL(2, \mathbb{F}_{\ell_i})$ is simple and nonabelian, the only quotient groups of $\Omega(4, \mathbb{F}_{\ell_i}) / \pm \cong PSL(2, \mathbb{F}_{\ell_i}) \times PSL(2, \mathbb{F}_{\ell_i})$ are the four obvious ones $(\{1\} \times \{1\}, \{1\} \times PSL(2, \mathbb{F}_{\ell_i}), PSL(2, \mathbb{F}_{\ell_i}) \times \{1\}, PSL(2, \mathbb{F}_{\ell_i}) \times PSL(2, \mathbb{F}_{\ell_i}))$. So the only quotient groups of $\Omega(4, \mathbb{F}_{\ell_i})$ are either these groups or, possibly, double covers of them. There is no quotient of order 2, since $\Omega(4, \mathbb{F}_{\ell_i})$ is its own commutator subgroup. Thus the only quotient groups $H_i \neq \{1\}$ of $\Omega(4, \mathbb{F}_{\ell_i})$ have the property that ℓ_i is the largest prime dividing the order of H_i (since ℓ_i is the largest prime dividing the order of $PSL(2, \mathbb{F}_{\ell_i})$). Therefore if $\ell_i \neq \ell_j$, then no quotient $H_i \neq \{1\}$ of $\Omega(4, \mathbb{F}_{\ell_i})$ is isomorphic to any quotient $H_j \neq \{1\}$ of $\Omega(4, \mathbb{F}_{\ell_j})$, simply because these quotients have different orders. So by Goursat's Lemma [Ribet-Gal, 5.2.1], D maps onto each pair of factors $\Omega(4, \mathbb{F}_{\ell_i}) \times \Omega(4, \mathbb{F}_{\ell_j}), i < j$, and the proof then concludes as before, by invoking Ribet's Lemma [Ribet-Gal, 5.2.2]. □

We now make a choice of the integer $r \geq 1$, and of the list of r good primes

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

Recall the real $\epsilon > 0$ in the statement of the theorem we are to prove. There are three separate cases to consider.

If $d = 2n + 1$ is odd, we choose r large enough that

$$(1 - 1/4n)^r < \epsilon/2,$$

and we take any list of r good primes

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r.$$

If $d = 2n$ is even, we first look to see whether or not there are infinitely many good primes ℓ where our orthogonal group $O(d, \mathbb{F}_\ell)$ is nonsplit. If there are, we choose r large enough that

$$(1 - 1/8n)^r < \epsilon/2,$$

and we take any list of r good primes

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r$$

at which the corresponding orthogonal group is nonsplit.

If $d = 2n$ is even, and there are at most finitely many good primes ℓ where our orthogonal group $O(d, \mathbb{F}_\ell)$ is nonsplit, then we choose r large enough that

$$(1 - 1/32n)^r < \epsilon/4,$$

and we take any list of r good primes

$$7 \leq \ell_1 < \ell_2 < ... < \ell_r$$

at which the corresponding orthogonal group is split.

We now study what happens in the geometric generic fibre of M/R. Denote by K the fraction field of R, by $\overline{K}$ an algebraic closure of K, and by $M_{\overline{\eta}}$ the $\overline{K}$-scheme obtained by the extension of scalars $R \subset \overline{K}$.

Denote by

$$\Gamma_{\overline{\eta}, geom, mod\ \ell_1, \ell_2, ... \ell_r} \subset G \subset \prod_i O(d, \mathbb{F}_{\ell_i})$$

the image of the geometric fundamental group $\pi_1^{geom}(M_{\overline{\eta}})$ under the direct sum of the various *mod* ℓ_i representations. By a fundamental specialization result of Pink [Ka-ESDE, 8.18.2, (1)], this group *contains* (an $\prod_i O(d, \mathbb{F}_{\ell_i})$-conjugate of) the group $\Gamma_{geom,mod\ \ell_1,\ell_2,\dots\ell_r}$ we obtained by looking at the image of $\pi_1^{geom}(M_{k,\phi})$. As $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ is a normal subgroup of $\prod_i O(d, \mathbb{F}_{\ell_i})$, being its commutator subgroup, we therefore have

$$\prod_i \Omega(d, \mathbb{F}_{\ell_i}) \subset \Gamma_{\overline{\eta},geom,mod\ \ell_1,\ell_2,\dots\ell_r} \subset G \subset \prod_i O(d, \mathbb{F}_{\ell_i}).$$

By this same result of Pink [Ka-ESDE, 8.18.2, (2)], there is a dense open set U in $Spec(R)$ such that for any geometric point $\overline{s}$ in U, the group

$$\Gamma_{\overline{s},geom,mod\ \ell_1,\ell_2,\dots\ell_r} \subset G \subset \prod_i O(d, \mathbb{F}_{\ell_i}),$$

obtained by looking at the image of $\pi_1^{geom}(M_{\overline{s}})$, is equal to (an $\prod_i O(d, \mathbb{F}_{\ell_i})$-conjugate of) $\Gamma_{\overline{\eta},geom,mod\ \ell_1,\ell_2,\dots\ell_r}$. As every subgroup of $\prod_i O(d, \mathbb{F}_{\ell_i})$ containing $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$ is normal, we therefore have equality:

$$\Gamma_{\overline{s},geom,mod\ \ell_1,\ell_2,\dots\ell_r} = \Gamma_{\overline{\eta},geom,mod\ \ell_1,\ell_2,\dots\ell_r}$$

for every geometric point $\overline{s}$ in U. Each of the primes $\ell_1, ..., \ell_r$ is nonzero in R (because each is invertible in k under ϕ), so by shrinking U we may further assume that each of them is invertible on U.

We will show that the theorem holds, for the fixed $\epsilon > 0$, if we take for $r \in R$ any nonzero element such that $Spec(R[1/r]) \subset U$. Denote by

$$\Gamma_{arith,mod\ \ell_1,\ell_2,\dots\ell_r} \subset G \subset \prod_i O(d, \mathbb{F}_{\ell_i})$$

the image of the arithmetic fundamental group $\pi_1(M[1/r])$. We now apply the Chebotarev density theorem in the uniform version given in [Ka-Sar, 9.7.13] to this situation, our $M[1/r]/R[1/r]$ taken as the X/S there, and with our groups

$$\Gamma_{\overline{\eta},geom,mod\ \ell_1,\ell_2,\dots\ell_r} \subset \Gamma_{arith,mod\ \ell_1,\ell_2,\dots\ell_r}$$

taken as the groups $K \subset K_{arith}$ there. In our situation, the quotient K_{arith}/K is abelian, so the sets $K_{arith,\gamma}$ there are just the cosets of K in K_{arith}. For a given pair (k, ϕ) consisting of a finite field k and a ring homomorphism $\phi : R[1/r] \to k$, all the Frobenius conjugacy classes attached to the k-points of $M_{k,\phi}$ lie in a single coset of K in K_{arith}, say $K_{arith,\gamma}$. Inside this coset $K_{arith,\gamma}$, take the subset W which is defined as follows.

If $d = 2n + 1$ is odd, or if $d = 2n$ and all the r orthogonal groups $O(d, \mathbb{F}_{\ell_i})$ are nonsplit, W consists of all elements $(A_1, ..., A_r)$ in the coset $K_{arith,\gamma}$such that for some i, $Rdet(1 - TA_i)$ is $\mathbb{F}_{\ell_i}$-irreducible.

If $d = 2n \geq 6$ and all the r orthogonal groups $O(d, \mathbb{F}_{\ell_i})$ are split, then W is the disjoint union of two sets, W_- and W_+, defined as follows. The set W_- consists of those elements $(A_1, ..., A_r)$ in the coset $K_{arith,\gamma}$ such that the common value of their determinant is -1 and such that for some i, $Rdet(1 - TA_i)$ is $\mathbb{F}_{\ell_i}$-irreducible. The set W_+ consists of those elements $(A_1, ..., A_r)$ in the coset $K_{arith,\gamma}$ such that the common value of their determinant is $+1$ and such that for some i, $Rdet(1 - TA_i)$ is of the form

$$(\mathbb{F}_{\ell_i} - \text{irreducible of degree 2})(\mathbb{F}_{\ell_i} - \text{irreducible of degree 2n} - 2),$$

AND such that for some j, $Rdet(1 - TA_j)$ is of the form

$$(\mathbb{F}_{\ell_j} - \text{irreducible of degree n})(\text{a different } \mathbb{F}_{\ell_j} - \text{irreducible of degree n}).$$

If $d = 4$ and all the r orthogonal groups $O(4, \mathbb{F}_{\ell_i})$ are split, then W is again the disjoint union of two sets, W_- and W_+. The set W_- is defined exactly as in the paragraph above. The set W_+ consists of those elements $(A_1, ..., A_r)$ in the coset $K_{arith,\gamma}$ such that the common value of their determinant is $+1$ and such that for some i, $Rdet(1 - TA_i)$ is of the form

$$P(T)Q(T)$$

with $P(T)$ and $Q(T)$ relatively prime $\mathbb{F}_{\ell_i}$-irreducibles of degree 2, neither of which is palindromic, and such that

$$Q(T) = (\text{some constant in } \mathbb{F}_{\ell_\text{i}}^\times)T^2P(1/T).$$

Decompose the K-coset $K_{arith,\gamma}$ into cosets under the smaller group $\prod_i \Omega(d, \mathbb{F}_{\ell_i})$, say

$$K_{arith,\gamma} = \coprod_a Coset_a.$$

In view of Theorems 6.7 through 6.10, we see that in each such coset, we have

$$\#(W \cap Coset_a)/\#Coset_a \geq 1 - \epsilon/2.$$

Summing over the cosets, we find that

$$\#W/\#K_{arith,\gamma} \geq 1 - \epsilon/2.$$

By the Chebotarev density theorem in the uniform version given in [Ka-Sar, 9.7.13], there exist constants C and A such that if $\#k \geq 4A^2$, then

$$|\#W/\#K_{arith,\gamma} - \#\{m \in M_{k,\phi}(k)|Frob_{k,m} \in W\}/\#M_{k,\phi}(k)|$$
$$\leq 2C\#K_{arith}/Sqrt(\#k).$$

For $\#k$ sufficiently large, we obviously have

$$2C\#K_{arith}/Sqrt(\#k) \le \epsilon/2,$$

and hence for $\#k$ sufficiently large we have

$$\#\{m \in M_{k,\phi}(k)|Frob_{k,m} \in W\}/\#M_{k,\phi}(k) \ge 1-\epsilon.$$

It remains only to show that whenever $Frob_{k,m}$ lies in W, then $Rdet(1-TFrob_{k,m})$ is $\mathbb{Q}$-irreducible. To see this, we argue as follows. This polynomial has coefficients in $\mathbb{Z}[1/\#k]$. If either d is odd, or d is even and each $O(d,\mathbb{F}_{\ell_i})$ is nonsplit, or d is even and the sign in the functional equation is -1, then for some i the reduction mod ℓ_i of this polynomial $Rdet(1-TFrob_{k,m})$ is $\mathbb{F}_{\ell_i}$-irreducible, this being the defining property of W, and hence $Rdet(1-TFrob_{k,m})$ is $\mathbb{Q}$-irreducible.

It remains to treat the case in which d is even, each $O(d,\mathbb{F}_{\ell_i})$ is split and the sign in the functional equation is $+1$. Suppose first that $d = 2n \ge 6$. Then for some i the reduction mod ℓ_i of $Rdet(1-TFrob_{k,m})$ is the product of two $\mathbb{F}_{\ell_i}$-irreducibles, of degrees 2 and $d-2$, while for some j the reduction mod ℓ_j of $Rdet(1-TFrob_{k,m})$ is the product of two $\mathbb{F}_{\ell_j}$-irreducibles, both of degree n, this being the defining property of W in this case. So once again $Rdet(1-TFrob_{k,m})$ must be $\mathbb{Q}$-irreducible. [For if it were $\mathbb{Q}$-reducible, its $\mathbb{Q}$-factorization would simultaneously be of the form (degree 2 irred.)(degree $d-2$ irred.) and of the form (degree n irred.)(degree n irred.).] Suppose now that $d=4$. Then for some i, $Rdet(1-TFrob_{k,m})$ is the product

$$P(T)Q(T)$$

with $P(T)$ and $Q(T)$ relatively prime $\mathbb{F}_{\ell_i}$-irreducibles of degree 2, neither of which is palindromic, and such that

$$Q(T) = (\text{some constant in } \mathbb{F}_{\ell_{\rm i}}^{\times})T^2P(1/T).$$

This implies that $Rdet(1-TFrob_{k,m})$ is $\mathbb{Q}$-irreducible. For if it were $\mathbb{Q}$-reducible, its $\mathbb{Q}$-factorization would be as the product of two relatively prime $\mathbb{Q}$-irreducibles of degree 2, neither of which is palindromic. But $Rdet(1-TFrob_{k,m})$ has all its eigenvalues on the unit circle (because pure of weight zero), hence both its $\mathbb{Q}$-irreducible quadratic factors have roots stable by inversion $\zeta \mapsto 1/\zeta$. Since these $\mathbb{Q}$-irreducible factors have degree 2, none of their roots is fixed by inversion (i.e., no root is ±1), and hence each $\mathbb{Q}$-irreducible factor has roots of the form $(\zeta, 1/\zeta)$, hence is palindromic.

8. Another application of Theorem 5.1: Universal families of hypersurface sections

Let R be a finitely generated $\mathbb{Z}$-algebra, $\mathbb{P} = \mathbb{P}^N/R$ the projective space of some dimension N, and $X \subset \mathbb{P}$ a closed subscheme which is smooth over R with geometrically connected fibres, all of some common odd dimension $\nu = 2n+1 \geq 3$. Fix an integer $d \geq 1$. Denote by M/R the parameter space for smooth, degree d hypersurfaces in the ambient $\mathbb{P}$ which are transversal to X, by $\mathcal{H}_d/M \subset \mathbb{P}/M$ the universal family of these hypersurfaces, and by $\pi : X \cap \mathcal{H}_d \to M$ the corresponding universal family of smooth, degree d hypersurface sections of X. Concretely, if k is a field and $\phi : R \to k$ is a ring homomorphism, then $M_{k,\phi}$ is the parameter space for smooth, degree d hypersurfaces which are transversal to $X_{k,\phi}$. For each prime ℓ, we have the lisse (but not necessarily torsion-free) $\mathbb{Z}_\ell$-sheaf $R^{2n}\pi_\star\mathbb{Z}_\ell(n)$ on $M[1/\ell]$, together with its cup product pairing

$$R^{2n}\pi_\star\mathbb{Z}_\ell(n) \times R^{2n}\pi_\star\mathbb{Z}_\ell(n) \to R^{4n}\pi_\star\mathbb{Z}_\ell(2n) \cong \mathbb{Z}_\ell,$$

which is an orthogonal autoduality modulo torsion. Let us denote by $\rho : X \to Spec(R)$ the structural morphism of X/R. On $Spec(R[1/\ell])$, we have the lisse $\mathbb{Z}_\ell$-sheaf $R^{2n}\rho_\star\mathbb{Z}_\ell(n)$, and we denote by $R^{2n}\rho_\star\mathbb{Z}_\ell(n)_{M[1/\ell]}$ its pullback to $M[1/\ell]$. The canonical restriction map on cohomology gives an inclusion

$$R^{2n}\rho_\star\mathbb{Z}_\ell(n)_{M[1/\ell]} \subset R^{2n}\pi_\star\mathbb{Z}_\ell(n).$$

We denote by

$$Ev_{\mathbb{Z}_\ell} \subset R^{2n}\pi_\star\mathbb{Z}_\ell(n)$$

the orthogonal to $R^{2n}\rho_\star\mathbb{Z}_\ell(n)_{M[1/\ell]}$ under the cup product pairing. The lisse sheaves $Ev_{\mathbb{Z}_\ell}$ on $M[1/\ell]$,carry the induced cup product pairing

$$Ev_{\mathbb{Z}_\ell} \times Ev_{\mathbb{Z}_\ell} \to \mathbb{Z}_\ell.$$

If we tensor this situation with $\mathbb{Q}_\ell$, the Hard Lefschetz Theorem [De-Weil II, 4.1.2] tells us that this pairing on $Ev_{\mathbb{Q}_\ell} := Ev_{\mathbb{Z}_\ell} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is an orthogonal autoduality. By the Riemann Hypothesis for projective smooth varieties over finite fields [De-Weil I, 1.6], we know that the sheaves $Ev_{\mathbb{Q}_\ell}$ are pure of weight zero, and form a compatible system. By Gabber's theorem [Gab-Tors], for all but finitely many primes ℓ, the sheaves $R^{2n}\rho_\star\mathbb{Z}_\ell(n)$, $R^{2n}\rho_\star\mathbb{Z}_\ell(n)_{M[1/\ell]}$, and $Ev_{\mathbb{Z}_\ell}$ are all torsion free, and the cup product pairing makes $Ev_{\mathbb{Z}_\ell}$ orthogonally self dual over $\mathbb{Z}_\ell$. A fundamental result of Deligne [De-Weil II, 4.4.1,4.4.2s,and 4.4.9], amplified by [Ka-LAMM, 2.2.4] and [Ka-Pan, Corollaries 2 and 3], tells us that the condition (2strong) holds for the compatible system given by the $Ev_{\mathbb{Q}_\ell}$, provided that $d \geq 3$ if $2n \geq 4$, or that $d \geq 4$ if $2n = 2$, and that, under these conditions, the common rank of the sheaves $Ev_{\mathbb{Q}_\ell}$ is ≥ 9. So Theorem 5.1 applies to this situation.

Let us spell out the simplest case of this situation. We take R to be $\mathbb{Z}$, and we take $X = \mathbb{P} = \mathbb{P}^{2n+1}/\mathbb{Z}$, $2n \geq 2$, with the identical embedding of $\mathbb{P}$ into itself. We fix an integer d with $d \geq 3$ if $2n \geq 4$, or that $d \geq 4$ if $2n = 2$. For a finite field $k = \mathbb{F}_q$, and a smooth hypersurface H_d/k of degree d and dimension 2n over k, we know that its Zeta function is of the form

$$Zeta(H_d/k,T) = 1/P(H_d/k,T)\prod_{i=0}^{2n}(1-q^iT).$$

Here $P(H_d/k,T) \in \mathbb{Z}[T]$ is the polynomial whose unitarization

$$P_u(H_d/k,T) := P(H_d/k,T/q^n)$$

is given by

$$P_u(H_d/k,T) = det((1 - TFrob_{k,H_d}|Ev_{\mathbb{Q}_\ell}),$$

for any prime ℓ invertible in k. The reduced unitarization $P_{u,red}$ is defined by

$$P_{u,red}(H_d/k,T) := Rdet((1 - TFrob_{k,H_d}|Ev_{\mathbb{Q}_\ell}).$$

For each finite field k, we denote by $IrrFrac(k,d,2n)$ the fraction of the smooth hypersurfaces H_d/k of degree d and dimension $2n$ over k for which the polynomial $P_{u,red}(H_d/k,T)$ is $\mathbb{Q}$-irreducible. Then Theorem 5.1 gives us the following result.

Theorem 8.1. *In any sequence $i \mapsto k_i$ of finite fields whose cardinalities are strictly increasing, the sequence of fractions $i \mapsto IrrFrac(k_i,d,2n)$ tend to* 1.

9. Alternative approaches

The Chavdarov approach to studying irreducibility requires knowledge of mod ℓ monodromy for infinitely many primes ℓ. We have used Larsen's theorem [Lar-Max, 3.17] to infer, from information about the ℓ-adic monodromy for all (invertible on the base) ℓ, information about mod ℓ monodromy for a set of primes ℓ of Dirichlet density one.There are two other approaches, which, when they apply, give information about mod ℓ monodromy for all but finitely many primes ℓ.

The first is based on the theorem of Mathews, Vaserstein, and Weisfeller [MVW][2], which concerns a smooth groupscheme $G/\mathbb{Z}[1/N]$ whose

[2] Unlike the Larsen result or the Zalesskii-Serezkin result to be discussed below, this result [MVW] depends upon the classification of finite simple groups.

complex fibre $G_{\mathbb{C}}$ is a connected, semisimple, simply connected group, and a finitely generated subgroup $\Gamma \subset G(\mathbb{Z}[1/N])$ which is Zariski dense in $G_{\mathbb{C}}$. For any ℓ which is prime to N, we have a "reduction mod ℓ" homomorphism

$$\Gamma \subset G(\mathbb{Z}[1/N]) \to G(\mathbb{F}_\ell).$$

The theorem asserts that Γ maps onto $G(\mathbb{F}_\ell)$ for all sufficiently large ℓ.

Let us explain an instance of when we can apply this method, and what kind of result it gives. Let us put ourselves in the general setup $E/U/M/R$ of Section 3, and assume that conditions (1) and (2weak) of that section hold, and that $d \geq 3$. Pick an embedding of R into $\mathbb{C}$, and make the corresponding extension of scalars. As explained in the proof of Theorem 3.1, we have, for some integer $N \geq 1$, an orthogonally self-dual lisse sheaf $\mathcal{H}^{an}_{\mathbb{Z}[1/N]}$ on M^{an}. Enlarging N, we will further suppose that N is even. Let us denote by

$$\rho^{an}_{\mathbb{C}} : \pi_1(M^{an}) \to O(d, \mathbb{Z}[1/N])$$

the corresponding "transcendental" monodromy representation attached to $\mathcal{H}^{an}_{\mathbb{Z}[1/N]}$. For every prime ℓ not dividing N, we also have the algebro-geometric ℓ-adic monodromy of $\mathcal{H}_{\mathbb{Z}_\ell}|M_{\mathbb{C}}$,

$$\rho_{\mathbb{C},\ell} : \pi_1(M_{\mathbb{C}}) \to O(d, \mathbb{Z}_\ell).$$

By the comparison theorem, the algebro-geometric fundamental group $\pi_1(M_{\mathbb{C}})$ is the profinite completion of $\pi_1(M^{an})$. For every ℓ not dividing N, the ℓ-adic image $\rho_{\mathbb{C},\ell}(\pi_1(M_{\mathbb{C}})) \subset O(d, \mathbb{Z}_\ell)$ is the closure (in $O(d, \mathbb{Z}_\ell)$ with its profinite topology) of the topological image $\rho^{an}_{\mathbb{C}}(\pi_1(M^{an})) \subset O(d, \mathbb{Z}[1/N])$. By Pink's specialization theorem [Ka-ESDE, 8.18.2, (2)] applied to $\mathcal{H}_{\mathbb{Z}_\ell}$ on $M[1/\ell]$, we may infer from condition (2weak) that the ℓ-adic image $\rho_{\mathbb{C},\ell}(\pi_1(M_{\mathbb{C}}))$ is Zariski dense in either $O(d, \overline{\mathbb{Q}}_\ell)$ or in $SO(d, \overline{\mathbb{Q}}_\ell)$. By the ℓ-adic continuity of polynomial functions, it then follows that the topological image $\rho^{an}_{\mathbb{C}}(\pi_1(M^{an})) \subset O(d, \mathbb{Z}[1/N])$ is Zariski dense in the same group, either $O(d, \overline{\mathbb{Q}}_\ell)$ or $SO(d, \overline{\mathbb{Q}}_\ell)$. Picking an embedding of fields $\overline{\mathbb{Q}}_\ell \subset \mathbb{C}$, we see that the topological image is Zariski dense in either $O(d, \mathbb{C})$ or in $SO(d, \mathbb{C})$. Since the topological fundamental group $\pi_1(M^{an})$ is finitely generated, its image

$$\Gamma_1 := \rho^{an}_{\mathbb{C}}(\pi_1(M^{an})) \subset O(d, \mathbb{Z}[1/N])$$

is a finitely generated subgroup of $O(d, \mathbb{Z}[1/N])$ which is Zariski dense in either $O(d)$ or $SO(d)$. We cannot yet apply [MVW], because the orthogonal group $O(d)$ is not connected and its identity component $SO(d)$ is not simply connected. We get around this difficulty following an argument of Ron Livne. First replace Γ_1 by the subgroup $\Gamma_2 \subset \Gamma_1$ of index 1 or 2 consisting of the elements of determinant $+1$. Then Γ_2

is a finitely generated, Zariski dense subgroup of $SO(d, \mathbb{Z}[1/N])$. Next consider the *Spin* group attached to our orthogonal group. The spinor norm gives an exact sequence

$$\{1\} \to \pm 1 \to Spin(d, \mathbb{Z}[1/N]) \to SO(d, \mathbb{Z}[1/N]) \to \mathbb{Z}[1/N]^\times/(\mathbb{Z}[1/N]^\times)^2,$$

in which the last term, $\mathbb{Z}[1/N]^\times/(\mathbb{Z}[1/N]^\times)^2$, is finite, generated by -1 and by the primes dividing N. Now consider the composite homomorphism

$$\Gamma_2 \subset SO(d, \mathbb{Z}[1/N]) \to \mathbb{Z}[1/N]^\times/(\mathbb{Z}[1/N]^\times)^2.$$

Its image is finite. So the subgroup

$$\Gamma_3 := Ker(\Gamma_2 \to \mathbb{Z}[1/N]^\times/(\mathbb{Z}[1/N]^\times)^2) \subset \Gamma_2$$

is a subgroup of finite index in Γ_2, so is still Zariski dense in SO, and still finitely generated. Every element of Γ_3 lifts, in two different ways, to $Spin(d, \mathbb{Z}[1/N])$. Denote by

$$\Gamma \subset Spin(d, \mathbb{Z}[1/N])$$

the complete inverse image of Γ_3. This group Γ is finitely generated (because Γ_3 is), and, as it maps onto Γ_3, it is Zariski dense in *Spin*. We may now apply the theorem of Mathews, Vaserstein, and Weisfeller [MVW], to $\Gamma \subset Spin(d, \mathbb{Z}[1/N])$, to conclude that for all sufficiently large ℓ prime to N, say for all ℓ not in the finite set S, Γ maps onto $Spin(d, \mathbb{F}_\ell)$. For any such ℓ, Γ_3 maps onto the image of $Spin(d, \mathbb{F}_\ell)$ in $SO(d, \mathbb{F}_\ell)$, i.e., Γ_3 maps onto $\Omega(d, \mathbb{F}_\ell)$. So for any such ℓ, the image of Γ_1 in $O(d, \mathbb{F}_\ell)$ contains $\Omega(d, \mathbb{F}_\ell)$. Because the algebro-geometric fundamental group $\pi_1(M_\mathbb{C})$ is the profinite completion of $\pi_1(M^{an})$, this last image is also the image of $\pi_1(M_\mathbb{C})$ in $O(d, \mathbb{F}_\ell)$. Thus we find that the image of $\pi_1(M_\mathbb{C})$ in $O(d, \mathbb{F}_\ell)$ contains $\Omega(d, \mathbb{F}_\ell)$ for every ℓ not in S.

So far, all of this is taking place on the complex fibre of M/R. Let us say that M/R is nicely compactifiable if there exists a proper smooth R-scheme $M^\wedge/R$ and a divisor $D \subset M^\wedge$ which has normal crossings relative to R, such that $M \cong M^\wedge \setminus D$. By resolution over the characteristic zero fraction field of R, we know that there exists a nonzero $r \in R$ such that $M[1/r]/R[1/r]$ is nicely compactifiable. [This passage, from R to some $R[1/r]$, is not entirely harmless. For instance, in the second example, of Weierstrass families, where we start, for a given (d_2, d_3), with $R = \mathbb{Z}[1/6]$ and the corresponding $M = M_{d_2,d_3}/\mathbb{Z}[1/6]$, we do not know which, if any, other primes p we need to invert to get a nice compactification, nor do we know how this set of p depends on (d_2, d_3). In our 2004-2005 course, we followed the [MVW] method when M/R was nicely compactifiable, as explained in the next paragraph, but then invoked the Larsen method to handle separately each of the finitely many unknown bad p.]

When M/R is nicely compactifiable, with R a normal integral domain whose fraction field has characteristic zero, Abhyankar's Lemma [SGA 1, XIII, 5.5] assures us that for any lisse sheaf on $M[1/\ell]$, and any geometric point s of $Spec(R[1/\ell])$, its restriction to the geometric fibre M_s of $M[1/\ell]/R[1/\ell]$ is tamely ramified at each maximal point of D_s. We apply this to the lisse sheaf $\mathcal{H}_{\mathbb{Z}_\ell} \otimes \mathbb{F}_\ell$ on $M[1/\ell]$, for each ℓ not in S. The Tame Specialization Theorem [Ka-ESDE, 8.17.14] then tells us that for every ℓ not in S, and for every geometric point s of $Spec(R[1/\ell])$, the image of $\pi_1(M_s)$ in $O(d, \mathbb{F}_\ell)$ contains $\Omega(d, \mathbb{F}_\ell)$.

We now turn to a second approach[3] to controlling the mod ℓ monodromy for all but finitely many ℓ. This approach is based on the Zalesskii-Serezkin classification [Zal-Ser, Theorem, page 478] of irreducible subgroups of $GL(n, \overline{\mathbb{F}_\ell}), \ell \geq 3, n \geq 3$, which are generated by reflections and which contain no transvections (:=unipotent pseudoreflections). We can apply this to describe all irreducible subgroups of orthogonal groups in odd characteristic generated by reflections because such orthogonal groups contain no transvections. Here is a baby version of their result in this case.

Theorem 9.1. (Zalesskii-Serezkin) *Given an integer $n \geq 3$, there exists a constant $C(n)$ with the following property. Let $\ell \geq 3$, and (V, Ψ) an n-dimensional $\mathbb{F}_\ell$-vector space with a symmetric autoduality Ψ. Let $G \subset O(V, \Psi)$ be an irreducible subgroup generated by reflections. Denote by $N_O(G)$ the normalizer of G in $O(V, \Psi)$. Then either $\Omega(V, \Psi) \subset G$, or we have the divisibility estimate $\#N_O(G)|C(n)$. Moreover, if $n \geq 9$, we can take $C(n) = 2^n(n+2)!$.*

Proof. We begin by recalling that if $G \subset O(V, \Psi)$ is an irreducible subgroup generated by reflections, then G is absolutely irreducible (i.e., G acts irreducibly after extending scalars from $\mathbb{F}_\ell$ to $\overline{\mathbb{F}_\ell}$). Now for any absolutely irreducible subgroup $G \subset O(V, \Psi)$, we have the divisibility estimate

$$\#N_O(G)|2\#Aut(G),$$

simply because the kernel of the conjugation action homomorphism

$$N_O(G) \to Aut(G)$$

lies in the subgroup of scalars in $O(V, \Psi)$, which is ± 1.

[3] A third approach would be to appeal to the results of Hall [Ha].

It is immediate from [Zal-Ser, Theorem, page 478] that for $n \geq 9$, there are at most two primitive such groups G which fail to contain $\Omega(V, \Psi)$, namely the symmetric group S_{n+1}, if ℓ is prime to $n+1$, and the symmetric group S_{n+2}, if ℓ divides $n+2$. For these G, every automorphism is inner. For $3 \leq n \leq 8$, there are finitely many more such primitive G, and these we handle by the $\#N_O(G)|2\#Aut(G)$ divisibility.

We now consider the imprimitive such G. For $n \geq 5$, any imprimitive such group has a *unique* [Zal-Ser, 4.1] system of imprimitivity consisting of the lines L_i spanned by n linearly independent vectors e_i, and the induced homomorphism maps G onto the symmetric group S_n. For each of $n = 3$ and $n = 4$, there is at most one imprimitive G for which the system of imprimitivity is not unique [Zal-Ser, 4.1], and these cases are handled by the $\#N_O(G)|2\#Aut(G)$ divisibility.

It remains to treat the case of an imprimitive such G which admits a unique system of imprimitivity. By uniqueness, the system of imprimitivity is respected by $N_O(G)$, so we have a homorphism of $N_O(G)$ onto S_n. It remains only to show the following claim: in the basis given by the vectors e_i, any element $g \in N_O(G)$ which lies in the kernel of this homomorphism, i.e., which is diagonal, has entries each ± 1. Indeed, we will show that any element $g \in O(V, \Psi)$ which is diagonal in this basis has entries ± 1. Let us denote by λ_i the diagonal entries of g.

From the fact that G induces every possible permutation of the lines L_i, we see that

(1) Either all square lengths $\Psi(e_i, e_i)$ are nonzero, or they are all zero.
(2) Either all cross terms $\Psi(e_i, e_j)$ are nonzero, for all $i \neq j$, or they are all zero.

If all $\Psi(e_i, e_i)$ are nonzero, our claim is obvious, since

$$\lambda_i^2 \Psi(e_i, e_i) = \Psi(g(e_i), g(e_i)) = \Psi(e_i, e_i).$$

If all $\Psi(e_i, e_i)$ vanish, then by nondegeneracy all $\Psi(e_i, e_j)$ are nonzero, for all $i \neq j$. From the identity

$$\lambda_i \lambda_j \Psi(e_i, e_j) = \Psi(g(e_i), g(e_j)) = \Psi(e_i, e_j),$$

we then infer that for every $i \neq j$, we have $\lambda_i \lambda_j = 1$, which in turn forces all λ_i to be equal to each other, with common value ± 1. □

Armed with this result, we can prove an "almost all ℓ" result about the mod ℓ monodromy of Lefschetz pencil of even fibre dimension $2n \geq 2$. Let us put ourselves in the situation of Section 8, but taking now the base ring R to be a finite field k. We take the degree d of the hypersurface sections large enough that the common rank N of the sheaves $Ev_{\mathbb{Q}_\ell}$, for every ℓ invertible in k, is ≥ 3. We suppose that the condition (2strong) holds, and that there exist, over $\overline{k}$, Lefschetz pencils on X of hypersurface sections of degree d for which (2strong) holds as well. [As noted above, the first condition is automatic if $d \geq 3$ and $d + 2n \geq 6$, in which case we have $N \geq 9$. Moreover, in this case Lefschetz pencils exist, and sufficiently general ones will satisify (2strong).]

Theorem 9.2. *For all sufficiently large primes ℓ, the image of the geometric fundamental group $\pi_1(M_{\overline{k}})$ in $O(N, \mathbb{F}_\ell)$ under the monodromy representation of $Ev_{\mathbb{Z}_\ell} \otimes \mathbb{F}_\ell$ contains $\Omega(N, \mathbb{F}_\ell)$. More precisely, it is the following subgroup of $O(N, \mathbb{F}_\ell)$: if $(-1)^n 2$ is a square in $\mathbb{F}_\ell$, it is the subgroup of elements of spinor norm one. If not, it is the subgroup of elements having $sp = det$. Moreover, for any (sufficiently general, if $char(k) = 2$) Lefschetz pencil satisfying (2strong), we have the same results for the image of its geometric monodromy, with a possibly larger set of "bad" ℓ.*

Proof. By Gabber's theorem [Gab-Tors], applied both to X and to any single smooth hypersurface section $X \cap H_d$ of degree d, we know that for all but finitely many ℓ, both spaces have their $\mathbb{Z}_\ell$-cohomology torsion free, and the hard Lefschetz theorem holds mod ℓ on both. These are the "good ℓ" for the theorem. Because the fibre dimension $2n$ is even, we know, by [SGA 7 II, XV 3.4, XVIII 6.2 and 6.3], that "condition A" of [SGA 7 II, XVIII 5.3.5] holds for any Lefschetz pencil on X. An attentive reading of the entire exposé [SGA 7 II, XVIII] then shows that for all these good ℓ, the mod ℓ geometric monodromy of any (sufficiently general, if $char(k) = 2$) Lefschetz pencil is an irreducible subgroup of $O(N, \mathbb{F}_\ell)$ (this uses the conjugacy of the vanishing cycles [De-Weil II, 4.2.7]) which is generated by reflections in various vectors δ_i with square length $\delta_i \cdot \delta_i = (-1)^n 2$ (this is the Picard Lefschetz formula [SGA 7 II, XV 3.4]).

Let us begin with a Lefschetz pencil, defined over $\overline{k}$ and hence over some finite extension E/k, for which (2strong) holds. Since the statements to be proven are geometric, we may extend scalars, and reduce to the case when our Lefschetz pencil satisfying (2strong) is defined over k. From the theorem of Zalesskii-Serezkin above, we see for a given good ℓ, there are only two possibilities: either the image $\Gamma_{geom,mod\ \ell}$ of the geometric monodromy group of our Lefschetz pencil is the asserted group, or its normalizer $N_O(\Gamma_{geom,mod\ \ell})$, which *contains* the mod ℓ image $\Gamma_{arith,mod\ \ell}$ of the arithmetic monodromy group, is a group whose order divides $C(N)$. We will show that this can happen for only finitely many good ℓ. Indeed, we will show that the inequality $\#\Gamma_{arith,mod\ \ell} \leq C(N)$ can hold for only finitely many good ℓ. For this, we argue as follows.

Because our pencil satisfies (2strong), we know by Deligne's equidistribution theorem, cf. [Ka-GKM, 3.6], that as we run over larger and larger finite extensions E/k, and consider all the smooth, degree d hypersurface sections $X \cap H_d$ defined over E, the (unique conjugacy classes having) reversed characteristic polynomials

$$det(1 - TFrob_{k,X\cap H_d}|Ev^n) \in \mathbb{Z}[1/\#k][T]$$

become equidistributed, for (the direct image of) Haar measure, in the space $O(N,\mathbb{R})^{\#}$ of conjugacy classes in the compact orthogonal group $O(N,\mathbb{R})$. The space $O(N,\mathbb{R})^{\#}$ is a compact metric space [namely, the set of all degree N polynomials in $1 + T\mathbb{R}[T]$ all of whose roots lie on the unit circle], every nonempty open set has strictly positive measure, and it is infinite. So if we take $1+C(N)$ distinct points A_i in $O(N,\mathbb{R})^{\#}$, and tiny open balls B_i around A_i which are pairwise disjoint, then for E sufficiently large, we can find $1 + C(N)$ different smooth, degree d hypersurface sections $X \cap H_{d,i}$ defined over E such that the reversed characteristic polynomial of $Frob_{k,X\cap H_{d,i}}$ lands in B_i. So these reversed characteristic polynomials are pairwise distinct. Let us enumerate these polynomials, say $P_0(T), P_1(T), ..., P_{C(N)}(T)$. Now consider the product polynomial

$$R(T) := \prod_{0\leq i<j\leq C(N)} (P_i(T) - P_j(T)).$$

This is a nonzero polynomial in $\mathbb{Z}[1/\#k][T]$, hence it is nonzero mod all sufficiently large primes ℓ. For any good prime ℓ mod which it is nonzero, the $1 + C(N)$ Frobenius conjugacy classes $Frob_{k,X\cap H_{d,i}}$ must have distinct images in $\Gamma_{arith,mod\ell}$, since they have distinct mod ℓ characteristic polynomials. So certainly we have $\#\Gamma_{arith,mod\ell} \geq 1 + C(N)$ for these good ℓ.

To treat the situation over M itself, we note that our single Lefschetz pencil above shows us for all sufficiently large good primes ℓ, the image of the geometric fundamental group $\pi_1(M_{\overline{k}})$ in $O(N,\mathbb{F}_\ell)$ under the monodromy representation of $Ev_{\mathbb{Z}_\ell}\otimes\mathbb{F}_\ell$ contains the asserted subgroup of $O(N,\mathbb{F}_\ell)$. To see that this image can be no bigger, use the fact that for any given good prime ℓ, Bertini's theorem says that already a sufficiently general Lefschetz pencil will have the same mod ℓ geometric monodromy as does M itself. Since other choices of Lefschetz pencils may require omitting fewer good ℓ than did our initial choice, the result over M may have fewer bad ℓ that the result for some particular choice of Lefschetz pencil. □

References

[Artin-GA] Artin, E., Geometric Algebra, Interscience Publishers, 1957. reprinted in Wiley Classics Library, John Wiley, 1988.

[AtBS-Clif] Atiyah, M. F.; Bott, R.; Shapiro, A., Clifford modules. Topology 3 1964 suppl. 1, 3-38.

[Bour-AlgIX] Bourbaki, N. Eléments de mathématique. Première partie: Les structures fondamentales de l'analyse. Livre II: Algèbre. Chapitre 9: Formes sesquilinéaires et formes quadratiques. Actualités Sci. Ind. no. 1272 Hermann, 1959.

[Chav] Chavdarov, N., The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. Duke Math. J. 87 (1997), no. 1, 151-180.

[Chev-Spin] Chevalley, C., The algebraic theory of spinors. Columbia University Press, New York, 1954. reprinted in The algebraic theory of spinors and Clifford algebras. Collected works. Vol. 2. Edited and with a foreword by Pierre Cartier and Catherine Chevalley. With a postface by J.-P. Bourguignon. Springer-Verlag, Berlin, 1997.

[deJ-Ka] de Jong, A. Johan, Katz, Nicholas M., Monodromy and the Tate conjecture: Picard numbers and Mordell-Weil ranks in families. Israel J. Math. 120 (2000), part A, 47-79.

[De-Weil I] Deligne, P., La conjecture de Weil. Publ. Math. IHES 43 (1974), 273-307.

[De-Weil II] Deligne, P., La conjecture de Weil II. Publ. Math. IHES 52 (1981), 313-428.

[Die-GC] Dieudonné, J. Sur les groupes classiques. Troisième édition revue et corrigée. Publications de l'Institut de Mathématique de l'Université de Strasbourg, VI. Actualités Scientifiques et Industrielles, No. 1040. Hermann, Paris, 1959.

[Dw-Rat] Dwork, B., On the rationality of the zeta function of an algebraic variety. Amer. J. Math. 82 (1960), 631-648.

[Gab-Tors] Gabber, O., Sur la torsion dans la cohomologie l-adique d'une variété. C. R. Acad. Sci. Paris Sér. I Math. 297 (1983), no. 3, 179-182.

[Gr-Rat] Grothendieck, A., Formule de Lefschetz et rationalité des fonctions L. Séminaire Bourbaki, Vol. 9, Exp. No. 279, 41-55, Soc. Math. France, 1995.

[Ha] Hall, C., Big symplectic or orthogonal monodromy modulo ℓ, Duke Math. J. 141 (2008), no. 1, 179-203.

[Jo] Jouve, F., Méthodes de crible et sommes d'exponentielles, thesis, Univ. Bordeaux I, Déc., 2008.

[Kar-Clif] Karoubi, M., Algèbres de Clifford et K-théorie. Ann. Sci. Ecole Norm. Sup. (4) 1 1968 161-270.

[Ka-ESDE] Katz, N., Exponential sums and differential equations, Annals of Math. Study 124, Princeton Univ. Press, 1990.

[Ka-GKM] Katz, N., Gauss sums, Kloosterman sums, and monodromy groups, Annals of Math. Study 116, Princeton Univ. Press, 1988.

[Ka-LAMM] Katz, N., Larsen's alternative, moments, and the monodromy of Lefschetz pencils. Contributions to automorphic forms, geometry, and number theory, 521-560, Johns Hopkins Univ. Press, Baltimore, MD, 2004.

[Ka-MMP] Katz, N., Moments, monodromy, and perversity: a Diophantine perspective. Annals of Math. Study 159. Princeton University Press, 2005.

[Ka-Pan] Katz, N.; Pandharipande, R., Inequalities related to Lefschetz pencils and integrals of Chern classes. Geometric aspects of Dwork theory. Vol. I, II, 805-818, Walter de Gruyter GmbH & Co. KG, Berlin, 2004.

[Ka-Sar] Katz, N.; Sarnak, P., Random matrices, Frobenius eigenvalues, and monodromy. American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999.

[Ka-TLFM] Katz, N., Twisted L-functions and monodromy. Annals of Math. Study 150. Princeton University Press, 2002.

[Kow-LSM] Kowalski, E., The large sieve, monodromy and zeta functions of curves, Crelle 601 (2006), 29-69.

[Kow-RQT] Kowalski, E., On the rank of quadratic twists of elliptic curves over function fields, Int'l. J. of Number Theory 2 (2006), 267-288.

[Lar-Max] Larsen, M. Maximality of Galois actions for compatible systems. Duke Math. J. 80 (1995), no. 3, 601-630.

[MVW] Matthews, C. R.; Vaserstein, L. N.; Weisfeiler, B. Congruence properties of Zariski-dense subgroups. I. Proc. London Math. Soc. (3) 48 (1984), no. 3, 514-532.

[Poonen] Poonen, B., Bertini theorems over finite fields. Ann. of Math. (2) 160 (2004), no. 3, 1099-1127.

[Ribet-Gal] Ribet, K., Galois action on division points of Abelian varieties with real multiplications. Amer. J. Math. 98 (1976), no. 3, 751-804.

[Saito-sign] Saito, T., The sign of the functional equation of the L-function of an orthogonal motive. Invent. Math. 120 (1995), no. 1, 119-142.

[SGA 1] Revêtements étales et groupe fondamental. Séminaire de Géométrie Algébrique du Bois Marie 1960-1961 (SGA 1). Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud. Lecture Notes in Mathematics, Vol. 224, Springer-Verlag, 1971.

[SGA 7 II] Groupes de monodromie en géométrie algébrique. II. Séminaire de Géométrie Algébrique du Bois-Marie 1967-1969 (SGA 7 II). Dirigé par P. Deligne et N. Katz. Lecture Notes in Mathematics, Vol. 340. Springer-Verlag, 1973.

[Weyl] Weyl, H., Classical Groups, Princeton University Press, 1946.

[Zal-Ser] Zalesskiĭ, A. E.; Serežkin, V. N. Finite linear groups generated by reflections. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 44 (1980), no. 6, 1279-1307, 38, translated in Math. USSR. Izvestijia 17 (1981), No. 3, 477-503.

Princeton University, Mathematics, Fine Hall, NJ 08544-1000, USA
E-mail address: nmk@math.princeton.edu