ON THE RANK OF QUADRATIC TWISTS OF ELLIPTIC CURVES OVER FUNCTION FIELDS

E. KOWALSKI

ABSTRACT. We prove quantitative upper bounds for the number of quadratic twists of a given elliptic curve $E/\mathbf{F}_q(C)$ over a function field over a finite field that have rank $\geqslant 2$, and for their average rank. The main tools are constructions and results of Katz and uniform versions of the Chebotarev density theorem for varieties over finite fields. Moreover, we conditionally derive a bound in some cases where the degree of the conductor is unbounded.

Let first $E/\mathbf{Q}$ be an elliptic curve over $\mathbf{Q}$, and for fundamental quadratic discriminants d, let E_d denote the curve E twisted by the associated Kronecker character χ_d. Goldfeld conjectured that E_d is most of the time of minimal rank compatible with the root number of E_d, which in this case means

$$\lim_{D\to+\infty} \frac{1}{|\{d \mid |d|\leqslant D\}|} \sum_{|d|\leqslant D} \operatorname{rank} E_d(\mathbf{Q}) = \frac{1}{2}.$$

This conjecture has been refined by Conrey, Keating, Rubinstein and Snaith [CKRS], using ideas based on Random Matrix Theory models and discretization properties of special values of L-functions. For instance, restricting the family to those d for which the sign of the functional equation of $L(E_d, s)$ is $+1$, they predict that for some constants $c_E > 0$ and $b_E \in \mathbf{R}$, we have

$$|\{d \mid |d|\leqslant D, \text{ the root number of } E_d \text{ is 1 and } \operatorname{rank} E_d(\mathbf{Q}) \geqslant 2\}| \sim c_E D^{3/4} (\log D)^{b_E} \tag{1}$$

as $D \to +\infty$, whereas the number of d being counted is of size D.

Note in particular that this predicts that there are few curves with large rank, but gives also a lower bound for this number.

From the analytic point of view, both conjectures are naturally seen as statements about the order of vanishing of L-functions at the central critical point, translated into the rank of E_d by assuming the Birch and Swinnerton-Dyer conjecture. This is indeed how they arise, and one may expect to make progress on the analytic side independently of the status of the Birch and Swinnerton-Dyer conjecture.

An analogue of this problem for elliptic curves over function fields has been developed by Katz [K1]: given an elliptic curve $E/\mathbf{F}_q(t)$ (or over another function field over a finite field), Katz shows how to construct various algebraic varieties $X/\mathbf{F}_q$ which parameterize twists of E subject to certain conditions. After a deep monodromy computation, he obtains what can be considered as an analogue of Goldfeld's original statement[1], up to the fact that the parameter which gets large is not the conductor of the twisted curve, but rather the degree of the coefficient field of the functions used to twist the curve (see also [U1, p. 134, 135] and Section 3).

It is tempting to attack the more refined conjecture of [CKRS] next, but there appear analytic difficulties in the application of Deligne's equidistribution theorem.

We will show how to use a uniform version of Chebotarev's density theorem (based on uniform estimates for ℓ-adic Betti numbers proved in [Ko]) to obtain a stronger quantitative form of the analogue of Goldfeld's conjecture, under some monodromy assumptions which follow from the results of Katz. This can be seen as a first progress towards the analogue of the upper bound

2000 *Mathematics Subject Classification.* Primary 11G05, Secondary 11G40, 11R45.

Key words and phrases. Elliptic curves over function field over finite fields, Chebotarev density theorem, rank of elliptic curves.

[1] Stated for the analytic rank, but from Ulmer's work on the Birch and Swinnerton-Dyer conjecture when the analytic rank is $\leqslant 1$, the case of algebraic rank follows, as explained in Section 3.

in (1) in this context; see Corollary 9 and Proposition 6 for precise statements (roughly, a small power of q is gained).

It would be very interesting also to obtain a lower bound, but we do not consider this question; notice however that over $\mathbf{Q}$, fairly strong lower bounds for the occurrence of algebraic rank $\geqslant 2$ are known by using results of sieve theory (see e.g. [GM]). This method should presumably extend to the function field case (the lower bound would probably be closer to the truth than our upper bounds are), and lower bounds for occurrence of algebraic rank $\geqslant 2$ are also lower bounds for occurrence of analytic rank $\geqslant 2$ in this case.

In principle, we could obtain results in situations where the conductor is unbounded and the twists are restricted to special one-parameter families. However, in that case we need rather stronger monodromy results, and those do not seem available (on the other hand, they are certainly within the realm of reason), even in special cases. Still, we describe what could be true in the last section of this paper.

We should also mention that the results of Katz are in fact much more general, and the method used here should adapt easily. We restrict our attention to the case of quadratic twists of elliptic curves partly for concreteness and partly in the hope of providing a reasonably readable introduction to those remarkable results for readers with an analytic number theory background.

Notation. As usual, $|X|$ denotes the cardinality of a set. By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geqslant 0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. The "implied constant" is any admissible value of C. It may depend on the set X which is always specified or clear in context.

Acknowledgments. Work on this paper was prompted by discussions with J. Keating. I wish also to thank N. Katz for explaining a number of points concerning the behavior of monodromy for sheaves with orthogonal symmetry.

1. A uniform version of the Chebotarev density theorem

In this section we prove a general uniform Chebotarev density theorem for varieties over finite fields. The main tools are the cohomological methods and results developed notably by Grothendieck and Deligne; a short and fairly concrete survey aimed at analytic number theorists, which should be sufficient to explain the terminology and the proofs below, can be found in [IK, 11.11].

We consider the following data: $U/\mathbf{F}_q$ is a smooth affine variety, absolutely irreducible and of dimension $d \geqslant 1$ over a finite field of characteristic p with q elements, $\ell \neq p$ is a prime number, and $\rho : \pi_1(U, \overline{\eta}) \to G$ is a surjective map from the arithmetic fundamental group of U (relative to a geometric generic point of U) to a finite group G. We denote by

$$G^g = \rho(\pi_1(\overline{U}, \overline{\eta})) \subset G$$

the image of the geometric fundamental group of U, where $\overline{U} = U \times \overline{\mathbf{F}}_q$. Recall there are exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1(\overline{U}, \overline{\eta}) & \longrightarrow & \pi_1(U, \overline{\eta}) & \xrightarrow{d} & \hat{\mathbf{Z}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & G^g & \longrightarrow & G & \xrightarrow{m} & \Gamma & \longrightarrow & 1, \end{array} \tag{2}$$

where the quotient Γ thus defined is a finite cyclic group.

For any $u \in U(\mathbf{F}_q)$, we denote by Fr_u the geometric Frobenius conjugacy class at u in $\pi_1(U, \overline{\eta})$. In other words, corresponding to the inclusion $\{u\} = \mathrm{Spec}(\mathbf{F}_q) \to U$, we have an induced homomorphism

$$\pi_1(\mathbf{F}_q) = \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q) \to \pi_1(U, \overline{\eta})$$

and Fr_u is the image, well-defined up to conjugation, of the inverse of the generator $x \mapsto x^q$ of $\mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q)$. (If we consider u as defined over a bigger field, then Fr_u changes, so Fr_u is defined

relative to the field $\mathbf{F}_q$; it is often denoted $\mathrm{Fr}_{u,\mathbf{F}_q}$ for this reason, but we consider the base field as fixed in our statements). In the exact sequence above, we have

$$d(\mathrm{Fr}_{u,\mathbf{F}_{q^n}}) = -n \in \hat{\mathbf{Z}}.$$

The uniform Chebotarev density theorem is the following:

Theorem 1. *With notation as above, let $C \subset G$ be a conjugacy-invariant subset such that $m(x) = \varphi(-1)$ for all $x \in C$. Put*

$$\pi(C; q) = |\{u \in U(\mathbf{F}_q) \mid \rho(\mathrm{Fr}_u) \in C\}|.$$

Assume that G^g is of order prime to p. Then we have

$$\pi(C; q) = \frac{|C|}{|G^g|}|U(\mathbf{F}_q)| + O(q^{d-1/2}|G||C|^{1/2}), \tag{3}$$

the implied constant depending only on $\overline{U} = U \times \overline{\mathbf{F}}_q$. In particular, this holds uniformly with q replaced by q^n and U by $U \times \mathbf{F}_{q^n}$, $n \geqslant 1$.

Proof. This is essentially the same as the statement in e.g. [C, Th. 4.1], except that we have to take care of the uniformity. Let f denote the characteristic function of C and let

$$f(g) = \sum_{\pi} \alpha(\pi) \operatorname{Tr} \pi(g) \tag{4}$$

be its Fourier expansion in terms of the irreducible representations π of G, which we realize as homomorphisms

$$\pi : G \to GL(\deg(\pi), E)$$

for some finite extension $E/\mathbf{Q}_\ell$, which can be chosen independent of π. If π is trivial on G^g, there is a unique (degree 1) character ψ of Γ such that $\operatorname{Tr} \pi(g) = \psi(m(g))$ for all $g \in G$. Hence $\operatorname{Tr} \pi(\rho(\mathrm{Fr}_u)) = \psi(\varphi(-1))$ by the assumption on C. Conversely, any character ψ gives a representation π of G trivial on G^g. So the contribution to (4) from all representations π which are trivial on G^g is equal to

$$\sum_{\psi} \alpha(\psi) \operatorname{Tr} \psi(\rho(\mathrm{Fr}_u)) = \psi(\varphi(-1)) \sum_{\psi} \frac{1}{|G|} \sum_{x \in C} \psi(x) = \frac{|C|}{|G^g|},$$

where ψ runs over characters of Γ.

Now applying the Fourier expansion to $f(\rho(\mathrm{Fr}_u))$ we find therefore that

$$\pi(C; q) = \frac{|C|}{|G^g|}|U(\mathbf{F}_q)| + \sum_{\pi | G^g \neq 1} \alpha(\pi) \sum_{u \in U(\mathbf{F}_q)} \operatorname{Tr} \pi(\rho_\ell(\mathrm{Fr}_u)).$$

The inner sum is the sum of local traces for the representation

$$\pi_1(U, \overline{\eta}) \xrightarrow{\pi \circ \rho} GL(\deg(\pi), E),$$

which can be seen as a lisse $\overline{\mathbf{Q}}_\ell$-adic sheaf, denoted $\pi(\rho)$. Since the image of ρ, hence of $\pi(\rho)$, is finite, this sheaf is pointwise pure of weight 0. By the Grothendieck-Lefschetz trace formula we have

$$\sum_{u \in U(\mathbf{F}_q)} \operatorname{Tr} \pi(\rho(\mathrm{Fr}_u)) = \sum_{i=0}^{2d} (-1)^i \operatorname{Tr}(\mathrm{Fr} \mid H_c^i(\overline{U}, \pi(\rho))),$$

where $\overline{U} = U \times \overline{\mathbf{F}}_q$ and Fr is the global geometric Frobenius automorphism.

In terms of the geometric fundamental group $\pi_1(\overline{U}, \overline{\eta})$, the coinvariant description of H_c^{2d} gives

$$H_c^{2d}(\overline{U}, \pi(\rho)) = E^{\deg(\pi)}_{\pi_1(\overline{U}, \overline{\eta})}(-d) = E^{\deg(\pi)}_{G^g}(-d) = 0$$

since π, being non-trivial when restricted to G^g, can not contain the trivial representation, simply because the space of invariants under G^g is a subrepresentation of G, which is irreducible.

Moreover, by Deligne's Theorem, the eigenvalues of the geometric Frobenius Fr acting on each $H_c^i(\overline{U}, \pi(\rho))$ are algebraic integers with absolute value in $\mathbf{C}$ of modulus $\leqslant q^{i/2}$. Thus we find

$$\Big| \sum_{u \in U(\mathbf{F}_q)} \operatorname{Tr} \pi(\rho(\mathrm{Fr}_u)) \Big| \leqslant q^{d-1/2} \sigma_c'(\overline{U}, \pi(\rho)),$$

where

$$\sigma_c'(\overline{U}, \pi(\rho)) = \sum_{i<2d} \dim H_c^i(\overline{U}, \pi(\rho)).$$

It only remains to bound the quantity

$$\sum_{\pi | G^g \neq 1} |\alpha(\pi)| \sigma_c'(\overline{U}, \pi(\rho))$$

uniformly in terms of π and ρ. By Proposition 4.7 of [Ko], using the assumption that $|G^g|$ is prime to p, there exists a constant $C \geqslant 0$, depending only on $\overline{U}$, such that

$$\sigma_c'(\overline{U}, \pi(\rho)) \leqslant C|G|(\deg \pi)$$

for all π. Hence

$$\sum_{\pi | G^g \neq 1} |\alpha(\pi)| \sigma_c'(\overline{U}, \pi(\rho)) \leqslant C|G| \sum_{\pi} |\alpha(\pi)| \deg \pi$$

and by Cauchy's inequality and the standard properties of representations of finite groups we get

$$\sum_{\pi} |\alpha(\pi)| \deg \pi \leqslant \Big(\sum_{\pi} |\alpha(\pi)|^2 \Big)^{1/2} \Big(\sum_{\pi} (\deg \pi)^2 \Big)^{1/2} = \sqrt{\frac{|C|}{|G|}} \sqrt{|G|} = \sqrt{|C|}.$$

Putting these inequalities together yields the stated result. □

Remark 2. Since

$$|U(\mathbf{F}_q)| = q^d + O(q^{d-1/2})$$

by the Lang-Weil estimate, the implied constant depending only on $\overline{U}$, we can also rephrase the result as

$$\pi(C; q) = \frac{|C|}{|G^g|} q^d + O(q^{d-1/2} |G| |C|^{1/2}).$$

Here is a variant of this theorem when the variety U is a smooth affine curve and the map ρ arises by reduction from a torsion-free $\mathbf{Z}_\ell$-adic sheaf, using Proposition 4.1 of [Ko] (or indeed, since we assume tameness, the last part of Theorem 4.1 in [C]) instead of Proposition 4.7. In this case, the dependence on U can be made explicit (and the error term is improved) which allows certain interesting applications (see the last section).

Theorem 3. *Let $U/\mathbf{F}_q$ be a smooth geometrically irreducible affine curve, realized as an open dense subset of a smooth projective curve $C/\mathbf{F}_q$ of genus g, with $m = |(C-U)(\overline{\mathbf{F}}_q)|$ "points at infinity". Let $\ell \neq p$ be a prime number, let $\mathcal{F}$ be a tame torsion free lisse $\mathbf{Z}_\ell$-adic sheaf of rank N, and let $\overline{\mathcal{F}} = \mathcal{F}/\ell\mathcal{F}$ be its reduction modulo ℓ. Denote*

$$\rho_\ell : \pi_1(U, \overline{\eta}) \to GL(N, \mathbf{F}_\ell)$$

the corresponding continuous representation and put

$$G_\ell = \rho_\ell(\pi_1(U, \overline{\eta})), \quad G_\ell^g = \rho_\ell(\pi_1(\overline{U}, \overline{\eta})),$$

let Γ_ℓ be the quotient and m, φ as in (2) in this case.

Then for any conjugacy invariant subset $C(\ell) \subset G_\ell$ such that $m(C(\ell)) = \{\varphi(-1)\}$, we have

$$\pi(C(\ell); q) = \frac{|C(\ell)|}{|G_\ell|} |U(\mathbf{F}_q)| + O((m+g) q^{1/2} |C(\ell)|^{1/2}),$$

where the implied constant is absolute.

Proof. As above we find by Fourier expansion that

$$\pi(C(\ell);q) = \frac{|C(\ell)|}{|G_\ell|}|U(\mathbf{F}_q)| + O(q^{1/2}|\mathfrak{S}|)$$

where

$$\mathfrak{S} = \sum_{\pi|G_\ell^q \neq 1} |\alpha(\pi)|\sigma_c'(\overline{U}, \pi(\rho_\ell))$$

and the implied constant is absolute (in fact, can be taken to be equal to 1).

By Proposition 3.1 of [Ko] (see eq. (3.1) and note that the term w there vanishes by the tameness assumption), we have

$$\sigma_c'(\overline{U}, \pi(\rho_\ell)) \leqslant (1 - \chi_c(\overline{U}, \mathbf{Q}_\ell))(\deg \pi)$$

where

$$\chi_c(\overline{U}, \mathbf{Q}_\ell) = \dim H_c^0(\overline{U}, \mathbf{Q}_\ell) - \dim H_c^1(\overline{U}, \mathbf{Q}_\ell) + \dim H_c^2(\overline{U}, \mathbf{Q}_\ell)$$

is the Euler-Poincaré characteristic of $\overline{U}$. This is equal to $2 - 2g - m$ (because it is "additive", so equal to $\chi_c(\overline{C}) - \chi_c(\overline{C} - \overline{U}) = 2 - 2g - m$), hence

$$\sigma_c'(\overline{U}, \pi(\rho_\ell)) \leqslant (2g + m - 1)(\deg \pi).$$

Summing over π yields the estimate

$$\mathfrak{S} \leqslant (m + 2g - 1) \sum_\pi |\alpha(\pi)| \deg \pi \leqslant (m + 2g - 1)\sqrt{|C(\ell)|},$$

hence the result claimed. □

Remark 4. There are other uniform versions of the Chebotarev density theorem for curves, for instance [FJ, Pr. 5.16], which is written and proved in a style closer to the standard number field case. (But note that the version in the first edition of loc. cit. has a mistake corrected in the second).

2. Application to sheaves with orthogonal monodromy

We will now apply the uniform Chebotarev density theorem to reductions of a lisse ℓ-adic sheaf with "orthogonal" symmetry. The method turns out to be essentially identical with that used by Serre in his applications of the Chebotarev density theorem over number fields (see [S1]).

As in the previous section we start with a smooth affine absolutely irreducible variety of dimension $d \geqslant 1$ defined over a finite field $\mathbf{F}_q$ of characteristic p. Let $N \geqslant 1$ be an integer and $\ell \neq p$ a prime number such that $GL(N, \mathbf{F}_\ell)$ has order prime to p. This also implies that for all $\nu \geqslant 1$, the group $GL(N, \mathbf{Z}/\ell^\nu\mathbf{Z})$ has order prime to p.

Consider now a lisse integral torsion free ℓ-adic sheaf $\mathcal{F}_\ell$ of rank N on U; equivalently, consider a continuous representation

$$\tau_\ell \,:\, \pi_1(U, \overline{\eta}) \to GL(N, \mathbf{Z}_\ell).$$

We assume that $\mathcal{F}_\ell$ is equipped with a non-degenerate symmetric pairing

$$\langle \cdot, \cdot \rangle \,:\, \mathcal{F}_\ell \otimes \mathcal{F}_\ell \to \mathbf{Z}_\ell,$$

equivalently, τ_ℓ acts on $\mathbf{Z}_\ell^N$ by transformations leaving invariant a non-degenerate symmetric pairing. We denote by $O(N, \mathbf{Z}_\ell)$ the whole group of transformations leaving this pairing invariant (which depends on the equivalence class of the pairing, but this will not be of any importance).

We make the following assumption of large monodromy on τ_ℓ:

$$[O(N, \mathbf{Z}_\ell) : \tau_\ell(\pi_1(U, \overline{\eta}))] < +\infty. \tag{5}$$

For any $\nu \geqslant 1$ we can consider the reduction modulo ℓ^ν of $\mathcal{F}_\ell$, i.e. $\overline{\mathcal{F}}_\nu = \mathcal{F}_\ell/\ell^\nu\mathcal{F}_\ell$, which corresponds to the maps

$$\rho_\nu \,:\, \pi_1(U, \overline{\eta}) \to GL(N, \mathbf{Z}/\ell^\nu\mathbf{Z}),$$

and we put

$$G_\nu = \rho_\nu(\pi_1(U, \overline{\eta})).$$

The assumption (5) ensures that the groups G_ν are also "large" when ν is large enough : the index

$$[O(N, \mathbf{Z}/\ell^\nu \mathbf{Z}) : G_\nu] \tag{6}$$

is *bounded* for $\nu \geqslant 1$ (the reductions of any finite set of coset representatives for $\tau_\ell(\pi_1(U, \overline{\eta}))$ in $O(N, \mathbf{Z}_\ell)$ give coset representatives for G_ν in $O(N, \mathbf{Z}/\ell^\nu \mathbf{Z})$).

We will apply the Chebotarev density theorem to sets $C_\nu \subset G_\nu$ defined by reference with the forced eigenvalues that exist for some orthogonal matrices. Precisely, recall that for $A \in O(N, k)$ (for an arbitrary field k of odd characteristic and an arbitrary non-degenerate symmetric bilinear form on k^N), the following "functional equation"

$$T^N P(1/T) = \det(-A) P(T) \tag{7}$$

holds for the polynomial $P = \det(1 - AT) \in k[T]$. At $T = 1$ this implies that if $\det(-A) = (-1)^N \det A = -1$, we have $P(1) = 0$, i.e., 1 is then an eigenvalue of A.

If N is even, that means that any matrix $A \in O(N, k)$ with determinant -1 has eigenvalue ± 1. If N is odd, that means that any orthogonal matrix in $SO(N, k)$ has eigenvalue 1. We will say that A has *no extra vanishing* if 1 is a root of $P(T)$ with minimal multiplicity compatible with this.[2] We denote by $O^{ev}(N)$ the set of orthogonal matrices which *have* extra vanishing. We thus see that $O^{ev}(N)$ is an algebraic variety defined over the same base as the orthogonal group under consideration, given by $O^{ev}(N) = O_1 \cup O_2$, where

$$O_1 = \{A \in O(N) \mid \det(A) = -1 \text{ and } \det(1 - A) = 0\}$$
$$O_2 = \{A \in SO(N) \mid \tfrac{d}{dT} \det(1 - TA)\Big|_{T=1} = 0\}$$

if N is odd and

$$O_1 = \{A \in SO(N) \mid \det(1 - A) = 0\}$$
$$O_2 = \{A \in O(N) \mid \det(A) = -1 \text{ and } \tfrac{d}{dT} \det(1 - TA)\Big|_{T=\pm 1} = 0\}$$

if N is even.

We see that $O^{ev}(N)$ intersects each of the two connected components of $O(N)$ in a closed hypersurface.

Denote by $C_\nu \subset G_\nu$ the image of

$$O^{ev}(N, \mathbf{Z}_\ell) \cap \tau_\ell(\pi_1(U, \overline{\eta}))$$

by reduction modulo ℓ^ν. We have the following simple lemma:

Lemma 5. (1) *We have*

$$|G_\nu| \leqslant \ell^{\nu N(N-1)/2}, \tag{8}$$

for $\nu \geqslant 1$.

(2) *We have*

$$|C_\nu| |G_\nu|^{-1} \ll \ell^{-\nu} \tag{9}$$

for all $\nu \geqslant 1$, *the implied constant depending on* N, ℓ *and the index* (5).

Proof. (1) The order of G_ν is at most the order of $O(N, \mathbf{Z}/\ell^\nu \mathbf{Z})$ so the upper bound follows easily.

(2) Because each $O^{ev}(N)$ is a hypersurface (i.e., of codimension 1 in each component of $O(N)$), the result follows from the bounds

$$|C_\nu| \ll \ell^{\nu(\dim O(N) - 1)}, \quad |G_\nu| \gg \ell^{\nu \dim O(N)},$$

[2] This may be different than saying that 1 is an eigenvalue with minimal multiplicity, if A is not semi-simple.

the first being a consequence of e.g. [S1, Th. 8] and the second of the boundedness of the indices (6) i.e., the finiteness of (5). (The upper bound can also be proved by more or less direct counting). □

We now make the following observation: for a point $u \in U(\mathbf{F}_q)$, the condition that Fr_u has extra vanishing acting on $\mathcal{F}_\ell$ implies that $\rho_\nu(\mathrm{Fr}_u) \in C_\nu$ for *all* $\nu \geqslant 1$. This leads to the basic bound

$$|\{u \in U(\mathbf{F}_q) \mid \mathrm{Fr}_u \text{ has extra vanishing on } \mathcal{F}_\ell\}| \leqslant \pi(C_\nu; q) \tag{10}$$

with notation as in Theorem 1, which is valid for all ν.

We will use this to prove:

Proposition 6. *With notation and assumptions as above, in particular under the monodromy assumption* (5)*, we have*

$$|\{u \in U(\mathbf{F}_q) \mid \mathrm{Fr}_u \text{ has extra vanishing on } \mathcal{F}_\ell\}| \ll q^{d-c}$$

where $c = \frac{1}{3N(N-1)+1}$*, the implied constant depending on* $\overline{U}$*,* ℓ*,* N *and the index* (5)*.*

For instance, the gain is $c = 1/13$ for $N = 3$, $c = 1/25$ for $N = 4$.

Proof of Proposition 6. Applying (10) and Theorem 1, we derive

$$|\{u \in U(\mathbf{F}_q) \mid \mathrm{Fr}_u \text{ has extra vanishing}\}| \leqslant \frac{|C_\nu|}{|G_\nu|} q^d + O(q^{d-1/2}|G_\nu||C_\nu|^{1/2})$$

for any $\nu \geqslant 1$, with an implied constant depending only on $\overline{U}$.

Using the bounds from the lemma, this leads to

$$|\{u \in U(\mathbf{F}_q) \mid \mathrm{Fr}_u \text{ has extra vanishing}\}| \ll q^d \ell^{-\nu} + q^{d-1/2}\ell^{\nu(N(N-1)-1)},$$

for $\nu \geqslant 1$ with an implied constant depending $\overline{U}$, ℓ, N and the index (5). For q large enough there exists ν such that

$$\frac{1}{\ell} q^c \leqslant \ell^\nu \leqslant q^c, \text{ with } c = \frac{1}{3N(N-1)+1},$$

and then we have

$$\ell^{-\nu} \leqslant \ell q^{-c}, \text{ and } q^{-1/2}\ell^{\nu(N(N-1)-1)} \leqslant q^{-c}$$

so that taking this ν yields

$$|\{u \in U(\mathbf{F}_q) \mid \mathrm{Fr}_u \text{ has extra vanishing}\}| \ll q^{d-c},$$

the implied constant depending only on the parameters indicated (the constant may need to be increased to account for small values of q where the ℓ above can not be found). □

We conclude by giving an equivalent rephrasing of the monodromy assumption (5).

Proposition 7. *Let* $U/\mathbf{F}_q$ *be a smooth absolutely irreducible variety over* $\mathbf{F}_q$*. Let* $\ell \neq p$ *be a prime number and* $\tau_\ell : \pi_1(\overline{U}, \overline{\eta}) \to GL(N, \mathbf{Z}_\ell)$ *a continuous representation of the geometric fundamental group of* U*. Assume* ρ_ℓ *takes value in* $O(N, \mathbf{Z}_\ell)$ *for some non-degenerate bilinear form. If the geometric monodromy group* G^g *of* τ_ℓ*, i.e., the Zariski closure of the image of* τ_ℓ *in* $GL(N, \overline{\mathbf{Q}}_\ell)$*, contains* $SO(N)$*, then we have*

$$[O(N, \mathbf{Z}_\ell) : \tau_\ell(\pi_1(U, \overline{\eta}))] < +\infty.$$

In concrete terms, the geometric monodromy group G^g is the set of matrices $x \in GL(N, \overline{\mathbf{Q}}_\ell)$ for which $f(x) = 0$ whenever f is a polynomial function on $GL(N, \overline{\mathbf{Q}}_\ell)$ (involving possibly $1/\det(x)$) that vanishes identically on the image Γ of $\pi_1(\overline{U}, \overline{\eta})$, and the assumption is that $G^g \supset SO(N, \overline{\mathbf{Q}}_\ell)$.

Thus, intuitively, both the condition (5) and the assumption of the proposition are statements saying that ρ_ℓ has a "large" image, and the proposition shows that those two different meanings are in fact quite close.

The condition (5) may be called the "old" way of stating this, whereas the assumption on the geometric monodromy group is the more "modern" style; it is the usual language of the works of Katz for instance (compare with [S1]). In [S3], Serre attributes the shift to Grothendieck.

Proof. Since the image of $\pi_1(U,\overline{\eta})$ is larger than that of $\pi_1(\overline{U},\overline{\eta})$, it suffices to show that

$$[O(N,\mathbf{Z}_\ell) : \tau_\ell(\pi_1(\overline{U},\overline{\eta}))] < +\infty.$$

Let Γ denote the image of the geometric fundamental group. In the ℓ-adic topology induced from $GL(N,\mathbf{Q}_\ell)$, Γ is compact (by continuity of τ_ℓ, as the fundamental group is compact) inside the compact group $O(N,\mathbf{Z}_\ell)$. The point is that from $G^g \supset SO(N)$, it follows that $\Gamma \cap SO(N,\mathbf{Z}_\ell)$ is also open in $SO(N,\mathbf{Z}_\ell)$, still for the ℓ-adic topology (see [S3, Cor. p. 120] for instance). But then the finiteness of $[SO(N,\mathbf{Z}_\ell) : \Gamma \cap SO(N,\mathbf{Z}_\ell)]$ is immediate from the existence of Haar measure μ with total mass one on $SO(N,\mathbf{Z}_\ell)$, since Γ as an open set must satisfy $\mu(\Gamma) > 0$. In fact,

$$[SO(N,\mathbf{Z}_\ell) : \Gamma \cap SO(N,\mathbf{Z}_\ell)] = \frac{1}{\mu(\Gamma)}.$$

The desired finiteness of $[O(N,\mathbf{Z}_\ell) : \Gamma]$ is obviously a trivial consequence of this. □

3. Twists of elliptic curves over function fields

We now explain how the result of the previous section apply to the study of extra vanishing for families of twists of elliptic curves over function fields.

We first survey the construction by Katz of varieties parameterizing twists of elliptic curves over function fields over finite fields (see [K1, Intro., V] and also [U1, 2,6,7]).

We assume for simplicity that the characteristic p is not 2 or 3. Let $C/\mathbf{F}_q$ be a smooth projective curve of genus g, absolutely irreducible, $K = \mathbf{F}_q(C)$ the function field of C and E/K an elliptic curve, which is assumed to have non-constant j-invariant. If $C = \mathbf{P}^1$ is the projective line, the twists considered can be described concretely as follows: take a Weierstrass equation for E of the type

$$y^2 = x^3 + a(t)x^2 + b(t)x + c(t)$$

with a, b, $c \in \mathbf{F}_q(t)$, and let $f \in \mathbf{F}_q[t]$ be a (squarefree) polynomial. Then the twist E_f of E by f is the elliptic curve E_f/K with equation

$$f(t)y^2 = x^3 + a(t)x^2 + b(t)x + c(t),$$

and coefficients of f serve as "algebraic" parameters for twists.

In the greater generality described by Katz, f is chosen to be a rational function on C with a prescribed set of poles D (an effective divisor on C) and with $\deg D$ distinct zeroes, none of which is a place of bad reduction of E. Katz shows that if $\deg(D) \geqslant 2g+1$, this set of functions is the set of $\mathbf{F}_q$-rational points of a smooth geometrically connected algebraic variety $X/\mathbf{F}_q$ (which depends on D and E).

Now for any $f \in X(\mathbf{F}_{q^n})$, $n \geqslant 1$, there is a twist E_f defined over $\mathbf{F}_{q^n}(C)$, generalizing the above description. For any prime $\ell \neq p$, the L-functions of all the twisted curves can be encoded in the "local" behavior of a certain lisse ℓ-adic sheaf $\mathcal{T}_\ell$ on X, of rank N which is independent of ℓ, corresponding to a representation

$$\tilde{\tau}_\ell \,:\, \pi_1(U,\overline{\eta}) \to GL(N,\mathbf{Z}_\ell).$$

Precisely, for any rational point $f \in X(\mathbf{F}_q)$, we have the identity

$$L(E_f/K,T) = \det(1 - T\,\mathrm{Fr}_x \mid \mathcal{T}_\ell), \text{ or } L(E_f/K,s) = \det(1 - q^{-s}\,\mathrm{Fr}_x \mid \mathcal{T}_\ell). \tag{11}$$

This sheaf is constructed by Katz [K1, Ch. V]. Moreover, Katz shows, as consequences of general properties of étale cohomology, that $\mathcal{T}_\ell$ is punctually pure of weight 2, and there exists a natural non-degenerate symmetric pairing

$$\mathcal{T}_\ell \otimes \mathcal{T}_\ell \to \mathbf{Z}_\ell(-2).$$

This means that the image of $\pi_1(U,\overline{\eta})$ by $\tilde{\tau}_\ell$ is contained in the group $CO(N,\mathbf{Z}_\ell)$ of similitudes for this pairing, and the image of Fr_{f,q^n}, for $f \in X(\mathbf{F}_{q^n})$, is a similitude with "multiplier" $m(\tilde{\tau}_\ell(\mathrm{Fr}_{f,q^n})) = q^{2n}$. In addition, the image of the geometric fundamental group is contained in the group $O(N,\mathbf{Z}_\ell)$ of orthogonal transformations for the pairing. Of course, we have an exact sequence

$$1 \to O(N,\mathbf{Z}_\ell) \to CO(N,\mathbf{Z}_\ell) \xrightarrow{m} \mathbf{Z}_\ell^\times \to 1.$$

The L-functions (11) have central critical point at $s = 1$, i.e., at $T = q^{-1}$, and it is convenient to make a Tate twist to translate it to $s = 0$, i.e., $T = 1$.

So we consider the sheaf $\mathcal{T}_\ell(1)$ instead of $\mathcal{T}_\ell$, which corresponds to taking the representation

$$\tau_\ell(x) = \tilde{\tau}_\ell(x) q^{-d(x)}$$

of $\pi_1(U,\overline{\eta})$, where d is the "degree" map in (2). The twisted representation τ_ℓ coincides with $\tilde{\tau}_\ell$ on $\pi_1(\overline{U},\overline{\eta})$ (by (2)). On the other hand, since $\pi_1(U,\overline{\eta})$ is topologically generated by the Fr_{f,q^n}, $f \in X(\mathbf{F}_{q^n})$, $n \geqslant 1$, and since

$$m(q^{-d(\mathrm{Fr}_{f,q^n})}\tilde{\tau}_\ell(\mathrm{Fr}_{f,q^n})) = q^{-2n}q^{2n} = 1,$$

it follows that $\tau_\ell(\pi_1(U,\overline{\eta})) \subset O(N,\mathbf{Z}_\ell)$.

With $\mathcal{F}_\ell = \mathcal{T}_\ell(1)$, this provides us with all the data occurring in Section 2. Now the point is that Katz has shown by a deep monodromy computation that the condition (5) holds for D suitably chosen. We state a precise version:

Proposition 8 (Katz)**.** *If the divisor D satisfies the conditions*

$$\deg(D) \geqslant 4g+4, \quad 2g-2+\deg(D) \geqslant \max(144, 2s), \tag{12}$$

where s is the number of places of bad reduction of E/K, then we have

$$[O(N,\mathbf{Z}_\ell) : \tau_\ell(\pi_1(U,\overline{\eta}))] < +\infty.$$

Proof. Under the condition stated, Katz has shown (see [K1, p. 15] for a summary) that the geometric monodromy group G^g associated to $\mathcal{T}_\ell(1)$ contains $SO(N)$. Therefore, we can apply Proposition 7. □

Corollary 9. *Let $C/\mathbf{F}_q$ be a smooth absolutely irreducible projective curve of genus $g \geqslant 0$, $E/\mathbf{F}_q(C)$ an elliptic curve with non-constant j-invariant, D an effective divisor on E of degree $\geqslant 2g+1$, and $X = X(D,E)$ the associated parameter space for twists. Assume that $p > N+2$ and that the twisting sheaves $\mathcal{T}_\ell(1)$ satisfy* (5)*; for instance assume that* (12) *holds.*

Then, for any $n \geqslant 1$, the number V_n of twisting parameters $f \in X(\mathbf{F}_{q^n})$ such that the L-function of $E_f/\mathbf{F}_{q^n}(C)$ vanishes at $s = 1$ with order strictly larger than that imposed by the functional equation satisfies

$$V_n \ll q^{n(\dim X - c)} \tag{13}$$

with $c = \frac{1}{3N(N-1)+1}$, the implied constant depending on D, E, and p. In particular this set has density 0 *as $n \to +\infty$.*

Proof. The condition $p > N+2$ implies that there exists a non-zero congruence class a modulo p such that $\ell \equiv a \pmod{p}$ implies that $GL(N,\mathbf{F}_\ell)$ is of order prime to p (see e.g. [K1, Lemma 7.5.1]). Pick such a prime ℓ, and then apply Proposition 6 and (11) to the sheaf $\mathcal{T}_\ell(1)$. □

It is interesting to notice that, together with the work of Ulmer (see [U2]) on the Birch and Swinnerton-Dyer conjecture which shows that

$$\operatorname{rank} E_f(\mathbf{F}_{q^n}(C)) = \operatorname{ord}_{s=1} L(E_f/\mathbf{F}_{q^n}(C), s)$$

if the right-hand side is at most 1, this also gives a strong version of the analogue of Goldfeld's Conjecture for the *algebraic* rank. To state it, we assume for simplicity that the image of the geometric fundamental group by the representation τ_ℓ is not contained in $SO(N,\mathbf{Z}_\ell)$. Katz has shown ([K1, Ex. 8.3.4.1]) that this is the case for instance if E/K has multiplicative reduction at a point $s \in S$.

Proposition 10. *With assumptions as in the previous corollary, assume moreover that the image of the geometric fundamental group by the representation τ_ℓ is not contained in $SO(N, \mathbf{Z}_\ell)$. Then we have*

$$\sum_{f\in X(\mathbf{F}_{q^n})} \operatorname{rank} E_f(\mathbf{F}_{q^n}(C)) = \frac{1}{2}|X(\mathbf{F}_{q^n})| + O(q^{n(\dim X - c)})$$

for $n \geqslant 1$, the implied constant depending on D, E and p.

Proof. The point is that all the twists have "analytic rank" bounded by the rank N of $\mathcal{T}_\ell$, since their L-functions are all polynomials of degree N. Since for an elliptic curve $E/\mathbf{F}_{q^n}(C)$ there is the a-priori inequality (due to Tate [T])

$$\operatorname{rank} E(\mathbf{F}_{q^n}(C)) \leqslant \operatorname{ord}_{s=1} L(E/\mathbf{F}_{q^n}(C), s),$$

the twists also have algebraic rank bounded by N, so the contribution to the average rank of those few f for which the analytic rank of E_f is $\geqslant 2$ is small. Precisely, notice that

$$\operatorname{rank} E_f(\mathbf{F}_{q^n}(C)) = \frac{1 - W(E_f)}{2} + \beta(E_f)$$

where $W(E_f)$ is the sign of the functional equation and $\beta(E_f)$ has the property that $\beta(E_f) = 0$ if the analytic rank of E_f is $\leqslant 1$ (this is the result of Ulmer), and $|\beta(E_f)|$ is bounded ($\leqslant N+1$) for all f and n. Thus the sum of $\beta(E_f)$ is

$$\ll q^{n(\dim X - c)}$$

for $n \geqslant 1$ by (13). On the other hand

$$\sum_{f\in X(\mathbf{F}_{q^n})} \frac{1 - W(E_f)}{2} = \frac{|X(\mathbf{F}_{q^n})|}{2} - \frac{1}{2} \sum_{f\in X(\mathbf{F}_{q^n})} W(E_f).$$

and we have

$$W(E_f) = (-1)^N \det(\tau_\ell(\mathrm{Fr}_f))$$

where τ_ℓ is as before the representation which corresponds to $\mathcal{T}_\ell$ (this is simply (7) and (11)).

The assumption that the image of τ_ℓ is not inside SO implies that the character $\det \circ \tau_\ell$ of order 2 is non-trivial on the geometric fundamental group. Thus $H_c^{2d}(\overline{X}, \det \circ \tau_\ell) = 0$ and by the Riemann hypothesis we have

$$\Big| \sum_{f\in X(\mathbf{F}_{q^n})} W(E_f) \Big| \leqslant q^{n(\dim X - 1/2)} \sum_{0\leqslant i < 2\dim X} \dim H_c^i(\overline{X}, \det \circ \tau_\ell) \ll q^{n(\dim X - 1/2)}$$

for $n \geqslant 1$, finishing the proof. □

4. Examples of one parameter families of twists

This section is a concrete illustration of the previous section. We will use some of the intermediate statements proved by Katz in [K1] to restrict our attention to one-parameter families of twists (i.e., replace the big parameter space X of the previous section by a curve) where the analog of Corollary 9 and Proposition 10 still hold. (In fact, it is by finding such one-parameter families inside the larger spaces that Katz shows that the geometric monodromy groups for those parameter spaces contain $SO(N)$).

To simplify, we will only consider curves over $\mathbf{P}^1$ and twists by polynomials; this allows us to write down explicit equations (in other words, $C = \mathbf{P}^1$, $g = 0$ and the divisor D is $d(\infty)$ in the notation of the previous section).

We start with an elliptic curve given by a fairly general Weierstrass equation (assuming always that the characteristic p is $\geqslant 5$)

$$E : y^2 = x^3 + a(t)x^2 + b(t)x + c(t)$$

with polynomials a, b and $c \in \mathbf{F}_q[t]$. Denote by S the set of points in $\mathbf{A}^1$ where E has bad reduction.

In Chapter 5 of [K1], two different types of one-parameter families with "large" monodromy are described. We will consider special cases of the first one (Theorem 5.4.1 of loc. cit.). Adapting the terminology found there and in [K1, Ch. 2], we say that a polynomial $f \in \overline{\mathbf{F}}_q[t]$ of degree $d \geqslant 1$ is *of Lefschetz type* if the following conditions hold:

(i) f has d distinct zeros in $\overline{\mathbf{F}}_q$;

(ii) f' has $d-1$ distinct zeros, and those have distinct images by f.

Moreover we say that f is of *Katz-Lefschetz type* for E if f is of Lefschetz type, and

(i') no two points of S have the same image by f;

(ii') $f(s) \neq 0$ for $s \in S$;

(iii') the fibers $f^{-1}(f(s))$ all have d distinct elements for $s \in S$.

Fix a polynomial f of Katz-Lefschetz type. Let V_f denote the (finite) variety, defined over $\mathbf{F}_q$, of critical values for f, i.e.

$$V_f = f(\{x \mid f'(x) = 0\}) \cup f(S),$$

and let $U_f = \mathbf{A}_1 - V_f$. Then Theorem 5.4.1 of [K1] states that if $d \geqslant \max(146, 2|S|)$, the one-parameter family of quadratic twists with equations

$$E_{f,\alpha} \,:\, (f(t)-\alpha)y^2 = x^3 + a(t)x^2 + b(t)x + c(t),$$

with $\alpha \in U_f$ has associated ℓ-adic twisting sheaves $\mathcal{F}_{\ell,f}$ on U_f, of fixed rank N_f, such that the geometric monodromy group (on U_f) of $\mathcal{F}_{\ell,f}$ contains $SO(N_f)$ for $\ell \neq p$. In particular this sheaf satisfies the condition (5).

Corollary 11. *Let $E/\mathbf{F}_q(t)$ be an elliptic curve with non-constant j-invariant and at least one finite place of multiplicative reduction. Let f be a polynomial of Katz-Lefschetz type for E of degree $d \geqslant \max(146, 2|S|)$.*

(i) *For $n \geqslant 1$, the number V_n of $\alpha \in U_f(\mathbf{F}_{q^n})$ where $E_{f,\alpha}/\mathbf{F}_{q^n}(t)$ has extra vanishing satisfies*

$$V_n \ll q^{n(1-c)}$$

with $c = \frac{1}{3N_f(N_f-1)+1}$, the implied constant depending on E, f and p.

(ii) *If the image of the geometric fundamental group is not contained in $SO(N, \mathbf{Z}_\ell)$, we have*

$$\sum_{\alpha \in U_f(\mathbf{F}_{q^n})} \operatorname{rank} E_{f,\alpha}(\mathbf{F}_{q^n}(t)) = \frac{1}{2}|U_f(\mathbf{F}_{q^n})| + O(q^{n(1-c)}),$$

for $n \geqslant 1$, the implied constant depending on E, f and p.

We could in fact state a slightly better result using the Chebotarev density theorem for curves instead of the general version (see the next section).

To be completely concrete, we will now take a specific example. Let $E/\mathbf{F}_p(t)$ be the following variant of the Legendre elliptic curve:

$$E \,:\, y^2 = x(x+1)(x-t). \tag{14}$$

Note E has additive reduction at ∞ and *multiplicative* reduction at the points in $S = \{0, -1\}$.

Now consider the following polynomials:

$$f_d = t^d - dt - 1 \in \mathbf{F}_p[t].$$

Lemma 12. (i) *If $p \nmid d(d-1)$ and $(p-1, d-1) = 1$, then f_d is of Lefschetz type.*

(ii) *If in addition $p \nmid d+1$, then f_d is of Katz-Lefschetz type for the above curve $E/\mathbf{F}_p(t)$.*

Proof. The derivative of f_d is $f_d' = d(t^{d-1} - 1)$ so since $p \nmid d$, the roots of f_d' are the $(d-1)$-st roots of unity. Since $p \nmid d-1$, there are $d-1$ of them in $\overline{\mathbf{F}}_p$. Now for μ a zero of f_d' we have

$$f_d(\mu) = \mu(1-d) - 1.$$

This already shows that the values of f_d at zeros of f_d' are distinct.

Notice that this formula also shows $f_d(\mu) \neq 0$ because otherwise μ would be in the prime field $\mathbf{F}_p$, so that $\mu = 1$ by the assumption $(p-1, d-1) = 1$, the equation becomes $1 - d = 1$,

but again $p \nmid d$ excludes this case. Since $f_d^{-1}(x)$, for $x \in \overline{\mathbf{F}}_p$, has d elements except if x is in the set $\{f_d(\mu)\}$, it follows that f_d has d distinct roots in $\overline{\mathbf{F}}_p$. Altogether, this establishes the first assertion that f_d is of Lefschetz type.

For the second, the conditions $(p-1, d-1) = 1$ and $p \geqslant 5$ imply that d is even. We compute f_d at the points in S: we have $f_d(0) = -1$ and $f_d(-1) = (-1)^d + d - 1 = d$. So $f_d(0) \neq f_d(-1)$ since $p \nmid d+1$. Moreover $f_d(0) = -1$ is not of the form $f_d(\mu) = \mu(1-d) - 1$ as above, since $p \nmid d$. Similarly $f_d(-1) = d$ is not of this form: $d = \mu(1-d) - 1$ implies again that μ is in the prime field, so $\mu = 1$, and again $p \nmid d$ shows that $d + 1 = 1 - d$ is impossible. So neither 0 nor -1 is in a fiber over a zero of f_d', which means that the fibers over points of S contain d distinct elements. □

Remark 13. So for $p = 5$, we have found explicit polynomials of Katz-Lefschetz type for E of any even degree d with $d \equiv 2 \pmod 5$, i.e., $d \equiv 2 \pmod{10}$.

In general, the density of integers $d \geqslant 1$ satisfying the conditions of the lemma is

$$\frac{\varphi(p-1)}{p}\Big(1 - \frac{3}{p}\Big) > 0$$

for all $p \geqslant 5$.

Let d be any integer satisfying the condition of the lemma. We then have the one-parameter family of twists

$$E_{d,\alpha} \,:\, (f_d(t) - \alpha)y^2 = x(x+1)(x-t),$$

or equivalently (change y to $(f_d - \alpha)y$)

$$E_{d,\alpha} \,:\, y^2 = (t^d - dt - 1 - \alpha)x(x+1)(x-t)$$

over $\mathbf{F}_p(t)$, with parameter α in the complement U_d of the finite variety of critical values for f_d, which has $d - 1 + 2 = d + 1$ points defined over $\overline{\mathbf{F}}_p$.

Let $\mathcal{F}_{d,\ell}$ denote the twisting sheaf $\mathcal{T}_\ell(1)$ for this subfamily. As observed by Katz [K1, Lemma 7.5.1], the twist sheaves associated to quadratic twists of elliptic curves are always tame in characteristic $p \geqslant 5$, so $\mathcal{F}_{d,\ell}$ is tame. The rank N_d of $\mathcal{F}_{d,\ell}$ is computed in [K1, Lemma 5.1.3, p. 16] and is given by

$$N_d = 2d$$

for d even. In particular, this means that the (degree of the) conductor of the twists goes to infinity when $d \to +\infty$.

As a special case of Theorem 5.4.1 of [K1], if $d \geqslant 146$, the geometric monodromy group for $\mathcal{F}_{d,\ell}$ is the full orthogonal group $O(N_d)$ for all ℓ.

So specializing again the previous corollary we get:

Corollary 14. *Let $p \geqslant 5$ be prime, let $d \geqslant 146$, f_d and U_d be as above. For $n \geqslant 1$, the number V_n of $\alpha \in U_d(\mathbf{F}_{q^n})$ for which the twisted Legendre curve*

$$y^2 = (t^d - dt + 1 - \alpha)x(x+1)(x-t)$$

over $\mathbf{F}_{p^n}(t)$ has extra vanishing satisfies

$$V_n \ll p^{n(1-c)}, \tag{15}$$

with $c = \frac{1}{8d^2}$, the implied constant depending on d and p.

5. Twists with unbounded conductor

This section is speculative. The idea is to exploit the strong bound (15) to prove a variant of Proposition 10 for a family of twists more closely resembling the quadratic twists of elliptic curves over $\mathbf{Q}$, namely one where the conductor (i.e., essentially, in this case, the degree of the L-function) increases, so that the rank of the elliptic curves is not uniformly bounded. The speculation consists in the fact that the result obtained is conditional on monodromy assumptions which are stronger than currently known.

We still work with the curve (14) of the previous section for concreteness. Take a sequence of polynomials (f_d) of Katz-Lefschetz type with increasing degrees d. We have corresponding twisting sheaves $\mathcal{F}_{d,\ell}$ for the 1-parameter family corresponding to f_d, with rank N_d.

We make the following strong assumption

(16) For all d considered and *all* odd $\ell \neq p$, the image of the representation
$$\rho_{d,\ell} : \pi_1(U_d, \overline{\eta}) \to GL(N_d, \mathbf{F}_\ell)$$
corresponding to the reduction $\mathcal{F}_{d,\ell}/\ell\mathcal{F}_{d,\ell}$ is of *bounded index* in $O(N_d, \mathbf{F}_\ell)$.

See the final paragraphs of the paper for comments on the plausibility of this.[3]

We denote by $G_{d,\ell}$ the image of $\rho_{d,\ell}$ and by B a bound for its index in $O(N_d, \mathbf{F}_\ell)$ valid for all d and $\ell \neq p$.

Corresponding to Lemma 5 we need the following uniform version for $\nu = 1$, which we make a little bit more precise:

Lemma 15. (1) *For all odd primes ℓ and all $d \geqslant 1$ we have*
$$|G_{d,\ell}| \leqslant \ell^{N_d(N_d-1)/2}.$$
(2) *Let $C_{d,\ell}$ be the set of $g \in G_{d,\ell}$ with extra vanishing. We have*
$$\frac{|C_{d,\ell}|}{|G_{d,\ell}|} \ll \frac{1}{\ell}$$
for all odd primes ℓ and all $d \geqslant 1$, the implied constant depending only on B, provided that $\ell \geqslant N_d^2$.

Proof. (1) The size of $G_{d,\ell}$ is bounded by that of $O(N_d, \mathbf{F}_\ell)$ for which the existing formulas immediately give the result stated.

(2) We bound $C_{d,\ell}$ by the number of elements with extra vanishing in $O(N_d, \mathbf{F}_\ell)$. In general, for $O(N, \mathbf{F}_\ell)$, the latter (say $R(N)$) is written as follows:
$$R(N) = \sum_g |\{x \in O(N, \mathbf{F}_\ell) \mid \det(1 - Tx) = g\}|$$
where g runs over characteristic polynomials of elements of $O(N, \mathbf{F}_\ell)$ which have extra vanishing. It is clear that the number of possible g is $\leqslant \ell^{N-1}$. For each g, we count the inner quantity by the same method as in [C, Proof of Th. 3.5] (with adaptations necessary because the orthogonal group is not simply connected like the symplectic group) which shows that it is
$$\ll (\ell+1)^{N(N-1)/2}(\ell-1)^{-N}$$
(with absolute implied constant), so we get
$$R(N) \ll \ell^{-1}\Big(\frac{\ell}{\ell-1}\Big)^N(\ell+1)^{N(N-1)/2}$$
with absolute implied constant, and because $|O(N, \mathbf{F}_\ell)| \geqslant (\ell-1)^{N(N-1)/2}$, this yields the result after an application of the mean value theorem. □

Here is the hypothetical result with unbounded conductors.

Proposition 16. *Let $p \geqslant 5$ be prime. Let D_p denote the set of integers $d \geqslant 1$ such that $p \nmid d(d-1)(d+1)$ and $(p-1, d-1) = 1$, and for $p \in D_p$, denote by k_d the finite field $\mathbf{F}_{p^{d^3}}$. Assume the monodromy hypothesis* (16) *for the sequence of Katz-Lefschetz polynomials $f_d = t^d - dt + 1$ for all integers $d \in D_p$.*

(i) *We have for $d \in D_p$*
$$|\{\alpha \in U_d(k_d) \mid E_{d,\alpha} \text{ has extra vanishing}\}| \ll dp^{d^3 - \frac{1}{2}d}.$$

[3]. Note also that (16) could be replaced without much change by a "vertical" version, namely that for some *fixed* $\ell \neq p$, the index of the image of $\pi_1(U_d, \overline{\eta}) \to O(N_d, \mathbf{Z}/\ell^\nu\mathbf{Z})$ is bounded for all d and $\nu \geqslant 1$.

(ii) *We have for* $d \in D_p$

$$\sum_{\alpha \in U_d(k_d)} \operatorname{rank} E_{d,\alpha}(k_d(t)) = \frac{p^{d^3}}{2} + O(d^2 p^{d^3 - \frac{1}{2}d}).$$

(Note that we consider f_d over $k_d = \mathbf{F}_{p^{d^3}}$ instead of some f_{d_n} over $\mathbf{F}_{p^n}$, as might seem more natural, because we would need a bound of the type $d_n^3 \leqslant n$, hence d_n would assume the same value many times, and we have only one explicit Katz-Lefschetz polynomial for each degree; however, with "more" polynomials, this would also be a possible option).

Proof. Because of all the assumptions, the Chebotarev density theorem for curves (Theorem 3, with $g = 0$, $m = d + 1$) and Lemma 15 imply that for $d \in D_p$ and $\ell \neq p$ we have

$$|\{\alpha \in U_d(k_d) \mid E_{d,\alpha} \text{ has extra vanishing}\}| \ll \frac{p^{d^3}}{\ell} + dp^{d^3/2}\ell^A$$

with

$$A = \frac{1}{2}\Big(\frac{N_d(N_d-1)}{2} - 1\Big),$$

the implied constant depending only on B if $\ell \geqslant N_d^2 = 4d^2$.

Since $2(A+1) = \frac{1}{2}(N_d(N_d-1)+1) \leqslant 2d^2$, taking ℓ such that

$$p^{\frac{d^3}{2(A+1)}} \leqslant \ell \leqslant 2p^{\frac{d^3}{2(A+1)}}$$

gives

$$|\{\alpha \in U_d(k_d) \mid E_{d,\alpha} \text{ has extra vanishing}\}| \ll dp^{d^3 - \frac{d^3}{2d^2}} = dp^{d^3 - d/2}$$

for $d \in D_p$, with an implied constant depending only on B. Note that for d large enough ($d \geqslant 7$ suffices) we have

$$d^3 \log p \geqslant 2d^2(\log 4d^2)$$

which implies $\ell \geqslant 4d^2$. Those d for which $\ell < 4d^2$ (or those with $d < 146$) can be incorporated in the estimate by replacing the implied constant, if needed, by a larger one (such as $|U(k_{146})|$).

For part (ii), the reasoning is as in the proof of Proposition 10, using Ulmer's result about the Birch and Swinnerton-Dyer conjecture. The contribution of the twists with analytic rank $\geqslant 2$ is estimated using (i) and the trivial bound

$$\operatorname{rank} E_{d,\alpha}(k_d(t)) \leqslant N_d = 2d$$

(so there too the uniformity of our estimates in terms of d is – or would be! – important). □

Remark 17. In terms of the parameter $X = p^{d^3}$, the error terms have the following shape:

$$dp^{d^3 - \frac{1}{2}d} \ll (\log X)^{1/3} X \exp(-\tfrac{1}{2}(\log X)^{1/3})$$

which may look more familiar to analytic number theorists.

We finish by commenting on our monodromy assumption (16). First of all, for *fixed* n, the uniformity in terms of ℓ is part of the standard conjectures (see e.g. [S2, 10.3?,10.7?]) about the variation of images of ℓ-adic representations.

In addition, since Katz has shown that the "rational" geometric monodromy group is always equal to $O(N)$, it is a consequence of a result of Larsen [L, Th. 3.17] that for a set of primes ℓ of density 1, the geometric monodromy group modulo ℓ contains the image in $O(N, \mathbf{F}_\ell)$ of the spin group $\mathrm{Spin}(N, \mathbf{F}_\ell)$, which is of index 2 in $SO(N, \mathbf{F}_\ell)$ and 4 in $O(N, \mathbf{F}_\ell)$ (this complication arises because $O(N, \mathbf{F}_\ell)$ is neither connected nor simply connected). Larsen's result is quite difficult (it uses the classification of simple finite groups), and the set of primes it produces is not easy to control.

Another example, still for fixed rank, is a result proved by Gabber concerning the monodromy of Kloosterman sheaves which is explained in [K3, Ch. 12]. Roughly speaking, the integral monodromy group associated to families of Kloosterman sums in an even number n of variables

is "big" for all ℓ large enough, depending on n, but again not in a way easy to describe for varying n.

When the rank is increasing, it is in fact not clear if the uniform bound we postulate is coherent with the general philosophy concerning ℓ-adic representations. The reason is that this variation of N does not fall into a well-understood theoretical framework: the "family" we consider is one only inasmuch as we manage to deal with its individual terms and get similar results; this is much the same as the case of "families" of classical automorphic L-functions, for which convincing examples exist abundantly without an *a priori* definition. Still, in the case of elliptic curves $E/\mathbf{Q}$, a similar result is expected: recall that Serre showed that for a fixed E without CM, there exists L_E such that for any prime $\ell > L_E$, the map

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[\ell]) \simeq GL(2, \mathbf{F}_\ell)$$

is surjective (i.e., the fields obtained by adjoining to $\mathbf{Q}$ the coordinates of the ℓ-torsion points of E are "as big as possible"). Then the conjectured statement that such an L as above exists which "works" for all elliptic curves $E/\mathbf{Q}$ (without CM) can be seen as an analogue of our assumption (see e.g. [S1, Question 2, p. 199]). It has been confirmed by Duke [D] that this can be done for "almost all" curves.

Finally, we can turn for encouragement to at least one similar situation where a result of the desired type has been unconditionally proved. Let $f \in \mathbf{F}_q[x]$ be a fixed polynomial of degree $2g$ with $2g$ distinct roots in $\overline{\mathbf{F}}_q$, and consider the family of hyperelliptic curves of genus $g \geqslant 1$ with equations

$$C_\alpha : y^2 = f(x)(x - \alpha),$$

over the open set $\mathbf{A}^1 - f^{-1}(0)$, with projection $\pi(x, y, \alpha) = \alpha$. The sheaves $R^1\pi_!\mathbf{F}_\ell$, which are of rank $2g$ and admit symplectic symmetry, are used to "globalize" the family of L-functions of C_α (modulo ℓ). Jiu-Kang Yu [Yu] has shown that the geometric monodromy group is equal to $Sp(2g, \mathbf{F}_\ell)$ for all f and all $\ell \neq 2$. This is one of the main examples in [C]. It is also used to give some results uniform in g in [Ko] (which are in fact of a rather more delicate nature). It is not inconceivable that his techniques could be used for the investigation of our assumption.

(**Added in proof**: C. Hall has informed the author that he has proved results on the monodromy modulo ℓ of elliptic curves over a function field over a finite field which should be sufficient to prove versions of (16) for many elliptic curves).

References

[C] N. Chavdarov: *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. 87 (1997), 151–180.

[CKRS] B. Conrey, J.P. Keating, M. Rubinstein and N. Snaith: *On the frequency of vanishing of quadratic twists of modular L-functions*, in Number theory for the millennium I, 301–315, A K Peters (2002).

[D] Duke, W.: *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. 325 (1997), no. 8, 813–818.

[FJ] M. Fried and M. Jarden: *Field arithmetic*, Ergebnisse der Math. und ihrer Grenzgebiete, 3 Folge, vol. 11, Springer Verlag (1986; 2nd ed. 2004).

[GM] F. Gouvêa and B. Mazur: *The square-free sieve and the rank of elliptic curves*, J. Am. Math. Soc. 4, No.1, 1-23 (1991).

[IK] H. Iwaniec and E. Kowalski: *Analytic Number Theory*, A.M.S Colloquium Series vol. 53 (2004).

[K1] N. Katz: *Twisted L-functions and monodromy*, Annals of Math. Studies 150 (2002).

[K3] N. Katz: *Gauss sums, Kloosterman sums and monodromy*, Annals of Math. Studies, 116, Princeton Univ. Press, 1988.

[Ko] E. Kowalski: *The large sieve, monodromy and zeta functions of curves*, J. reine angew. Math, to appear, `arXiv:math.NT/0503714`.

[L] M. Larsen: *Maximality of Galois actions for compatible systems*, Duke Math. J. 80 (1995), no. 3, 601–630.

[S1] J-P. Serre: *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES 54 (1981), 323–401.

[S2] J-P. Serre: *Propriétés conjecturales des groupes de Galois motiviques et des représentations ℓ-adiques*, in Motives (Seattle 1991), 377–400, Proc. Sympos. Pure Math. 55, Part 1, AMS 1994.

[S3] J-P. Serre: *Sur les groupes de Galois attachés aux groupes p-divisibles*, Proc. Conf. Local Fields, Springer-Verlag (1966), 118–131; also in Œuvres, t. II, 325–338.

[T] J. Tate: *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Exp. 306, 1966.

[U1] D. Ulmer: *Geometric non-vanishing*, Invent. math. 159 (2005), 133–186.

[U2] D. Ulmer: *Elliptic curves and analogies between number fields and function fields*, MSRI Publication 59, 285–315, Cambridge Univ. Press (2004).

[Yu] J.-K. Yu: *Toward a proof of the Cohen-Lenstra conjecture in the function field case*, preprint (1996).

Université Bordeaux I - A2X, 351, cours de la Libération, 33405 Talence Cedex, France
E-mail address: emmanuel.kowalski@math.u-bordeaux1.fr