On the L-polynomials of curves over finite fields

Francesco Ballini, Davide Lombardo, Matteo Verzobio

Abstract

We discuss, in a non-Archimedean setting, the distribution of the coefficients of L-polynomials of curves of genus g over $\mathbb{F}_q$. This allows us to prove, among other things, that the $\mathbb{Q}$-vector space spanned by such characteristic polynomials has dimension $g+1$. We also state a conjecture about the Archimedean distribution of the number of rational points of curves over finite fields.

1 Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic p and order $q = p^f$. For every $g \geq 1$, we let $\mathcal{M}_g(\mathbb{F}_q)$ be the set of smooth projective curves of genus g over $\mathbb{F}_q$, up to isomorphism over $\mathbb{F}_q$. Recall that, given a (smooth projective) curve $C/\mathbb{F}_q$, one may introduce its zeta function

$$Z(C/\mathbb{F}_q, s) = \exp\left(\sum_{m\geq 1} \frac{\#C(\mathbb{F}_{q^m})}{m} q^{-ms}\right),$$

and that by work of Schmidt [Sch31] and Weil [Wei48] we know that $Z(C/\mathbb{F}_q, s)$ is a rational function of $t := q^{-s}$. More precisely, we can write

$$Z(C/\mathbb{F}_q, s) = \frac{P_C(t)}{(1-t)(1-qt)},$$

where $P_C(t)$ is a polynomial (often called the L-polynomial of C) that satisfies the following:

Lemma 1.1. *1. $P_C(t)$ has integral coefficients and $P_C(0) = 1$;*

2. $\deg P_C(t) = 2g$, where $g = g(C)$ is the genus of C;

3. writing $P_C(t) = \sum_{i=0}^{2g} a_i t^i$ we have the symmetry relations $a_{g+i} = q^i a_{g-i}$ for every $i = 0, \ldots, g$.

Our main object of interest in this paper is the set of L-polynomials of all the curves of a given genus over a finite field $\mathbb{F}_q$:

Definition 1.2. *Given a finite field $\mathbb{F}_q$ and a positive integer g we define*

$$\mathcal{P}_g(\mathbb{F}_q) := \{P_C(t) \;\big|\; C \in \mathcal{M}_g(\mathbb{F}_q)\}.$$

We will focus in particular on the non-Archimedean distribution of these L-polynomials. For a fixed integer $N \geq 2$, upon reduction modulo N one obtains from $\mathcal{P}_g(\mathbb{F}_q)$ a set $\mathcal{P}_{g,N}(\mathbb{F}_q)$ of polynomials in $(\mathbb{Z}/N\mathbb{Z})[t]$. Considering this set of reduced polynomials both for a fixed value of q and in the limit $q \to \infty$, we obtain results in three different but related directions:

1. We adapt results of Katz-Sarnak from the Archimedean to the non-Archimedean setting, obtaining equidistribution statements for $\mathcal{P}_{g,N}(\mathbb{F}_q)$ as $q \to \infty$ (Theorem 2.1). While special instances of this result appear in the literature (especially for the case of elliptic curves, see [CH13, Gek03]), the general case does not seem to have been explored previously – but see [Ach08] for related results.
2. The previous result allows us to disprove a recent conjecture by Bergström–Howe–Lorenzo-García–Ritzenthaler [BHLGR24, Conjecture 5.1] about the *Archimedean* distribution of the number of rational points of non-hyperelliptic curves over finite fields (Proposition A.3). Theorem 2.1, combined with the general Lang-Trotter philosophy, leads us to propose a new conjecture (Conjecture 3.4), which seems both more natural (in view of the general principles that seem to regulate statistical phenomena in arithmetic) and in better accord with the numerical evidence (see Section 3.2).

3. Finally, Theorem 2.1 easily implies that, for a fixed genus g and for $q \gg_g 1$, the set $\mathcal{P}_g(\mathbb{F}_q)$ spans a $\mathbb{Q}$-vector space of dimension $g+1$ (Remark 2.9). By considering more carefully the set $\mathcal{P}_{g,2}(\mathbb{F}_q)$ for every fixed value of q, we are able to prove that this statement does, in fact, hold for all pairs (g,q) (Theorem 1.4), thus confirming a conjecture of Kaczorowski and Perelli [KP18, Remark 8]. Using Theorem 2.1 we can also obtain an asymptotic result for non-linear relations among the coefficients of elements of $\mathcal{P}_g(\mathbb{F}_q)$, see Theorem 6.1.

Recently, much attention has been devoted to questions close to those that we consider here: in addition to the aforementioned [BHLGR24], we also refer the reader to [AEK$^+$15], as well as [AAGG23], [Ma23], and [Shm23]. We discuss some relations between our work and these latter papers in Remark 3.13. We believe that different parts of the mathematical community are approaching the same questions we discuss in this paper from complementary perspectives, and we hope that the present work will also encourage a fruitful exchange of ideas between these different points of view.

For this introduction, we focus more specifically on our contributions. The non-Archimedean behaviour of the L-polynomials is closely related to the (geometric version of the) Chebotarev density theorem, in the following sense. Let $\mathcal{C} \xrightarrow{\pi} S \to \operatorname{Spec}\mathbb{Z}$ be a versal family of curves of genus g, that is, a family in which every isomorphism class of curves of genus g appears at least once (we use the tri-canonically embedded family, see Section 2 for details). Considering the N-torsion sections of $\operatorname{Jac}\mathcal{C} \to S$ gives rise to a Galois cover $S' \to S$ whose Galois group G_N is a subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z})$ – essentially, S' is the minimal cover of S over which all the N-torsion sections of $\operatorname{Jac}\mathcal{C}$ are defined. For every closed point $s \in S$ we have a curve C_s, defined over the finite field $\kappa(s)$, and a Frobenius element $\mathrm{Frob}_{s,N} \in G_N$. Note that this Frobenius is an element of the Galois group of the cover, and is determined by the property of inducing the finite-field Frobenius $t \mapsto t^{(\#\kappa(s))}$ on the residue field at a point $s' \in S'$ lying over s. As usual, $\mathrm{Frob}_{s,N}$ is only well-defined up to conjugacy, or equivalently, up to the choice of the point $s' \in S'$ lying over s. The reduction modulo N of the L-polynomial of C_s is determined by the characteristic polynomial of $\mathrm{Frob}_{s,N}$, so equidistribution results for $\mathrm{Frob}_{s,N}$ translate into equidistribution results for $P_C \bmod N$. We make this precise in Section 2, using Deligne and Katz's equidistribution theorem instead of Chebotarev's.

Having precise control over the non-Archimedean distribution of L-polynomials is sufficient to show that the values of $F_q(t) = \#\{C : C \in \mathcal{M}_g(\mathbb{F}_q), \#C(\mathbb{F}_q) = t\}$ show significant local oscillations – consecutive values of $t \in \mathbb{N}$ can correspond to wildly different values of $F_q(t)$. As already mentioned, we use this to disprove [BHLGR24, Conjecture 5.1].

We propose a new conjecture that takes these local oscillations into account to compute $F_q(t)$. Here we give an informal statement: for a precise version, see Conjecture 3.4 and Remark 3.6 for an interpretation of the quantity $\nu_\ell(q,t)$.

Conjecture 1.3. *Let $g \geq 1$ and q be a prime power. Let $H'(q,t)$ be the 'probability' that a curve $C/\mathbb{F}_q$ of genus g has $q+1-t$ rational points. Given a prime ℓ define $\nu_\ell(q,t)$ as the 'normalised probability that a matrix $M \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ with multiplier q has trace t'. Let $\nu_\infty(q,t) = \mathrm{ST}_g(t/\sqrt{q})$, where ST_g is the Sato-Tate measure in dimension g. Let $\nu'(q,\cdot)$ be the probability measure equal to $c \cdot \nu_\infty(q,\cdot) \prod_{\ell<\infty} \nu_\ell(q,\cdot)$ where c is the normalisation constant that ensures that ν' is a probability measure. Then, the L^1-distance between $H'(q,\cdot)$ and $\nu'(q,\cdot)$ tends to 0 as $q \to \infty$.*

Finally, Theorem 1.4 answers the following natural question: does Lemma 1.1 capture all the (linear) relations among the coefficients of the polynomials $P_C(t)$? In other words, what is the dimension of the $\mathbb{Q}$-vector subspace of $\mathbb{Q}[t]$ spanned by the polynomials in $\mathcal{P}_g(\mathbb{F}_q)$? As a consequence of Lemma 1.1, it is immediate to see that this space has dimension at most $g+1$. Equality holds if and only if all the linear relations among the coefficients are already listed in Lemma 1.1. We show that equality does in fact hold for all genera and all finite fields: this extends work of Birch [Bir68] for curves of genus 1 and of Howe-Nart-Ritzenthaler [HNR09] for curves of genus 2, and confirms the aforementioned conjecture of Kaczorowski and Perelli [KP18, Remark 8]:

Theorem 1.4. *Let p be a prime, let $f \geq 1$, and denote by $\mathbb{F}_q$ the finite field with $q = p^f$ elements. Let $\mathcal{P}_g(\mathbb{F}_q)$ be as in Definition 1.2 and let $L_g(\mathbb{F}_q)$ be the $\mathbb{Q}$-vector subspace of $\mathbb{Q}[t]$ spanned by $\mathcal{P}_g(\mathbb{F}_q)$. We have*

$$\dim_{\mathbb{Q}} L_g(\mathbb{F}_q) = g+1.$$

The proof is based on the following observation: in order to establish the linear independence of a set of polynomials with integral coefficients, it is certainly enough to show that they are linearly independent

modulo 2. In the case of the L-polynomial of a curve C, the reduction modulo 2 can be read off the action of Galois on the set of 2-torsion points of the Jacobian of C. In turn, when C is hyperelliptic, this action is easy to write down explicitly in terms of a defining equation of C: it is then a simple matter to find $g+1$ curves whose L-polynomials form a basis of $L_g(\mathbb{F}_q)$. Since the properties of the 2-torsion points are slightly different depending on whether the characteristic is odd or even, we split our proof into two parts, one for the case p odd and one for the case $p=2$. We remark in particular that our proof is constructive: Corollary 5.4 for the case p odd and the proof in Section 5.2 for the case $p=2$ explicitly give $g+1$ curves whose L-polynomials form a basis of $L_g(\mathbb{F}_q)$.

We conclude this introduction by briefly describing the structure of the paper. In Section 2, we prove an equidistribution result for $\mathcal{P}_{g,N}$ (see Theorem 2.1). In Section 3 we state our conjecture on the probability that a curve has a given number of rational points (see Conjecture 3.4). We also explain why we believe this conjecture to be true and present some numerical evidence that supports it. Then, in Section 4, we prove some technical results necessary to state Conjecture 3.4. Finally, in Section 5, we prove Theorem 1.4 and in Section 6 we study non-linear relations among the coefficients of the polynomials in $\mathcal{P}_g(\mathbb{F}_q)$. In Appendix A, we disprove [BHLGR24, Conjecture 5.1].

1.1 Notation and classical results

We fix our notation for symplectic groups:

Definition 1.5. *Let $g \geq 1$ and $N \geq 2$ be integers. Fix a non-degenerate antisymmetric bilinear form on $(\mathbb{Z}/N\mathbb{Z})^{2g}$, represented by the matrix Ω (note that the form is non-degenerate if and only if $\det\Omega \in (\mathbb{Z}/N\mathbb{Z})^\times$). The group $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ is by definition*

$$\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z}) = \{M \in \mathrm{GL}_{2g}(\mathbb{Z}/N\mathbb{Z}) : \exists \lambda \in (\mathbb{Z}/N\mathbb{Z})^\times \text{ such that } {}^tM\Omega M = \lambda\Omega\}.$$

The multiplier of a matrix $M \in \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ is the uniquely determined $\lambda \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that ${}^tM\Omega M = \lambda\Omega$. We denote it by $\mathrm{mult}(M)$. For every integer q prime to N, we let $\mathrm{GSp}_{2g}^q(\mathbb{Z}/N\mathbb{Z})$ be the subset of the finite matrix group $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ consisting of those matrices that have multiplier equal to q (equality in the finite ring $\mathbb{Z}/N\mathbb{Z}$).

Remark 1.6. By definition, the group $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ depends on the choice of Ω, but different choices lead to isomorphic groups. We will therefore refer to $\mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ without necessarily specifying the choice of anti-symmetric form.

Before beginning with the proofs, it will be useful to recall the well-known connection between the L-polynomial of a curve C of genus g and the Galois representations attached to the Jacobian J of C. Let p be a prime, let q be a power of p, and let C be a curve of genus g defined over $\mathbb{F}_q$. Denote by J the Jacobian of C. Let ℓ be any prime different from p and let $T_\ell J$ be the ℓ-adic Tate module of J, that is,

$$T_\ell J := \varprojlim_n J(\overline{\mathbb{F}_q})[\ell^n].$$

There is a natural action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on $T_\ell J$ (induced by the action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on the torsion points of J), and it can be shown that $T_\ell J$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. Fixing a $\mathbb{Z}_\ell$-basis of $T_\ell J$ we thus obtain a representation $\rho_{\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ whose image is contained in $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$; the relevant antisymmetric bilinear form is given by the Weil pairing. Since $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is procyclic, generated by the Frobenius automorphism Frob, we are mostly interested in the action of Frob on $T_\ell J$, which is captured by its characteristic polynomial

$$f_{C,\ell^\infty}(t) = \det(t\,\mathrm{Id} - \rho_{\ell^\infty}(\mathrm{Frob})) \in \mathbb{Z}_\ell[t].$$

The matrix representing the action of Frobenius is symplectic with multiplier q. Notice that we also have an action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on the ℓ-torsion points of $J(\overline{\mathbb{F}_q})$, which form an $\mathbb{F}_\ell$-vector space of dimension $2g$; we can thus obtain a mod-ℓ representation $\rho_\ell : \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ and a corresponding characteristic polynomial $f_{C,\ell}(t) = \det(t\,\mathrm{Id} - \rho_\ell(\mathrm{Frob})) \in \mathbb{F}_\ell[t]$. It is clear from the definitions that $f_{C,\ell}(t)$ is nothing but the reduction modulo ℓ of $f_{C,\ell^\infty}(t)$. We can now recall the connection between $P_C(t)$ and $f_{C,\ell^\infty}(t)$:

Theorem 1.7 (Grothendieck–Lefschetz formula, [Del77])**.** *The equality $P_C(t) = t^{2g} f_{C,\ell^\infty}(1/t)$ holds for every prime $\ell \neq p$.*

Notice in particular that the polynomial $f_{C,\ell^\infty}(t) \in \mathbb{Z}_\ell[t]$ has integer coefficients and does not depend on ℓ.

2 The distribution of L-polynomials modulo an integer N

In this section we adapt [KS99, §10] to the problem of the distribution of characteristic polynomials of Frobenius modulo a fixed integer N (as opposed to the distribution of the coefficients with respect to the Archimedean metric which is considered in [KS99]).

Fix a genus $g \geq 2$ and a finite field $\mathbb{F}_q$ of characteristic $p > 0$. We denote by $\mathcal{M}_g$ the stack of smooth projective curves of genus g, so that $\mathcal{M}_g(\mathbb{F}_q)$ denotes the set of isomorphism classes of smooth projective curves of genus g over $\mathbb{F}_q$. We see $\mathcal{M}_g(\mathbb{F}_q)$ as a probability space by endowing it with one of the following two natural measures:

- the 'naive' counting measure $\mathbb{P}^{\mathrm{naive}}_{g,q}$, which assigns equal measure to every singleton $\{C\}$, and which we normalise by requiring $\mathbb{P}^{\mathrm{naive}}_{g,q}(\mathcal{M}_g(\mathbb{F}_q)) = 1$.
- the 'intrinsic' measure $\mathbb{P}^{\mathrm{intr}}_{g,q}$ such that

$$\mathbb{P}^{\mathrm{intr}}_{g,q}(\{C\}) = \alpha \frac{1}{\#\operatorname{Aut}(C_{\mathbb{F}_q})},$$

where $\operatorname{Aut}(C_{\mathbb{F}_q})$ is the group of automorphisms of C defined over $\mathbb{F}_q$ and

$$\alpha = \left(\sum_{C \in \mathcal{M}_g(\mathbb{F}_q)} \frac{1}{\#\operatorname{Aut}(C_{\mathbb{F}_q})} \right)^{-1}$$

is the uniquely determined normalisation constant that ensures

$$\sum_{C \in \mathcal{M}_g(\mathbb{F}_q)} \mathbb{P}^{\mathrm{intr}}_{g,q}(\{C\}) = \mathbb{P}^{\mathrm{intr}}_{g,q}(\mathcal{M}_g(\mathbb{F}_q)) = 1.$$

Our objective in this section is to study the random variable

$$\begin{array}{rccc} \mathrm{charpol}: & \mathcal{M}_g(\mathbb{F}_q) & \to & \mathbb{Z}[t] \\ & C & \mapsto & f_{C,\ell^\infty}(t), \end{array}$$

where ℓ is any auxiliary prime different from p that we use to compute the characteristic polynomial of the Frobenius acting on $\mathrm{Jac}(C)$. More precisely, we will consider the (infinitely many) random variables

$$\begin{array}{rccc} \mathrm{charpol}_N: & \mathcal{M}_g(\mathbb{F}_q) & \to & \mathbb{Z}/N\mathbb{Z}[t] \\ & C & \mapsto & f_{C,\ell^\infty}(t) \bmod N \end{array}$$

obtained from charpol by reducing the characteristic polynomials modulo N, for all $N \not\equiv 0 \pmod{p}$. For simplicity, since $\mathrm{charpol}(C)$ is always a monic polynomial of degree $2g$, we restrict the codomain to be the finite set $\mathbb{Z}/N\mathbb{Z}[t]_{\leq 2g}$, the additive group of polynomials with coefficients in $\mathbb{Z}/N\mathbb{Z}$ and degree at most $2g$. For each integer N not divisible by p we obtain a measure μ^q_N on $\mathbb{Z}/N\mathbb{Z}[t]_{\leq 2g}$ as follows. Consider the finite set $\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})$ and its natural counting measure $\mu_{\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})}$, normalised so that the total mass is 1. The map

$$\mathrm{charpol}: \mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{Z}/N\mathbb{Z}[t]_{\leq 2g}$$

that sends each matrix in $\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})$ to its characteristic polynomial allows us to define the measure

$$\mu^q_N := (\mathrm{charpol})_* \mu_{\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})}.$$

We will show:

Theorem 2.1. *With the notation above, as $q \to \infty$ along prime powers with $(q, N) = 1$, the measures $(\mathrm{charpol}_N)_* \mathbb{P}^{\mathrm{naive}}_{g,q} - \mu^q_N$ and $(\mathrm{charpol}_N)_* \mathbb{P}^{\mathrm{intr}}_{g,q} - \mu^q_N$ converge weakly to 0.*

Remark 2.2. For $g = 1$, very precise results about the distribution of characteristic polynomials modulo N are proven in [CH13]. In particular, the results of that paper describe a very explicit measure $\tilde{\mu}^q_N$ and show that for $g = 1$ the difference $(\mathrm{charpol}_N)_* \mathbb{P}^{\mathrm{naive}}_{1,g} - \tilde{\mu}^q_N$ converges to zero with an error of size at most $O_N(q^{-1/2})$. Thus, the case $g = 1$ is very well understood. For this reason, and since Theorem 2.4 below does not apply in genus 1, we exclude the case $g = 1$ from our discussion.

We begin by recalling a version of Deligne's equidistribution theorem, as extended by Katz. We follow in part the presentation in [AH03, §2]. We fix a prime ℓ and a geometrically connected normal $\mathbb{Z}[1/\ell]$-scheme U of finite type over $\mathbb{Z}[1/\ell]$ with generic point η and geometric generic point $\overline{\eta}$. Let $\mathcal{F}$ be a local system of symplectic free $\mathbb{Z}/N\mathbb{Z}$-modules of rank $2g$ on U – equivalently, a representation

$$\rho : \pi_1(U, \overline{\eta}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{Sp}(\mathcal{F}_{\overline{\eta}}) \subset \mathrm{Aut}(\mathcal{F}_{\overline{\eta}}).$$

Theorem 2.3 (Katz)**.** *In the situation above, suppose the sheaf gives rise to a commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1^{\mathrm{geom}}(U,\overline{\eta}) & \longrightarrow & \pi_1(U,\overline{\eta}) & \longrightarrow & \mathrm{Gal}(\overline{k_0}/k_0) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \rho_{\mathcal{F}}^{\mathrm{geom}}} & & \downarrow{\scriptstyle \rho_{\mathcal{F}}} & & \downarrow{\scriptstyle \rho_{\mathcal{F}}^{k_0}} & & \\ 1 & \longrightarrow & \mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & \mathbb{G}_m(\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & 1 \end{array}$$

where $\rho_{\mathcal{F}}^{\mathrm{geom}}$ is surjective. There is a constant C such that, for any union of conjugacy classes $W \subset \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ and any finite field k of characteristic $\neq \ell$,

$$\left| \frac{\#\left\{u \in U(k) : \rho_{\mathcal{F}}(\mathrm{Frob}_{u,k}) \in W\right\}}{\#U(k)} - \frac{\#(W \cap \mathrm{GSp}_{2g}^{\gamma(k)}(\mathbb{Z}/N\mathbb{Z}))}{\#\,\mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})} \right| \leq \frac{C}{\sqrt{\#k}},$$

where $\gamma(k)$ is the image of the canonical generator of $\mathrm{Gal}(\overline{k}/k)$ under $\rho_{\mathcal{F}}^{k_0}$.

Proof. This is a special case of [KS99, 9.7.13]. □

Let $\mathcal{C} \xrightarrow{\pi} U \to \mathrm{Spec}\,\mathbb{Z}[1/\ell]$ be a smooth, irreducible family of curves of genus $g \geq 1$ with geometrically irreducible fibres. The sheaf $\mathcal{F} = \mathcal{F}_{\mathcal{C},N} := R^1\pi_*\mathbb{Z}/N\mathbb{Z}$ is a sheaf of $\mathbb{Z}/N\mathbb{Z}$-free symplectic modules of rank $2g$ whose fibre at a geometric point $\overline{x} \in U$ is the N-torsion of the Jacobian $\mathrm{Jac}(\mathcal{C}_x)[N]$. Theorem 2.3 applies to this situation provided that $\rho_{\mathcal{F}}^{\mathrm{geom}}$ is surjective. We will say that the family of curves $\mathcal{C} \to U$ has full N-monodromy if the associated representation $\rho_{\mathcal{F}} : \pi_1^{\mathrm{geom}}(U, \overline{\eta}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})$ is surjective.

For the proof of Theorem 2.1 we will rely on the functor $\mathcal{M}_{g,3K}$ of tri-canonically embedded curves. Referring the reader to [KS99, §10.6] and [DM69] for more details, we recall that for a field k one has

$$\mathcal{M}_{g,3K}(k) = \left\{ (C/k, \alpha) : \begin{array}{c} C/k \text{ is a smooth projective} \\ \text{curve of genus } g \\ \alpha \text{ is a basis of } H^0\left(C, (\Omega^1_{C/k})^{\otimes 3}\right) \end{array} \right\} / \text{isomorphism}.$$

The functor $\mathcal{M}_{g,3K}$ was extensively studied by Mumford [Mum65] and Deligne-Mumford [DM69]. We will need the following results:

Theorem 2.4 (Deligne-Mumford [DM69, §5], see also [KS99, Theorem 10.6.10])**.** *Let $g \geq 2$. The following hold:*

1. *The functor $\mathcal{M}_{g,3K}$ is represented by a smooth $\mathbb{Z}$-scheme of relative dimension $3g - 3 + (5g-5)^2$, with geometrically connected fibres.*
2. *$\mathcal{M}_{g,3K}$ is a fine moduli space: there exists a universal curve $\mathcal{C}_{g,3K} \to \mathcal{M}_{g,3K}$.*

There is an obvious forgetful functor

$$\mathcal{M}_{g,3K} \to \mathcal{M}_g$$

which on field-valued points is given by

$$\begin{array}{ccc} \mathcal{M}_{g,3K}(k) & \to & \mathcal{M}_g(k) \\ (C/k, \alpha) & \mapsto & C/k. \end{array}$$

This map is surjective for every field k, and, when k is finite, the fibre over any $C/k \in \mathcal{M}_g(k)$ has cardinality $\dfrac{\#\,\mathrm{GL}_{5g-5}(k)}{\#\,\mathrm{Aut}(C/k)}$ [KS99, Lemma 10.6.8]. As an immediate consequence [KS99, Lemma 10.7.8], the intrinsic measure $\mathbb{P}_{g,q}^{\mathrm{intr}}$ on $\mathcal{M}_g(\mathbb{F}_q)$ can be described as

$$\frac{1}{\#\mathcal{M}_{g,3K}(\mathbb{F}_q)} \sum_{(C,\alpha) \in \mathcal{M}_{g,3K}(\mathbb{F}_q)} \delta_C, \tag{1}$$

where δ_C is the characteristic function of the singleton $\{C\}$. By Theorem 2.4 (2), the sum

$$\sum_{(C,\alpha)\in\mathcal{M}_{g,3K}(\mathbb{F}_q)} \delta_C$$

can be replaced by

$$\sum_{u\in\mathcal{M}_{g,3K}(\mathbb{F}_q)} \delta_{(\mathcal{C}_{g,3K})_u}, \tag{2}$$

where $(\mathcal{C}_{g,3K})_u$ is the fibre over $u \in \mathcal{M}_{g,3K}(\mathbb{F}_q)$ of the universal curve $\mathcal{C}_{g,3K} \to \mathcal{M}_{g,3K}$. We will apply Theorem 2.3 to $U = \mathcal{M}_{g,3K}$ and $\mathcal{F} = \mathcal{F}_{\mathcal{C}_{g,3K},N}$. For $g \geq 2$ and $p \nmid N$, this family has full N-monodromy by [DM69, 5.12] (see also the discussion in [LSTX19, §5]). We are almost ready to prove Theorem 2.1, but before doing so, we need a few estimates on the size of $\mathcal{M}_g(\mathbb{F}_q)$:

Lemma 2.5. *For every $g \geq 3$, the following hold:*

1. $\#\mathcal{M}_g(\mathbb{F}_q) = \sum_{C\in\mathcal{M}_g(\mathbb{F}_q)} 1 = q^{3g-3}(1 + O_g(q^{-1/2}))$;
2. $\sum_{C\in\mathcal{M}_g(\mathbb{F}_q)} \frac{1}{\#\operatorname{Aut}(C_{\mathbb{F}_q})} = q^{3g-3}(1 + O_g(q^{-1/2}))$;
3. $\#\left\{C \in \mathcal{M}_g(\mathbb{F}_q) : \#\operatorname{Aut}(C_{\overline{\mathbb{F}_q}}) \geq 2\right\} = O_g(q^{3g-3-1})$.

For $g = 2$ one has

1'. $\#\mathcal{M}_2(\mathbb{F}_q) = \sum_{C\in\mathcal{M}_2(\mathbb{F}_q)} 1 = q^3(1 + O(q^{-1/2}))$;
2'. $\sum_{C\in\mathcal{M}_2(\mathbb{F}_q)} \frac{1}{\#\operatorname{Aut}(C_{\mathbb{F}_q})} = \frac{1}{2}q^3(1 + O(q^{-1/2}))$;
3'. $\#\left\{C \in \mathcal{M}_g(\mathbb{F}_q) : \#\operatorname{Aut}(C_{\overline{\mathbb{F}_q}}) > 2\right\} = O(q^2)$.

Proof. For $g \geq 3$, all the statements follow from [KS99, Lemmas 10.6.23, 10.6.25 and 10.6.26], together with the obvious asymptotic relation $\#\operatorname{GL}_{5g-5}(\mathbb{F}_q) \sim q^{(5g-5)^2}(1 + O_g(q^{-1}))$. For $g = 2$, one can adapt the proof of the same lemmas in [KS99], simply taking into account that the open subset $U_{\leq 2}$ of $\mathcal{M}_2$ parametrising curves whose geometric automorphism group has order 2 meets every geometric fibre of $\mathcal{M}_{2,3K}/\mathbb{Z}$ [KS99, Lemma 10.6.13, Remark 10.6.20]. In particular, the generic value of $\#\operatorname{Aut}(C_{\mathbb{F}_q})$ for (smooth projective) curves of genus 2 is 2. Note that when the group $\operatorname{Aut}(C_{\mathbb{F}_q})$ has order 2 it is generated by the hyperelliptic involution. □

Corollary 2.6. *For all $g \geq 2$ we have*

$$\sum_{C'\in\mathcal{M}_g(\mathbb{F}_q)} \left|\mathbb{P}^{\mathrm{naive}}_{g,q}(\{C'\}) - \mathbb{P}^{\mathrm{intr}}_{g,q}(\{C'\})\right| = O_g(q^{-1/2}).$$

Proof. For $g \geq 3$, using the definition of $\mathbb{P}^{\mathrm{naive}}_{g,q}$ and $\mathbb{P}^{\mathrm{intr}}_{g,q}$ and Lemma 2.5 (1), (2) and (3) we obtain

$$\begin{aligned}
\sum_{C'\in\mathcal{M}_g(\mathbb{F}_q)} \left|\mathbb{P}^{\mathrm{naive}}_{g,q}(\{C'\}) - \mathbb{P}^{\mathrm{intr}}_{g,q}(\{C'\})\right| &= \sum_{C'\in\mathcal{M}_g(\mathbb{F}_q)} \left|\frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} - \frac{1/\#\operatorname{Aut}(C'_{\mathbb{F}_q})}{\sum_{C\in\mathcal{M}_g(\mathbb{F}_q)} 1/\#\operatorname{Aut}(C_{\mathbb{F}_q})}\right| \\
&= \sum_{C'\in\mathcal{M}_g(\mathbb{F}_q)} \left|q^{3-3g}(1 + O_g(q^{-1/2})) - \frac{q^{3-3g}(1 + O_g(q^{-1/2}))}{\#\operatorname{Aut}(C'_{\mathbb{F}_q})}\right| \\
&= \sum_{\substack{C'\in\mathcal{M}_g(\mathbb{F}_q) \\ \#\operatorname{Aut}(C'_{\mathbb{F}_q})=1}} O_g(q^{3-3g-1/2}) + \sum_{\substack{C'\in\mathcal{M}_g(\mathbb{F}_q) \\ \#\operatorname{Aut}(C'_{\mathbb{F}_q})\geq 2}} O_g(q^{3-3g}) \\
&= O_g\left(\frac{\#\left\{C \in \mathcal{M}_g(\mathbb{F}_q) : \#\operatorname{Aut}(C_{\overline{\mathbb{F}_q}}) \geq 2\right\}}{q^{3g-3}}\right) \\
&\quad + O_g\left(\frac{\#\mathcal{M}_g(\mathbb{F}_q)}{q^{3g-3}}q^{-1/2}\right) \\
&= O_g(q^{-1}) + O_g(q^{-1/2}) = O_g(q^{-1/2}).
\end{aligned}$$

The same proof applies, with minimal changes, also to $g = 2$, simply using (1'), (2'), and (3') of Lemma 2.5 instead of (1), (2) and (3). □

Proof of Theorem 2.1. By definition, the weak convergence in the statement means that – for every continuous bounded function f on $\mathbb{Z}/N\mathbb{Z}[x]_{\leq 2g}$ – the integrals of f with respect to $(\mathrm{charpol}_N)_*\mathbb{P}^{\mathrm{naive}}_{g,q} - \mu^q_N$ converge to 0 as $q \to \infty$, and similarly for the sequence of measures $(\mathrm{charpol}_N)_*\mathbb{P}^{\mathrm{intr}}_{g,q} - \mu^q_N$.

We begin by treating the case of the measures $(\mathrm{charpol}_N)_*\mathbb{P}^{\mathrm{intr}}_{g,q} - \mu^q_N$. Since any function $f : \mathbb{Z}/N\mathbb{Z}[x]_{\leq 2g} \to \mathbb{R}$ is a linear combination of characteristic functions of singletons, it suffices to show the result when f is of the form

$$f(h(t)) = \begin{cases} 1, \text{ if } h(t) \equiv h_0(t) \pmod N \\ 0, \text{ otherwise} \end{cases}$$

for some polynomial $h_0(t) \in \mathbb{Z}/N\mathbb{Z}[t]_{\leq 2g}$. Fix $h_0(t)$. The condition $\mathrm{charpol}(M) = h_0(t) \in \mathbb{Z}/N\mathbb{Z}[t]$ defines a (possibly empty) union of conjugacy classes $W_{h_0} \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}/N\mathbb{Z})$. For a curve $C/\mathbb{F}_q$, we denote by ρ_N the natural representation of $\mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right)$ on the N-torsion of $\mathrm{Jac}(C)$. Recall that we introduced the sheaf $\mathcal{F} = \mathcal{F}_{\mathcal{C}_{g,3K},N}$ and that the universal family over $\mathcal{M}_{g,3K}$ has full N-monodromy [DM69, 5.12]. For any fixed q, using Equations (1) and (2) we have

$$\begin{aligned} \int_{\mathcal{M}_g(\mathbb{F}_q)} f(\mathrm{charpol}(C) \bmod N)\, d\mathbb{P}^{\mathrm{intr}}_{g,q}(C) &= \frac{1}{\#\mathcal{M}_{g,3K}(\mathbb{F}_q)} \sum_{C \in \mathcal{M}_{g,3K}(\mathbb{F}_q)} f(\mathrm{charpol}_N(C)) \\ &= \frac{1}{\#\mathcal{M}_{g,3K}(\mathbb{F}_q)} \sum_{u \in \mathcal{M}_{g,3K}(\mathbb{F}_q)} \mathbf{1}_{\rho_N(\mathrm{Frob}_{C_u}) \in W_{h_0}} \\ &= \frac{\#\{u \in \mathcal{M}_{g,3K}(\mathbb{F}_q) : \rho_N(\mathrm{Frob}_{u,k}) \in W_{h_0}\}}{\#\mathcal{M}_{g,3K}(\mathbb{F}_q)}. \end{aligned} \tag{3}$$

We now apply Theorem 2.3 to rewrite the above as

$$\int_{\mathcal{M}_g(\mathbb{F}_q)} f(\mathrm{charpol}_N(C))\, d\mathbb{P}^{\mathrm{intr}}_{g,q}(C) = \frac{\#\left(W_{h_0} \cap \mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})\right)}{\#\,\mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})} + O_g(q^{-1/2}) \tag{4}$$

On the other hand, by definition we have

$$\begin{aligned} \int_{\mathbb{Z}/N\mathbb{Z}[t]_{\leq 2g}} f(h(t))\, d\mu^q_N(h) &= \int_{\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})} f(\mathrm{charpol}(M))\, d\mu_{\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})}(M) \\ &= \int_{\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})} \mathbf{1}_{\mathrm{charpol}(M)=h_0}\, d\mu_{\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})}(M) \\ &= \frac{\#(W_{h_0} \cap \mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z}))}{\#\,\mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z})} \\ &= \frac{\#(W_{h_0} \cap \mathrm{GSp}^q_{2g}(\mathbb{Z}/N\mathbb{Z}))}{\#\,\mathrm{Sp}_{2g}(\mathbb{Z}/N\mathbb{Z})}. \end{aligned} \tag{5}$$

The claim follows upon comparing Equations (4) and (5).

We now show that $(\mathrm{charpol}_N)_*\mathbb{P}^{\mathrm{naive}}_{g,q} - \mu^q_N$ converges weakly to 0. We have already established that

$$(\mathrm{charpol}_N)_*\mathbb{P}^{\mathrm{intr}}_{g,q} - \mu^q_N$$

weakly converges to 0. Thus, it suffices to show that $(\mathrm{charpol}_N)_*(\mathbb{P}^{\mathrm{intr}}_{g,q} - \mathbb{P}^{\mathrm{naive}}_{g,q})$ converges weakly to 0, which in turn is implied by the following statement: for every $\varepsilon > 0$ there exists q_0 such that, for all $q > q_0$ and all subsets A of $\mathcal{M}_g(\mathbb{F}_q)$, one has

$$|\mathbb{P}^{\mathrm{intr}}_{g,q}(A) - \mathbb{P}^{\mathrm{naive}}_{g,q}(A)| < \varepsilon.$$

This follows immediately from Corollary 2.6, because

$$\begin{aligned} |\mathbb{P}^{\mathrm{intr}}_{g,q}(A) - \mathbb{P}^{\mathrm{naive}}_{g,q}(A)| &= \left| \sum_{C' \in A} \left(\mathbb{P}^{\mathrm{intr}}_{g,q}(\{C'\}) - \mathbb{P}^{\mathrm{naive}}_{g,q}(\{C'\}) \right) \right| \\ &\leq \sum_{C' \in A} |\mathbb{P}^{\mathrm{intr}}_{g,q}(\{C'\}) - \mathbb{P}^{\mathrm{naive}}_{g,q}(\{C'\})| = O_g(q^{-1/2}). \end{aligned}$$

□

Remark 2.7. Note that the measure μ_N^q only depends on q mod N. In particular, if we take a sequence of prime powers q_i such that q_i mod N is constant (say equal to r mod N), Theorem 2.1 shows that the measures $(\mathrm{charpol}_N)_*\mathbb{P}^{\mathrm{intr}}_{q_i,g}$ converge weakly to μ_N^r. As a special case, taking $N=2$, this applies to any choice of q_i that are not powers of 2.

Remark 2.8. Continuing from Remark 2.7, we take $N=2$, q_i to be the sequence of all odd primes, and apply the weak convergence of measures to the function $f = \mathbf{1}_{\mathrm{Tr}\equiv 0 \pmod 2}$, where

$$\mathrm{Tr}(x^{2g} - a_{2g-1}x^{2g-1} + \cdots + a_0) = a_{2g-1}.$$

In this way, if C is a curve over $\mathbb{F}_q$,

$$f(\mathrm{charpol}_N(C)) = \begin{cases} 1, \text{ if } \mathrm{Tr}(C) := q+1-\#C(\mathbb{F}_q) \equiv 0 \pmod 2 \\ 0, \text{ otherwise.} \end{cases}$$

Applying Theorem 2.1 to the case of the naive measure $\mathbb{P}^{\mathrm{naive}}_{g,q}$ we obtain the convergence

$$\frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{C\in\mathcal{M}_g(\mathbb{F}_q)} f(\mathrm{charpol}_2(C)) \to \mu_2^1\left(\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) : \mathrm{Tr}(M) \equiv 0 \pmod 2\}\right),$$

where

$$\mu_2^1\left(\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) : \mathrm{Tr}(M) \equiv 0 \pmod 2\}\right) = \frac{\#\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) : \mathrm{Tr}(M) \equiv 0 \pmod 2\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z})}$$

and

$$\frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{C\in\mathcal{M}_g(\mathbb{F}_q)} f(\mathrm{charpol}_2(C)) = \frac{\#\{C \in \mathcal{M}_g(\mathbb{F}_q) : \mathrm{Tr}(C) \equiv 0 \pmod 2\}}{\#\mathcal{M}_g(\mathbb{F}_q)}.$$

Thus, we have proven

$$\lim_{q\to\infty} \frac{\#\{C \in \mathcal{M}_g(\mathbb{F}_q) : \mathrm{Tr}(C) \equiv 0 \pmod 2\}}{\#\mathcal{M}_g(\mathbb{F}_q)} = \frac{\#\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) : \mathrm{Tr}(M) \equiv 0 \pmod 2\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z})},$$

where the limit is taken along the sequence of odd primes (or of their powers).

Remark 2.9. Theorem 2.1 implies Theorem 1.4, at least when the order q of the finite field is sufficiently large compared to g. For simplicity, we only discuss the case of odd q. Using [Kir69], or equivalently [Riv08, Theorem A.1] (see also Proposition 6.3 and Remark 6.4 below), one checks that the set of characteristic polynomials of matrices in $\mathrm{GSp}_{2g}(\mathbb{F}_2)$ is the $\mathbb{F}_2$-vector space of reciprocal polynomials (which has dimension $g+1$). Theorem 2.1 with $N=2$ implies that, if $q \gg_g 1$, all characteristic polynomials of elements in $\mathrm{GSp}_{2g}(\mathbb{F}_2)$ are also the reduction modulo 2 of the characteristic polynomial of Frobenius corresponding to some curve $C/\mathbb{F}_q$. This immediately implies that the $\mathbb{Q}$-vector space $L_g(\mathbb{F}_q)$ of Theorem 1.4 has dimension at least $g+1$.

3 A conjecture on the distribution of $\#C(\mathbb{F}_q)$

In this section we describe a heuristic (motivated by the Lang-Trotter philosophy and by results of Gekeler [Gek03] in genus 1) that gives precise predictions for the number of (smooth projective) curves over a finite field with a given number of rational points. We define the *trace* of a curve $C/\mathbb{F}_q$ by the formula

$$\mathrm{Tr}(C/\mathbb{F}_q) = \mathrm{Tr}(C) = q+1-\#C(\mathbb{F}_q);$$

by the Hasse-Weil bound, $\mathrm{Tr}(C)$ is an integer in the interval $[-2g\sqrt{q}, 2g\sqrt{q}]$.

We begin by recalling the definition of the Sato-Tate measure on the real interval $[-2g, 2g]$. Consider the complex Lie group $\mathrm{GSp}_{2g}(\mathbb{C})$ and let USp_{2g} be the maximal compact subgroup of $\mathrm{GSp}_{2g}(\mathbb{C})$ given by unitary symplectic matrices. The group USp_{2g}, being compact, is canonically equipped with a unique Haar measure $\mu_{\mathrm{USp}_{2g}}$ normalised so that $\mu_{\mathrm{USp}_{2g}}(\mathrm{USp}_{2g}) = 1$.

The trace map $\mathrm{tr} : \mathrm{USp}_{2g} \to \mathbb{C}$ has image contained in the real interval $[-2g, 2g]$. We denote by $d\,\mathrm{ST}_g := \mathrm{tr}_*\,\mu_{\mathrm{USp}_{2g}}$ the push-forward of the Haar measure of USp_{2g} along the trace map, and we call it the *Sato-Tate measure in dimension g*. It can be shown (for example using [Ser12, Lemma 8.5]) that $d\,\mathrm{ST}_g$ is absolutely continuous with respect to the Lebesgue measure, so we also denote by $\mathrm{ST}_g : [-2g, 2g] \to \mathbb{R}$ the density function of $d\,\mathrm{ST}_g$.

Remark 3.1. Explicit expressions for the function $\mathrm{ST}_2(x)$ can be found in [Lac16], see in particular Theorem 5.2 of *op. cit.*, and we discuss the computation of $\mathrm{ST}_g(x)$ for general g in Remark 3.14.

Let $g \geq 2$ and let $q = p^n$ be an odd prime power. Given an integer t, define

$$\nu_\infty(q,t) = \mathrm{ST}_g(t/\sqrt{q})$$

and, for each prime $\ell \neq p$,

$$\nu_\ell(q,t) = \lim_{k\to\infty} \frac{\#\left\{ M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) : \exists \tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) : \tilde{M} \equiv M \pmod{\ell^k} \text{ with } \begin{array}{c}\mathrm{tr}(\tilde{M}) = t,\\ \mathrm{mult}(\tilde{M}) = q\end{array} \right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})/(\ell^k\varphi(\ell^k))}, \tag{6}$$

while for $\ell = p$ we set

$$\nu_p(q,t) = \lim_{k\to\infty} \frac{\#\left(\mathrm{Im}\left\{ \tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Q}_p) \cap \mathrm{Mat}_{2g}(\mathbb{Z}_p) \text{ with } \begin{array}{c}\mathrm{tr}(\tilde{M}) = t,\\ \mathrm{mult}(\tilde{M}) = q\end{array} \right\} \to \mathrm{Mat}_{2g}(\mathbb{Z}/p^k\mathbb{Z})\right)}{\#\left(\mathrm{Im}\left\{ \tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Q}_p) \cap \mathrm{Mat}_{2g}(\mathbb{Z}_p) \text{ with } \mathrm{mult}(\tilde{M}) = q \right\} \to \mathrm{Mat}_{2g}(\mathbb{Z}/p^k\mathbb{Z})\right)/p^k}. \tag{7}$$

Remark 3.2. The limit in the definition of $\nu_\ell(q,t)$, including for $\ell = p$, exists thanks to [Oes82, Théorème 2] (see also [Ser81, Equation (62), Page 348, Section 3]). Indeed, the $\mathbb{Q}_\ell$-variety defined by $\{\tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) : \mathrm{Tr}(\tilde{M}) = t, \mathrm{mult}\,\tilde{M} = q\}$ has dimension $d := \dim \mathrm{GSp}_{2g,\mathbb{Q}_\ell} - 2$, so by Oesterlé's theorem the numerators of (6) and (7) are asymptotic to $c\ell^{dk}$ for some constant c. For a similar reason, the denominators also admit an asymptotic of the form $c'\ell^{dk}$ for some constant c' (this is also easy to prove directly, at least for the case $\ell \neq p$). Therefore, the ratio converges when $k \to \infty$. We justify the definition given in Equation (7) in Remark 3.6.

We will work under the assumption that $q > 4g^2 - 1$; see Remark 3.7 for a discussion of what happens when q is small with respect to g. Let

$$\nu(q,t) = \nu_\infty(q,t) \prod_{\ell<\infty} \nu_\ell(q,t). \tag{8}$$

Notice that $\nu_\infty(q,t) = 0$ for $t \notin [-2g\sqrt{q}, 2g\sqrt{q}]$ and in particular $\nu(q,t)$ is non-zero for finitely many t (for a fixed q). The fact that the product (8) converges for all t is far from obvious. We will show this in Section 4. Define

$$\nu'(q,t) = \frac{\nu(q,t)}{\sum_{t\in\mathbb{Z}} \nu(q,t)}. \tag{9}$$

The denominator is non-zero, as we will show in Lemma 4.9. By definition, we have

$$\sum_{t\in\mathbb{Z}} \nu'(q,t) = 1.$$

Definition 3.3. *Let $g \geq 2$, let q be an odd prime power, and let t be an integer. Denote by $H(q,t)$ the number of isomorphism classes of (smooth projective) curves of genus g defined over $\mathbb{F}_q$ with trace t, that is, for which $q + 1 - \#C(\mathbb{F}_q) = t$. Define*

$$H'(q,t) = \frac{H(q,t)}{\sum_{t\in\mathbb{Z}} H(q,t)} = \frac{H(q,t)}{\#\mathcal{M}_g(\mathbb{F}_q)} = \mathbb{P}_{g,q}^{\mathrm{naive}}\left(\{C \in \mathcal{M}_g(\mathbb{F}_q) : \mathrm{Tr}(C) = t\}\right). \tag{10}$$

Thus, $H'(q,t)$ is the 'naive probability' that a curve of genus g, defined over $\mathbb{F}_q$, has trace t.

Notice that $H'(q,t) = 0$ for $t \notin [-2g\sqrt{q}, 2g\sqrt{q}]$. We conjecture that, for fixed g, as $q \to \infty$ the measures $\nu'(q,t)$ and $H'(q,t)$ converge to one another. To make this precise, we use the L^1-norm on the space of probability measures on $\mathbb{Z}$: we define the distance $d(\mu_1, \mu_2)$ between two probability measures as

$$d(\mu_1, \mu_2) := \sum_{t \in \mathbb{Z}} |\mu_1(t) - \mu_2(t)| .$$

Note that, since our probability spaces are countable, the L^1-norm is equal up to a factor of 2 to another natural distance on the space of probability measures, namely the total variation distance

$$d^{\text{tot.var.}}(\mu_1, \mu_2) = \sup_{A \subseteq \mathbb{Z}} |\mu_1(A) - \mu_2(A)| .$$

We can now formulate our conjecture: we phrase it in terms of d, but clearly we obtain an equivalent statement by replacing d with $d^{\text{tot.var.}}$

Conjecture 3.4. *Fix an integer $g \geq 2$. As $q \to \infty$ along prime powers, we have*

$$d(H'(q,\cdot), \nu'(q,\cdot)) \to 0, \tag{11}$$

where $H'(q,\cdot)$ and $\nu'(q,\cdot)$ are considered as probability measures on $\mathbb{Z}$.

We now give our reasons for believing in Conjecture 3.4. First of all, notice that by Corollary 2.6 one may as well state Conjecture 3.4 using the intrinsic measure $\mathbb{P}^{\text{intr}}_{g,q}$.

- For the case of elliptic curves and the intrinsic measure $\mathbb{P}^{\text{intr}}_{g,q}$, the analogue of our conjecture has been proved in [Gek03, Theorem 5.5], at least when q is a prime number. In the proof, the author computes the value of $\nu'(q,t)$ (see [Gek03, Corollary 4.8]) and shows that it is *equal* to $H'(q,t)$, which is computed in [Deu41].
- Let C be a curve of genus g defined over $\mathbb{F}_q$. The trace t of C modulo ℓ^k is equal to the trace of the matrix $M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ that represents the action of the Frobenius Frob_q on the ℓ^k-torsion points of the Jacobian of C. Notice that there exists $\tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ such that $\tilde{M} \equiv M \pmod{\ell^k}$ with $\mathrm{tr}(\tilde{M}) = t$ and $\mathrm{mult}(\tilde{M}) = q$: indeed, it suffices to take as $\tilde{M}$ the matrix representing the action of Frobenius on the full Tate module $T_\ell \operatorname{Jac}(C) \cong \mathbb{Z}_\ell^{2g}$. Hence, by Theorem 2.1, as $q \to \infty$ the probability that a curve C has trace t modulo ℓ^k converges to

  $$\frac{\#\left\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) : \mathrm{tr}(M) = t, \mathrm{mult}(M) = q\right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})/(\ell^k\varphi(\ell^k))}.$$

  Taking the limit $k \to \infty$, $\nu_\ell(q,t)$ should represent the probability that, given a random curve C, the Frobenius endomorphism acts on the ℓ^∞-torsion points of the Jacobian of the curve with trace t. (For the case $\ell = p$ see Remark 3.6 below; see also Remark 3.12 for the condition that there exists a lift $\tilde{M}$ of M to $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$).

  Our conjecture can then be seen as a minimalist one: we are essentially claiming that the distributions of the trace of Frobenius in $\mathbb{Z}_\ell$ for different primes ℓ are independent of each other (which we know is the case by Theorem 2.1, at least for $\ell \neq q$), and that (as $q \to \infty$) they also become independent of the distribution of the absolute value of $\mathrm{Tr}(\mathrm{Frob}) \in \mathbb{R}$. To put it in another way, Conjecture 3.4 is the simplest joint distribution that reproduces the correct (known) 'marginal' distributions for $\mathrm{Tr}(C) \bmod N$ and for $\frac{|\mathrm{Tr}(C)|}{|\sqrt{q}|} \in [-2g, 2g]$.
- The 'minimalist' philosophy just outlined is, of course, the same that underlies the widely believed Lang-Trotter conjecture [LT76, Part I, Section 3].
- Finally, numerical evidence points in the direction of the conjecture being true, see Section 3.2.

Our conjecture should be contrasted with [BHLGR24, Conjecture 5.1], which makes a different prediction for $H'(q,t)$. The authors of [BHLGR24] define (the analogue of our) $\nu(q,t)$ purely in terms of the Sato-Tate density ν_∞ (for more details, see (24)). We believe that – as happens for $g = 1$ – one should also take into account the measures ν_ℓ for all finite ℓ. In fact, even though we cannot prove Conjecture 3.4, the results of Section 2 are enough to show that [BHLGR24, Conjecture 5.1] is not correct. We show this in Appendix A. The proof in the appendix is a bit technical: [BHLGR24, Conjecture 5.1] refers only to non-hyperelliptic curves and replaces $t/\sqrt{q}$ with the nearest integer, both facts which

introduce formal difficulties. However, the key idea is comparatively simple, so we isolate it in the next proposition, which shows that the measures ν_∞ and H' are substantially different infinitely often. Intuitively, this contradicts [BHLGR24, Conjecture 5.1]; as already mentioned, a complete argument showing that [BHLGR24, Conjecture 5.1] does not hold is given in Appendix A. The following proposition is stated for $g = 3$, but we suspect it should hold for all $g \geq 3$.

Proposition 3.5. *Let $g = 3$. There exists $\varepsilon > 0$ such that for all odd prime powers q bigger than a constant $q_0 > 0$ there exists $t \in [-2g\sqrt{q}, 2g\sqrt{q}] \cap \mathbb{Z}$ such that*

$$\left|\sqrt{q}\mathbb{P}^{\mathrm{naive}}_{g,q}(\operatorname{Tr} C/\mathbb{F}_q = t) - \mathrm{ST}_g(t/\sqrt{q})\right| \geq \varepsilon.$$

Proof. We denote simply by $\mathbb{P}$ the naive probability measure $\mathbb{P}^{\mathrm{naive}}_{g,q}$ on $\mathcal{M}_g(\mathbb{F}_q)$. We claim that

$$\forall \varepsilon > 0\, \forall q_0 > 0\, \exists q > q_0 \text{ odd prime power such that } \forall t \in [-2g\sqrt{q}, 2g\sqrt{q}] \cap \mathbb{Z}$$

one has

$$\left|\mathbb{P}(\operatorname{Tr} C/\mathbb{F}_q = t) - \frac{\mathrm{ST}_g(t/\sqrt{q})}{\sqrt{q}}\right| < \frac{\varepsilon}{\sqrt{q}}. \tag{12}$$

We assume that this holds and aim for a contradiction. Fix $\varepsilon > 0$ and let p be an odd prime. Let $q = p^n$. We have

$$\begin{aligned}
\mathbb{P}(\operatorname{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2) &= \sum_{\substack{t \in [-2g\sqrt{q}, 2g\sqrt{q}] \cap \mathbb{Z} \\ t \equiv 0 \pmod 2}} \left(\mathbb{P}(\operatorname{Tr}(C/\mathbb{F}_q) = t) - \frac{\mathrm{ST}_g(t/\sqrt{q})}{\sqrt{q}} + \frac{\mathrm{ST}_g(t/\sqrt{q})}{\sqrt{q}}\right) \\
&= \sum_{\substack{t \in [-2g\sqrt{q}, 2g\sqrt{q}] \cap \mathbb{Z} \\ t \equiv 0 \pmod 2}} \frac{\mathrm{ST}_g(t/\sqrt{q})}{\sqrt{q}} + \sum_{\substack{t \in [-2g\sqrt{q}, 2g\sqrt{q}] \cap \mathbb{Z} \\ t \equiv 0 \pmod 2}} \left(\mathbb{P}(\operatorname{Tr} C/\mathbb{F}_q = t) - \frac{\mathrm{ST}_g(t/\sqrt{q})}{\sqrt{q}}\right) \\
&= \frac{1}{\sqrt{q}} \sum_{\substack{t \in [-2g\sqrt{q}, 2g\sqrt{q}] \cap \mathbb{Z} \\ t \equiv 0 \pmod 2}} \mathrm{ST}_g(t/\sqrt{q}) + E,
\end{aligned}$$

with

$$|E| \leq (4g+1)\sqrt{q} \cdot \frac{\varepsilon}{\sqrt{q}} \leq (4g+1)\varepsilon \tag{13}$$

by (12). On the other hand, some basic analysis shows that (since ST_g is Riemann-integrable)

$$\frac{1}{\sqrt{q}} \sum_{\substack{t \in [-2g\sqrt{q}, 2g\sqrt{q}] \cap \mathbb{Z} \\ t \equiv 0 \pmod 2}} \mathrm{ST}_g(t/\sqrt{q})$$

converges, as $q = p^n$ goes to infinity, to

$$\frac{1}{2\sqrt{q}} \int_{-2g\sqrt{q}}^{2g\sqrt{q}} \mathrm{ST}_g(t/\sqrt{q})dt = \frac{1}{2}\int_{-2g}^{2g} \mathrm{ST}_g(t)dt = \frac{1}{2}.$$

Therefore,

$$\left|\mathbb{P}(\operatorname{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2) - \frac{1}{2}\right| \leq |E| + \varepsilon \tag{14}$$

for $q = p^n$ large enough.

Let

$$L_1(g) \coloneqq \frac{\#\{M \in \mathrm{GSp}_{2g}(\mathbb{F}_2) : \operatorname{Tr} M \equiv 0 \pmod 2, \operatorname{mult} M = q \equiv 1 \pmod 2\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_2)}.$$

By Remark 2.8, as $q \to \infty$ we have

$$|L_1(g) - \mathbb{P}(\operatorname{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)| = o(1),$$

and in particular, for q large enough, we have

$$|L_1(g) - \mathbb{P}(\operatorname{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)| < \varepsilon. \tag{15}$$

We now prove that the initial claim does not hold for $g = 3$. It seems likely that a similar strategy can be applied for every $g > 3$. By direct computation, $L_1(3) = \frac{1436}{2835} \approx 0.5065\ldots$ is strictly greater than $1/2$. Fix $0 < \varepsilon < \frac{|L_1(g)-1/2|}{8g}$ for $g = 3$. Passing to the limit $n \to \infty$, by Equations (13), (14) and (15) we get

$$\begin{aligned}\left|L_1(3) - \frac{1}{2}\right| &\leq |L_1(3) - \mathbb{P}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)| + \left|\mathbb{P}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2) - \frac{1}{2}\right| \\ &\leq |E| + 2\varepsilon \leq (4g+3)\varepsilon < \left|L_1(3) - \frac{1}{2}\right|,\end{aligned}$$

contradiction. □

3.1 Further remarks on Conjecture 3.4

In this section, we collect several other remarks on Conjecture 3.4 and the possible limits of its validity. As all the material in this section is speculative, we do not go into much detail, but we hope that this discussion will encourage others to investigate the issues raised here.

Our point of departure is the following. Since the statistics of the distribution of the trace of principally polarised abelian varieties (PPAV) of a fixed dimension g over finite fields are the same as those of Jacobians (equivalently, of curves of genus g), it seems reasonable to extend Conjecture 3.4 to the family of all PPAVs of a fixed dimension. In particular, Gekeler's results [Gek03] should perhaps be interpreted in this light, especially since they apply to the case of elliptic curves, not to general curves of genus 1. From this perspective, one should perhaps ask if Conjecture 3.4 could not be upgraded to an actual *equality* for fixed q (as opposed to an asymptotic statement for $q \to \infty$) when one considers the better-behaved family of all PPAVs. We will see that, while the measures $H'(q,t)$ and $\nu'(q,t)$ *cannot* be equal in general, even for abelian varieties (Remark 3.7), this point of view can still be helpful.

Remark 3.6 (Local factor at p)**.** We justify the choice of the local factor (7). Observe first that the more general formula

$$\nu_\ell(q,t) = \lim_{k\to\infty} \frac{\#\left(\mathrm{Im}\left\{\tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) \cap \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \text{ with } \begin{array}{c}\mathrm{tr}(\tilde{M}) = t, \\ \mathrm{mult}(\tilde{M}) = q\end{array}\right\} \to \mathrm{Mat}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})\right)}{\#\left(\mathrm{Im}\left\{\tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) \cap \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \text{ with } \mathrm{mult}(\tilde{M}) = q\right\} \to \mathrm{Mat}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})\right)/\ell^k}$$

reduces to (6) and (7) respectively when $\ell \neq p$ and $\ell = p$. It is an easy exercise to check that the denominator of this formula is simply the average over t of the numerator, so the ratio does measure the deviation from the average of the number of symplectic matrices with a given trace. For $g = 1$, Gekeler shows [Gek03] that this formula does give the correct local factor at p. In general, for p equal to the characteristic of the relevant finite field, one can consider the action of Frobenius on a suitable p-adic cohomology theory (for example, rigid cohomology): in this way, Frobenius acts on a $2g$-dimensional $\mathbb{Q}_p$-vector space preserving a $\mathbb{Z}_p$-lattice, so it defines a matrix with entries in $\mathbb{Z}_p$ and multiplier q. It seems likely that an equidistribution result similar to Theorem 2.3 should also hold in rigid cohomology (see [Ked22, HP20]), which would lead to the local factor (7), just like Theorem 2.3 leads to (6).

Remark 3.7 (q small with respect to g)**.** Notice that $\nu'(q,t)$ can be positive also for values of t such that $q+1-t < 0$. Of course, this does not make sense, because $q+1-t$ should represent the number of $\mathbb{F}_q$-rational points of a curve. The point is that the support of $\nu'(q,t)$ is the full interval $[-2g\sqrt{q}, 2g\sqrt{q}]$, and when q is small with respect to g it may well happen that $q+1-2g\sqrt{q} < 0$.

There are also subtler issues. The Sato-Tate distribution arises as the pushforward via the trace map of the Haar measure on USp_{2g}. Suppose that $M \in \mathrm{USp}_{2g}$ corresponds to the unitarised Frobenius $\frac{\mathrm{Frob}_{C/\mathbb{F}_q}}{\sqrt{q}}$, where $C/\mathbb{F}_q$ is a smooth projective curve of genus g. Then, for every $m \geq 1$ one has

$$\#C(\mathbb{F}_{q^m}) = q^m + 1 - q^{m/2}\,\mathrm{tr}(M^m),$$

and in particular, for all integers $m_1 \mid m_2$ we must have

$$\#C(\mathbb{F}_{q^{m_1}}) = q^{m_1} + 1 - q^{m_1/2}\,\mathrm{tr}(M^{m_1}) \leq q^{m_2} + 1 - q^{m_2/2}\,\mathrm{tr}(M^{m_2}) = \#C(\mathbb{F}_{q^{m_2}}).$$

When q is small with respect to g, there are matrices in USp_{2g} and integers $m_1 \mid m_2$ for which this inequality does not hold. In this regime, one should perhaps replace the usual Sato-Tate measure with the following. Let X be the subset of USp_{2g} consisting of those matrices that satisfy all the inequalities

$$0 \leq q^{m_1} + 1 - q^{m_1/2} \operatorname{tr}(M^{m_1}) \leq q^{m_2} + 1 - q^{m_2/2} \operatorname{tr}(M^{m_2}) = \#C(\mathbb{F}_{q^{m_2}})$$

for all $m_1 \mid m_2$. A candidate to replace ST_g is the pushforward via the trace of the restriction of the Haar measure to the set X (renormalised so as to have mass 1).

Recall that we are fixing g and sending q to infinity, so this issue does not affect our Conjecture 3.4.

Remark 3.8 (Asymmetry of the distribution $H'(q,t)$)**.** An advantage of working with PPAVs rather than curves is that the former always admit quadratic twists, which implies that the distribution of their traces is always symmetric around 0. This is further indication that perhaps Conjecture 3.4 is more natural for the family of PPAVs. In fact, we remark that while $\nu'(q,t)$ is symmetric (that is, $\nu'(q,-t) = \nu'(q,t)$), this is not necessarily the case for $H'(q,t)$ as soon as $g \geq 3$, as one can see for example in [BHLGR24, Figure 4], or below in our own Figure 3. See also [BHLGR24, §5] for a more extensive discussion of the asymmetry of $H'(q,t)$. In particular, we note again that one cannot have an exact equality $H'(q,t) = \nu'(q,t)$ for general g, because the right-hand side is easily seen to be symmetric. All the same, we expect the two measures to be arbitrarily close in the limit $q \to \infty$.

Remark 3.9 (Speed of convergence)**.** The limit in Conjecture 3.4 cannot converge too quickly. We briefly show why.

Given a measure μ on $\mathbb{Z}$, let $(-1)^*\mu(\cdot)$ be the measure defined as $(-1)^*\mu(t) = \mu(-t)$ for all $t \in \mathbb{Z}$. By definition, $(-1)^*\nu'(q,\cdot) - \nu'(q,\cdot) = 0$ since $\nu'(q,\cdot)$ is symmetric. In particular, the moments of $(-1)^*(\sqrt{q}\nu'(q,\cdot)) - (\sqrt{q}\nu'(q,\cdot))$ are 0 for all q. Assume that $d(H'(q,\cdot), \nu'(q,\cdot))$ converges to zero sufficiently quickly (for example, assume that the difference is $O(q^{-k-1})$ for some $k \geq 0$): the first $2k$ moments of $(-1)^*(\sqrt{q}H'(q,\cdot)) - (\sqrt{q}H'(q,\cdot))$ then also converge to zero as q goes to infinity. By [BHLGR24, Corollary 5.3], the n-th moment of $(-1)^*(\sqrt{q}H'(q,\cdot)) - (\sqrt{q}H'(q,\cdot))$ converges, for n odd, to a real number b_n and b_n is non-zero for n large enough (see [BHLGR24, Proposition 2.3]). Hence, for n large enough, the n-th moment of $(-1)^*(\sqrt{q}H'(q,\cdot)) - (\sqrt{q}H'(q,\cdot))$ does not tend to zero as q goes to infinity. If $b_n \neq 0$ and $2k \geq n$, this is a contradiction.

We thank Christophe Ritzenthaler and Elisa Lorenzo García for their comments that led to this remark.

Remark 3.10 (Jacobians among PPAVs)**.** We again take the view that Conjecture 3.4 should be a shadow of a (possibly sharper) statement for the family of PPAVs of a given dimension. From this point of view, it is important to note that – asymptotically – 100% of PPAvs of dimension 2 or 3 are Jacobians (those that are not are either products of PPAVs of lower dimension or Weil restrictions of elliptic curves). Thus, for $g \leq 3$, the two conjectures that one can formulate (for curves of genus g and for g-dimensional PPAVs) should be essentially equivalent. As the dimension grows, Conjecture 3.4 can then be interpreted as saying that Jacobians are 'typical' among PPAVs – the distribution of the trace on the subfamily of Jacobians is the same as the distribution among all PPAVs. While we believe that Conjecture 3.4 holds for all genera g, we should point out that it is very hard to get numerical evidence when the genus/dimension is 4 or more. This is precisely the threshold above which the difference between Jacobians and PPAVs becomes (asymptotically) relevant, so it would be interesting to study this regime more closely. See Figure 5 for an example in which we show the difference between taking into account only Jacobians or all PPAVs.

Remark 3.11 (Principally polarised abelian surfaces with trace zero)**.** In dimension two, PPAVs that are not Jacobians are either products of elliptic curves (with the product polarisation) or Weil restrictions of elliptic curves defined over a quadratic extension. In particular, over the finite field with q elements, there are $\gg q^2$ abelian surfaces that are Weil restrictions of elliptic curves defined over $\mathbb{F}_{q^2}$, but not over $\mathbb{F}_q$. The Galois representation attached to $A := \mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E)$ is the induction from $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_{q^2})$ to $\mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right)$ of the representation attached to $E/\mathbb{F}_{q^2}$, which implies that the Frobenius trace of A is zero for any such Weil restriction. Since the total number of genus-2 curves over $\mathbb{F}_q$ is of order q^3 (see Lemma 2.5), we expect that the proportion of PP abelian surfaces with trace 0 should be significantly higher than the proportion of genus-2 curves with trace 0 (the difference should be of order $q^2/q^3 = 1/q$). If we interpret Conjecture 3.4 as a prediction for the distribution of the number of points of PPAVs, this helps in explaining the peak at 0 in Figure 5 (this peak is particularly noticeable since for $q = 37$ the quantity

$1/q$ is not at all negligible). Similar comments apply in higher dimensions, but the proportion of PPAVs having trace zero for geometric reasons becomes less significant as the dimension increases.

Remark 3.12 (Lift to $\mathbb{Z}_\ell$)**.** Equation (6) requires that the matrix $M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})$ should lift to a matrix $\tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$. While this condition is natural in our setting (since Frobenius is in fact represented by an ℓ-adic matrix with the given trace and multiplier), we believe that omitting this condition should lead to the same result, that is, we conjecture that

$$\tilde{\nu}_\ell(q,t) := \lim_{k\to\infty} \frac{\#\left\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) : \mathrm{tr}(M) = t, \mathrm{mult}(M) = q\right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})/(\ell^k\varphi(\ell^k))}$$

coincides with $\nu_\ell(q,t)$. It is not hard to check that this holds for $g = 1$, but we have been unable to prove the result in general. The difficulties that arise lie in understanding the singularities of the variety X_t^q, that is the $\mathbb{Z}_\ell$-scheme defined as the subscheme of $\mathrm{GSp}_{2g}^{\mathrm{mult}=m}(\mathbb{Z}_\ell)$ defined by the equation $\mathrm{Tr}(M) = t$. When X_t^q is smooth over $\mathbb{Z}_\ell$, an application of Hensel's lemma show that $\nu_\ell(q,t)$ and $\tilde{\nu}_\ell(q,t)$ both coincide with

$$\frac{\#\left\{M \in \mathrm{GSp}_{2g}(\mathbb{F}_\ell) : \mathrm{tr}(M) = t, \mathrm{mult}(M) = q\right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)/(\ell\varphi(\ell))}.$$

Remark 3.13 (Comparison to other recent work)**.** The recent preprint [Shm23] relates the moments

$$M_n(g,q) = \mathbb{E}_{\mathbb{P}^{\mathrm{intr}}_{g,q}}[\#A(\mathbb{F}_q)^n]$$

of the random variable 'number of rational points of A' (here A is drawn at random from $\mathcal{A}_g(\mathbb{F}_q)$ using a suitable intrinsic measure) to the higher cohomology of certain moduli spaces, see [Shm23, p. 2]. This yields explicit formulas for these moments for small g and n [Shm23, Corollaries 4.3 and 5.4] and it would be interesting to compare these results with the predictions of Conjecture 3.4. It may be possible to carry out this comparison by using the techniques of [AG17, AAGG23].

In particular, [AAGG23, Theorem A] comes near to proving Conjecture 3.4 in the context of principally polarised abelian varieties. However, we point out that to establish Conjecture 3.4 one would still need to overcome several obstacles: the formula of [AAGG23, Theorem A] only applies to certain isogeny classes of abelian varieties and involves Tamagawa numbers that would have to be averaged; even more substantially, it is not clear how one would isolate Jacobians among all abelian varieties. Finally, even though this is perhaps only a technical problem, the existence of the limits (6) and (7) seems substantially easier to prove in the context of [AAGG23, Theorem A] than it is in the general case we consider here (essentially because in the setting of [AAGG23, Theorem A] the expression appearing under the limit sign in (6) is constant for $k \gg 0$, which is not necessarily true in our generality).

3.2 Numerical evidence

In this section we report on numerical experiments that seem to support Conjecture 3.4. The data are computed using MAGMA [BCP97]. All the MAGMA scripts to verify our data are available online [BLV23].

In the graphs below we plot the distribution $t \mapsto H'(q,t)$ for various values of g and q. These distributions are obtained by directly counting all isomorphism classes of curves of the given genus over the given finite field (the data for $q = 53, g = 3$ is taken from [LRRS14]). In addition, on the same graphs, we also plot an approximation of the Sato-Tate density and of $\nu'(q,t)$. We briefly explain how we obtain these approximations, starting with a general technique to compute the Sato-Tate density in arbitrary dimension.

Remark 3.14 (Computation of $\mathrm{ST}_g(x)$ for arbitrary g)**.** For general g, the density $\mathrm{ST}_g(x)$ can be calculated up to arbitrary precision by using a technique due to Kedlaya-Sutherland [KS09] and Lachaud [Lac16]. One can first use [KS09, Section 4.1] to compute the *moments* of ST_g, that is,

$$m_n = \int_{-2g}^{2g} x^n \, d\,\mathrm{ST}_g(x).$$

Once the moments (or at least, sufficiently many moments) are known, we can recover $\mathrm{ST}_g(x)$ as follows. Let $L_n(x)$ be the Legendre polynomials, which form a complete orthogonal basis of $L^2([-1,1])$. By

rescaling, the polynomials

$$\tilde{L}_n(x) := \left(\int_{-2g}^{2g} L_n(x/2g)^2\right)^{-1/2} L_n(x/2g)$$

form an orthonormal basis of $L^2([-2g, 2g])$. From the explicit expression of $\tilde{L}_n(x) = \sum_{i=0}^{n} a_{n,i}x^i$ as a polynomial, one can easily compute

$$c_n = \int_{-2g}^{2g} \tilde{L}_n(x)\, d\,\mathrm{ST}_g(x) = \sum_{i=0}^{n} a_{n,i} m_i.$$

Finally, we have the convergent expansion in $L^2([-2g, 2g])$

$$\mathrm{ST}_g(x) = \sum_{n\geq 0} c_n \tilde{L}_n(x), \tag{16}$$

which allows the computation of $\mathrm{ST}_g(x)$ to arbitrary precision. In our numerical experiments, we use this technique to approximate $\mathrm{ST}_3(x)$.

In our numerical experiments, we approximate the Sato-Tate density with the value of the series in Equation (16) truncated at $n \leq 100$. For $\nu'(q,t)$, we approximate the value of $\nu(q,t)$ (see Equation 8) by considering the product of $\nu_\ell(q,t)$ for $\ell \leq 100$ and $\ell = \infty$. To compute an approximation of $\nu_\ell(q,t)$ for ℓ prime, we compute the value of the expression appearing under the limit sign in Equation 6 for $k = 1$ or 2. To compute an approximation of $\nu_\infty(q,t)$, we use our approximation of the Sato-Tate density.

Let

$$H'_{\mathrm{intr}}(q,t) = \mathbb{P}^{\mathrm{intr}}_{g,q}\left(\{C \in \mathcal{M}_g(\mathbb{F}_q) : \mathrm{Tr}(C) = t\}\right).$$

We compute the value of $H'_{\mathrm{intr}}(q,t)$ by direct enumeration of all the curves of genus g defined over $\mathbb{F}_q$.

Finally, below each graph we also give the distance d between the measures $H' := H'_{\mathrm{intr}}(q,\cdot)$ and $\nu' := \nu'(q,\cdot)$, as well as the distance between H' and the Sato-Tate measure. Our conjecture predicts that $d(H', \nu')$ should go to 0 as q goes to infinity. As a consequence of [BHLGR24, Conjecture 5.1] (see (24)), $d(H', \nu_\infty)$ should go to 0. We proved in Proposition A.3 that the conjecture does not hold.

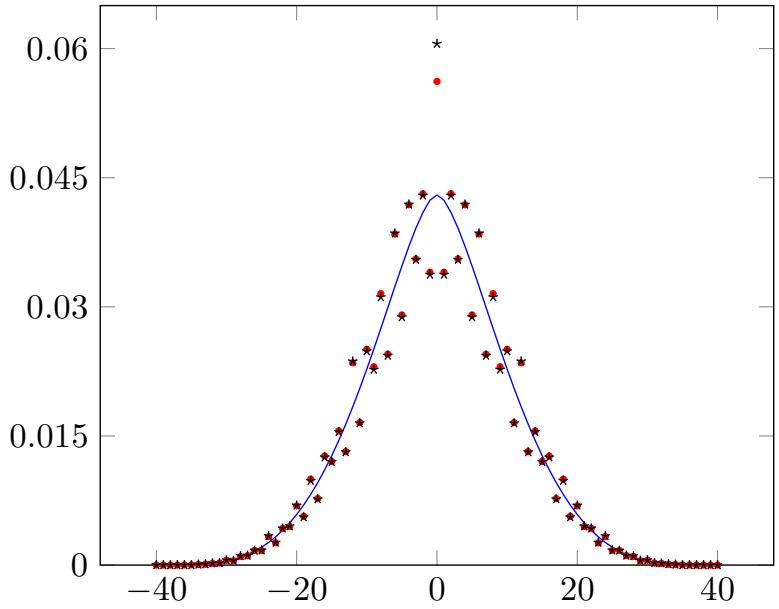

Figure 2: Case $g = 2$ and $q = 101$. The red dots are the values of H'. The black stars are the values of the approximation of $\nu'(q,t)$. The blue graph is the approximation of the Sato-Tate density. In this case, $d(H',\nu') \approx 0.01117$ and $d(H',\nu_\infty) \approx 0.15166$.

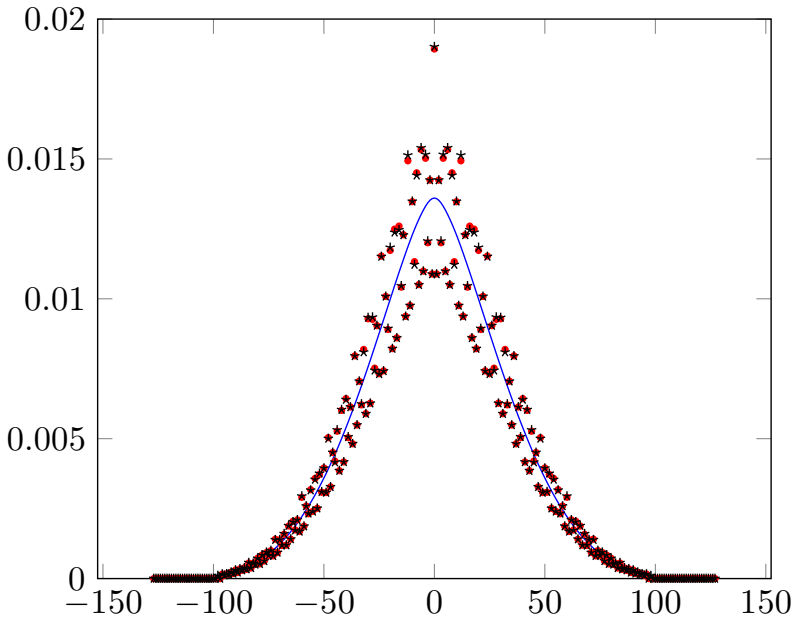

Figure 1: Case $g = 2$ and $q = 1009$. The red dots are the values of H'. The black stars are the values of the approximation of $\nu'(q,t)$. The blue graph is the approximation of the Sato-Tate density. In this case, $d(H',\nu') \approx 0.00439$ and $d(H',\nu_\infty) \approx 0.15528$.

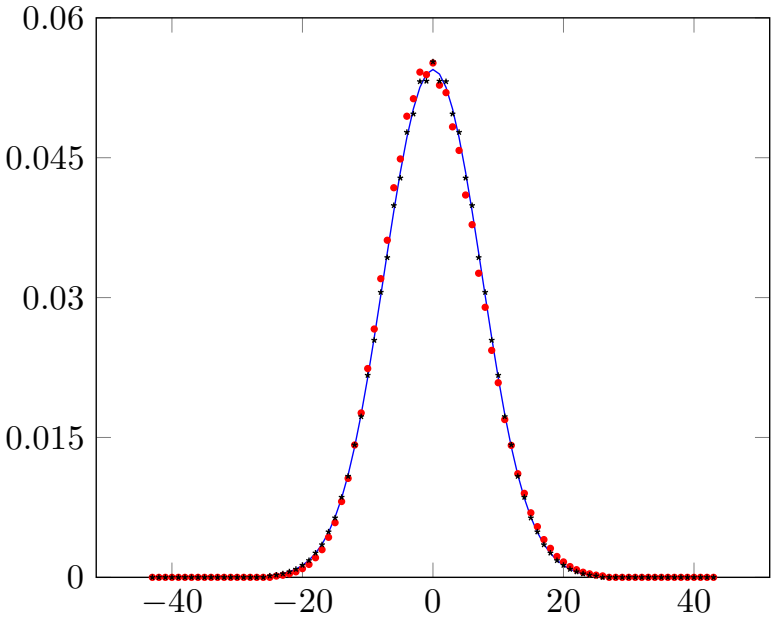

Figure 3: Case $g = 3$ and $q = 53$. The red dots are the values of H'. The black stars are the values of the approximation of $\nu'(q,t)$. The blue graph is the approximation of the Sato-Tate density. In this case, $d(H', \nu') \approx 0.03842$ and $d(H', \nu_\infty) \approx 0.03940$.

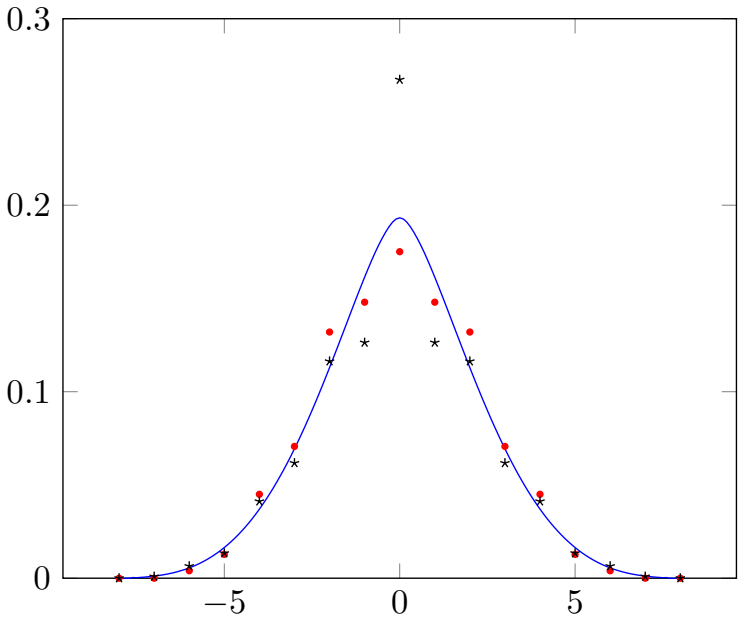

Figure 4: Case $g = 2$ and $q = 5$. As pointed out in Remark 3.7, there is an issue when $q + 1 - t < 0$ (for example when $t = 7$). Indeed, $H'(q, 7) = 0$ because $q + 1 - t$ represents the number of $\mathbb{F}_q$-rational points of a curve. Instead, both $\nu'(q, 7) \approx 0.0009$ and $\nu_\infty(q, 7) \approx 0.0011$ are strictly positive.

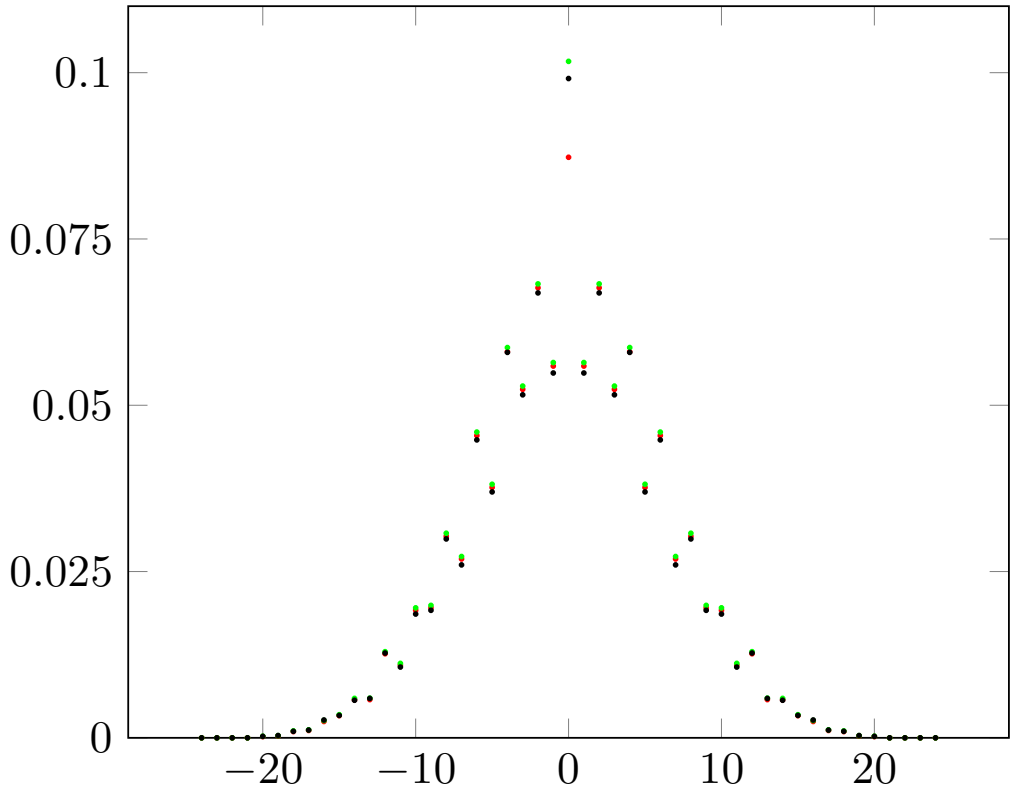

Figure 5: This graph shows the difference between considering all PPAVs or only Jacobians of curves (see Remark 3.10). We take $g = 2$ and $q = 37$. We plot in red the distribution H' and in black (an approximation of) the distribution $\nu'(q,t)$. The green dots represent the probabilities of the various traces when we take into account all principally polarised abelian surfaces over $\mathbb{F}_q$. Call this distribution H''. The distance between the distributions H' and $\nu'(q,t)$ is ≈ 0.02673. The distance between H'' and $\nu'(q,t)$ is ≈ 0.02775. Notice that the approximations are very close to each other, except at $t = 0$, where taking into account all PPAVs gives a much better agreement with our prediction. An explanation for this phenomenon is given in Remark 3.11.

4 Well-posedness of Equation (8)

In this section we prove that the quantity $\nu(q,t)$ is well-defined. We have already observed (Remark 3.2) that $\nu_\ell(q,t)$ is well-defined for all $\ell \leq \infty$, so it suffices to show that, as $\ell \to \infty$ among the prime numbers, we have $\nu_\ell(q,t) = 1 + O(\ell^{-2})$. This suffices to ensure that the product (8) converges.

As a preparation for the proof, we introduce the following notation and make some remarks.

Notation 4.1. *Let R be a (commutative unitary) ring and let $m \in R^\times$ be a fixed element. We define $\mathrm{GSp}_{2g,R}^{\mathrm{mult}=m}$ as the subscheme of $\mathrm{GSp}_{2g,R}$ cut by the equation $\mathrm{mult}(M) = m$.*

Remark 4.2. Let us fix the antisymmetric form $\begin{pmatrix} 0 & \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix}$. The matrix

$$M_m := \begin{pmatrix} m & & & & & & \\ & \ddots & & & & & \\ & & m & & & & \\ & & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \end{pmatrix}$$

is in $\mathrm{GSp}_{2g}(R)$ and has multiplier m. Multiplication by M_m gives an algebraic isomorphism between the R-schemes $\mathrm{Sp}_{2g,R}$ and $\mathrm{GSp}_{2g,R}^{\mathrm{mult}=m}$. The same applies for any matrix $M_m \in \mathrm{GSp}_{2g}(R)$ with multiplier m. In particular, $\mathrm{GSp}_{2g,R}^{\mathrm{mult}=m}$ is smooth for any value of m. If R is a field, the dimension of $\mathrm{GSp}_{2g,R}^{\mathrm{mult}=m}$ is equal to $\dim \mathrm{Sp}_{2g,R}$.

In what follows we will be interested in the subschemes of $\mathrm{GSp}_{2g,R}^{\mathrm{mult}=m}$ defined by the equation $\mathrm{Tr}(M) = t$ for a fixed value of $t \in R$. We will mostly work with $R = \mathbb{Z}_\ell$ and $R = \mathbb{F}_\ell$.

Definition 4.3. *For $m \in R^\times, t \in R$, we define the R-scheme X_t^m as the subscheme of $\mathrm{GSp}_{2g,R}^{\mathrm{mult}=m}$ defined by the equation $\mathrm{Tr}(M) = t$.*

Notice that, if we fix $m \in \mathbb{Z} \setminus \{0\}$, then m is invertible in $\mathbb{Z}[1/m]$, and hence X_t^m makes sense as a scheme over $\mathrm{Spec}\,\mathbb{Z}[1/m]$. We will be able to reduce this scheme modulo any prime that does not divide m.

4.1 Number of points of X_t^m over finite fields

In this section we study the number of $\mathbb{F}_\ell$-points of X_m^t (Theorem 4.4 and Lemma 4.5) and show that a large proportion of them correspond to smooth points of X_m^t (Lemma 4.6). For the first objective, our approach is inspired by [Lee01]. More precisely, the main result of [Lee01] gives a formula counting the number of elements in $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with given trace and *determinant*. The same strategy allows us to prove the following version, where we count matrices with given trace and *multiplier*. Before stating the result, we remind the reader that the q-binomial coefficient $\begin{bmatrix} n \\ r \end{bmatrix}_q$ is defined as $\prod_{j=0}^{r-1} \frac{q^{n-j}-1}{q^{r-j}-1}$. For ease of comparison with [Lee01], we adopt the same notation as in op. cit.

Theorem 4.4. *Let q be a prime power, $\zeta \in \mathbb{F}_q^\times$, and $\eta \in \mathbb{F}_q$. Let*

$$T_m = q \sum_{\alpha_1,\ldots,\alpha_m \in \mathbb{F}_q^\times} t\left(\alpha_1 + \zeta\alpha_1^{-1} + \cdots + \alpha_m + \zeta\alpha_m^{-1}\right) - (q-1)^m,$$

where

$$t(x) = \begin{cases} 1, & \text{if } x = \eta \\ 0, & \text{otherwise,} \end{cases}$$

and the sum is regarded as $t(0)$ for $m = 0$. Let

$$C(\zeta,\eta) := \left|\{g \in \mathrm{GSp}_{2n}(\mathbb{F}_q) \mid \mathrm{mult}\, g = \zeta, \mathrm{tr}\, g = \eta\}\right| = \left|X_\eta^\zeta(\mathbb{F}_q)\right|.$$

We have the following exact formula for $C(\zeta,\eta)$:

$$C(\zeta,\eta) = q^{n^2-1}\prod_{j=1}^{n}\left(q^{2j}-1\right) + E, \tag{17}$$

where

$$E = q^{n^2-1}\sum_{b=0}^{\lfloor n/2\rfloor}\left(q^{b^2+b}\begin{bmatrix} n \\ 2b\end{bmatrix}_q \prod_{j=1}^{b}(q^{2j-1}-1)\sum_{l=0}^{\lfloor n/2-b\rfloor} q^l R(n-2b+1,l)T_{n-2b-2l}\right), \tag{18}$$

$R(m,l)$ *denotes*

$$R(m,l) = \sum_{0<j_1<\cdots<j_l<m-l}\prod_{\nu=1}^{l}(q^{m-\nu-j_\nu}-1),$$

and we set by convention $R(m,0)=1$.

Proof. The proof is virtually identical to that of [Lee01, Theorem 1]: if one simply replaces every occurrence of det with mult in the proof of [Lee01, Theorem 1] everything goes through without difficulty. More precisely, let

$$e(x) = \begin{cases} 1 \text{ if } x=\zeta, \\ 0 \text{ otherwise.}\end{cases}$$

Throughout the proof, several instances of $\det(d_\alpha)=\alpha^n$ are replaced by $\mathrm{mult}(d_\alpha)=\alpha$, where $d_\alpha = \begin{pmatrix}\mathrm{Id}_n & 0 \\ 0 & \alpha\,\mathrm{Id}_n\end{pmatrix}$. In particular, the sums $\sum_{\alpha\in\mathbb{F}_q^\times} e(\alpha^n)$ are replaced by $\sum_{\alpha\in\mathbb{F}_q^\times} e(\alpha)$. In the proof of [Lee01, Theorem 1], the sum $\sum_{\alpha\in\mathbb{F}_q^\times} e(\alpha^n)$ evaluates to the number S of n-th roots of ζ in $\mathbb{F}_q^\times$; in our case, the sum $\sum_{\alpha\in\mathbb{F}_q^\times} e(\alpha)$ simply evaluates to 1 for all $\zeta\in\mathbb{F}_q^\times$. □

We will think of the expression E appearing in Equation (18) as an error term. We now proceed to bound this error. We work with a fixed value of n: this implies in particular that the number of summands (resp. factors) in the sum (resp. products) appearing in (18) is $O(1)$. We then have the following estimates (where the implicit constants may depend on n, but not on q):

1. $\begin{bmatrix} n \\ r\end{bmatrix}_q = \prod_{j=0}^{r-1}\frac{q^{n-j}-1}{q^{r-j}-1} \ll \prod_{j=0}^{r-1}\frac{q^{n-j}}{q^{r-j}} = \prod_{j=0}^{r-1} q^{n-r} = q^{nr-r^2}$, and hence in particular
$$\begin{bmatrix} n \\ 2b\end{bmatrix}_q \ll q^{2bn-4b^2}.$$
2. $\prod_{j=1}^{b}(q^{2j-1}-1) \le \prod_{j=1}^{b} q^{2j-1} = q^{\sum_{j=1}^{b}(2j-1)} = q^{b^2}$.
3. We claim that $R(m,l)\ll q^{ml-l(l+1)}$ for $m\le n$. To see this, notice that the length of the sum defining $R(m,l)$ is $O(1)$, so it suffices to estimate the largest summand. (The length of the sum is $O(1)$ because it is bounded by a function of m, and m is bounded in terms of n.) Clearly the condition $j_k > j_{k-1}$ for $k=2,\dots,l$ yields $j_\nu \ge \nu$, so $q^{m-\nu-j_\nu}\le q^{m-2\nu}$. We can then estimate
$$R(m,l) \ll \prod_{\nu=1}^{l} q^{m-2\nu} = q^{ml-l(l+1)},$$
as claimed.
4. We also claim that $|T_m|\ll q^m$. To show this, we first remark that, for fixed values of $\alpha_1,\dots,\alpha_{m-1}\in\mathbb{F}_q^\times$, the equation
$$\alpha_1+\zeta\alpha_1^{-1}+\cdots+\alpha_m+\zeta\alpha_m^{-1}=\eta$$
has at most 2 solutions $\alpha_m\in\mathbb{F}_q^\times$. We can then rewrite and estimate $|T_m|$ as follows:
$$\Big|q\sum_{\alpha_1,\dots,\alpha_{m-1}\in\mathbb{F}_q^\times}\ \sum_{\substack{\alpha_m\in\mathbb{F}_q^\times \\ \alpha_1+\zeta\alpha_1^{-1}+\cdots+\alpha_m+\zeta\alpha_m^{-1}=\eta}} 1-(q-1)^m\Big| \le q\cdot(q-1)^{m-1}\cdot 2+(q-1)^m \ll q^m,$$
as desired.

We now give an upper bound for the quantity $|E|$, with E as in Equation (18). According to our previous estimates,

$$\left|\sum_{l=0}^{\lfloor n/2-b\rfloor} q^l R(n-2b+1,l)T_{n-2b-2l}\right| \ll \sum_{l=0}^{\lfloor n/2-b\rfloor} q^l q^{(n-2b+1)l-l(l+1)} q^{n-2b-2l}$$
$$\ll q^{n-2b} \sum_{l=0}^{\lfloor n/2-b\rfloor} q^{(n-2b-1)l-l^2}.$$

Notice again that the length of this sum is $O(1)$, so it suffices to give an upper bound for its largest summand. For a fixed value of b, the exponent $(n-2b-1)l-l^2$ is maximal for $l=\frac{n-2b-1}{2}$ (which might not be an integer, but still provides an upper bound for the value of the exponent). We thus get

$$\left|\sum_{l=0}^{\lfloor n/2-b\rfloor} q^l R(n-2b+1,l)T_{n-2b-2l}\right| \ll q^{n-2b} q^{\left(\frac{n-2b-1}{2}\right)^2}.$$

We now consider the expression

$$\left|q^{b^2+b}\begin{bmatrix} n \\ 2b \end{bmatrix}_q \prod_{j=1}^{b}(q^{2j-1}-1) \sum_{l=0}^{\lfloor n/2-b\rfloor} q^l R(n-2b+1,l)T_{n-2b-2l}\right| \ll q^{b^2+b} q^{2bn-4b^2} q^{b^2} q^{n-2b} q^{\left(\frac{n-2b-1}{2}\right)^2},$$

corresponding to a fixed value of b in the sum (18). The exponent of q on the right-hand side is again a quadratic function of b (to be precise, it is given by $-b^2+bn+\frac{1}{4}n^2+\frac{1}{2}n+1/4$), which is easily seen to achieve its maximum for $b=n/2$. This maximum value is given by $\frac{1}{2}n^2+\frac{1}{2}n+\frac{1}{4}$. Thus, $q^{(1/2)n^2+(1/2)n+1/4}$ is an upper bound for each summand. Keeping once again in mind that the length of the sum is $O(1)$, we have proved that

$$|E| \ll q^{n^2-1} q^{\frac{1}{2}n^2+\frac{1}{2}n+\frac{1}{4}} = q^{\frac{3}{2}n^2+\frac{1}{2}n-\frac{3}{4}}.$$

We can finally prove:

Lemma 4.5. *For all $g \geq 2$, all primes ℓ, and all m with $(m,\ell)=1$ we have*

$$\frac{\#X_t^m(\mathbb{F}_\ell)}{\#\operatorname{GSp}_{2g}(\mathbb{F}_\ell)/(\ell\varphi(\ell))} = \frac{\#\{M \in \operatorname{GSp}_{2g}(\mathbb{F}_\ell) : \operatorname{Tr}(M)=t, \operatorname{mult} M = m\}}{\#\operatorname{GSp}_{2g}(\mathbb{F}_\ell)/(\ell\varphi(\ell))} = 1+O(\ell^{-2}), \tag{19}$$

where the constant implicit in the big-O sign depends only on g.

Proof. The numerator of (19) is given by (17) (with $n=g$, $q=\ell$, $\zeta=m$ and $\eta=t$). Note that $\ell^{g^2-1}\prod_{j=1}^{g}\left(\ell^{2j}-1\right)$ is exactly $\frac{\#\operatorname{GSp}_{2g}(\mathbb{F}_\ell)}{\ell\varphi(\ell)}$. Thus, the ratio in (19) is given by

$$1+\frac{E}{\frac{1}{\ell(\ell-1)}\#\operatorname{GSp}_{2g}(\mathbb{F}_\ell)}.$$

Since

$$\frac{1}{\ell(\ell-1)}\#\operatorname{GSp}_{2g}(\mathbb{F}_\ell) = \frac{1}{\ell(\ell-1)}(\ell-1)\#\operatorname{Sp}_{2g}(\mathbb{F}_\ell) = \ell^{g^2-1}\prod_{j=1}^{g}(\ell^{2j}-1) \gg \ell^{2g^2+g-1},$$

we obtain that (19) is

$$1+O\left(\ell^{\frac{3}{2}g^2+\frac{1}{2}g-\frac{3}{4}-(2g^2+g-1)}\right) = 1+O\left(\ell^{-\frac{1}{2}g^2-\frac{1}{2}g+\frac{1}{4}}\right),$$

which is $1+O(\ell^{-2})$ for all $g \geq 2$. ∎

Lemma 4.6. *Fix $t, m \in \mathbb{Z}$ and let $\ell \geq 3$ be a prime number not dividing m. Let*

$$X := (X_t^m)_{\mathbb{F}_\ell} = \mathrm{GSp}_{2g,\mathbb{F}_\ell} \cap \{\mathrm{Tr} = t\} \cap \{\mathrm{mult} = m\},$$

considered as a variety over $\mathbb{F}_\ell$. Write X^{smooth} for the smooth locus of X. The singular locus X^{sing} has codimension at least 3 in X. We have $\#X^{\mathrm{sing}}(\mathbb{F}_\ell) = O(\ell^{2g^2+g-4})$ and

$$\#X^{\mathrm{smooth}}(\mathbb{F}_\ell) = \frac{\#\,\mathrm{GSp}_{2g,\mathbb{F}_\ell}(\mathbb{F}_\ell)}{\ell\varphi(\ell)}(1 + O(\ell^{-2})).$$

The implied constants depend on t and m, but not on ℓ.

Proof. We view X as a subvariety of the affine space $\mathbb{A}^{(2g)^2}_{\mathbb{F}_\ell}$, considered as the space of matrices of size $2g \times 2g$. The variety X is the intersection of $\mathrm{GSp}^{\mathrm{mult}=m}_{2g,\mathbb{F}_\ell} \cong \mathrm{Sp}_{2g,\mathbb{F}_\ell}$ with the hyperplane H defined by the condition $\mathrm{Tr}(M) = t$. The hyperplane section $\mathrm{GSp}^{\mathrm{mult}=m}_{2g,\mathbb{F}_\ell} \cap H$ is smooth at a point $x \in X(\overline{\mathbb{F}_\ell})$ unless the (tangent space to the) hyperplane H contains the tangent space of $\mathrm{GSp}^{\mathrm{mult}=m}_{2g,\overline{\mathbb{F}_\ell}}$ at the point x. Take any point $x \in X(\overline{\mathbb{F}_\ell})$. Since x has multiplier m, left multiplication by $x \in \mathrm{GSp}_{2g}(\overline{\mathbb{F}_\ell})$ gives an isomorphism L_x between $\mathrm{Sp}_{2g,\overline{\mathbb{F}_\ell}}$ and $\mathrm{GSp}^{\mathrm{mult}=m}_{2g,\overline{\mathbb{F}_\ell}}$. The differential of L_x gives an isomorphism between the tangent space at Id and the tangent space at x. If we identify both tangent spaces to subspaces of the tangent space to $\mathbb{A}^{(2g)^2}_{\overline{\mathbb{F}_\ell}}$ (that is, to matrices of size $2g \times 2g$), the differential in question is simply multiplication by x itself. Thus, we may view the tangent space at x as the image via x of the tangent space at Id, which is the Lie algebra of $\mathrm{Sp}_{2g,\overline{\mathbb{F}_\ell}}$. This can be written down explicitly: choose the anti-symmetric bilinear form represented by the matrix

$$\Omega := \begin{pmatrix} 0 & \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix}.$$

Differentiating the condition ${}^tM\Omega M = \Omega$, we find that the Lie algebra of $\mathrm{Sp}_{2g,\overline{\mathbb{F}_\ell}}$ is given by those matrices M that satisfy ${}^tM\Omega + \Omega M = 0$. Writing M in block form, we obtain that $\mathrm{Lie}\,\mathrm{Sp}_{2g,\overline{\mathbb{F}_\ell}}$ is the vector space of $\overline{\mathbb{F}_\ell}$-matrices

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

with ${}^tB = B, {}^tC = C, {}^tD = -A$ (see [FH91, §16.1] for the identical calculation over the complex numbers). From the previous arguments, it follows that x can only be a singular point if

$$x\,\mathrm{Lie}(\mathrm{Sp}_{2g,\overline{\mathbb{F}_\ell}}) \subseteq \{\mathrm{Tr} = 0\},$$

which is to say

$$\mathrm{Tr}(xL) = 0 \quad \forall L \in \mathrm{Lie}(\mathrm{Sp}_{2g,\overline{\mathbb{F}_\ell}}).$$

Write $x = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and $L = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with B, C symmetric and $D = -{}^tA$. This easily gives $\mathrm{Tr}(\beta C) = \mathrm{Tr}(\gamma B) = 0$ for all symmetric B, C (which implies that β, γ are anti-symmetric) and

$$\mathrm{Tr}(\alpha A - \delta \cdot {}^tA) = \mathrm{Tr}(\alpha A - A \cdot {}^t\delta) = \mathrm{Tr}(\alpha A - {}^t\delta \cdot A) = 0$$

for all A (which implies $\alpha = {}^t\delta$).

Thus, the locus of non-smooth points is contained in the linear space defined by the equations

$${}^t\beta = -\beta, {}^t\gamma = -\gamma, {}^t\delta = \alpha.$$

This linear space has dimension $g^2 + 2\frac{g(g-1)}{2} = 2g^2 - g$, and hence codimension at least $2g - 1 \geq 3$ in X, each of whose irreducible components has dimension at least $\dim \mathrm{GSp}^{\mathrm{mult}=m}_{2g,\mathbb{F}_\ell} - 1 = \dim \mathrm{Sp}_{2g,\mathbb{F}_\ell} - 1 = 2g^2 + g - 1$ (at least one irreducible component has exactly this dimension). We now observe that by the Lang-Weil estimates [LW54, Theorem 1] we have $\#X^{\mathrm{sing}}(\mathbb{F}_\ell) = O(\ell^{\dim X^{\mathrm{sing}}}) = O(\ell^{\dim X - 3})$, with an implicit constant that depends only on X and not ℓ. Taking into account the obvious decomposition $X^{\mathrm{smooth}}(\mathbb{F}_\ell) \bigsqcup X^{\mathrm{sing}}(\mathbb{F}_\ell) = X(\mathbb{F}_\ell)$ and the fact that

$$\#X(\mathbb{F}_\ell) = \frac{\#\,\mathrm{GSp}_{2g,\mathbb{F}_\ell}(\mathbb{F}_\ell)}{\ell\varphi(\ell)}(1 + O(\ell^{-2}))$$

by Lemma 4.5, we obtain the desired estimate

$$\#X^{\mathrm{smooth}}(\mathbb{F}_\ell) = \frac{\#\,\mathrm{GSp}_{2g,\mathbb{F}_\ell}(\mathbb{F}_\ell)}{\ell\varphi(\ell)}(1+O(\ell^{-2})).$$

□

4.2 Convergence of the infinite product (8)

Lemma 4.7. *Let $g \geq 2$, q be a prime power, and $t \in \mathbb{Z}$. Let $\ell \geq 3$ be a prime that does not divide q. We have $\nu_\ell(q,t) = 1 + O(\ell^{-2})$, where the implied constant depends on g, q, and t.*

Proof. Let $X := X_t^q$. We denote by $X^{\mathrm{sing}}(\mathbb{Z}/\ell^n\mathbb{Z})$ the subset of $X(\mathbb{Z}/\ell^n\mathbb{Z})$ consisting of points that map to singular points of $X^{\mathrm{sing}}(\mathbb{F}_\ell)$ (this does agree with the set of $\mathbb{Z}/\ell^n\mathbb{Z}$-valued points of the singular subscheme X^{sing} of X). We apply [Oes82, Property (U), page 326] to

$$X(\mathbb{Z}_\ell) = \{M \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) : \mathrm{Tr}\, M = t, \mathrm{mult}\, M = mq\}$$

$$m = 1, \quad N = (2g)^2, \quad n = n, \quad B = x_0 + \ell\mathbb{Z}_\ell^{(2g)^2}$$

where $x_0 \bmod \ell$ is a matrix lying in $X^{\mathrm{sing}}(\mathbb{F}_\ell)$. We first assume that $X_{\mathbb{Z}_\ell}$ is irreducible. Considering X as a scheme over the spectrum of the DVR $\mathbb{Z}_\ell$, [Sta22, Lemma 0B2J] shows that $X_{\mathbb{F}_\ell}$ is equidimensional of some dimension d, and Oesterlé's result gives

$$\#\{\text{closed balls } A \text{ of radius } \ell^{-n} : A \cap X \neq \emptyset \text{ and } A \subseteq B\} \leq C\ell^{\dim X(n-1)}$$

for a constant C that depends only on the degree in dimension d [Oes82, §0.6] of $X_{\mathbb{F}_\ell}$, which is clearly bounded independently of ℓ. On the other hand, we have

$$\begin{aligned}&\#\{\text{closed balls A of radius } \ell^{-n} : A \cap X \neq \emptyset \text{ and } A \subseteq B\}\\ &= \#\left\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}) : \begin{array}{cc} & \exists \tilde{M} \in X(\mathbb{Z}_\ell) \\ \tilde{M} \equiv M & \pmod{\ell^n} \\ M \equiv x_0 & \pmod{\ell}\end{array}\right\}.\end{aligned}$$

Hence, summing over the points $x_0 \in X^{\mathrm{sing}}(\mathbb{F}_\ell)$ we obtain

$$\#\left\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}) : \begin{array}{cc} & \exists \tilde{M} \in X(\mathbb{Z}_\ell) \\ \tilde{M} \equiv M & \pmod{\ell^n} \\ M \bmod \ell & \in X^{\mathrm{sing}}(\mathbb{F}_\ell)\end{array}\right\} \leq C\#X^{\mathrm{sing}}(\mathbb{F}_\ell)\ell^{(n-1)\dim X}. \tag{20}$$

If $X_{\mathbb{Z}_\ell}$ is not irreducible, we can repeat the above argument with each irreducible component X_i. If C_i is the constant that corresponds to the component X_i, we easily obtain

$$\begin{aligned}\#\left\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}) : \begin{array}{cc} & \exists \tilde{M} \in X(\mathbb{Z}_\ell) \\ \tilde{M} \equiv M & \pmod{\ell^n} \\ M \bmod \ell & \in X^{\mathrm{sing}}(\mathbb{F}_\ell)\end{array}\right\} &\leq \sum_i C_i \#X_i^{\mathrm{sing}}(\mathbb{F}_\ell)\ell^{(n-1)\dim X_i}\\ &\leq \left(\sum_i C_i\right)\#X^{\mathrm{sing}}(\mathbb{F}_\ell)\ell^{(n-1)\dim X}.\end{aligned}$$

Note that the number of irreducible components is bounded independently of ℓ, and so is the constant $\left(\sum_i C_i\right)$ (because the degrees are bounded in terms of the equations of X, which are independent of ℓ). The conclusion is that there exists a constant C such that (20) holds for all n and all but finitely many ℓ.

Recall now the definition of $\nu_\ell(q,t)$ from Equation (6): it is the limit over k of the ratio

$$\frac{\#\left\{M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) : \exists \tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) : \tilde{M} \equiv M \pmod{\ell^k} \text{ with } \begin{array}{c}\mathrm{tr}(\tilde{M}) = t,\\ \mathrm{mult}(\tilde{M}) = q\end{array}\right\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})/(\ell^k\varphi(\ell^k))}. \tag{21}$$

Clearly, a matrix M counted in the numerator of this expression in particular reduces modulo ℓ to a point in $X(\mathbb{F}_\ell)$. For a fixed $x_0 \in X(\mathbb{F}_\ell)$, denote by $N(x_0,k)$ the quantity

$$N(x_0,k) = \left\{ M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) : M \equiv x_0 \pmod{\ell}, \exists \tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \text{ with } \begin{array}{c} \tilde{M} \equiv M \pmod{\ell^k} \\ \mathrm{tr}(\tilde{M}) = t \\ \mathrm{mult}(\tilde{M}) = q \end{array} \right\}$$
$$= \left\{ M \in \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) : M \equiv x_0 \pmod{\ell}, \exists \tilde{M} \in X(\mathbb{Z}_\ell) \text{ with } \tilde{M} \equiv M \pmod{\ell^k} \right\}.$$

When x_0 is a smooth point of $X(\mathbb{F}_\ell)$, Hensel's lemma shows that x_0 has precisely $\ell^{(k-1)\dim X_{\mathbb{F}_\ell}}$ lifts to $X(\mathbb{Z}/\ell^k\mathbb{Z})$, and each of these further lifts to a point in $X(\mathbb{Z}_\ell)$ (note that a smooth point necessarily lies on a component of dimension equal to $\dim X_{\mathbb{F}_\ell}$: indeed, X is a hyperplane section of a smooth variety, so every smooth point lies on a component of maximal dimension). Therefore, we have $N(x_0,k) = \ell^{(k-1)\dim X_{\mathbb{F}_\ell}}$ for such x_0. On the other hand, Equation (20) and Lemma 4.6 show that $\sum_{x_0 \in X^{\mathrm{sing}}(\mathbb{F}_\ell)} N(x_0,k) = O(\ell^{k\dim X_{\mathbb{F}_\ell} - 3})$.

Thus, the numerator of (21) is given by

$$\begin{aligned} \sum_{x_0 \in X(\mathbb{F}_\ell)} N(x_0,k) &= \sum_{x_0 \in X^{\mathrm{smooth}}(\mathbb{F}_\ell)} N(x_0,k) + \sum_{x_0 \in X^{\mathrm{sing}}(\mathbb{F}_\ell)} N(x_0,k) \\ &= \#X^{\mathrm{smooth}}(\mathbb{F}_\ell)\ell^{(k-1)\dim X_{\mathbb{F}_\ell}} + O(\ell^{k\dim X_{\mathbb{F}_\ell}-3}) \\ &= \frac{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}{\ell\varphi(\ell)}(1+O(\ell^{-2}))\cdot\ell^{(k-1)\dim X_{\mathbb{F}_\ell}} + O(\ell^{k\dim X_{\mathbb{F}_\ell}-3}), \end{aligned}$$

where in the last equality we have applied Lemma 4.6. Using $\dim X_{\mathbb{F}_\ell} = \dim \mathrm{GSp}_{2g,\mathbb{F}_\ell} - 2$ and dividing by

$$\frac{\#\,\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})}{\ell^k\varphi(\ell^k)} = \frac{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_\ell)}{\ell\varphi(\ell)}\ell^{(k-1)\dim X_{\mathbb{F}_\ell}},$$

we obtain that (21) is $1 + O(\ell^{-2})$. The claim follows upon passing to the limit in k. □

Theorem 4.8. *Let q be a prime power and $t \in \mathbb{Z}$. The infinite product*

$$\nu(q,t) = \nu_\infty(q,t)\prod_{\ell<\infty}\nu_\ell(q,t)$$

converges.

Proof. By Lemma 4.7 we have $\nu_\ell(q,t) = 1 + O(\ell^{-2})$ as ℓ ranges over primes $\ell \geq 3$ that do not divide q. The factors $\nu_\infty(q,t)$, $\nu_2(q,t)$ and $\nu_p(q,t)$ are well-defined, as already argued. It follows that the infinite product $\prod_{\ell<\infty}\nu_\ell(q,t)$ converges. □

We conclude this section by proving that $\nu(q,t)$ is strictly positive for $t \in \mathbb{Z}$ lying in the interval $(-2g\sqrt{q}, 2g\sqrt{q})$. This also proves that the denominator in Equation (9) is non-zero and that $\nu'(q,t)$ is strictly positive for $t \in \mathbb{Z}$ lying in the interval $(-2g\sqrt{q}, 2g\sqrt{q})$.

Lemma 4.9. *Let t be an integer in the open interval $(-2g\sqrt{q}, 2g\sqrt{q})$. The quantity $\nu(q,t)$ is non-zero (hence strictly positive).*

Proof. Since the infinite product defining $\nu(q,t)$ converges, it suffices to show that each factor in this product is non-zero. This is well-known to be true for the infinite factor $\nu_\infty(q,t)$, whose support is the interval $[-2g\sqrt{q}, 2g\sqrt{q}]$. To show that $\nu_\ell(q,t)$ is non-zero (including for $\ell = p$) we proceed as follows. We rewrite the definition of $\nu_\ell(q,t)$ in the form of Remark 3.6,

$$\nu_\ell(q,t) = \lim_{k\to\infty} \frac{\#\left(\mathrm{Im}\left\{\tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) \cap \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \text{ with } \begin{array}{c}\mathrm{tr}(\tilde{M}) = t, \\ \mathrm{mult}(\tilde{M}) = q\end{array}\right\} \to \mathrm{Mat}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})\right)}{\#\left(\mathrm{Im}\left\{\tilde{M} \in \mathrm{GSp}_{2g}(\mathbb{Q}_\ell) \cap \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \text{ with } \mathrm{mult}(\tilde{M}) = q\right\} \to \mathrm{Mat}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})\right)/\ell^k}.$$

Set $d := \dim \mathrm{GSp}_{2g,\mathbb{Q}_\ell} - 2 = 2g^2 + g - 1$ and multiply both numerator and denominator by ℓ^{-kd}. Let X_t^q be as in Definition 4.3 (for the ring $R = \mathbb{Q}_\ell$) and let for simplicity $X^q := \mathrm{GSp}_{2g,\mathbb{Q}_\ell}^{\mathrm{mult}=q}$. We see both X^q and

X_t^q as subschemes of $\mathbb{A}^{(2g)^2}_{\mathbb{Q}_\ell}$, so that their $\mathbb{Q}_\ell$-points are subsets of $\mathbb{Q}_\ell^{(2g)^2}$. Let $Y_t^q := X_t^q(\mathbb{Q}_\ell) \cap \mathbb{Z}_\ell^{(2g)^2}$ and $Y^q := X^q(\mathbb{Q}_\ell) \cap \mathbb{Z}_\ell^{(2g)^2}$. The sets Y_t^q and Y^q are closed analytic subsets of $\mathbb{Z}_\ell^{(2g)^2}$. Note that X^q is smooth and irreducible of dimension $d+1$, hence X_t^q – which is a subscheme of X^q defined by a single non-trivial equation – has dimension d: slicing with a hyperplane makes the dimension drop at most by 1; on the other hand, the dimension *must* drop (if X_t^q had a component of dimension $d+1$, by the irreducibility of X^q we would have $X_t^q \supseteq X^q$, which is not the case). More precisely, by the same argument, every irreducible component of X_t^q has dimension d. We can thus write

$$\nu_\ell(q,t) = \lim_{k\to\infty} \frac{\ell^{-dk} \# \operatorname{im}(Y_t^q \to (\mathbb{Z}/\ell^k\mathbb{Z})^{(2g)^2})}{\ell^{-(d+1)k} \# \operatorname{im}(Y^q \to (\mathbb{Z}/\ell^k\mathbb{Z})^{(2g)^2})}. \tag{22}$$

Recall from [Oes82, §2] the notion of *measure in dimension d* of a closed analytic subset Y of $\mathbb{Z}_\ell^{(2g)^2}$ of dimension $\leq d$ (denoted by $\mu_d(Y)$). By [Oes82, Théorème 2], the numerator and denominator of (22) admit limit as $k \to \infty$, and these limits are given by $\mu_d(Y_t^q)$ and $\mu_{d+1}(Y^q)$, respectively. Hence,

$$\nu_\ell(q,t) = \frac{\mu_d(Y_t^q)}{\mu_{d+1}(Y^q)}.$$

To conclude, it suffices to show that $\mu_{d+1}(Y^q)$ and $\mu_d(Y_t^q)$ are both strictly positive; by definition, this is equivalent to the fact that Y^q intersects the open locus $(X^q)^{d+1}_{\text{smooth}}$ of smooth points x of $X^q(\mathbb{Q}_\ell)$ such that $\dim_x(X^q) = d+1$ (resp. Y_t^q intersects $(X_t^q)^d_{\text{smooth}}$). Note that Y^q is open in $X^q(\mathbb{Q}_\ell)$ for the ℓ-adic topology, since it is the intersection of $X^q(\mathbb{Q}_\ell)$ with the ℓ-adically open set $(\mathbb{Z}_\ell)^{(2g)^2}$; a similar comment applies to X_t^q. Since X^q, X_t^q are of pure dimensions $d+1, d$ respectively, we are reduced to checking that Y^q, Y_t^q contain smooth points of X^q, X_t^q respectively.

For X^q, which is smooth, this amounts to constructing a symplectic matrix with coefficients in $\mathbb{Z}_\ell$ and given multiplier; this follows immediately from either Proposition 6.3 and Remark 6.5 or from Remark 4.2 after observing that the identity matrix lies in $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$. For X_t^q we construct the relevant point explicitly.

We observe that X_t^q arises as a fibre of the trace map:

$$\text{trace} : X^q \to \mathbb{A}^1$$

i.e., $X_t^q = \text{trace}^{-1}(t)$. A sufficient condition for a point $P \in X_t^q$ to be smooth is the existence of a curve $C \subseteq X^q$ containing P such that the restriction of the trace map

$$\text{trace} : C \to \mathbb{A}^1$$

has non-vanishing differential at P. To see this, notice that the dimension of the tangent space at P in X_t^q is the dimension of the tangent space at P in X^q minus the dimension of the image of the differential of the trace map (restricted to X^q) at P. Let us fix the symplectic form

$$\Omega = \begin{pmatrix} 0 & \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix}.$$

We consider the curve M_a, parametrised by $a \in \mathbb{A}^1$, given by

$$M_a = \begin{bmatrix} a & z & a-q & z \\ {}^t z & q\,\mathrm{Id}_{g-1} & {}^t z & 0_{g-1} \\ 1 & z & 1 & z \\ {}^t z & 0_{g-1} & {}^t z & \mathrm{Id}_{g-1} \end{bmatrix}$$

where z is the $1 \times (g-1)$ vector $(0, \ldots, 0)$. One checks that $M_a \in X^q(\mathbb{Q}_\ell)$: up to a suitable change of basis, the symplectic form is represented by $\operatorname{diag}\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\right)$, and in the same basis M_a becomes the matrix $\operatorname{diag}\left(\begin{pmatrix} a & a-q \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}\right)$, which is manifestly symplectic since every 2×2 block has determinant q. Moreover, $\text{trace}(M_a) = a + qg - q + g$; the composition

$$a \to M_a \to \text{trace}(M_a) = a + qg - q + g$$

is just a translation of $\mathbb{A}^1$, which implies that the differential of the trace map at M_a is surjective. Therefore, the point $M_{t-qg+q-g} \in X_t^q$ is smooth and its entries are elements of $\mathbb{Z}_\ell$. This concludes the proof.

□

5 Proof of Theorem 1.4

The goal of this section is to show that the set $\mathcal{P}_g(\mathbb{F}_q)$ of Definition 1.2 spans a $\mathbb{Q}$-vector space of dimension $g+1$ for all pairs (g,q). For a fixed genus g and $q \gg_g 1$, this follows from Theorem 2.1 (see Remark 2.9). Studying more precisely the set $\mathcal{P}_{g,2}(\mathbb{F}_q)$ for every fixed value of q, we prove the statement for all q and g. Recall that $\mathcal{P}_g(\mathbb{F}_q)$ is defined in Definition 1.2 and $\mathcal{P}_{g,2}(\mathbb{F}_q)$ is its reduction modulo 2. As we pointed out in the introduction, we split our proof of Theorem 1.4 into two parts, one for the case p odd and one for the case $p=2$, since the properties of the 2-torsion points are slightly different when the characteristic is odd or even.

5.1 Proof of Theorem 1.4: p odd

Throughout this section, the prime $p = \mathrm{char}(\mathbb{F}_q)$ is assumed to be odd. Thanks to Theorem 1.7, it makes sense to define $f_C(t) \in \mathbb{Z}[t]$ as $f_{C,\ell^\infty}(t)$, where ℓ is any prime different from p; from now on, we shall choose $\ell = 2$. This choice has the additional advantage that working modulo 2 makes the connection between the L-polynomial and the characteristic polynomial of Frobenius particularly simple:

Corollary 5.1. *We have $P_C(t) \equiv f_C(t) \pmod 2$.*

Proof. Write $P_C(t) = \sum_{i=0}^{2g} a_i t^i \in \mathbb{Z}[t]$ and $f_C(t) = \sum_{i=0}^{2g} b_i t^i$. By Theorem 1.7 we have the equality $b_i = a_{2g-i}$, and since q is odd we also have

$$b_i = a_{2g-i} = q^{g-i} a_i \equiv a_i \pmod 2.$$

□

We now recall a concrete description for the vector space of 2-torsion points of a hyperelliptic Jacobian, at least in the case when the hyperelliptic model is given by a polynomial of odd degree. Let $f(x) \in \mathbb{F}_q[x]$ be a separable polynomial of degree $2g+1$ and let $C/\mathbb{F}_q$ be the unique smooth projective curve birational to the affine curve $y^2 = f(x)$. Furthermore, let $J/\mathbb{F}_q$ be the Jacobian of C and $\{\alpha_1, \dots, \alpha_{2g+1}\}$ be the set of roots of $f(x)$ in $\overline{\mathbb{F}_q}$. Then for $i = 1, \dots, 2g+1$ we have a point $(\alpha_i, 0) \in C(\overline{\mathbb{F}_q})$; also notice that C, being given by an odd-degree model, has a unique point at infinity, which we denote by ∞. We denote by $R_i = [(\alpha_i, 0) - \infty]$ the classes of the divisors $Q_i = (\alpha_i, 0) - \infty$ in $J(\overline{\mathbb{F}_q})$. We then have the following well-known description for the 2-torsion of J (see for example [Gro12, Section 4]):

Lemma 5.2. *The following hold:*

1. *Each of the divisor classes $R_i \in J(\overline{\mathbb{F}_q})$ represents a point of order 2.*
2. *The classes R_i span $J[2]$.*
3. *The only linear relation satisfied by the R_i is $R_1 + \cdots + R_{2g+1} = 0$.*

We can now compute the action of Frobenius on the 2-torsion points of C:

Lemma 5.3. *With notation as above, write $f(x) = \prod_{i=1}^r f_i(x)$ for the factorisation of $f(x)$ as a product of irreducible polynomials in $\mathbb{F}_q[x]$, and let $d_i = \deg(f_i)$. Let $\rho_2 : \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{Aut}_{\mathbb{F}_2}(J[2])$ be the Galois representation attached to the 2-torsion points of J. Then*

$$f_{C,2}(t) = \det(t\,\mathrm{Id} - \rho_2(\mathrm{Frob})) = (t-1)^{-1} \prod_{i=1}^r (t^{d_i} - 1) \in \mathbb{F}_2[t].$$

Proof. As above, let ∞ be the unique point at infinity of C, and for $i = 1, \dots, 2g+1$ let $Q_i = (\alpha_i, 0) - \infty \in \mathrm{Div}_C(\overline{\mathbb{F}_q})$. Write P_i for the image of Q_i in the $\mathbb{F}_2$-vector space $\mathrm{Div}_C(\overline{\mathbb{F}_q}) \otimes \mathbb{F}_2$, and let V be the $(2g+1)$-dimensional $\mathbb{F}_2$-vector subspace of $\mathrm{Div}_C(\overline{\mathbb{F}_q}) \otimes \mathbb{F}_2$ spanned by the P_i. There is a natural action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on V, which we consider as a representation $\rho : \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{GL}(V)$. By Galois theory,

it is clear that Frob acts on the set $\{\alpha_i\}_{i=1}^{2g+1}$ with r orbits, one corresponding to each irreducible factor of $f(x)$. The lengths of the orbits are given by the degrees d_i of the factors $f_i(x)$. This means that, in the natural basis of V given by the P_i, the action of Frobenius is given by a permutation matrix corresponding to a permutation of cycle type

$$(d_1, d_2, \ldots, d_r).$$

It follows immediately that the characteristic polynomial of $\rho(\text{Frob})$ is

$$\det(t\,\mathrm{Id} - \rho(\text{Frob})) = (t^{d_1} - 1)\cdots(t^{d_r} - 1) \in \mathbb{F}_2[t].$$

On the other hand, by Lemma 5.2 there is a Galois-equivariant exact sequence

$$0 \to \mathbb{F}_2 \to V \to J[2] \to 0,$$

where the first map is given by $1 \to P_1 + P_2 + \ldots P_{2g+1}$ and the action of Frob on the sum $P_1 + \cdots + P_{2g+1}$ is trivial. This implies that

$$\det(t\,\mathrm{Id} - \rho(\text{Frob})) = \det(t\,\mathrm{Id} - \rho_2(\text{Frob}))(t-1),$$

which, combined with our previous determination of the characteristic polynomial of $\rho(\text{Frob})$, concludes the proof. □

Thanks to the previous lemma, it is easy to obtain the reduction modulo 2 of the L-polynomial of any given hyperelliptic curve with an odd degree model. In the next corollary, we use this to produce curves whose L-polynomials have particularly simple reductions modulo 2.

Corollary 5.4. *Let $f_0(x) = 1$ and, for $d = 1, \ldots, 2g+1$, let $f_d(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree d. Further set $f_0(x) = 1$. For $d = 0, \ldots, g$ consider the unique smooth projective curve C_d birational to the affine curve*

$$y^2 = f_d(x) f_{2g+1-d}(x).$$

For $d = 1, \ldots, g$ we have the congruence

$$(t-1)P_{C_d}(t) \equiv (t^d - 1)(t^{2g+1-d} - 1) \equiv t^{2g+1} + t^{2g+1-d} + t^d + 1 \pmod 2,$$

while for $d = 0$ we have

$$(t-1)P_{C_0}(t) \equiv t^{2g+1} - 1 \equiv t^{2g+1} + 1 \pmod 2.$$

Proof. This is a direct application of Lemma 5.3, combined with the fact that by Corollary 5.1 we have $P_C(t) \equiv f_C(t) \pmod 2$. □

Proof of Theorem 1.4 for p odd. The inequality $\dim_{\mathbb{Q}} L_g(\mathbb{F}_q) \leq g+1$ follows immediately from the symmetry relation $a_{g+i} = q^i a_{g-i}$ satisfied by the coefficients of the L-polynomials; it thus suffices to establish the lower bound $\dim_{\mathbb{Q}} L_g(\mathbb{F}_q) \geq g+1$.

Consider the $g+1$ curves $C_0, \ldots, C_g$ of Corollary 5.4 (any choice of the irreducible polynomials $f_d(x)$ will work) and the corresponding L-polynomials $P_{C_0}(t), \ldots, P_{C_g}(t)$. Let $M \subseteq \mathbb{Z}[t]$ be the $\mathbb{Z}$-module generated by these polynomials; it is clear that in order to prove the theorem it suffices to show that $\operatorname{rank}_{\mathbb{Z}} M \geq g+1$. Notice that $M \otimes \mathbb{F}_2$ is in a natural way a vector subspace of $\mathbb{F}_2[t]$, and that

$$\operatorname{rank}_{\mathbb{Z}} M \geq \dim_{\mathbb{F}_2}(M \otimes \mathbb{F}_2).$$

Let $N \subset \mathbb{F}_2[t]$ be the image of the linear map

$$\begin{array}{ccc} M \otimes \mathbb{F}_2 & \to & \mathbb{F}_2[t] \\ q(t) & \mapsto & (t-1)q(t). \end{array}$$

The $\mathbb{F}_2$-vector space N is generated by the $g+1$ polynomials $(t-1)P_{C_i}(t)$ for $i = 0, \ldots, g$, hence, by Corollary 5.4, by the $g+1$ polynomials

$$t^{2g+1} + 1 \quad \text{and} \quad t^{2g+1} + t^{2g+1-i} + t^i + 1 \text{ for } i = 1, \ldots, g.$$

It is immediate to check that these $g+1$ polynomials are $\mathbb{F}_2$-linearly independent, which implies

$$\operatorname{rank}_{\mathbb{Z}} M \geq \dim_{\mathbb{F}_2}(M \otimes \mathbb{F}_2) = \dim_{\mathbb{F}_2} N = g+1.$$

□

5.2 Proof of Theorem 1.4: $p = 2$

We now give the proof of Theorem 1.4 in the case $p = 2$. As in the case of odd characteristic, we will exhibit $g + 1$ curves whose L-polynomials form a basis of $L_g(\mathbb{F}_q)$. Recall from Definition 1.2 the set $\mathcal{P}_g(\mathbb{F}_q)$.

Proof of Theorem 1.4 for $p = 2$. Fix $0 \leq r \leq g$. Let $h(x) \in \mathbb{F}_q[x]$ be a separable polynomial of degree r such that $h(0) \neq 0$. Such a polynomial exists: for $r = 0, 1$ we may take $h(x) = 1$ or $h(x) = x + 1$, respectively, and for $r \geq 2$ it suffices to take as $h(x)$ the minimal polynomial of any element that generates $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.

Consider the affine curve defined by the equation $y^2 + yh(x) = x^{2g+1-r}h(x)$. We claim that this curve is smooth. Indeed, an $\overline{\mathbb{F}_q}$-point (x_0, y_0) on the curve is singular if and only if

$$\begin{cases} y_0^2 + y_0 h(x_0) = x_0^{2g+1-r} h(x_0) \\ h(x_0) = 0 \\ y_0 h'(x_0) = (2g + 1 - r)x_0^{2g-r} h(x_0) + x_0^{2g+1-r} h'(x_0) \end{cases}$$

Here the second and third equations are given by the vanishing of the partial derivatives in y and x of the defining equation, respectively. By the second equation, x_0 is a root of h. So, by the first one, $y_0 = 0$. Hence, the third equation becomes $x_0^{2g+1-r} h'(x_0) = 0$: but $x_0 \neq 0$ since $h(0) \neq 0$, and $h'(x_0) \neq 0$ since h is separable, so the above system has no solutions. Let $C/\mathbb{F}_q$ be the smooth projective curve given by the completion of the curve above. The curve C has genus g, because the degree of $x^{2g+1-r}h(x)$ is $2g+1$ and the degree of $h(x)$ is at most g. In particular, $P_C(t)$ is an element of $\mathcal{P}_g(\mathbb{F}_q)$. We will show that the reduction of $P_C(t)$ modulo 2 has degree r.

Let ℓ be an odd prime and let $T_\ell J$ be the ℓ-adic Tate module of the Jacobian J of C. Let $f_{C,\ell^\infty}(t) := \det(t\,\mathrm{Id} - \rho_{\ell^\infty}(\mathrm{Frob}) \mid T_\ell J)$. If $\alpha \in \overline{\mathbb{F}_q}$ is a root of $f_{C,\ell^\infty}(t)$ with multiplicity d, then q/α is a root of $f_{C,\ell^\infty}(t)$ with multiplicity d. Hence, we can write $f_{C,\ell^\infty}(t) = t^g Q_C(t + q/t)$ with $Q_C(t) \in \mathbb{Z}[t]$ of degree g. Let r_2 be the 2-rank of J, as defined in [Gon98, Section 1]. By [Gon98, Proposition 3.1], r_2 is equal to the sum of the multiplicities of the non-zero roots of $Q_C(t)$ modulo 2. Hence,

$$Q_C(t) \equiv t^{g-r_2} \tilde{Q}_C(t) \pmod 2$$

with $\tilde{Q}_C(t) \in \mathbb{F}_2[t]$ a polynomial of degree r_2 such that $\tilde{Q}_C(0) \neq 0$ (in $\mathbb{F}_2$). In [CST14, Proof of Theorem 23], the authors show that the 2-rank of J is equal to one less than the number of distinct projective points where $H_1(X, Z) := h(X/Z)Z^{g+1}$ vanishes (see also [EP13]). In our case, since $h(x)$ is separable, this implies $r_2 = \deg h(x) = r$. Hence, we have

$$Q_C(t) \equiv t^{g-r} \tilde{Q}_C(t) \pmod 2$$

with $\tilde{Q}_C(t)$ of degree r. As q is a power of 2, we obtain

$$f_{C,\ell^\infty}(t) \equiv t^g Q_C\left(t + \frac{q}{t}\right) \equiv t^g Q_C\left(t\right) \equiv t^{2g-r} \tilde{Q}_C(t) \pmod 2.$$

By Theorem 1.7,

$$P_C(t) \equiv t^{2g} f_{C,\ell^\infty}\left(t^{-1}\right) \equiv t^{2g} t^{-2g+r} \tilde{Q}_C\left(t^{-1}\right) \equiv t^r \tilde{Q}_C\left(t^{-1}\right) \pmod 2. \tag{23}$$

Since $\tilde{Q}_C(0) \not\equiv 0 \pmod 2$ we see that the reduction of $P_C(t)$ modulo 2 has degree r.

So, for each $0 \leq r \leq g$, we can find a smooth hyperelliptic curve C_r of genus g such that $P_{C_r}(t)$ modulo 2 has degree r. Therefore, the polynomials $\{P_{C_r}(t) \mid 0 \leq r \leq g\}$ are linearly independent modulo 2. The result follows as in the proof of Theorem 1.4.

□

Remark 5.5. The polynomial $f_{C,\ell^\infty}(t)$ is monic by definition, which implies that also $Q_C(t)$ and $\tilde{Q}_C(t)$ are monic. By (23), the constant term of $P_C(t)$ modulo 2 is 1. Hence,

$$P_{C_r}(t) \equiv t^r + 1 + \sum_{i=1}^{r-1} a_{i,r} t^i \pmod 2.$$

In fact, one can show that $P_{C_r}(t) \equiv t^r + 1 \pmod 2$. To see this, recall from [DK69, Theorem 3.1] that, for a smooth projective curve $C/\mathbb{F}_q$, with $q = 2^f$, one has

$$P_C(t) \equiv \det\left(1 - t\varphi_q^{-1} \mid H^1_{\text{ét}}\left(C_{\overline{\mathbb{F}_q}}, \mathbb{Z}/2\mathbb{Z}\right)\right) \pmod 2,$$

where $\varphi_q : \mathbb{F}_q \to \mathbb{F}_q$ is the Frobenius automorphism $x \mapsto x^q$. Next, recall that $H^1_{\text{ét}}\left(C_{\overline{\mathbb{F}_q}}, \mathbb{Z}/2\mathbb{Z}\right)$ is canonically dual to $J(\overline{\mathbb{F}_q})[2]$, so that we may compute $P_C(t)$ as the inverse characteristic polynomial of Frobenius acting on $J[2]$. For the curve C_r, the explicit description of $J[2]$ given in [CST14, Proof of Theorem 23] shows that the action of φ_q on $J[2]$ is the natural Galois action on the roots of $h(x)$, that is, an r-cycle. It follows that the characteristic polynomial in question is $P_C(t) \equiv t^r - 1 \pmod 2$, as claimed.

6 Algebraic independence

Theorem 1.4 asserts that Lemma 1.1 captures all the linear relations among the coefficients of the polynomials $P_C(t)$. In this section, we prove an analogous result that deals with higher-order polynomial relations on the coefficients. Lemma 1.1 already gives a number of constraints: for $P_C(t) = \sum_{i=0}^{2g} a_i t^i$ we have $a_0 = 1$ and $a_{g+i} = q^i a_{g-i}$ for every $i = 0, \dots, g$; it is therefore natural to restrict our analysis to $a_1, \dots, a_g$. The following is the main result of this section:

Theorem 6.1. *Let g, d be positive integers. There is a constant $e_{g,d}$ such that for any prime power $q > e_{g,d}$ and for any non-zero polynomial $f(x_1, \dots, x_g) \in \mathbb{Z}[x_1, \dots, x_g]$ of degree $\leq d$ in each variable there is a curve $C \in \mathcal{M}_g(\mathbb{F}_q)$ with L-polynomial $P_C(t) = \sum_{i=0}^{2g} a_i t^i$ such that $f(a_1, \dots, a_g) \neq 0$.*

Notice that, unlike Theorem 1.4, $e_{g,d}$ cannot be equal to 0 for all g and d, since for fixed q and g we can always find a polynomial $f(x_1, \dots, x_g)$ (that may depend on q) which vanishes on all the finitely many values of $(a_1, \dots, a_g)$.

As is the case for Theorem 1.4, the proof of Theorem 6.1 exploits the reduction of $f(x_1, \dots, x_g)$ modulo a positive integer N. In this case, instead of a direct computation of the action of the Frobenius on the N-torsion points, we use Theorem 2.1, which guarantees that, for q large enough, all the characteristic polynomials of the matrices in $\mathrm{GSp}_{2g}^q(\mathbb{Z}/N\mathbb{Z})$ come from some element of $\mathcal{P}_{g,N}(\mathbb{F}_q)$.

To be more precise, for a $C \in \mathcal{M}_g(\mathbb{F}_q)$ and $P_C(t) \in \mathbb{Z}[t]$ its L-polynomial, let $f_C(t) = t^{2g} P_C(1/t)$ be its reciprocal polynomial. By Theorem 1.7 $f_C(t)$ is equal to the characteristic polynomial of the action of the Frobenius of C (modulo every ℓ). Theorem 2.1 implies that, for q large enough (in terms of N) and for any $M \in \mathrm{GSp}_{2g}^q(\mathbb{Z}/N\mathbb{Z})$, the characteristic polynomial of M is equal to the reduction of $f_C(t)$ modulo N for some $C \in \mathcal{M}_g(\mathbb{F}_q)$.

We then prove that there are too many characteristic polynomials of elements of $\mathrm{GSp}_{2g}^q(\mathbb{Z}/N\mathbb{Z})$ for their coefficients to lie in the zero locus of some $f(x_1, \dots, x_g)$ of fixed degree. We are free to choose N, and we will always take it to be an odd prime number. We set $N = r$ and use the letter r to avoid confusion.

The following lemma is a version of the well-known Schwartz-Zippel bound. Notice that a polynomial in g variables having degree at most d in each of them has total degree at most dg.

Lemma 6.2. *Let g, d be natural numbers with $g \geq 1$, let r be a prime number and let $f(x_1, \dots, x_g) \in \mathbb{F}_r[x_1, \dots, x_g]$ be a non-zero polynomial of degree $\leq d$ in each variable. We have*

$$\#\{(u_1, \dots, u_g) \in \mathbb{F}_r^g \mid f(u_1, \dots, u_g) = 0\} \leq dg \cdot r^{g-1}.$$

Next, we identify the set of characteristic polynomials of matrices in $\mathrm{GSp}_{2g}^q(\mathbb{F}_r)$. We show the following more general result:

Proposition 6.3. *Let n be a positive integer, let R be a commutative ring with 1, and let $q \in R^\times$. Let $p(x) = a_0 + a_1 x + \cdots + a_{2n} x^{2n} \in R[x]$ be a monic polynomial satisfying $a_{n-i} = q^i a_{n+i}$ for all $i = 0, \dots, n$. There exists $M \in \mathrm{GSp}_{2n}(R)$ with multiplier q and characteristic polynomial $p(x)$.*

Remark 6.4. The statement is a simple variant of [Riv08, Theorem A.1]. We give a detailed argument since, unfortunately, the proof of [Riv08, Theorem A.1] seems to contain some typos. For example, in op. cit. the matrix B is declared to have determinant 1, but the construction does not ensure this property; more importantly, in some examples we tried, the given construction does not seem to yield

matrices with the claimed characteristic polynomials. Our construction is therefore slightly different from that of [Riv08, Theorem A.1], which we could not fully understand.

Proof. We work with the symplectic form given by the matrix $J = \begin{pmatrix} 0 & \mathrm{Id}_n \\ -\mathrm{Id}_n & 0 \end{pmatrix}$. We construct the desired M as a block-matrix $M = \begin{pmatrix} 0 & B \\ C & D \end{pmatrix}$, where B, C, D satisfy the following:

1. B, C, D are square $n \times n$ matrices with B invertible;
2. B is the symmetric matrix

$$B = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & b_2 \\ 0 & 0 & 0 & \cdots & b_2 & b_3 \\ & & & \iddots & & \\ 0 & 1 & b_2 & \cdots & b_{n-2} & b_{n-1} \\ 1 & b_2 & b_3 & \cdots & b_{n-1} & b_n \end{pmatrix},$$

   or, in symbols,

$$B_{ij} = b_{i+j-n}\delta_{i+j\geq n+1} = \begin{cases} 0, \text{ if } i+j \leq n \\ 1, \text{ if } i+j = n+1 \\ b_{i+j-n}, \text{ if } i+j > n+1, \end{cases}$$

   where we have set $b_1 = 1$ and $\delta_{i+j\geq n+1} = \begin{cases} 1, \text{ if } i+j \geq n+1 \\ 0, \text{ otherwise.} \end{cases}$. Note that any matrix B of this form is invertible for any choice of the b_i;
3. $C = -q({}^tB)^{-1} = -qB^{-1}$;
4. D is the companion matrix given by $D = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & d_1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & d_2 \\ & & & \ddots & & & \\ 0 & 0 & 0 & \cdots & 0 & 0 & d_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & 0 & d_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix}$. In symbols,

$$D_{ij} = \begin{cases} 1, \text{ if } i = j+1 \\ d_i, \text{ if } j = n \\ 0, \text{ otherwise.} \end{cases}$$

Here $b_2, \ldots, b_n \in R$ and $d_1, \ldots, d_n \in R$ are coefficients to be chosen later. We check the conditions for the matrix M to be symplectic with multiplier q. We compute

$${}^tMJM = \begin{pmatrix} 0 & -{}^tCB \\ {}^tBC & {}^tBD - {}^tDB \end{pmatrix},$$

which is equal to qJ if and only if

$$\begin{cases} -{}^tCB = q\,\mathrm{Id} \\ {}^tBC = -q\,\mathrm{Id} \\ {}^tBD - {}^tDB = 0. \end{cases}$$

The first two equations are equivalent to one another and automatically satisfied by our choice of C. The third equation is equivalent to the matrix ${}^tBD = BD$ being symmetric. We claim that this is achieved by taking ($b_1 = 1$ and) $b_{k+1} = \sum_{i=1}^{k} b_i d_{n+i-k}$ for $k = 1, \ldots, n-1$ (notice that d_1 does not occur). Indeed, the first $n-1$ columns of the product BD are given by the second, third, ..., n-th column of B, while the last one is the linear combination $d_1B^1 + d_2B^2 + \cdots + d_nB^n$, where we denote by B^i the i-th column of B. From this, it is immediate to check that the top-left block of BD of size $(n-1)\times(n-1)$ is symmetric (independently of the values of $b_2, \ldots, b_n, d_1, \ldots, d_n$), and we only need to impose that the last line of

BD is equal to (the transpose of) its last column. We can also ignore the coefficient in position (n,n), so we compare the first $n-1$ coefficients of the last line of BD with the first $n-1$ coefficients of its last column. The k-th coefficient on the last line is the coefficient on the last line of the $(k+1)$-th column of B, that is, b_{k+1}. The k-th coefficient on the last column is given by

$$d_1B_{k1} + d_2B_{k2} + \cdots + d_nB_{kn} = \sum_{i=1}^{n} d_iB_{ki} = \sum_{i=1}^{n} d_i\delta_{k+i\geq n+1}b_{k+i-n} = \sum_{i'=1}^{k} b_{i'}d_{i'+n-k}.$$

Thus, the symmetry condition is satisfied if and only if for $k = 1, \ldots, n-1$ we have $b_{k+1} = \sum_{i=1}^{k} b_i d_{n+i-k}$, as claimed. Also note that a symplectic matrix with invertible multiplier is itself invertible (because the determinant of a symplectic matrix is a power of its multiplier), so M is invertible and therefore an element of $\mathrm{GSp}_{2n}(R)$. In particular, for any choice of $d_1, \ldots, d_n$, we have constructed a corresponding matrix M that is symplectic of multiplier q and has D as its bottom-right block of size $n \times n$. We now compute the characteristic polynomial of this matrix M. Consider the identity

$$\begin{aligned}\begin{pmatrix} x\,\mathrm{Id}_n & -B \\ -C & x\,\mathrm{Id}_n - D \end{pmatrix}\begin{pmatrix} B & 0 \\ x\,\mathrm{Id}_n & B^{-1} \end{pmatrix} &= \begin{pmatrix} 0 & -\mathrm{Id}_n \\ x^2\,\mathrm{Id}_n - xD - CB & xB^{-1} - DB^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 0 & -\mathrm{Id}_n \\ (x^2+q)\,\mathrm{Id}_n - xD & xB^{-1} - DB^{-1} \end{pmatrix},\end{aligned}$$

where we have used that – by definition – $CB = -q\,\mathrm{Id}$. Taking determinants on both sides and using that the determinant of the block-matrix $\begin{pmatrix} B & 0 \\ x\,\mathrm{Id} & B^{-1} \end{pmatrix}$ is 1, we obtain

$$\det(x\,\mathrm{Id}_{2n} - M) = \det\begin{pmatrix} 0 & -\mathrm{Id}_n \\ (x^2+q)\,\mathrm{Id}_n - xD & xB^{-1} - DB^{-1} \end{pmatrix} = \det((x^2+q)\,\mathrm{Id}_n - xD),$$

where the last equality uses basic properties of the determinant of block matrices. Finally, we can rewrite this in the form

$$\det(x\,\mathrm{Id}_{2n} - M) = x^n \det\left(\left(x + \frac{q}{x}\right)\mathrm{Id}_n - D\right),$$

so the characteristic polynomial of M is equal to $x^n p_D\left(x + \frac{q}{x}\right)$, where $p_D(x)$ is the characteristic polynomial of D.

To conclude the proof, it suffices to show that we can choose D in such a way that $x^n p_D\left(x + \frac{q}{x}\right) = p(x)$, where $p(x)$ is the polynomial given in the statement. This is easy: D is a companion matrix, so any monic polynomial with coefficients in R can be realised as $p_D(x)$ for suitable values of $d_1, \ldots, d_n$. Finally, it is an easy exercise to show that a monic polynomial $p(x) = \sum_{i=0}^{2n} a_i x^i$ that satisfies $a_{n-i} = q^i a_{n+i}$ for all $i = 0, \ldots, n$ can be written as $x^n p_1\left(x + \frac{q}{x}\right)$ for some monic polynomial $p_1 \in R[x]$ of degree n. □

Remark 6.5. Inspection of the proof shows that the following slightly stronger statement is true for the case of R being the fraction field of a domain A: if the characteristic polynomial $p(x)$ has coefficients in A and $q \in A$, then we may choose M to have coefficients in A, *even if the multiplier q is not invertible in A*. This applies in particular when $A = \mathbb{Z}_\ell$ and $R = \mathbb{Q}_\ell$.

Corollary 6.6. *Let r be a prime and let q be an integer prime to r. The set* $\{\mathrm{charpol}\, M : M \in \mathrm{GSp}_{2g}^q(\mathbb{F}_r)\}$ *has cardinality r^g.*

Proof. By Proposition 6.3, the set in question is the set of all monic polynomials in $\mathbb{F}_r[x]$ of degree $2g$ whose coefficients a_i satisfy $a_{g-i} = q^i a_{g+i}$ for all $i = 0, \ldots, g$. Since any choice of the coefficients $a_1, \ldots, a_g$ corresponds to precisely one such polynomial, the total number of polynomials is r^g. □

Finally, we connect characteristic polynomials of matrices in $\mathrm{GSp}_{2g}^q(\mathbb{F}_r)$ with characteristic polynomials of Frobenius:

Lemma 6.7. *Let g, r be positive integers. There is a constant $h_{g,r}$ such that for any prime power $q > h_{g,r}$ with $(q,r) = 1$ and for any element M of $\mathrm{GSp}_{2g}^q(\mathbb{Z}/r\mathbb{Z})$, there is a curve $C \in \mathcal{M}_g(\mathbb{F}_q)$ such that the reduction of $f_C(t)$ modulo r is the characteristic polynomial of M.*

Proof. For $g = 1$, this follows from the well-known fact that a polynomial of the form $t^2 + at + q$ is the characteristic polynomial of Frobenius of an elliptic curve over $\mathbb{F}_q$ if and only if a lies in the Hasse-Weil interval $[-2\sqrt{q}, 2\sqrt{q}]$ (in turn, this can be proved in many ways, including for example Honda-Tate theory). All residue classes modulo r are therefore realised as soon as the number of integers in the Hasse-Weil interval, that is $1 + 2\lfloor 2\sqrt{q} \rfloor$, is at least r.

For $g \geq 2$, the result follows from Theorem 2.1, as we now show. Let $p(t)$ be the characteristic polynomial of M. Notice that μ_r^q gives positive mass to the singleton $\{p(t)\}$, since $\mathrm{GSp}_{2g}^q(\mathbb{Z}/r\mathbb{Z})$ is a finite set. In fact, since the cardinality of $\mathrm{GSp}_{2g}^q(\mathbb{Z}/r\mathbb{Z})$ is independent of q (it is equal to $\#\,\mathrm{Sp}_{2g}(\mathbb{Z}/r\mathbb{Z})$, provided only that $(q, r) = 1$), we have $\mu_r^q\{p(t)\} \geq c_{g,r} > 0$ for some absolute constant $c_{g,r}$. By Theorem 2.1, this implies that $(\mathrm{charpol}_r)_* \mathbb{P}_{g,q}^{\mathrm{naive}}$ is positive at $\{p(t)\}$ for q large enough. Repeating the argument for the finitely many possible polynomials $p(t)$ concludes the proof. □

We can now combine our bounds to conclude the proof of Theorem 6.1.

Proof of Theorem 6.1. Let r be an odd prime number, which will later be required to be large enough. We prove the result for every q which is not a power of r; repeating the argument with a different r will prove the statement for every q.

First, we can assume that our polynomial $f(x_1, \dots, x_g) \in \mathbb{Z}[x_1, \dots, x_g]$ has a coefficient which is non-zero modulo r (otherwise, divide by an appropriate power of r). Hence, its reduction modulo r is non-zero.

By Lemma 6.7, the set of characteristic polynomials of curves in $\mathcal{M}_g(\mathbb{F}_q)$ modulo r is the same as the set of characteristic polynomials of matrices of $\mathrm{GSp}_{2g}^q(\mathbb{F}_r)$ for q large enough and relatively prime with r. Suppose that for every $M \in \mathrm{GSp}_{2g}^q(\mathbb{F}_r)$, writing $\mathrm{charpol}(M) = \sum_{i=0}^{2g} a_i t^i$, we have $f(a_1, \dots, a_g) = 0$. By combining Lemma 6.2 and Corollary 6.6 we obtain

$$r^g \leq dg \cdot r^{g-1},$$

which implies $r \leq dg$. If r is chosen larger than this quantity, we obtain a contradiction. □

Acknowledgments. We thank Umberto Zannier for bringing the problem to our attention, for many useful suggestions and especially for pointing out the relevance of the equidistribution results of Katz-Sarnak, noting that they imply the case $q \gg_g 0$ of Theorem 1.4. In addition, the first author would like to thank Umberto Zannier for his guidance during his undergraduate studies, on a topic that ultimately inspired much of the work in this paper. We are grateful to J. Kaczorowski and A. Perelli for sharing their work [KP18] before publication. We thank Christophe Ritzenthaler and Elisa Lorenzo García for their interesting comments on the first version of this paper.

Funding. The second and third authors have been partially supported by MIUR grant PRIN 2017 "Geometric, algebraic and analytic methods in arithmetic" and MUR grant PRIN-2022HPSNCR (funded by the European Union project Next Generation EU), and by the University of Pisa through PRA 2018 and 2022 "Spazi di moduli, rappresentazioni e strutture combinatorie".

The third author has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 101034413.

A Appendix

The goal of this appendix is to prove that [BHLGR24, Conjecture 5.1] does not hold. Let q be a prime and $g \geq 3$ be a fixed integer. We will use the following notation: for every $\tau \in [-2g, 2g]$, we let $t = t(q, \tau)$ be the unique integer in the interval $(\sqrt{q}\tau - 1/2, \sqrt{q}\tau + 1/2]$. Recall from [BHLGR24, §5] the function

$$\mathcal{N}_{q,g}^{\mathrm{nhyp}}(\tau) := \frac{1}{\#\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q)} \sum_{\substack{C \in \mathcal{M}_g^{\mathrm{nhyp}\prime}(\mathbb{F}_q) \\ \tau(C) = \tau}} \frac{1}{\#\,\mathrm{Aut}(C)}.$$

Here by $\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q)$ we mean the set of $\overline{\mathbb{F}}_q$-isomorphism classes of non-hyperelliptic curves of genus g over $\mathbb{F}_q$, and by $\mathcal{M}_g^{\mathrm{nhyp}\prime}(\mathbb{F}_q)$ we mean the set of $\mathbb{F}_q$-isomorphism classes of such curves. Moreover, $\tau(C) = \mathrm{Tr}(C)/\sqrt{q}$ is the normalised trace of C.

Conjecture 5.1 in [BHLGR24] states that, for fixed $g, \tau \in [-2g, 2g]$ and $\varepsilon > 0$ we have

$$\left|\sqrt{q}\mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q}) - \mathrm{ST}_g(t/\sqrt{q})\right| < \varepsilon \tag{24}$$

for all q greater than some $q_0 = q_0(g, \tau, \varepsilon)$, where as before t is the unique integer in the interval $(\sqrt{q}\tau - 1/2, \sqrt{q}\tau + 1/2]$.

Remark A.1. Note that [BHLGR24, Conjecture 5.1] requires the existence of an integer t with $|\tau - \frac{t}{\sqrt{q}}| < \frac{1}{2\sqrt{q}}$. For fixed q, the strict inequality cannot be achieved in general: if $\tau = \frac{n+1/2}{\sqrt{q}}$, then both $t = n$ and $t = n+1$ give $|\tau - \frac{t}{\sqrt{q}}| = \frac{1}{2\sqrt{q}}$. On the other hand, for fixed τ, when q is a large enough prime there is a single integer t that satisfies this inequality, namely, the unique integer in the interval $(\sqrt{q}\tau - 1/2, \sqrt{q}\tau + 1/2]$.

The next lemma is simply a technical verification, and the reader is encouraged to skip its proof at first reading.

Lemma A.2. *[BHLGR24, Conjecture 5.1] implies the following statement: fix $g \geq 3$, $\tau \in [-2g, 2g]$ and $\varepsilon > 0$. There exists $q_0 = q_0(g, \tau, \varepsilon)$ such that the inequality*

$$\left|\mathrm{ST}_g(t/\sqrt{q}) - \sqrt{q}H'(q,t)\right| < \varepsilon$$

holds for all primes $q > q_0$, where t is the unique integer in the interval $(\sqrt{q}\tau - 1/2, \sqrt{q}\tau + 1/2]$.

Proof. Given that (24) holds for all large enough q by assumption, it suffices to show that

$$\left|\sqrt{q}\mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q}) - \sqrt{q}H'(q,t)\right|$$

tends to 0 as $q \to \infty$. We estimate the difference between $\mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q})$ and $H'(q,t)$. Corollary 2.6 gives

$$\sum_{\substack{C \in \mathcal{M}_g^{\mathrm{nhyp}\prime}(\mathbb{F}_q) \\ \tau(C) = t/\sqrt{q}}} \left|\frac{1}{\#\operatorname{Aut}(C)} - 1\right| = O_g(q^{-1/2}),$$

hence, dividing by $\#\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q) \gg q^{3g-3}$ (see Lemma 2.5) we get

$$\mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q}) = \frac{1}{\#\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q)} \sum_{\substack{C \in \mathcal{M}_g^{\mathrm{nhyp}\prime}(\mathbb{F}_q) \\ \tau(C) = t/\sqrt{q}}} 1 + O_g(q^{-1/2}q^{-3g+3}).$$

By Lemma 2.5 again we have

$$\sum_{\substack{C \in \mathcal{M}_g(\mathbb{F}_q) \setminus \mathcal{M}_g^{\mathrm{nhyp}\prime}(\mathbb{F}_q) \\ \tau(C) = t/\sqrt{q}}} 1 = O_g(q^{3g-3-1}),$$

so dividing by $\#\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q) \gg q^{3g-3}$ and using the above estimates we obtain

$$\begin{aligned} \mathcal{N}_{q,g}^{\mathrm{nhyp}}(\tau) &= \frac{1}{\#\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q)} \sum_{\substack{C \in \mathcal{M}_g^{\mathrm{nhyp}\prime}(\mathbb{F}_q) \\ \tau(C) = \tau}} 1 + O_g(q^{-1/2}q^{-3g+3}) \\ &= \frac{1}{\#\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q)} \sum_{\substack{C \in \mathcal{M}_g(\mathbb{F}_q) \\ \tau(C) = t/\sqrt{q}}} 1 + O_g(q^{-1}). \end{aligned} \tag{25}$$

We now want to replace the denominator $\#\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q)$ with $\#\mathcal{M}_g(\mathbb{F}_q)$. To do this, we need to compare isomorphism classes over $\mathbb{F}_q$ and over $\overline{\mathbb{F}_q}$. Let C, C' be two (smooth projective) curves of genus g over $\mathbb{F}_q$. If $\operatorname{Aut}(C_{\overline{\mathbb{F}_q}})$ is trivial, then C, C' are isomorphic over $\overline{\mathbb{F}_q}$ if and only if they are isomorphic over $\mathbb{F}_q$

(one implication is trivial. For the other, if C, C' are isomorphic over $\overline{\mathbb{F}_q}$, then C' is an $\mathbb{F}_q$-twist of C; but twists of C are parametrised by $H^1(\mathbb{F}_q, \mathrm{Aut}(C_{\overline{\mathbb{F}_q}})) = \{1\}$). It follows from this that we have

$$\#\left\{C \in \mathcal{M}_g(\mathbb{F}_q) \mid \mathrm{Aut}_{\overline{\mathbb{F}_q}}(C) = \{1\}\right\} \leq \mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q) \leq \#\mathcal{M}_g(\mathbb{F}_q).$$

Dividing by $\#\mathcal{M}_g(\mathbb{F}_q)$ and using Lemma 2.5 we obtain

$$1 + O_g(q^{-1}) = \frac{\#\left\{C \in \mathcal{M}_g(\mathbb{F}_q) \mid \mathrm{Aut}_{\overline{\mathbb{F}_q}}(C) = \{1\}\right\}}{\#\mathcal{M}_g(\mathbb{F}_q)} \leq \frac{\mathcal{M}_g^{\mathrm{nhyp}}(\mathbb{F}_q)}{\#\mathcal{M}_g(\mathbb{F}_q)} \leq 1.$$

Combined with (25), this immediately gives

$$\mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q}) = \frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{\substack{C \in \mathcal{M}_g(\mathbb{F}_q) \\ \tau(C) = t/\sqrt{q}}} 1 + O_g(q^{-1}) = H'(q,t) + O_g(q^{-1}),$$

which in turn implies that

$$\left|\sqrt{q}\mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q}) - \sqrt{q}H'(q,t)\right|$$

is $O_g(q^{-1/2})$ as $q \to \infty$, as desired. □

Define the function $f_q : [-2g-1, 2g+1] \to \mathbb{R}$ by the formula $f_q(\tau) = \sqrt{q}H'(q,t)$, where as before t is the unique integer in the interval $(\sqrt{q}\tau - 1/2, \sqrt{q}\tau + 1/2]$. Putting $\tau_1 = \sqrt{q}\tau$ we obtain

$$\int_{-2g-1}^{2g+1} f_q(\tau)d\tau = \int_{-(2g+1)\sqrt{q}}^{(2g+1)\sqrt{q}} \frac{f_q(\tau_1/\sqrt{q})}{\sqrt{q}} d\tau_1 = \left(\sum_{\substack{t \in \mathbb{Z} \\ t \in [-(2g+1)\sqrt{q}, (2g+1)\sqrt{q}]}} \frac{H'(q,t)\sqrt{q}}{\sqrt{q}}\right) = 1, \tag{26}$$

because the function $f_q(\tau_1/\sqrt{q})$ is locally constant and equal to $H'(q,t)\sqrt{q}$ for $\tau_1 \in \left[t - \frac{1}{2}, t + \frac{1}{2}\right)$, and it vanishes around the endpoints of the integration interval: indeed, for τ sufficiently close to $2g+1$ we have $\sqrt{q}\tau - \frac{1}{2} > 2g\sqrt{q}$, hence $H'(q,t) = 0$ since there is no genus-g curve over $\mathbb{F}_q$ with trace greater than $2g\sqrt{q}$ (one can argue similarly for τ near $-(2g+1)$).

In particular,

$$\int_{-2g-1}^{2g+1} f_q(\tau)d\tau = 1 = \int_{-2g-1}^{2g+1} \mathrm{ST}_g(\tau)d\tau. \tag{27}$$

Proposition A.3. *[BHLGR24, Conjecture 5.1] does not hold.*

Proof. Fix $\tau \in [-(2g+1), (2g+1)]$ and $\varepsilon > 0$. Assuming [BHLGR24, Conjecture 5.1], we will show that the difference $|\mathrm{ST}_g(\tau) - f_q(\tau)|$ is smaller than 2ε for q large enough.

This is easy for $|\tau| > 2g$. Indeed, let q be such that $|\tau| - 2g > 1/2\sqrt{q}$ (this happens for all q large enough). Then, $|t(q,\tau)| > 2\sqrt{q}g$ (for example, if τ is positive, then $t > \sqrt{q}\tau - 1/2 > 2g\sqrt{q}$) and $\#\{C : \mathrm{Tr}(C) = t\} = 0$. In particular, $\mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q}) = 0$, and on the other hand $\mathrm{ST}_g(t/\sqrt{q}) = 0$ since $\mathrm{ST}_g(x)$ is concentrated on the interval $[-2g, 2g]$. We can then assume $|\tau| \leq 2g$. The triangular inequality gives

$$|\mathrm{ST}_g(\tau) - f_q(\tau)| \leq |\mathrm{ST}_g(\tau) - \mathrm{ST}_g(t/\sqrt{q})| + |\mathrm{ST}_g(t/\sqrt{q}) - f_q(\tau)|. \tag{28}$$

By definition we have $f_q(\tau) = f_q(t) = \sqrt{q}H'(q,t)$. If [BHLGR24, Conjecture 5.1] holds, by Lemma A.2 we have

$$|\mathrm{ST}_g(t/\sqrt{q}) - f_q(\tau)| = \left|\mathrm{ST}_g(t/\sqrt{q}) - \sqrt{q}H'(q,t)\right| < \varepsilon \tag{29}$$

for q large enough (depending on τ and ε). Since ST_g is uniformly continuous on $[-2g, 2g]$ and $\tau - \frac{t}{\sqrt{q}}$ goes to 0 as $q \to \infty$, we have

$$|\mathrm{ST}_g(\tau) - \mathrm{ST}_g(t/\sqrt{q})| < C_q \tag{30}$$

with C_q that goes to 0 as q goes to infinity. Combining Equations (28), (29), and (30), we obtain $|\mathrm{ST}_g(\tau) - f_q(\tau)| \leq 2\varepsilon$ for q large enough. Therefore, for all $\tau \in [-(2g+1), 2g+1]$ we have

$$\lim_{q \to \infty} |\mathrm{ST}_g(\tau) - f_q(\tau)| = 0.$$

By Scheffé's Lemma (see [BHLGR24, End of page 20]) this, together with (27), yields

$$\lim_{q\to\infty}\int_{-2g-1}^{2g+1}|\mathrm{ST}_g(\tau)-f_q(\tau)|\,d\tau=0.$$

Let now

$$L_1(g)\coloneqq\frac{\#\{M\in\mathrm{GSp}_{2g}(\mathbb{F}_2):\operatorname{Tr}M\equiv 0\pmod 2,\operatorname{mult}(M)=q\equiv 1\pmod 2\}}{\#\,\mathrm{GSp}_{2g}(\mathbb{F}_2)}.$$

By a direct computation, we have $L_1(3)=\frac{1436}{2835}\approx 0.5065\neq 1/2$ (we suspect that $L_1(g)\neq\frac{1}{2}$ holds for all $g\geq 3$). Fix $0<\varepsilon<\frac{|L_1(g)-1/2|}{2}$ and take q large enough so that the inequality

$$\int_{-2g-1}^{2g+1}|\mathrm{ST}_g(\tau)-f_q(\tau)|\,d\tau<\varepsilon \tag{31}$$

holds. Let

$$O=\left(\bigcup_{\substack{t\in\mathbb{Z}\cap[-(2g+1)\sqrt{q},(2g+1)\sqrt{q}]\\ t\equiv 0\pmod 2}}\left(\frac{t}{\sqrt{q}}-\frac{1}{2\sqrt{q}},\frac{t}{\sqrt{q}}+\frac{1}{2\sqrt{q}}\right]\right)\cap[-2g-1,2g+1]$$

and

$$E=\left(\bigcup_{\substack{t\in\mathbb{Z}\cap[-(2g+1)\sqrt{q},(2g+1)\sqrt{q}]\\ t\equiv 1\pmod 2}}\left(\frac{t}{\sqrt{q}}-\frac{1}{2\sqrt{q}},\frac{t}{\sqrt{q}}+\frac{1}{2\sqrt{q}}\right]\right)\cap[-2g-1,2g+1].$$

Note that E and O are disjoint and that their union covers $[-2g-1,2g+1]$ up to a set of (Lebesgue) measure $O(1/\sqrt{q})$. Note moreover that both O and E are disjoint unions of intervals over which $f_q(\tau)$ is constant, and that

$$\int_{\frac{t}{\sqrt{q}}-\frac{1}{2\sqrt{q}}}^{\frac{t}{\sqrt{q}}+\frac{1}{2\sqrt{q}}}f_q(\tau)\,d\tau=\int_{t-1/2}^{t+1/2}\frac{\sqrt{q}H'(q,t)}{\sqrt{q}}\,d\tau_1=H'(q,t).$$

In particular, since $H'(q,t)$ vanishes for $|t|>2g\sqrt{q}$, the integral of $f_q(\tau)$ over O, resp. E, gives $\sum_{t\text{ odd}}H'(q,t)=\mathbb{P}^{\mathrm{naive}}_{g,q}(\operatorname{Tr}(C/\mathbb{F}_q)\equiv 1\pmod 2)$, resp. $\mathbb{P}^{\mathrm{naive}}_{g,q}(\operatorname{Tr}(C/\mathbb{F}_q)\equiv 0\pmod 2)$.

The triangular inequality and (31) give

$$\begin{aligned}
&\left|\int_E f_q(\tau)\,d\tau-\int_O f_q(\tau)\,d\tau\right|\\
&=\left|\int_E\left(f_q(\tau)-\mathrm{ST}_g(\tau)\right)\,d\tau+\int_E\mathrm{ST}_g(\tau)\,d\tau-\int_O\left(f_q(\tau)-\mathrm{ST}_g(\tau)\right)\,d\tau-\int_O\mathrm{ST}_g(\tau)\,d\tau\right|\\
&\leq\left|\int_E\mathrm{ST}_g(\tau)\,d\tau-\int_O\mathrm{ST}_g(\tau)\,d\tau\right|+\int_{-2g-1}^{2g+1}|\mathrm{ST}_g(\tau)-f_q(\tau)|\,d\tau\\
&<\varepsilon+\left|\int_E\mathrm{ST}_g(\tau)\,d\tau-\int_O\mathrm{ST}_g(\tau)\,d\tau\right|.
\end{aligned}$$

Since ST_g is Riemann-integrable, both $\int_E\mathrm{ST}_g(\tau)\,d\tau$ and $\int_O\mathrm{ST}_g(\tau)\,d\tau$ converge to $\frac{1}{2}\int_{-2g-1}^{2g+1}\mathrm{ST}_g(\tau)\,d\tau=\frac{1}{2}$ as $q\to\infty$, hence for q large enough we have

$$\left|\int_E\mathrm{ST}_g(\tau)\,d\tau-\int_O\mathrm{ST}_g(\tau)\,d\tau\right|<\varepsilon$$

and

$$\left|\int_E f_q(\tau)\,d\tau-\int_O f_q(\tau)\,d\tau\right|<2\varepsilon<|L_1(g)-1/2|.$$

On the other hand, as remarked above we have

$$\begin{aligned}\left|\int_E f_q(\tau)\,d\tau - \int_O f_q(\tau)\,d\tau\right| &= \left|\mathbb{P}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2) - \mathbb{P}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 1 \pmod 2)\right| \\ &= \left|1 - 2\mathbb{P}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)\right|.\end{aligned}$$

It follows that

$$\begin{aligned}\left|L_1(g) - \frac{1}{2}\right| &\leq \left|L_1(g) - \mathbb{P}_{g,q}^{\mathrm{naive}}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)\right| + \left|\mathbb{P}_{g,q}^{\mathrm{naive}}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2) - \frac{1}{2}\right| \\ &= \left|L_1(g) - \mathbb{P}_{g,q}^{\mathrm{naive}}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)\right| + \frac{\left|\int_E f_q(\tau)\,d\tau - \int_O f_q(\tau)\,d\tau\right|}{2} \\ &< \left|L_1(g) - \mathbb{P}_{g,q}^{\mathrm{naive}}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)\right| + \frac{\left|L_1(g) - \frac{1}{2}\right|}{2}\end{aligned}$$

and therefore

$$\left|L_1(g) - \frac{1}{2}\right| < 2\left|L_1(g) - \mathbb{P}_{g,q}^{\mathrm{naive}}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)\right|.$$

On the other hand, for q large enough by Remark 2.7 we have

$$2\left|L_1(g) - \mathbb{P}_{g,q}^{\mathrm{naive}}(\mathrm{Tr}(C/\mathbb{F}_q) \equiv 0 \pmod 2)\right| < \varepsilon :$$

this is a contradiction, because it yields $\left|L_1(g) - \frac{1}{2}\right| < \varepsilon$, while ε was assumed to be less than $\frac{|L_1(g)-1/2|}{2}$. Hence, [BHLGR24, Conjecture 5.1] cannot hold. □

References

[AAGG23] Jeffrey D. Achter, Salim A. Altuğ, Luis Garcia, and Julia Gordon. Counting abelian varieties over finite fields via Frobenius densities. *Algebra Number Theory*, 17(7):1239–1280, 2023. Appendix by Wen-Wei Li and Thomas Rüd.

[Ach08] Jeffrey D. Achter. Results of Cohen-Lenstra type for quadratic function fields. In *Computational arithmetic geometry*, volume 463 of *Contemp. Math.*, pages 1–7. Amer. Math. Soc., Providence, RI, 2008.

[AEK+15] Jeffrey D. Achter, Daniel Erman, Kiran S. Kedlaya, Melanie Matchett Wood, and David Zureick-Brown. A heuristic for the distribution of point counts for random curves over finite field. *Philos. Trans. Roy. Soc. A*, 373(2040):1–12, 2015.

[AG17] Jeffrey D. Achter and Julia Gordon. Elliptic curves, random matrices and orbital integrals. *Pacific J. Math.*, 286(1):1–24, 2017. With an appendix by S. Ali Altuğ.

[AH03] Jeffrey D. Achter and Joshua Holden. Notes on an analogue of the Fontaine-Mazur conjecture. *J. Théor. Nombres Bordeaux*, 15(3):627–637, 2003.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BHLGR24] Jonas Bergström, Everett W. Howe, Elisa Lorenzo García, and Christophe Ritzenthaler. Refinements of Katz–Sarnak theory for the number of points on curves over finite fields. *Canadian Journal of Mathematics*, page 1–27, 2024.

[Bir68] Bryan J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[BLV23] Francesco Ballini, Davide Lombardo, and Matteo Verzobio. Statistics of L-polynomials over finite fields, 2023. Available at `https://github.com/DavideLombardoMath/distribution-L-polynomials`.

[CH13] Wouter Castryck and Hendrik Hubrechts. The distribution of the number of points modulo an integer on elliptic curves over finite fields. *Ramanujan J.*, 30(2):223–242, 2013.

[CST14] Wouter Castryck, Marco Streng, and Damiano Testa. Curves in characteristic 2 with non-trivial 2-torsion. *Adv. Math. Commun.*, 8(4):479–495, 2014.

[Del77] Pierre Deligne. *Cohomologie étale*, volume 569 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1977. Séminaire de géométrie algébrique du Bois-Marie SGA $4\frac{1}{2}$.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[DK69] Pierre Deligne and Nicholas M. Katz. *Groupes de monodromie en géométrie algébrique. II*, volume SGA 7 II of *Lecture Notes in Mathematics, Vol. 340*. Springer-Verlag, Berlin-New York, 1967–1969. Séminaire de Géométrie Algébrique du Bois-Marie.

[DM69] Pierre Deligne and David Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, 36:75–109, 1969.

[EP13] Arsen Elkin and Rachel Pries. Ekedahl-Oort strata of hyperelliptic curves in characteristic 2. *Algebra Number Theory*, 7(3):507–532, 2013.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[Gek03] Ernst-Ulrich Gekeler. Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.*, 37:1999–2018, 2003.

[Gon98] Josep González. On the p-rank of an abelian variety and its endomorphism algebra. *Publ. Mat.*, 42(1):119–130, 1998.

[Gro12] Benedict H. Gross. Hanoi lectures on the arithmetic of hyperelliptic curves. *Acta Math. Vietnam.*, 37(4):579–588, 2012.

[HNR09] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler. Jacobians in isogeny classes of abelian surfaces over finite fields. *Ann. Inst. Fourier (Grenoble)*, 59(1):239–289, 2009.

[HP20] Urs Hartl and Ambrus Pal. Crystalline Chebotarëv density theorems, 2020.

[Ked22] Kiran S. Kedlaya. Notes on isocrystals. *J. Number Theory*, 237:353–394, 2022.

[Kir69] David Kirby. Integer matrices of finite order. *Rend. Mat. (6)*, 2:403–408, 1969.

[KP18] Jerzy Kaczorowski and Alberto Perelli. Zeta functions of finite fields and the Selberg class. *Acta Arith.*, 184(3):247–265, 2018.

[KS99] Nicholas M. Katz and Peter Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.

[KS09] Kiran S. Kedlaya and Andrew V. Sutherland. Hyperelliptic curves, L-polynomials, and random matrices. In *Arithmetic, geometry, cryptography and coding theory*, volume 487 of *Contemp. Math.*, pages 119–162. Amer. Math. Soc., Providence, RI, 2009.

[Lac16] Gilles Lachaud. On the distribution of the trace in the unitary symplectic group and the distribution of Frobenius. In *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*, volume 663 of *Contemp. Math.*, pages 185–221. Amer. Math. Soc., Providence, RI, 2016.

[Lee01] Kwankyu Lee. A counting formula about the symplectic similitude group. *Bull. Austral. Math. Soc.*, 63(1):15–20, 2001.

[LRRS14] Reynald Lercier, Christophe Ritzenthaler, Florent Rovetta, and Jeroen Sijsling. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS J. Comput. Math.*, 17:128–147, 2014.

[LSTX19] Aaron Landesman, Ashvin Swaminathan, James Tao, and Yujie Xu. Surjectivity of Galois representations in rational families of abelian varieties. *Algebra Number Theory*, 13(5):995–1038, 2019. With an appendix by Davide Lombardo.

[LT76] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions*, volume Vol. 504 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[LW54] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[Ma23] Zhao Yu Ma. Refinements on vertical Sato-Tate, 2023.

[Mum65] David Mumford. *Geometric invariant theory*, volume Band 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete, (N.F.)*. Springer-Verlag, Berlin-New York, 1965.

[Oes82] Joseph Oesterlé. Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbf{Z}_p^N$. *Invent. Math.*, 66(2):325–341, 1982.

[Riv08] Igor Rivin. Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms. *Duke Math. J.*, 142(2):353–379, 2008.

[Sch31] Friedrich K. Schmidt. Analytische Zahlentheorie in Körpern der Charakteristik p. *Math. Z.*, 33(1):1–32, 1931.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, 54:323–401, 1981.

[Ser12] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[Shm23] Aleksander Shmakov. Cohomological arithmetic statistics for principally polarized abelian varieties over finite fields, 2023.

[Sta22] The Stacks project authors. The stacks project. `https://stacks.math.columbia.edu`, 2022.

[Wei48] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*, volume 7 (1945) of *Publications de l'Institut de Mathématiques de l'Université de Strasbourg*. Hermann & Cie, Paris, 1948.

Francesco Ballini, University of Oxford, Andrew Wiles building, Woodstock Road, Oxford, United Kingdom
E-mail address: `ballini@maths.ox.ac.uk`
Davide Lombardo, Università di Pisa, Dipartimento di matematica, Largo Bruno Pontecorvo 5, Pisa, Italy
E-mail address: `davide.lombardo@unipi.it`
Matteo Verzobio, IST Austria, Am Campus 1, Klosterneuburg, Austria
E-mail address: `matteo.verzobio@gmail.com`