Canad. J. Math. 2024, pp. 1–26
http://dx.doi.org/10.4153/S0008414X2400004X

Refinements of Katz–Sarnak theory for the number of points on curves over finite fields

Jonas Bergström, Everett W. Howe, Elisa Lorenzo García, and Christophe Ritzenthaler

Abstract. This paper goes beyond Katz–Sarnak theory on the distribution of curves over finite fields according to their number of rational points, theoretically, experimentally, and conjecturally. In particular, we give a formula for the limits of the moments measuring the asymmetry of this distribution for (non-hyperelliptic) curves of genus $g \geq 3$. The experiments point to a stronger notion of convergence than the one provided by the Katz–Sarnak framework for all curves of genus ≥ 3. However, for elliptic curves and for hyperelliptic curves of every genus, we prove that this stronger convergence cannot occur.

1 Introduction

Katz–Sarnak theory [KS99] gives a striking unified framework to understand the distribution of the traces of Frobenius for a family of curves[1] of genus g over a finite field $\mathbb{F}_q$ when q goes to infinity. It has been used in many specific cases (see [AS10, BCD+18, CDSS17, FKRS12, HKL+20, KS09, Vlă01] among others). Although powerful, this theory can neither in general predict the number of curves over a given finite field with a given trace, nor distinguish between the family of all curves and the family of hyperelliptic curves when $g \geq 3$. This paper can be seen as an attempt to go beyond Katz–Sarnak results, theoretically, experimentally, and conjecturally. We hope that this blend will excite the curiosity of the community.

We begin by resuming our study of sums of powers of traces initiated in [BHLGR23]. If $C/\mathbb{F}_q$ is a curve of genus g, we denote by $[C]$ the set of representatives of its twists and define

$$s_n(C) = \sum_{C' \in [C]} \frac{(q+1-\#C'(\mathbb{F}_q))^n}{\#\operatorname{Aut}_{\mathbb{F}_q}(C')}.$$

As shown in [BHLGR23, Proposition 3.1], the $s_n(C)$ are integers and we denote by $S_n(q, \mathcal{X})$ the sum of the $s_n(C)$ when C runs over a set of representatives for the

Received by the editors April 6, 2023; revised November 30, 2023; accepted January 1, 2024.
Published online on Cambridge Core January 9, 2024.
AMS subject classification: **11G20**, **11R45**, **14H10**, **14H25**.
Keywords: Katz–Sarnak theory, distribution, moments, Serre's obstruction.

[1]Throughout this paper, the word "curve" will always mean a projective, absolutely irreducible, smooth variety of dimension 1.

$\overline{\mathbb{F}}_q$-isomorphism classes of curves C over $\mathbb{F}_q$ in $\mathcal{X}$, where $\mathcal{X}$ can be, for example,

- the moduli space $\mathcal{M}_{1,1}$ of elliptic curves,
- the moduli space $\mathcal{M}_g$ of curves of genus $g > 1$,
- the moduli space $\mathcal{H}_g$ of hyperelliptic curves of genus $g > 1$, or
- the moduli space $\mathcal{M}_g^{\mathrm{nhyp}}$ of non-hyperelliptic curves of genus $g > 2$.

In Remark 2.2, we will briefly recall that $S_n(q, \mathcal{M}_{1,1})$ can be determined for all q and n in terms of traces of Hecke operators on spaces of elliptic modular cusp forms. For every q and n, we can also find expressions for $S_n(q, \mathcal{M}_2) = S_n(q, \mathcal{H}_2)$ in terms of traces of Hecke operators acting on spaces of Siegel modular cusp forms of genus 2 (and genus 1) starting from [Pet15, Theorem 2.1] (see [BF22, Section 4.5] for a few more details). For every $g \geq 3$, there are known explicit formulae for $S_n(q, \mathcal{X})$ only for the first values of n (see, for instance, [BHLGR23, Theorem 3.4] for $\mathcal{H}_g$ (note that the odd n values are equal to 0 in this case) and [Ber08] for $\mathcal{M}_3^{\mathrm{nhyp}}$). However, it is possible to give an interpretation for

$$\mathfrak{a}_n(\mathcal{X}) := \lim_{q\to\infty} \frac{S_n(q, \mathcal{X})}{q^{\dim \mathcal{X} + n/2}}$$

with $\mathcal{X} = \mathcal{M}_g$, $\mathcal{H}_g$, or $\mathcal{M}_g^{\mathrm{nhyp}}$ for every $g \geq 2$ and even $n \geq 2$ in terms of representation theory of the compact symplectic group USp_{2g}. This is achieved in [BHLGR23, Theorem 3.8] using the ideas of Katz and Sarnak.

Our first contributions are gathered in Theorem 2.1. Using the results of Johnson [Joh83] and Hain [Hai95], together with results of Petersen [Pet15, Pet16] about the first cohomology group of symplectic local systems on $\mathcal{M}_g$, we can prove that for even values of $n > 0$, we have

$$\mathfrak{a}_n(\mathcal{M}_g) - \frac{S_n(q, \mathcal{M}_g)}{q^{\dim \mathcal{M}_g + n/2}} = O(q^{-1}) \tag{1.1}$$

when $g \geq 2$, whereas Katz–Sarnak would only give $O(q^{-1/2})$. Since $\mathfrak{a}_n(\mathcal{M}_g) = 0$ for odd values of n, this suggests replacing the exponent in the power of q in the denominator of the expression defining $\mathfrak{a}_n(\mathcal{M}_g)$ with a smaller number. As far as we know, this has not been considered previously. We therefore introduce for odd n

$$\mathfrak{b}_n(\mathcal{M}_g) := -\lim_{q\to\infty} \frac{S_n(q, \mathcal{M}_g)}{q^{3g-3+(n-1)/2}}.$$

Theorem 2.1 gives $\mathfrak{b}_n(\mathcal{M}_g)$ in terms of an explicit integral and in terms of the representation theory of USp_{2g}. This second description makes it easy to compute. The idea to use information about the cohomology of moduli space of curves to predict the number of curves over a given finite field with a given trace can also be found in [AEK+15], but there g goes to infinity.

The deep relations between the sum of traces and Katz–Sarnak theory become clearer once we switch to a probabilistic point of view. In Section 3, we introduce the classical probability measure $\mu_{q,g}$ on the interval $[-2g, 2g]$ derived from the numbers of $\mathbb{F}_q$-isomorphism classes of curves of genus $g > 1$ with given traces of Frobenius. From Katz–Sarnak, we then know that the sequence of measures $(\mu_{q,g})$

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

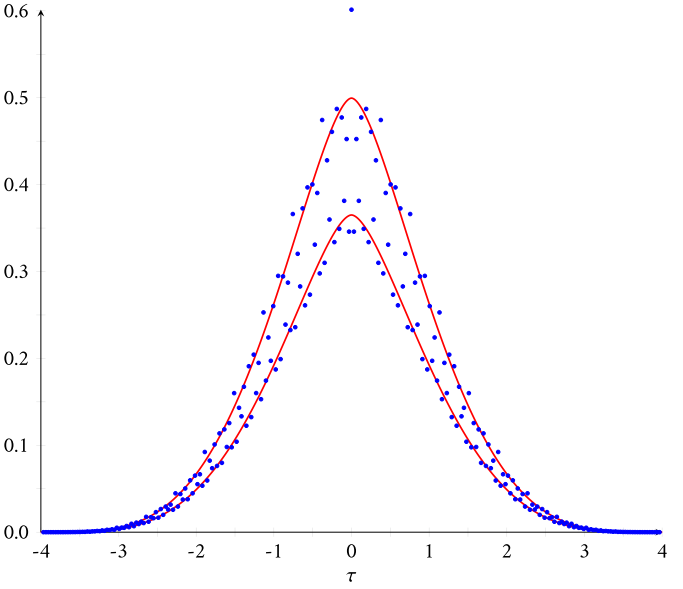

Figure 1: Data for curves of genus 2 over $\mathbb{F}_q$ for $q = 1,009$. The blue dots are the points $(t/\sqrt{q}, \sqrt{q}\,\mathcal{N}_{q,2}^{\mathrm{hyp}}(t/\sqrt{q}))$ for integers $t \in [-126, 126]$. The red curves are the functions $b\mathfrak{f}_2(\tau)$ and $c\mathfrak{f}_2(\tau)$, where $b = 38/45$ and $c = 52/45$ are the bounds given by Proposition 4.2 for $g = 2$ when $\varepsilon = 0$.

weakly converges to a continuous measure μ_g with an explicit density $\mathfrak{f}_g$ (see [Bil95, Theorem 2.1] for equivalent definitions of weak convergence of measures). In this language, the numbers $\mathfrak{a}_n(\mathcal{M}_g)$ can be understood as the nth moments of the measure μ_g, and we can refine Katz–Sarnak theory using a second continuous function $\mathfrak{h}_g$ whose nth moments are the numbers $\mathfrak{b}_n(\mathcal{M}_g)$ (see Theorem 3.1).

In Section 4, we investigate whether the Katz–Sarnak limiting distributions can be used to approximate the number of curves over a given finite field $\mathbb{F}_q$ of a given genus and with a given trace of Frobenius; one might hope that integrating that distribution over an interval of length $1/\sqrt{q}$ around $t/\sqrt{q}$ would give a value close to the number of genus-g curves over $\mathbb{F}_q$ having trace t. We show that this does *not* happen for elliptic curves or for hyperelliptic curves of any genus. For elliptic curves, Proposition 4.5 shows that the number of elliptic curves with a given trace can be an arbitrarily large multiple of this naïve Katz–Sarnak prediction (see also Figure 3). For hyperelliptic curves, Proposition 4.2 shows (roughly speaking) that if the number of curves is asymptotically bounded above and below by two multiples of the naïve Katz–Sarnak prediction, then the ratio of these two multiples is bounded below by a fixed number strictly greater than 1 (see Figure 1).

On the other hand, numerical experiments suggest that the elliptic and hyperelliptic cases differ in the sense that it is easy to "correct" the distribution in the hyperelliptic cases to observe a good approximation by the density function $\mathfrak{f}_g$ (see Figure 2). Even stronger, computations for all non-hyperelliptic curves of genus 3 (see Figure 4) make

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

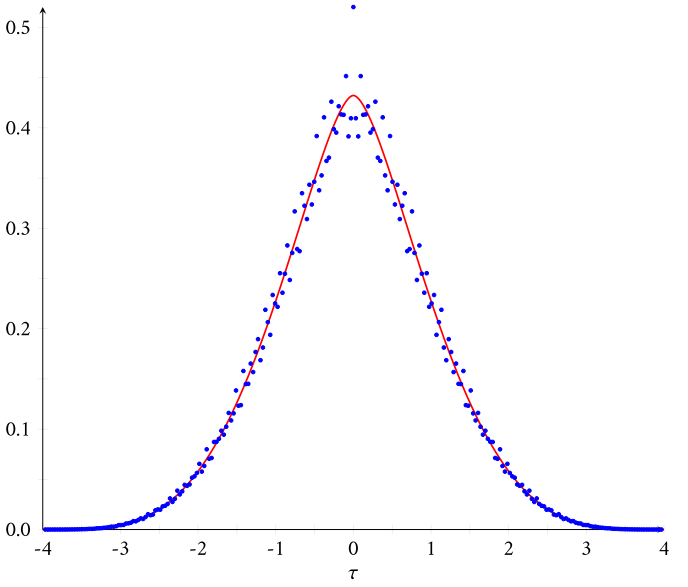

Figure 2: Scaled data for curves of genus 2 over $\mathbb{F}_q$ for $q = 1,009$. The blue dots are the points $(t/\sqrt{q}, s\sqrt{q}\,\mathcal{N}_{q,2}^{\mathrm{hyp}}(t/\sqrt{q}))$ for integers $t \in [-126, 126]$, where $s = 45/52$ if t is even and $s = 45/38$ if t is odd. The red curve is the function $\mathfrak{f}_2(\tau)$.

us dream that the naïve Katz–Sarnak approximation *does* directly give an accurate estimate for the number of curves with a given number of points. This leads us to claim the bold Conjecture 5.1. The heuristic idea behind this conjecture is that for each trace, one is averaging over many isogeny classes which somehow would allow this stronger convergence as long as there are no obvious arithmetic obstructions. Our attempts to use the better convergence rates of the moments in the case of $\mathcal{M}_g$ for $g \geq 3$ to prove this conjecture were unfortunately unsuccessful. However, for $g = 1$, we would like to point out the shortening of the intervals of convergence obtained in [Ma23], which may give some hints for addressing the question.

Finally, in Section 5, we revisit the work of [LRR+19] on the symmetry breaking for the trace distribution of (non-hyperelliptic) genus 3 curves, by looking at the difference between the number of curves with trace t and the number of curves with trace $-t$. In probabilistic terms, this asymmetry is given by a signed measure $\nu_{q,g}$. Although this signed measure weakly converges to 0 when q goes to infinity, by Corollary 5.3, the moments of $\sqrt{q}\,\nu_{q,g}$ converge to $-2\mathfrak{b}_n(\mathcal{M}_g)$ when n is odd (and are trivially 0 when n is even). In particular, this shows that by "zooming in" on the Katz–Sarnak distribution, one can spot a difference between the behavior for hyperelliptic curves (for which the corresponding signed measures would all be 0) and for non-hyperelliptic curves.

In the same spirit as Section 4, the experimental data for $g = 3$ (see Figure 5) and the convergence of moments lead us to conjecture that the sequence of signed measures $(\sqrt{q}\,\nu_{q,g})$ weakly converges to the continuous signed measure with density

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

$-2\mathfrak{h}_g$ for all $g \geq 3$. Notice that in contrast to the case of positive bounded measures, the convergence of moments of signed measures on a compact interval does not directly imply weak convergence (see Example 5.4).

With such a conjecture in hand, one may then improve on the result of [LRR+19] that heuristically approximated the limit density of $(\sqrt{q}\,\nu_{q,g})$ by the function

$$x(1-x^2/3)\cdot\left(\frac{1}{\sqrt{2\pi}}e^{-x^2/2}\right).$$

Using the first values of $\mathfrak{b}_n(\mathcal{M}_3)$, we get the better approximation

$$x\left(5/4-x^2/2+x^4/60\right)\left(\frac{1}{\sqrt{2\pi}}e^{-x^2/2}\right).$$

2 Limits of sums of powers of traces

Fix a prime power q. Let us start by recalling some definitions and results from [BHLGR23].

Definition 2.1 Let $\mathcal{X} = \mathcal{H}_g$, $\mathcal{M}_g$ or $\mathcal{M}_g^{\mathrm{nhyp}}$ for any $g \geq 2$, or $\mathcal{X} = \mathcal{M}_{1,1}$.

⋆ Recall from Section 1 that one defines

$$S_n(q,\mathcal{X}) = \sum_{[C]\in\mathcal{X}(\mathbb{F}_q)}\ \sum_{C'\in[C]}\frac{(q+1-\#C'(\mathbb{F}_q))^n}{\#\operatorname{Aut}_{\mathbb{F}_q}(C')},$$

where $[C]$ is a point of $\mathcal{X}(\mathbb{F}_q)$ representing the $\overline{\mathbb{F}}_q$-isomorphism class of a curve $C/\mathbb{F}_q$, and the second sum spans the set of representatives of all twists C' of C.

⋆ For every $n \geq 1$, let

$$\mathfrak{a}_n(\mathcal{X}) := \lim_{q\to\infty}\frac{S_n(q,\mathcal{X})}{q^{\dim\mathcal{X}+n/2}}$$

with $\mathcal{X} = \mathcal{H}_g$ or $\mathcal{M}_g$ or $\mathcal{M}_g^{\mathrm{nhyp}}$ for any $g \geq 2$, or with $\mathcal{X} = \mathcal{M}_{1,1}$.

Define $w_k := \sum_{j=1}^{g} 2\cos k\theta_j$ and

$$dm_g := \frac{1}{g!\,\pi^g}\prod_{i<j}(2\cos\theta_i - 2\cos\theta_j)^2\prod_i 2\sin^2\theta_i\, d\theta_1\ldots d\theta_g,$$

and recall from [BHLGR23, Theorem 2.1] that for every $g \geq 2$ and $n \geq 1$,

$$\mathfrak{a}_n(\mathcal{X}) = \int_{(\theta_1,\ldots,\theta_g)\in[0,\pi]^g} w_1^n\, dm_g,$$

with $\mathcal{X} = \mathcal{H}_g$ or $\mathcal{M}_g$ or $\mathcal{M}_g^{\mathrm{nhyp}}$. Notice that for a fixed value of g, $\mathfrak{a}_n(\mathcal{X})$ does not depend on $\mathcal{X}$, and $\mathfrak{a}_n(\mathcal{X}) = 0$ for odd n.

In order to go deeper in the limit distribution, we will also look at the "next term" of the limit of $\frac{S_n(q,\mathcal{X})}{q^{\dim\mathcal{X}+n/2}}$ when $\mathcal{X} = \mathcal{M}_g$.

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

Definition 2.2 For every $g \geq 2$ and $n \geq 1$, let

$$\mathfrak{b}_n(\mathcal{M}_g) := -\lim_{q\to\infty} \sqrt{q}\left(\frac{S_n(q,\mathcal{M}_g)}{q^{3g-3+n/2}} - \mathfrak{a}_n(\mathcal{M}_g)\right).$$

To state our results, we need to recall basic facts about the representations of USp_{2g} with coefficients in $\mathbb{Q}_\ell$, where ℓ is a prime distinct from the characteristic of $\mathbb{F}_q$. The irreducible representations V_λ of USp_{2g} are indexed by the highest weight $\lambda = (\lambda_1, \dots, \lambda_g)$ with $\lambda_1 \geq \cdots \geq \lambda_g \geq 0$. The corresponding characters χ_λ are the symplectic Schur polynomials $\mathbf{s}_{\langle\lambda\rangle}(x_1, \dots, x_g) \in \mathbb{Z}[x_1, \dots, x_g, x_1^{-1}, \dots, x_g^{-1}]$ in the sense that if $A \in \mathrm{USp}_{2g}$ has eigenvalues $\alpha_1, \dots, \alpha_g, \alpha_1^{-1}, \dots, \alpha_g^{-1}$, then $\chi_\lambda(A) = \mathbf{s}_{\langle\lambda\rangle}(\alpha_1, \dots, \alpha_g)$ (see [FH91, Proposition 24.22 and (A.45)]). In the notation, we will suppress the λ_j that are 0. Put $|\lambda| = \lambda_1 + \cdots + \lambda_g$ and note that $V_\lambda^\vee \cong V_\lambda$.

Theorem 2.1 *Let $V = V_{(1)}$ denote the standard representation.*

(1) *Let $\mathcal{X} = \mathcal{H}_g$, $\mathcal{M}_g$, $\mathcal{M}_g^{nhyp}$ for any $g \geq 2$, or $\mathcal{M}_{1,1}$. For every $n \geq 1$, $\mathfrak{a}_n(\mathcal{X})$ is equal to the number of times the trivial representation appears in the USp_{2g}-representation $V^{\otimes n}$.*[2]

(2) *For every $g \geq 3$ and $n \geq 1$, $\mathfrak{b}_n(\mathcal{M}_g)$ is equal to the number of times the representation $V_{(1,1,1)}$ appears in the USp_{2g}-representation $V^{\otimes n}$. In particular, $\mathfrak{b}_n(\mathcal{M}_g) = 0$ for n even.*

(3) *For every $n \geq 1$, $\mathfrak{b}_n(\mathcal{M}_2) = 0$.*

(4) *For every $g \geq 2$ and $n \geq 1$,*

$$\mathfrak{a}_n(\mathcal{M}_g) - \frac{\mathfrak{b}_n(\mathcal{M}_g)}{\sqrt{q}} = \frac{S_n(q,\mathcal{M}_g)}{q^{3g-3+n/2}} + O(q^{-1}).$$

(5) *For every $g \geq 3$ and $n \geq 1$, we have*

$$\mathfrak{b}_n(\mathcal{M}_g) = \int_{(\theta_1,\dots,\theta_g)\in[0,\pi]^g} w_1^n\left(\frac{1}{6}w_1^3 - \frac{1}{2}w_1w_2 + \frac{1}{3}w_3 - w_1\right) dm_g. \tag{2.1}$$

Proof Poincaré duality gives a symplectic pairing on the first ℓ-adic étale cohomology group of a curve. We will be interested in the action of Frobenius on these cohomology groups, and since we need to take the size of the eigenvalues of Frobenius into account, we will consider representations of GSp_{2g}. Let $\mathbb{Q}_\ell(-1)$ denote the *multiplier representation* or *similitude character*; if we identify GSp_{2g} as the group of automorphisms of a $2g$-dimensional vector space that preserve a symplectic form s up to scaling, then $\mathbb{Q}_\ell(-1)$ is the representation η that sends an element of $\mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$ to the factor by which it scales s. Let $\mathbb{Q}_\ell(1)$ be the inverse (or dual) of $\mathbb{Q}_\ell(-1)$, and for an integer j, put $\mathbb{Q}_\ell(j) = \mathbb{Q}_\ell(\mathrm{sgn}\, j)^{\otimes|j|}$. For a representation U, put $U(j) := U \otimes \mathbb{Q}_\ell(j)$. With the standard representation W of GSp_{2g}, we can get irreducible representations W_λ, for $\lambda = (\lambda_1, \dots, \lambda_g)$ with $\lambda_1 \geq \cdots \geq \lambda_g \geq 0$, using the same construction as for USp_{2g} (see [FH91, (17.9)]). If we homogenize the polynomial $s_{\langle\lambda\rangle}(x_1, \dots, x_g, t)$ to degree $|\lambda|$ using a variable t of weight 2 and with x_i of weight 1 for $i = 1, \dots, g$,

[2] This is precisely [BHLGR23, Theorem 3.8], but we will give a different proof.

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

then for $A \in \mathrm{GSp}_{2g}$ with $\eta(A) = s$ and eigenvalues $\alpha_1, \dots, \alpha_g, s\alpha_1^{-1}, \dots, s\alpha_g^{-1}$, we have $\chi_\lambda(A) = s_{\langle\lambda\rangle}(\alpha_1, \dots, \alpha_g, s)$. Now, for every n, there are integers $c_{\lambda,n} \geq 0$ such that

$$W^{\otimes n} \cong \bigoplus_{|\lambda| \leq n} W_\lambda^{\oplus c_{\lambda,n}}\big((-n + |\lambda|)/2\big). \tag{2.2}$$

Note that if $n \not\equiv |\lambda| \bmod 2$, then $c_{\lambda,n} = 0$. Note also that (2.2) holds with the same $c_{\lambda,n}$ when replacing GSp_{2g} with USp_{2g}, i.e., replacing W by V and ignoring the multiplier representation. Note also that $W_\lambda^\vee \cong W_\lambda(|\lambda|)$.

Let $\mathcal{X} = \mathcal{H}_g, \mathcal{M}_g$ or $\mathcal{M}_g^{\mathrm{nhyp}}$ for any $g \geq 2$, or $\mathcal{X} = \mathcal{M}_{1,1}$. Let $\pi : \mathcal{Y} \to \mathcal{X}$ be the universal object and define the ℓ-adic local system $\mathbb{V} = R^1\pi_*\mathbb{Q}_\ell$. To any irreducible representation of GSp_{2g} (the symplectic pairing coming as above from the first cohomology group of the curves) corresponding to λ, we can then use Schur functors to define a local system $\mathbb{V}_\lambda$. Let H_c^j denote compactly supported ℓ-adic cohomology and Fr_q the geometric Frobenius acting on $\mathcal{X} \otimes \overline{\mathbb{F}}_q$. For general results on étale cohomology of stacks, see, for instance, [Sun12].

For almost all primes p, we have $H_c^j(\mathcal{X} \otimes \mathbb{C}, \mathbb{V}_\lambda) \cong H_c^j(\mathcal{X} \otimes \overline{\mathbb{Q}}_p, \mathbb{V}_\lambda) \cong H_c^j(\mathcal{X} \otimes \overline{\mathbb{F}}_p, \mathbb{V}_\lambda)$. From this, we get bounds on $\dim_{\mathbb{Q}_\ell} H_c^j(\mathcal{X} \otimes \overline{\mathbb{F}}_p, \mathbb{V}_\lambda)$ that are independent of p. This will tacitly be used below when we let q go to infinity.

Put $\overline{\mathcal{X}} = \mathcal{X} \otimes \overline{\mathbb{F}}_q$. The Lefschetz trace formula and (2.2) then tell us that

$$\begin{aligned} S_n(q, \mathcal{X}) &= \sum_{j=0}^{2\dim \mathcal{X}} (-1)^j \operatorname{Tr}(\mathrm{Fr}_q, H_c^j(\overline{\mathcal{X}}, \mathbb{V}_1^{\otimes n})) \\ &= \sum_\lambda c_{\lambda,n} \sum_{j=0}^{2\dim \mathcal{X}} (-1)^j \operatorname{Tr}(\mathrm{Fr}_q, H_c^j(\overline{\mathcal{X}}, \mathbb{V}_\lambda))\, q^{(n-|\lambda|)/2} \end{aligned}$$

(compare [BFvdG14, Section 8]). Since $\mathbb{V}_\lambda$ is pure of weight λ, it follows from Deligne's theory of weights [Del80, Sun12] that the trace of Frobenius on $H_c^j(\overline{\mathcal{X}}, \mathbb{V}_\lambda)$ is equal (after choosing an embedding of $\overline{\mathbb{Q}}_\ell$ in $\mathbb{C}$) to a sum of complex numbers with absolute value at most $q^{(j+|\lambda|)/2}$.

From this, we see that only when $j = 2\dim \mathcal{X}$ can we get a contribution to $\mathfrak{a}_n(\mathcal{X})$. Since $\mathcal{X}$ is a smooth Deligne–Mumford stack, Poincaré duality shows that for every i with $0 \leq i \leq 2\dim \mathcal{X}$, we have

$$H_c^{2\dim \mathcal{X} - i}(\overline{\mathcal{X}}, \mathbb{V}_\lambda) \cong H^i(\overline{\mathcal{X}}, \mathbb{V}_\lambda)^\vee(-\dim \mathcal{X} - |\lambda|).$$

The zeroth cohomology group of a local system consists of the global invariants, and among the irreducible local systems, only the constant local system $\mathbb{V}_{(0)} \cong \mathbb{Q}_\ell$ has such. Moreover, $H^0(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ is one-dimensional, since $\mathcal{X}$ is irreducible. Finally, since the action of Fr_q on $H^0(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ is trivial, we get by Poincaré duality that Fr_q acts on $H_c^{2\dim \mathcal{X}}(\overline{\mathcal{X}}, \mathbb{Q}_\ell)$ by multiplication by $q^{\dim \mathcal{X}}$. It follows that $\mathfrak{a}_n(\mathcal{X}) = c_{(0),n}$. This proves (1).

Assume now that $g \geq 3$. From the work of Johnson and Hain, we know that $H^1(\mathcal{M}_g, \mathbb{V}_\lambda)$ is nonzero if and only if $\lambda = (1,1,1)$ (see [Hai95, Joh83] and [Kab98, Theorem 4.1 and Corollary 4.2]). In these references, it is the rational Betti cohomology group of $\mathcal{M}_g$ over the complex numbers that is considered. Furthermore,

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

$H^1(\mathcal{M}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_{(1,1,1)})$ is one-dimensional and generated by the Gross–Schoen cycle, which lives in the second Chow group (see [PTY21, Remark 12.1 and Example 6.4]). Since this result also holds in ℓ-adic cohomology, as noted in [PTY21, Section 1.2], the action of Fr_q on this cohomology group is by multiplication by q^2.

Recall that $\dim \mathcal{M}_g = 3g-3$. By Poincaré duality, we find that the action of Fr_q on $H_c^{6g-7}(\mathcal{M}_g \otimes \overline{\mathbb{F}}_q, \mathbb{V}_{(1,1,1)})$ is by $q^{3g-3+3-2}$. We can now conclude the following. If n is even, then $c_{(1,1,1),n} = 0$, and so every eigenvalue of Frobenius contributing to $q^{3g-3+n/2}c_{(0),n} - S_n(q, \mathcal{M}_g)$ has absolute value at most $q^{3g-4+n/2}$. If n is odd, then $c_{(0),n} = 0$, and so there are no eigenvalues of Frobenius contributing to $S_n(q, \mathcal{M}_g)$ of absolute value $q^{3g-3+n/2}$ and we can conclude by the above that $\mathfrak{b}_n(\mathcal{M}_g) = c_{(1,1,1),n}$. This proves (2.1).

Because of the hyperelliptic involution, $H_c^i(\mathcal{M}_2, \mathbb{V}_\lambda) = 0$ for all λ such that $|\lambda|$ is odd. Moreover, $H^1(\mathcal{M}_2, \mathbb{V}_\lambda)$ is nonzero precisely when $\lambda = (2,2)$. It is then one-dimensional and Fr_q acts by multiplication by q^3. This result is proven but not stated explicitly in [Pet15, Pet16], as explained in [Wat18, Corollary 6.7]. By Poincaré duality, Fr_q acts on $H_c^5(\mathcal{M}_2, \mathbb{V}_{2,2})$ by multiplication by q^{3+4-3}. Hence, for all even n, every eigenvalue of Frobenius contributing to $q^{3+n/2}c_{(0),n} - S_n(q, \mathcal{M}_2)$ has absolute value at most $q^{3+(n-2)/2}$. This proves (2.1).

Statement (4) is only a reformulation of the properties of $\mathfrak{a}_n(\mathcal{M}_g)$ and $\mathfrak{b}_n(\mathcal{M}_g)$ proven above.

Finally, for every $k \geq 1$, put $p_k(x_1, \ldots, x_g) := \sum_{i=1}^g (x_i^k + x_i^{-k})$. The polynomial $\mathbf{s}_{\langle(1,1,1)\rangle}(x_1, \ldots, x_g)$ equals

$$\frac{1}{6}p_1^3 - \frac{1}{2}p_1p_2 + \frac{1}{3}p_3 - p_1.$$

The irreducible representations of USp_{2g} are self-dual. As a consequence, if U is a representation of USp_{2g}, then the number of times the representation V_λ appears in U equals the number of times the trivial representation appears in $V_\lambda \otimes U$. If $A \in \mathrm{USp}_{2g}$ has eigenvalues $\alpha_1, \ldots, \alpha_g, \alpha_1^{-1}, \ldots, \alpha_g^{-1}$, with $\alpha_j = e^{i\theta_j}$ for $j = 1, \ldots, g$, then $p_k(\alpha_1, \ldots, \alpha_g) = w_k(\theta_1, \ldots, \theta_g)$. Statement (5) now follows from (2.1). ∎

Remark 2.2 Why did we not define $\mathfrak{b}_n$ for $\mathcal{M}_{1,1}$? For every prime p and $n > 0$, it follows from [Del71] (see also [Bir68] and [BFvdG14, Section 2]) that

$$\begin{aligned}\sum_{j=0}^{2}(-1)^j \operatorname{Tr}(\mathrm{Fr}_p, H_c^j(\mathcal{M}_{1,1} \otimes \overline{\mathbb{F}}_p, \mathbb{V}_{(n)})) &= -\operatorname{Tr}(\mathrm{Fr}_p, H_c^1(\mathcal{M}_{1,1} \otimes \overline{\mathbb{F}}_p, \mathbb{V}_{(n)})) \\ &= -1 - \operatorname{Tr}(T_p, \mathbf{S}_{n+2}),\end{aligned}$$

where T_p is the pth Hecke operator acting on $\mathbf{S}_{n+2}$, the (complex) vector space of elliptic modular cusp forms of level 1 and weight $n+2$. Moreover, for every prime power q, the eigenvalues of Fr_q acting on $H_c^1(\mathcal{M}_{1,1} \otimes \overline{\mathbb{F}}_p, \mathbb{V}_{(n)})$ will have absolute value $q^{(n+1)/2}$. It is in general not clear that the limit

$$-\lim_{q\to\infty} \sqrt{q}\left(\frac{S_n(q, \mathcal{M}_{1,1})}{q^{1+n/2}} - \mathfrak{a}_n(\mathcal{M}_{1,1})\right), \tag{2.3}$$

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

which would be the way to define $\mathfrak{b}_n(\mathcal{M}_{1,1})$, always exists when n is even. (For odd n, $S_n(q, \mathcal{M}_{1,1}) = 0$; hence, the limit (2.3) will be 0.)

For even $0 \le n \le 8$, the limit (2.3) is also 0 since there are no elliptic cusp forms level 1 and weight less than or equal to 10. We then have that $S_{10}(p, \mathcal{M}_{1,1}) = 42p^6 - \mathrm{Tr}(T_p, \mathbf{S}_{12}) + O(p^5)$ and $S_{12}(p, \mathcal{M}_{1,1}) = 132p^7 - 11p \cdot \mathrm{Tr}(T_p, \mathbf{S}_{12}) + O(p^6)$. The so-called Frobenius angle, $0 \le \varphi_p \le \pi$, of the Hecke eigenform (the Ramanujan Δ function) in the one-dimensional space $\mathbf{S}_{12}$ is defined by $a_p := \mathrm{Tr}(T_p, \mathbf{S}_{12}) = 2p^{11/2}\cos\varphi_p$. The Sato–Tate conjecture for Δ (proven in [BLGHT11]) then tells us that there are sequences of primes $p_1', p_2', \ldots$ and $p_1'', p_2'', \ldots$ such that the Frobenius angles of $a_{p_1'}, a_{p_2'}, \ldots$ (respectively, $a_{p_1''}, a_{p_2''}, \ldots$) are all between 0 and $\pi/3$ (respectively, $2\pi/3$ and π). This implies that the limit (2.3) does not exist for $n = 10$ and $n = 12$. It is unlikely to exist for even $n > 12$, but the limit will then involve an interplay between different Hecke eigenforms.

In [BHLGR23, Theorem 3.9], it is shown that for fixed g, we have

$$\lim_{n\to\infty} \mathfrak{a}_{2n}(\mathcal{M}_g)^{1/(2n)} = 2g.$$

In the remainder of this section, we prove a similar result for $\mathfrak{b}_{2n+1}(\mathcal{M}_g)$.

Proposition 2.3 *For fixed $g \ge 3$, one has*

$$\lim_{n\to\infty} \mathfrak{b}_{2n+1}(\mathcal{M}_g)^{1/(2n+1)} = 2g.$$

Proof Consider the functions w_1 and $f := \frac{1}{6}w_1^3 - \frac{1}{2}w_1w_2 + \frac{1}{3}w_3 - w_1$ on $X := [0, \pi]^g$. The maximum value of $|w_1|$ is attained at exactly two points in X, namely the points $x := (0, \ldots, 0)$ and $y := (\pi, \ldots, \pi)$. We have $w_1(x) = 2g$ and $w_1(y) = -2g$, and we also have $f(x) = (2/3)(2g^3 - 3g^2 - 2g) > 0$ and $f(y) = (-2/3)(2g^3 - 3g^2 - 2g) < 0$.

Let V be the (open) subset of X where $w_1 f > 0$, so that x and y both lie in V, and let $W = X\backslash V$. Let M be the supremum of $|w_1|$ on W, so that $M < 2g$. For $\varepsilon \in (0, 2g - M)$, let U_ε be the subset of X where $|w_1| > 2g - \varepsilon$, so that $U_\varepsilon \subset V$, and let $V_\varepsilon = V\backslash U_\varepsilon$.

Then, for every n, we have

$$\begin{aligned}
\mathfrak{b}_{2n+1}(\mathcal{M}_g) &= \int_X w_1^{2n+1} f \, dm_g \\
&= \int_{U_\varepsilon} w_1^{2n+1} f \, dm_g + \int_{V_\varepsilon} w_1^{2n+1} f \, dm_g + \int_W w_1^{2n+1} f \, dm_g \\
&\ge \int_{U_\varepsilon} w_1^{2n+1} f \, dm_g + \int_W w_1^{2n+1} f \, dm_g \\
&\ge (2g - \varepsilon)^{2n+1} \int_{U_\varepsilon} |f| \, dm_g - M^{2n+1} \int_W |f| \, dm_g,
\end{aligned}$$

where the third line follows from the fact that $w_1^{2n+1} f$ is positive on V_ε and the fourth follows from the bounds on $|w_1|$ in U_ε and W. Let $A := \int_{U_\varepsilon} |f| \, dm_g$ and $B := \int_W |f| \, dm_g$. Then

$$\mathfrak{b}_{2n+1}(\mathcal{M}_g)^{1/(2n+1)} \ge (2g - \varepsilon)\left(A - \left(\frac{M}{2g - \varepsilon}\right)^{2n+1} B\right)^{1/(2n+1)},$$

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

and the rightmost factor tends to 1 as $n \to \infty$. Therefore, $\liminf \mathfrak{b}_{2n+1}(\mathcal{M}_g)^{1/(2n+1)} \geq 2g$.

We also have

$$\begin{aligned}\mathfrak{b}_{2n+1}(\mathcal{M}_g) &= \int_{U_\varepsilon} w_1^{2n+1} f \, dm_g + \int_{X \setminus U_\varepsilon} w_1^{2n+1} f \, dm_g \\ &\leq (2g)^{2n+1} \int_{U_\varepsilon} |f| \, dm_g + (2g-\varepsilon)^{2n+1} \int_{X \setminus U_\varepsilon} |f| \, dm_g,\end{aligned}$$

so if we let $C := \int_X |f| \, dm_g$, then $\mathfrak{b}_{2n+1}(\mathcal{M}_g) \leq (2g)^{2n+1} A + (2g-\varepsilon)^{2n+1} C$, so

$$\mathfrak{b}_{2n+1}(\mathcal{M}_g)^{1/(2n+1)} \leq 2g \left(A + \left(\frac{2g-\varepsilon}{2g} \right)^{2n+1} C \right)^{1/(2n+1)}.$$

Once again the rightmost factor tends to 1 as $n \to \infty$, so $\limsup \mathfrak{b}_{2n+1}(\mathcal{M}_g)^{1/(2n+1)} \leq 2g$, and the proposition is proven. ∎

Remark 2.4 Let $\mathcal{X}_g$ be either $\mathcal{M}_g$ or $\mathcal{M}_{g,1}$, where the latter denotes the moduli space of curves of genus g together with a marked point. For any $k \geq 0$, λ as in the proof of Theorem 2.1, and $g \geq \frac{3}{2}(k+1+|\lambda|)$, there is an isomorphism in Betti cohomology, $H^k(\mathcal{X}_g, \mathbb{V}_\lambda) \cong H^k(\mathcal{X}_{g+1}, \mathbb{V}_\lambda)$ (see [Loo96, Theorem 1.1] and [Wah13]). These are called *stable* cohomology groups.

In [BDPW23, Theorem 3.5.12], there is an alternative formula to that of [Loo96, Theorem 1.1] for the dimensions of the stable cohomology groups of $\mathcal{M}_g$. Using this formula, one can prove, in a way analogous to [BDPW23, Theorem 7.0.2], that if $k < |\lambda|/3$ and $g \geq \frac{3}{2}(k+1+|\lambda|)$, then $H^k(\mathcal{M}_g, \mathbb{V}_\lambda) = 0$. It follows that for each k, there are finitely many λ for which $H^k(\mathcal{M}_g, \mathbb{V}_\lambda)$, with $g = \lceil \frac{3}{2}(k+1+|\lambda|) \rceil$, is nonzero. Again using [BDPW23, Theorem 3.5.12], we find, for instance, that there are 5 such λ for $k = 2$ (see below) and 14 such λ for $k = 3$. Note also that for $g \geq \frac{3}{2}(k+1+|\lambda|)$, $H^k(\mathcal{M}_g, \mathbb{V}_\lambda)$ is zero if $k + |\lambda|$ is odd.

The result above also holds in ℓ-adic cohomology. Moreover, every eigenvalue of Frobenius F_q acting on the compactly supported ℓ-adic cohomology group $H_c^{6g-6-k}(\mathcal{M}_g, \mathbb{V}_\lambda)$, for $g \geq \frac{3}{2}(k+1+|\lambda|)$, is equal to $q^{3g-3+(|\lambda|-k)/2}$ (see, for instance, [PTY21]).

In [MPPR24], it is shown that for $g \geq 3k+3$ (i.e., a bound that is independent of λ), there is an isomorphism in Betti cohomology, $H^k(\mathcal{M}_{g,1}, \mathbb{V}_\lambda) \cong H^k(\mathcal{M}_{g+1,1}, \mathbb{V}_\lambda)$. It should be possible to show that this leads to an isomorphism $H^k(\mathcal{M}_g, \mathbb{V}_\lambda) \cong H^k(\mathcal{M}_{g+1}, \mathbb{V}_\lambda)$ for all $g \geq g_{\mathrm{stab}}(k)$, with $g_{\mathrm{stab}}(k)$ a function that only depends upon k (cf. [CM09] and [BDPW23, Remark 3.5.11]). If we assume this to be true, then we can combine the results above with the techniques in the proof of Theorem 2.1 to conclude the following.

Let $d_{n,\lambda}$ denote the number of times the representation V_λ appears in the USp_{2g}-representation $V^{\otimes n}$. Fix any $K \geq 0$. Then, for any $n \geq 1$ and $g \geq g_{\mathrm{stab}}(K)$, we have

$$\sum_{k=0}^{K} (-1)^k \, \mathfrak{c}_{k,n} \cdot q^{-k/2} = S_n(\mathcal{M}_g, q)/q^{3g-3+n/2} + O(q^{-(K+1)/2}), \tag{2.4}$$

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

where

$$\mathfrak{c}_{k,n} = \sum_{\lambda} d_{n,\lambda} \cdot \dim H^k(\mathcal{M}_{g_{\mathrm{stab}}(k)}, \mathbb{V}_\lambda).$$

From [BDPW23, Theorem 3.5.12], we can, for instance, compute that

$$\mathfrak{c}_{2,n} = d_{n,(0)} + d_{n,(1^2)} + d_{n,(1^4)} + d_{n,(1^6)} + d_{n,(2^2,1^2)}.$$

Note that by Theorem 2.1, $\mathfrak{c}_{0,n} = \mathfrak{a}_n(\mathcal{M}_g)$ for $g \geq 2$, $\mathfrak{c}_{1,n} = \mathfrak{b}_n(\mathcal{M}_g)$ for $g \geq 3$, and equation (2.4) holds with $g_{\mathrm{stab}}(0) = 2$ and $g_{\mathrm{stab}}(1) = 3$.

3 Convergence of moments of the measures $\mu_{q,g}$

Let $\mathcal{M}'_g(\mathbb{F}_q)$ be the set of $\mathbb{F}_q$-isomorphism classes of curves of genus $g > 1$ over $\mathbb{F}_q$. If $g = 1$, we abuse notation and let $\mathcal{M}_1 = \mathcal{M}_{1,1}$ be the moduli space of elliptic curves and $\mathcal{M}'_1(\mathbb{F}_q)$ the set of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$. Define a measure $\mu_{q,g}$ by

$$\mu_{q,g} := \frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{C \in \mathcal{M}'_g(\mathbb{F}_q)} \frac{\delta_{\tau(C)}}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)},$$

where $\tau(C) := \operatorname{Tr}(C)/\sqrt{q}$ is the *normalized trace* of C and $\delta_{\tau(C)}$ is the Dirac δ measure supported at $\tau(C)$. We see that $\mu_{q,g}$ is a discrete probability measure on $I_g := [-2g, 2g]$, since

$$\begin{aligned}\mu_{q,g}(I_g) &= \frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{C \in \mathcal{M}'_g(\mathbb{F}_q)} \frac{1}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)} \\ &= \frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{C \in \mathcal{M}_g(\mathbb{F}_q)} \underbrace{\sum_{C' \in \mathrm{Twist}(C)} \frac{1}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)}}_{=1 \text{ by [vdGvdV92, Prop. 5.1]}} = 1.\end{aligned}$$

We can introduce $\mathcal{N}_{q,g}(\tau)$ defined by

$$\mathcal{N}_{q,g}(\tau) := \frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{C \in \mathcal{M}'_g(\mathbb{F}_q), \tau(C) = \tau} \frac{1}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)}$$

and rewrite $\mu_{q,g} = \sum_{\tau \in I_g} \mathcal{N}_{q,g}(\tau)\delta_\tau$. Note that the definition of $\mathcal{N}_{q,g}(\tau)$ differs from the ones of [LRRS14, Appendix B] and [LRR+19, Section 4], in particular by a factor of $\sqrt{q}$ (this factor will appear again in Section 4, but this definition is more natural for the measure).

From [Lac16, Remark 3.5], as a direct consequence of Katz–Sarnak results [KS99, Theorems 10.7.12 and 10.8.2], there exists a probability measure $\mu_g : I_g \to \mathbb{R}$ with a $\mathcal{C}^\infty$ density function $\mathfrak{f}_g$ such that we have weak convergence of $\mu_{q,g}$ to μ_g. Writing

$$\mathfrak{f}_g(\tau) = \int_{A_\tau} dm_g \quad \text{with } A_\tau = \left\{(\theta_1, \ldots, \theta_g) \in [0, \pi]^g : \textstyle\sum_j 2\cos\theta_j = \tau\right\},$$

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

we see this is equivalent to

$$\lim_{q\to\infty} \int_{I_g} f\, d\mu_{q,g} = \int_{I_g} f(\tau)\mathfrak{f}_g(\tau)\, d\tau \tag{3.1}$$

for all continuous functions $f\colon I_g \to \mathbb{R}$. Moreover, for all polynomial functions[3] $P\colon I_g \to \mathbb{R}$,

$$\int_{I_g} P\, d\mu_{q,g} = \int_{I_g} P(\tau)\mathfrak{f}_g(\tau)\, d\tau + O\left(\frac{1}{\sqrt{q}}\right). \tag{3.2}$$

We will now find a refinement of (3.2) when $g \geq 2$.

Theorem 3.1 *Let*

$$\mathfrak{h}_g(\tau) = \int_{A_\tau} \left(\frac{1}{6}w_1^3 - \frac{1}{2}w_1w_2 + \frac{1}{3}w_3 - w_1\right) dm_g \tag{3.3}$$

be the function whose nth moments are equal to the numbers $\mathfrak{b}_n(\mathcal{M}_g)$ given by the expression (2.1). For $g \geq 2$ and every polynomial function $P : I_g \to \mathbb{R}$, we have

$$\int_{I_g} P\, d\mu_{q,g} = \int_{I_g} P(\tau)\left(\mathfrak{f}_g(\tau) - \frac{\mathfrak{h}_g(\tau)}{\sqrt{q}}\right) d\tau + O\left(q^{-1}\right). \tag{3.4}$$

Proof Notice that

$$\frac{S_n(q,\mathcal{M}_g)}{\#\mathcal{M}_g(\mathbb{F}_q)\cdot q^{n/2}} = \int_{I_g} \tau^n\, d\mu_{q,g}.$$

Using Deligne's theory of weights, as in the proof of Theorem 2.1, we find that

$$\#\mathcal{M}_g(\mathbb{F}_q) = \mathrm{Tr}\big(\mathrm{Fr}_q, H_c^{6g-6}(\mathcal{M}_g,\mathbb{Q}_\ell)\big) + O\left(q^{3g-4}\right) = q^{3g-3} + O\left(q^{3g-4}\right),$$

since $\mathcal{M}_g$ is irreducible of dimension $3g-3$. Hence,

$$\frac{S_n(q,\mathcal{M}_g)}{\#\mathcal{M}_g(\mathbb{F}_q)\cdot q^{n/2}} = \frac{S_n(q,\mathcal{M}_g)}{q^{3g-3+n/2}} + O(q^{-1}).$$

Using Theorem 2.1 (4) for $g \geq 2$, we then get

$$\begin{aligned}
\int_{I_g} \tau^n\, d\mu_{q,g} &= \frac{S_n(q,\mathcal{M}_g)}{\#\mathcal{M}_g(\mathbb{F}_q)\cdot q^{n/2}} \\
&= \frac{S_n(q,\mathcal{M}_g)}{q^{3g-3+n/2}} + O(q^{-1}) \\
&= \mathfrak{a}_n(\mathcal{M}_g) - \frac{\mathfrak{b}_n(\mathcal{M}_g)}{\sqrt{q}} + O(q^{-1}) \\
&= \int_{I_g} \tau^n \left(\mathfrak{f}_g(\tau) - \frac{\mathfrak{h}_g(\tau)}{\sqrt{q}}\right) d\tau + O\left(q^{-1}\right).
\end{aligned}$$

■

[3] In an earlier version and in [BHLGR23] following [Lac16, Corollary 4.3], we wrote that this convergence rate holds for any continuous function. We cannot find a proof for this and prefer to state it now only for polynomial functions as Katz and Sarnark do. Fortunately, this change has no consequence on the rest of [BHLGR23]: for instance, Corollary 2.3 can be proven only using the pointwise convergence of the cumulative distributions which is equivalent to the weak convergence above.

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

4 The elliptic and hyperelliptic cases: results and experiments

Katz–Sarnak results show that for every interval $J \subseteq I_g$, the probability that a random curve of genus g over $\mathbb{F}_q$ (or a random hyperelliptic curve of genus g over $\mathbb{F}_q$) has normalized trace in J tends toward a fixed value as $q \to \infty$, this value being $\int_J \mathfrak{f}_g(\tau)\, d\tau$, where $\mathfrak{f}_g$ is the density function for the measure μ_g defined at the beginning of Section 3. Here, the interval J is fixed, and we let q tend to infinity. One can wonder how rapid this convergence is. For instance, suppose the interval J has length x. How large must q become in order for the actual probability that a normalized trace lies in J is well-approximated by the Katz–Sarnak prediction? Could it even be the case that the approximation is reasonably good when q is as large as $1/x^2$, so that $x \approx 1/\sqrt{q}$ and there is exactly one integer t with $t/\sqrt{q} \in J$? In other words, can we use the Katz–Sarnak distribution to estimate the number of curves over $\mathbb{F}_q$ with a given trace? Since the measures $\mu_{q,g}$ converge weakly to μ_g, one might hope that for every $\tau \in I_g$, the integral of $\mu_{q,g}$ over an interval of length $1/\sqrt{q}$ containing τ would be close to the integral of μ_g over this interval. If we let t be the unique integer such that $t/\sqrt{q}$ is contained in this interval, this optimistic approximation then translates to

$$\sqrt{q}\,\mathcal{N}_{q,g}\left(\frac{t}{\sqrt{q}}\right) \approx \mathfrak{f}_g\left(\frac{t}{\sqrt{q}}\right).$$

Since $\mathcal{N}_{q,g}(t/\sqrt{q})$ gives us the weighted number of curves with trace t, if this approximation is close to the truth, we would have a good estimate for the number of such curves.

Remark 4.1 We do not know how to prove that this estimate holds, and indeed we will see below that it does *not* hold, without modification, for hyperelliptic curves. One consequence of this estimate, however, is the much weaker statement that for every fixed value of t, the value of $\mathcal{N}_{q,g}(t)$ converges to 0 as q increases. It is at least easy to show that this weaker statement holds for $t = 0$, by the following argument.

Given $\varepsilon > 0$, let $f\colon I_g \to [0,1]$ be a continuous function with $f(0) = 1$ and with $f(\tau) = 0$ when $|\tau| \geq \varepsilon$. From (3.1), we find that for q large enough, we have

$$\left| \int_{I_g} f\, d\mu_{q,g} - \int_{I_g} f(\tau)\mathfrak{f}_g(\tau)\, d\mu_g \right| \leq \varepsilon.$$

Hence,

$$0 \leq \mathcal{N}_{q,g}(0) \leq \int_{I_g} f\, d\mu_{q,g} \leq \int_{|\tau|<\varepsilon} f(\tau)\mathfrak{f}_g(\tau)\, d\tau + \varepsilon \leq (2\left\|\mathfrak{f}_g\right\|_\infty + 1)\varepsilon.$$

As we intimated in the preceding remark, for hyperelliptic curves, we can prove that the naïve approximation for $\mathcal{N}_{q,g}$ described above cannot hold. To state our result precisely, we introduce a function $\mathcal{N}^{\mathrm{hyp}}_{q,g}(\tau)$, which we define analogously to how we defined $\mathcal{N}_{q,g}(\tau)$:

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

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

Here, by $\mathcal{H}_g(\mathbb{F}_q)$, we mean the set of $\overline{\mathbb{F}}_q$-isomorphism classes of hyperelliptic curves of genus g over $\mathbb{F}_q$, and by $\mathcal{H}'_g(\mathbb{F}_q)$, we mean the set of $\mathbb{F}_q$-isomorphism classes of such curves. Note that for an integer t in I_g, the value $q^{2g-1}\mathcal{N}^{\mathrm{hyp}}_{q,g}(t/\sqrt{q})$ is then the weighted number of genus-g hyperelliptic curves over $\mathbb{F}_q$ with trace t.

Proposition 4.2 *Fix $g > 1$ and $\varepsilon \in [0, 2g)$, let $r_g := \sum_{i=0}^{2g+2}(-2)^i/i!$, and let $\nu = \int_{2g-\varepsilon}^{2g} \mathfrak{f}_g(\tau)\,d\tau$. Suppose there are constants $b_g \le c_g$ such that for every sufficiently large prime power q and for every integer t in $[-(2g-\varepsilon)\sqrt{q}, (2g-\varepsilon)\sqrt{q}\,]$, we have*

$$\frac{b_g}{\sqrt{q}}\mathfrak{f}_g\left(\frac{t}{\sqrt{q}}\right) \le \mathcal{N}^{hyp}_{q,g}\left(\frac{t}{\sqrt{q}}\right) \le \frac{c_g}{\sqrt{q}}\mathfrak{f}_g\left(\frac{t}{\sqrt{q}}\right).$$

Then $b_g \le (1-r_g)/(1-2\nu)$ and $c_g \ge (1+r_g-4\nu)/(1-2\nu)$.

The proof is based on the following lemma.

Lemma 4.3 *Fix $g > 1$, and let r_g be as in Proposition 4.2. If q is an odd prime power, then*

$$\sum_{t\ even} \mathcal{N}^{hyp}_{q,g}\left(\frac{t}{\sqrt{q}}\right) = \frac{1+r_g}{2} + O\left(\frac{1}{q}\right) \quad \text{and} \quad \sum_{t\ odd} \mathcal{N}^{hyp}_{q,g}\left(\frac{t}{\sqrt{q}}\right) = \frac{1-r_g}{2} + O\left(\frac{1}{q}\right).$$

Proof Fix an odd prime power q, fix a nonsquare $n \in \mathbb{F}_q$, and consider the set H consisting of all pairs (c, f), where $c \in \{1, n\}$ and $f \in \mathbb{F}_q[x]$ is a monic separable polynomial of degree $2g+1$ or $2g+2$. A result of Carlitz [Car32, Section 6] shows that $\#H = 2q^{2g+2} - 2q^{2g}$. The group $\mathrm{PGL}_2(\mathbb{F}_q)$ acts on H: Given a matrix $\left[\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right]$ and an element (c, f) of H, let (d, g) be the unique element of H such that

$$dg(x) = ce^2(tx+u)^{2g+2} f\left(\frac{rx+s}{tx+u}\right)$$

for some $e \in \mathbb{F}_q^\times$. Note that the stabilizer of (c, f) is isomorphic to the reduced automorphism group $\mathrm{RedAut}(C)$ of the hyperelliptic curve $C: y^2 = cf$, that is, the quotient of the full automorphism group of C by the subgroup generated by the hyperelliptic involution.

The map γ that sends $(c, f) \in H$ to the hyperelliptic curve $y^2 = cf$ takes H onto $\mathcal{H}'_g(\mathbb{F}_q)$. Given a curve $C \in \mathcal{H}'_g(\mathbb{F}_q)$, let $(c, f) \in H$ be such that $\gamma((c, f)) = C$. Then

$$\#(\mathrm{PGL}_2(\mathbb{F}_q) \cdot (c, f)) = \frac{\#\,\mathrm{PGL}_2(\mathbb{F}_q)}{\#\,\mathrm{RedAut}(C)},$$

so that

$$\frac{\#\gamma^{-1}(C)}{\#\,\mathrm{PGL}_2(\mathbb{F}_q)} = \frac{1}{\#\,\mathrm{RedAut}(C)} = \frac{2}{\#\,\mathrm{Aut}(C)}. \tag{4.1}$$

Let H_{even} be the subset of H consisting of the pairs (c, f) such that the curve $\gamma(c, f)$ has even trace. Let H'_{even} be the subset of H consisting of the pairs (c, f) such that f has degree $2g+2$ and has an even number of roots. Then $H'_{\mathrm{even}} \subseteq H_{\mathrm{even}}$, and $H_{\mathrm{even}} \backslash H'_{\mathrm{even}}$

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

consists of pairs $(c, f) \in H_{\text{even}}$ such that f has degree $2g+1$. Therefore,

$$\left|\#H_{\text{even}} - \#H'_{\text{even}}\right| \le 2q^{2g+1}.$$

Leont'ev [Leo06a, Lemma 4, p. 302] gives the generating function for the number of (not necessarily separable) monic polynomials of a fixed degree over $\mathbb{F}_q$ that have a given number of roots. To find the number of such polynomials with an even number of roots, we simply need to take the average of the values of this generating function evaluated at -1 and at 1. We find that

$$\#\left\{\begin{matrix}\text{monic polynomials of degree } 2g+2\\ \text{over } \mathbb{F}_q \text{ with an even number of roots}\end{matrix}\right\} = \frac{1+r_g}{2}q^{2g+2} + O(q^{2g+1}).$$

The result of Carlitz mentioned earlier shows that

$$\#\left\{\begin{matrix}\text{non-separable monic polynomials}\\ \text{of degree } 2g+2 \text{ over } \mathbb{F}_q\end{matrix}\right\} = q^{2g+1}.$$

Therefore, $\#H'_{\text{even}} = (1+r_g)q^{2g+2} + O(q^{2g+1})$, so that $\#H_{\text{even}} = (1+r_g)q^{2g+2} + O(q^{2g+1})$ as well.

Using (4.1), we see that

$$\begin{aligned}
\sum_{t \text{ even}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right) &= \frac{1}{\#\mathcal{H}_g(\mathbb{F}_q)} \sum_{\substack{C \in \mathcal{H}'_g(\mathbb{F}_q)\\ \operatorname{Tr}(C) \text{ even}}} \frac{1}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)}\\
&= \frac{1}{\#\mathcal{H}_g(\mathbb{F}_q)} \sum_{\substack{C \in \mathcal{H}'_g(\mathbb{F}_q)\\ \operatorname{Tr}(C) \text{ even}}} \frac{\#\gamma^{-1}(C)}{2\#\operatorname{PGL}_2(\mathbb{F}_q)}\\
&= \frac{1}{2\#\mathcal{H}_g(\mathbb{F}_q)\#\operatorname{PGL}_2(\mathbb{F}_q)} \#H_{\text{even}}\\
&= \frac{1}{2q^{2g-1}(q^3-q)}\left((1+r_g)q^{2g+2} + O(q^{2g+1})\right)\\
&= \frac{1+r_g}{2} + O\left(\frac{1}{q}\right).
\end{aligned}$$

This gives us the first equality in the conclusion of the lemma. The second follows analogously. ∎

Proof of Proposition 4.2 Suppose the hypothesis of the proposition holds for a given g and ε. For a given q, we let $m = \lfloor 2\sqrt{q} \rfloor$ and we consider several subintervals of $[-2g\sqrt{q}, 2g\sqrt{q}]$:

$$\begin{aligned}
J_0 &:= \left[-mg, mg\right], & J_2 &:= \left[-2g\sqrt{q}, -(2g-\varepsilon)\sqrt{q}\right),\\
J_1 &:= \left[-(2g-\varepsilon)\sqrt{q}, (2g-\varepsilon)\sqrt{q}\right], & J_3 &:= \left((2g-\varepsilon)\sqrt{q}, 2g\sqrt{q}\right].
\end{aligned}$$

Now we interpret the sum

$$S_{\text{even}} := \sum_{t \text{ even}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right)$$

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

in two ways. On the one hand, from Lemma 4.3, we have

$$S_{\text{even}} = \left(\frac{1+r_g}{2}\right) + O\left(\frac{1}{q}\right).$$

On the other hand, for q large enough, we have

$$\begin{aligned} S_{\text{even}} &= \sum_{\substack{t\in J_1\\ t \text{ even}}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right) + \sum_{\substack{t\in J_2\\ t \text{ even}}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right) + \sum_{\substack{t\in J_3\\ t \text{ even}}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right) \\ &= \sum_{\substack{t\in J_1\\ t \text{ even}}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right) + 2\sum_{\substack{t\in J_3\\ t \text{ even}}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right) \\ &\le \frac{c_g}{2} \sum_{\substack{t\in J_1\\ t \text{ even}}} \mathfrak{f}_g\left(\frac{t}{\sqrt{q}}\right)\left(\frac{2}{\sqrt{q}}\right) + 2\sum_{t\in J_3} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right). \end{aligned} \tag{4.2}$$

The first sum in (4.2) is a Riemann sum for the integral of $\mathfrak{f}_g(\tau)\,d\tau$ over the interval $[-2g+\varepsilon, 2g-\varepsilon]$, so as $q\to\infty$ the first term in (4.2) approaches $c_g(1-2\nu)/2$. The second sum is the measure, with respect to $\mu_{q,g}$, of the interval $[2g-\varepsilon, 2g]$. Since the $\mu_{q,g}$ converge weakly to μ_g, the second term of (4.2) approaches 2ν as $q\to\infty$.

Combining these two interpretations of S_{even}, we find that

$$\left(\frac{1+r_g}{2}\right) \le \frac{c_g(1-2\nu)}{2} + 2\nu$$

so that $c_g \ge (1+r_g-4\nu)/(1-2\nu)$.

Similarly, we can consider the sum

$$S_{\text{odd}} := \sum_{t \text{ odd}} \mathcal{N}^{\text{hyp}}_{q,g}\left(\frac{t}{\sqrt{q}}\right).$$

From Lemma 4.3, we see that

$$S_{\text{odd}} = \left(\frac{1-r_g}{2}\right) + O\left(\frac{1}{q}\right).$$

But we also have

$$S_{\text{odd}} \ge \frac{b_g}{2} \sum_{\substack{t\in J_1\\ t \text{ odd}}} \mathfrak{f}_g\left(\frac{t}{\sqrt{q}}\right)\left(\frac{2}{\sqrt{q}}\right),$$

and the expression on the right approaches $b_g(1-2\nu)/2$ as $q\to\infty$. This shows that

$$\left(\frac{1-r_g}{2}\right) \ge \frac{b_g(1-2\nu)}{2},$$

so we find that $b_g \le (1-r_g)/(1-2\nu)$. ∎

Remark 4.4 In the statement of Proposition 4.2, we only assume that the condition on $\mathcal{N}^{\text{hyp}}_{q,g}(t/\sqrt{q})$ holds for t more than $\varepsilon\sqrt{q}$ away from the ends of the interval

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

$[-2g\sqrt{q}, 2g\sqrt{q}\,]$ because when $|t| > g\lfloor 2\sqrt{q}\rfloor$ we have $\mathcal{N}^{\mathrm{hyp}}_{q,g}(t/\sqrt{q}) = 0$. If we did not exclude the tail ends of the interval, the hypothesis of the proposition would only hold if we took $b_g = 0$, which is not an interesting approximation.

Figure 1 shows the value of $\mathcal{N}^{\mathrm{hyp}}_{q,g}(t/\sqrt{q})$ for all integers $t \in [-4\sqrt{q}, 4\sqrt{q}]$, where $q = 1,009$, together with the density function $\mathfrak{f}_2$ for the limiting Katz–Sarnak measure, scaled by the two factors $b = 38/45$ and $c = 52/45$ given by Proposition 4.2 for $g = 2$ and $\varepsilon = 0$.

The key to Proposition 4.2 is the imbalance between the likelihood of even versus odd traces for hyperelliptic curves. The obvious work-around would be to scale the counts for the even and odd traces by the factors given in the proposition for $\varepsilon = 0$. One can ask whether the scaled curve counts then better match the limiting Katz–Sarnak distribution. Figure 2 suggests that perhaps this parity factor is the main obstruction to obtaining decent estimates from the naïve Katz–Sarnak approximation.

The proof of Proposition 4.2 carries through for elliptic curves exactly as it does for hyperelliptic curves of a given genus $g > 1$. We do not include genus-1 curves in the statement of the proposition, however, because as we will see in Proposition 4.5, for $g = 1$ there is no value of c_1 that satisfies the hypothesis of the proposition when $\varepsilon \le 1$, while the conclusion of the proposition is trivial when $\varepsilon > 1$ because the resulting upper bound on b_1 will be greater than 1 and the lower bound on c_1 will be less than 1.

When $g = 1$, the density function of the limiting Katz–Sarnak measure on I_1 is $\mathfrak{f}_1 = (2\pi)^{-1}\sqrt{4-\tau^2}$. Let $N_{q,t}$ denote the weighted number of elliptic curves over $\mathbb{F}_q$ with trace t. For some values of t in $[-2\sqrt{q}, 2\sqrt{q}\,]$, we have $N_{q,t} = 0$; in addition to those t with $|t| > \lfloor 2\sqrt{q}\rfloor$, this happens for most values of t that are not coprime to q. But even if we exclude these values, and even if we restrict attention to values of t that are near the center of the interval $[-2\sqrt{q}, 2\sqrt{q}\,]$, the following proposition shows that we cannot hope to approximate $N_{q,t}$ by the quantity

$$q^{1/2}\mathfrak{f}_1\left(\frac{t}{\sqrt{q}}\right) = \frac{1}{2\pi}\sqrt{4q-t^2}\,.$$

Proposition 4.5 *For every $c > 0$, there are infinitely many values of q and t such that $|t| \le \sqrt{q}$ and $N_{q,t} > c\sqrt{4q-t^2}$.*

Proof Let Δ_0 be a fundamental quadratic discriminant with $\Delta_0 < -4$, and let χ be the quadratic character modulo Δ_0. For a given value of n, let f be the product of the first n primes p that are inert in $\mathbb{Q}(\sqrt{\Delta_0})$. Since the product over all inert primes of $1 + 1/p$ diverges (see [Cox13, Lemma 1.14] and [Apo76, Exercise 6, p. 176]), when n is large enough, we have

$$\prod_{p\mid f}\left(1+\frac{1}{p}\right) > \frac{c\pi^2}{3}\frac{\sqrt{|\Delta_0|}}{h(\Delta_0)}\,.$$

Choose n so that this holds, and let q_0 be a prime of the form $x^2 - f^2\Delta_0 y^2$, where x and y are positive integers. Note that x must be coprime to q_0 because $0 < x < q_0$. Let $\varpi = x + fy\sqrt{\Delta_0}$, viewed as an element of the upper half plane. Since x is coprime to q_0, ϖ is the Weil number of an isogeny class of ordinary elliptic curves over $\mathbb{F}_{q_0}$.

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

Let θ be the argument of ϖ, and let m be the smallest integer such that $\pi/3 \le m\theta < 2\pi/3$. Write $\varpi^m = u + fv\sqrt{\Delta}$ for integers u and v, let $q = q_0^m = u^2 - f^2v^2\Delta$, and let $t = 2u$. Then ϖ^m is the Weil number for an isogeny class $\mathcal{I}$ of ordinary elliptic curves over $\mathbb{F}_q$, and the trace of this isogeny class is t. We have $|t| \le \sqrt{q}$ because the argument of ϖ^m lies between $\pi/3$ and $2\pi/3$.

The number of elliptic curves in the isogeny class $\mathcal{I}$ is equal to the Kronecker class number $H(\Delta)$ of the discriminant $\Delta := t^2 - 4q = 4f^2v^2\Delta_0$. By [How22, p. 696], we have

$$H(\Delta) = h(\Delta_0) \prod_{p^e \| F} \left(1 + \left(1 - \tfrac{\chi(p)}{p}\right)(p + \cdots + p^e)\right),$$

where $F = 2fv$, so

$$\frac{H(\Delta)}{\sqrt{4q - t^2}} = \frac{h(\Delta_0)}{\sqrt{|\Delta_0|}} \prod_{p^e \| F} \left(p^{-e} + \left(1 - \tfrac{\chi(p)}{p}\right)(1 + p^{-1} + \cdots + p^{1-e})\right).$$

Now,

$$p^{-e} + \left(1 - \tfrac{\chi(p)}{p}\right)(1 + p^{-1} + \cdots + p^{1-e}) \ge \begin{cases} 1 + 1/p, & \text{if } \chi(p) = -1, \\ 1 - 1/p^2, & \text{if } \chi(p) \ne -1, \end{cases}$$

so we have

$$\begin{aligned} \frac{H(\Delta)}{\sqrt{4q - t^2}} &\ge \frac{h(\Delta_0)}{\sqrt{|\Delta_0|}} \prod_{\substack{p \mid F \\ \chi(p) = -1}} \left(1 + \frac{1}{p}\right) \prod_{\substack{p \mid F \\ \chi(p) \ne -1}} \left(1 - \frac{1}{p^2}\right) \\ &\ge \frac{h(\Delta_0)}{\sqrt{|\Delta_0|}} \prod_{p \mid f} \left(1 + \frac{1}{p}\right) \prod_{p} \left(1 - \frac{1}{p^2}\right) \\ &\ge \frac{h(\Delta_0)}{\sqrt{|\Delta_0|}} \left(\frac{c\pi^2}{3} \frac{\sqrt{|\Delta_0|}}{h(\Delta_0)}\right)\left(\frac{6}{\pi^2}\right) \\ &\ge 2c. \end{aligned}$$

Since the curves in $\mathcal{I}$ are ordinary and the discriminants of their endomorphism rings are neither -3 nor -4, they all have automorphism groups of order 2, so $N_{q,t} = H(\Delta)/2$. It follows that

$$N_{q,t} \ge c\sqrt{4q - t^2},$$

as claimed. ∎

Figure 3 shows the weighted number of elliptic curves over $\mathbb{F}_{1000003}$ of each possible trace, as well as the limiting density function $\mathfrak{f}_1(\tau) = (2/\pi)\sqrt{4 - \tau^2}$. We see that the plotted points do not appear to be near the density function.

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

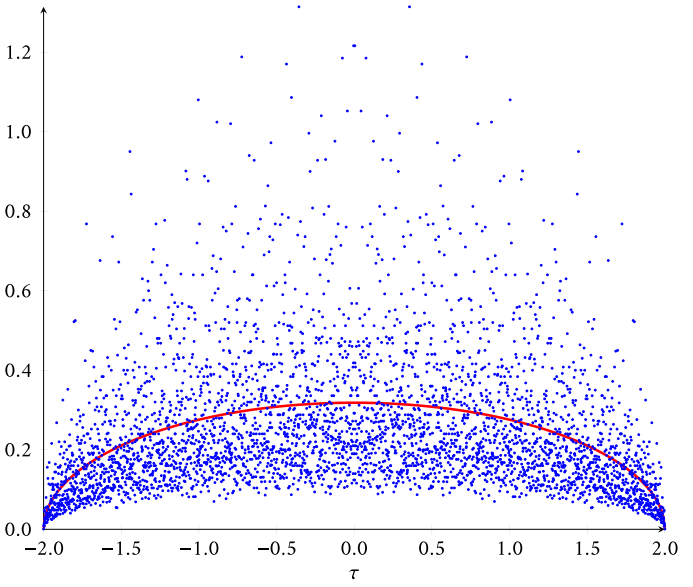

Figure 3: Data for elliptic curves over $\mathbb{F}_q$ for $q = 1,000,003$. The blue dots are the points $(t/\sqrt{q}, N_{q,t}/\sqrt{q})$ for $t \in [-2000, 2000]$, where $N_{q,t}$ is the weighted number of elliptic curves over $\mathbb{F}_q$ with trace t. The red curve is the density function $\mathfrak{f}_1(\tau) = (2\pi)^{-1}\sqrt{4-\tau^2}$ of the distribution μ_1.

5 The non-hyperelliptic case: experiments and conjectures

We consider now the case of non-hyperelliptic curves of genus $g = 3$. For this purpose, for $g \geq 3$, we introduce the function $\mathcal{N}_{q,g}^{\mathrm{nhyp}}(\tau)$, which we define analogously to how we defined $\mathcal{N}_{q,g}(\tau)$ and $\mathcal{N}_{q,g}^{\mathrm{hyp}}(\tau)$:

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

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. The associated measures will still weakly converge to the measure μ_g with density $\mathfrak{f}_g$. But experimentally, the behavior looks much smoother than in the elliptic or hyperelliptic cases as illustrated by Figure 4 for $g = 3$ and $q = 53$.[4] Note that a similar behavior would certainly hold considering all curves of genus 3.

[4] When using the data of [LRRS14] to draw this figure, we noticed that there were some errors in the code when computing the automorphism group of twists for small dimensional strata, giving 728 extra "weighted" curves. This is a very small proportion with respect to $53^6 + 1$ curves and does not affect the general shape of the curve.

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

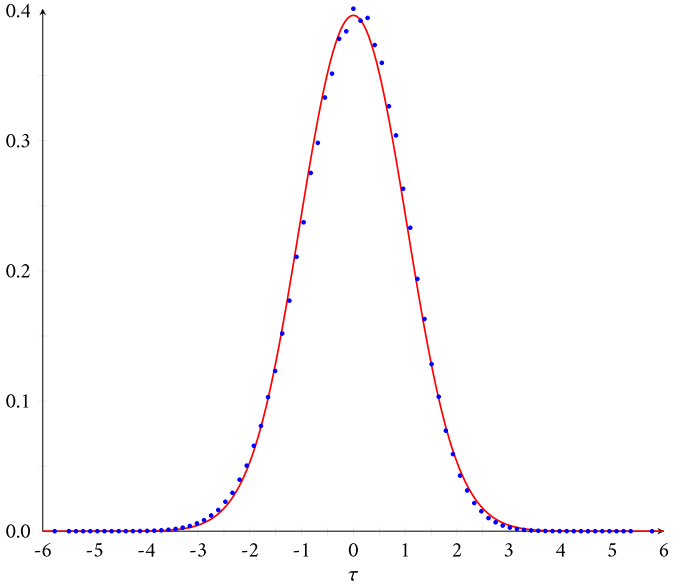

Figure 4: Data for non-hyperelliptic curves of genus 3 over $\mathbb{F}_q$ for $q = 53$. The blue dots are the points $(t/\sqrt{q}, \sqrt{q}\,\mathcal{N}_{q,3}(t/\sqrt{q}))$ for integers $t \in [-42, 42]$. The red curve is the function $\mathfrak{f}_3(\tau)$.

Heuristically, these patterns could be understood as an averaging for a given trace over several isogeny classes, but this idea does not work for the hyperelliptic locus as we have seen in Section 4 and something more is needed for a family of curves to "behave nicely." Still, the experimental data in genus 3 lead us to state the following conjecture.

Conjecture 5.1 *Let $g \geq 3$. For all $\tau \in I_g$, for all $\varepsilon > 0$, and for all large enough q, there exists $t \in \mathbb{N}$ such that $|\tau - t/\sqrt{q}| < 1/(2\sqrt{q})$ and $|\sqrt{q} \cdot \mathcal{N}_{q,g}^{nhyp}(t/\sqrt{q}) - \mathfrak{f}_g(t/\sqrt{q})| < \varepsilon$.*

Another way to phrase this conjecture is to replace the measure $\mu_{q,g}$ by a measure with density given by the histogram with height $\sqrt{q} \cdot \mathcal{N}_{q,g}^{\mathrm{nhyp}}(t/\sqrt{q})$ and base centered at $t/\sqrt{q}$ of length $1/\sqrt{q}$ for all $t \in [-2g\sqrt{q}, 2g\sqrt{q}]$. The conjecture asserts that the densities of these measures converge to the density $\mathfrak{f}_g$ at each point of I_g. This is stronger than weak convergence of the measures [Sch47].

We now conclude by looking at the symmetry breaking for the trace distribution of (non-hyperelliptic) genus 3 curves. In general, if C is a hyperelliptic curve of genus g over $\mathbb{F}_q$ with trace t, then its quadratic twist for the hyperelliptic involution has trace $-t$ and therefore the distribution of the number of hyperelliptic curves of genus g over $\mathbb{F}_q$ as a function of their trace is symmetric. For non-hyperelliptic curves, the distribution has no reason to be symmetric anymore. Actually, if a principally polarized abelian variety over $\mathbb{F}_q$ is the Jacobian (over $\mathbb{F}_q$) of a non-hyperelliptic curve, then its quadratic twist is never a Jacobian. This obstruction, known as *Serre's obstruction*, is a huge obstacle to finding a closed formula for the maximal number of rational points for

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

$g = 3$ [Lau02], whereas such formulas are known for $g = 1$ [Deu41] and $g = 2$ [Ser83]. Although we cannot improve on the state-of-the-art of this question, we can study this asymmetry with the probabilistic angle and the results we got before.

To visualize this asymmetry, let us consider the signed measure $\nu_{q,g} = \mu_{q,g} - (-1)^*\mu_{q,g}$ where $(-1)^*\mu_{q,g}$ is the discrete image signed measure defined by

$$(-1)^*\mu_{q,g} = \frac{1}{\#\mathcal{M}_g(\mathbb{F}_q)} \sum_{C \in \mathcal{M}'_g(\mathbb{F}_q)} \frac{\delta_{-\tau(C)}}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)}.$$

We get the following consequence of Theorem 2.1.

Proposition 5.2 *The sequence of signed measures $(\nu_{q,g})$ weakly converges to the 0 measure.*

Proof By definition, the even moments of $\nu_{q,g}$ are zero. By Theorem 2.1, the odd moments of $\sqrt{q}\,\nu_{q,g}$ are equal to

$$2\frac{S_n(q, \mathcal{M}_g)}{q^{3g-3+(n-1)/2}} = -2\mathfrak{b}_n(\mathcal{M}_g) + O\left(\frac{1}{\sqrt{q}}\right).$$

Hence, all moments of $\nu_{q,g}$ are 0. Now, if f is any continuous function on the compact interval $I_g = [-2g, 2g]$, then by the Stone–Weierstrass theorem, for every $\varepsilon > 0$, we can find a polynomial P such that $|f(\tau) - P(\tau)| \leq \varepsilon$ for all $\tau \in I_g$. Therefore, we have

$$\left|\int_{I_g} f\, d\nu_{q,g}\right| \leq \left|\int_{I_g} (f - P)\, d\nu_{q,g} + \int_{I_g} P\, d\nu_{q,g}\right| \leq \varepsilon \|\nu_{q,g}\| + \left|\int_{I_g} P\, d\nu_{q,g}\right|.$$

The last term is a sum of moments which converges to 0 when q goes to infinity. The variation of $\nu_{g,q}$ is also uniformly bounded since

$$\|\nu_{q,g}\| = |\nu_{q,g}|(I_g) = \sum_{\tau} \left|\mathcal{N}_{q,g}(\tau) - \mathcal{N}_{q,g}(-\tau)\right| \leq 2\sum_{\tau} \mathcal{N}_{q,g}(\tau) = 2\mu_{q,g}(I_g) = 2.$$

■

Having a 0 measure is not very interesting, and the proof of Proposition 5.2 shows that it would be much more interesting to study the weak convergence of the sequence of signed measures $(\sqrt{q}\,\nu_{q,g})$. We have from the previous proof the following corollary.

Corollary 5.3 *The even moments of $\sqrt{q}\,\nu_{q,g}$ are zero, and the odd nth moments of the sequence $(\sqrt{q}\,\nu_{q,g})$ converge to $-2\mathfrak{b}_n(\mathcal{M}_g)$.*

Unfortunately, we cannot prove weak convergence: The rest of the proof fails as we do not know if one can bound $\sqrt{q}\,\|\nu_{q,g}\|$ uniformly in q (which is a necessary condition for weak convergence). Moreover, one cannot expect a general result from the convergence of moments alone as in the case of (positive) measures as the following counterexample shows.

Example 5.4 Consider the sequence of signed measures (μ_i) with density $i \sin ix$ on the interval $[0, 2\pi]$. The sequence of nth moments converges to $-(2\pi)^n$ which is the nth moment of the signed measure $\mu = -\delta_{2\pi}$. But $\|\mu_i\| = 4i$, which is not bounded

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

and therefore the sequence (μ_i) does not weakly converge (to μ) (see, for instance, [Bog18, Proposition 1.4.7]).

Recall from (3.3) that the nth moment of the function

$$\mathfrak{h}_g(\tau) = \int_{A_\tau} \left(\frac{1}{6}w_1^3 - \frac{1}{2}w_1w_2 + \frac{1}{3}w_3 - w_1\right) dm_g,$$

with $A_\tau = \{(\theta_1, \dots, \theta_g) \in [0,\pi]^g : \sum_j 2\cos\theta_j = \tau\}$, is equal to $\mathfrak{b}_n(\mathcal{M}_g)$. Because of the convergence of the moments above, we conjecture the following.

Conjecture 5.5 *For $g \geq 3$, the sequence of signed measures $(\sqrt{q}\,\nu_{q,g})$ weakly converges to the continuous signed measure with density $-2\mathfrak{h}_g$.*

Such a result would, for instance, imply that $\sqrt{q}\,\|\nu_{q,g}\|$ is uniformly bounded; hence, there exists a constant $C > 0$ such that for all q and all $\tau = t/\sqrt{q}$, we have $|\mathcal{N}_{q,g}(\tau) - \mathcal{N}_{q,g}(-\tau)| \leq C/\sqrt{q}$.

In genus 3, in the same spirit as in Section 4, one can run experiments which illustrate how the values

$$\left\{q\left(\mathcal{N}_{q,g}\left(\frac{t}{\sqrt{q}}\right) - \mathcal{N}_{q,g}\left(\frac{-t}{\sqrt{q}}\right)\right)\right\}_{0\leq t\leq g\lfloor 2\sqrt{q}\rfloor}$$

are close to the values $-2\mathfrak{h}_3(t/\sqrt{q})$. See, for instance, Figure 5 for $q = 53$. Seeing the data, one may even wonder if something stronger would hold in the same line as Conjecture 5.1, at least for $g = 3$.

Under this conjecture, one can use the moments of the density function $\mathfrak{h}_3$ to revisit the result of [LRR+19]. Based on results of [BDFL10], the authors gave a heuristic explanation for the distribution of the points

$$p_{t,q} = \left(\frac{t}{\sqrt{q}}, q\left(\mathcal{N}_{q,g}\left(\frac{t}{\sqrt{q}}\right) - \mathcal{N}_{q,g}\left(\frac{-t}{\sqrt{q}}\right)\right)\right)$$

when $0 \leq t \leq g\lfloor 2\sqrt{q}\rfloor$ by comparing it with the distribution of differences around the mean in the binomial law [LRR+19, Corollary 2.3]. With the arguments given there, the distribution is approximated by the function

$$\mathcal{V}^{\lim}(\tau) = \tau(1 - \tau^2/3)\cdot\left(\frac{1}{\sqrt{2\pi}}e^{-\tau^2/2}\right).$$

Graphically, for $q = 53$, the comparison looks acceptable but not perfect (see Figure 5). This is fair as the heuristic grew from a result true when the degree of the plane curves in play is larger than $2q - 1$. As presently we are dealing with non-hyperelliptic curves of genus 3, represented as plane curves of degree 4, the condition is obviously never fulfilled. It is therefore already stunning that a close, albeit imperfect, match was found in this way.

We now take a different road based on Conjecture 5.5 and approximate the density $-2\mathfrak{h}_3$ by a function $\nu^{\lim}$ using the moments $\mathfrak{b}_n(\mathcal{M}_3)$. By Theorem 2.1, they can be efficiently computed using any symmetric polynomial package. We used Maple and the package SF [Ste95] to compute $\mathfrak{b}_n(\mathcal{M}_3)$ for $n = 1, 3, 5, \dots, 25$, and found the following values:

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

n	$\mathfrak{b}_n(\mathcal{M}_3)$	n	$\mathfrak{b}_n(\mathcal{M}_3)$	n	$\mathfrak{b}_n(\mathcal{M}_3)$
1	0	11	10,395	19	481,835,250
3	1	13	135,564	21	8,308,361,040
5	9	15	1,927,926	23	150,309,679,212
7	84	17	29,524,716	25	2,836,568,118,720
9	882				

Taking $\nu^{\lim}(\tau)$ of the form $P(\tau)\left(\frac{1}{\sqrt{2\pi}}e^{-\tau^2/2}\right)$ with P an odd polynomial of degree 5, we want

$$\int_{\mathbb{R}} \tau^{2n+1} \cdot \nu^{\lim}(\tau)\, d\tau = -2\mathfrak{b}_{2n+1}(\mathcal{M}_3),$$

for $n = 0, 1$, and 2, and one finds that

$$\nu^{\lim}(\tau) = \left(1/60\,\tau^5 - 1/2\,\tau^3 + 5/4\,\tau\right)\left(\frac{1}{\sqrt{2\pi}}e^{-\tau^2/2}\right).$$

Remarkably, the moments of $\nu^{\lim}(\tau)$ still agree with $-2\mathfrak{b}_{2n+1}(\mathcal{M}_3)$ for $n = 3, 4$, and 5. However, for $n = 6$, we find that $\int_{\mathbb{R}} \tau^{13} \cdot \nu^{\lim}(\tau)\, d\tau = -2 \cdot 135135 \neq -2 \cdot \mathfrak{b}_{13}(\mathcal{M}_3)$.

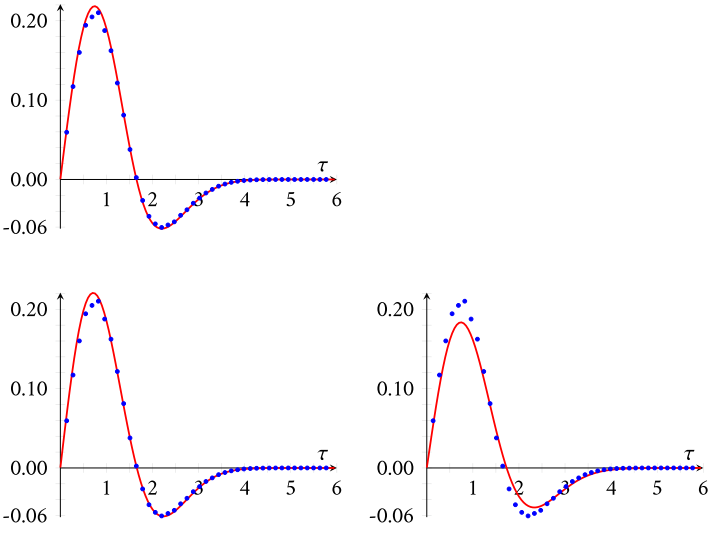

Figure 5: Comparison of genus-3 data for $q = 53$ with theoretical approximations. In each graph, the blue dots are the points $\{(\tau, q\,(\mathcal{N}_{53,3}(\tau) - \mathcal{N}_{53,3}(-\tau)))\}$ with $\tau = t/\sqrt{53}$ and $0 \le t \le 42$. The upper-left graph shows $-2\mathfrak{h}_3$ in red. The bottom-left graph shows $\nu^{\lim}$ in red. The bottom-right graph shows $\mathcal{V}^{\lim}$ in red.

https://doi.org/10.4153/S0008414X2400004X Published online by Cambridge University Press

In Figure 5, we see a comparison between the graph of points $\{p_{t,53}\}_{0\le t\le 42}$ and the functions $\mathcal{V}^{\lim}(\tau)$ and $v^{\lim}(\tau)$, in favor of the latter.

Acknowledgments We thank Dan Petersen for helpful conversations in connection with the Gross–Schoen cycle and Remark 2.4.

References

[AEK+15] J. D. Achter, D. Erman, K. S. Kedlaya, M. M. Wood, and D. Zureick-Brown, *A heuristic for the distribution of point counts for random curves over finite field*. Philos. Trans. Roy. Soc. A **373**(2015), no. 2040, Article no. 20140310, 12 pp. https://doi.org/10.1098/rsta.2014.0310

[AS10] O. Ahmadi and I. E. Shparlinski, *On the distribution of the number of points on algebraic curves in extensions of finite fields*. Math. Res. Lett. **17**(2010), no. 4, pp. 689–699. https://doi.org/10.4310/MRL.2010.v17.n4.a9

[Apo76] T. M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York–Heidelberg, 1976. https://doi.org/10.1007/978-3-662-28579-4.

[BLGHT11] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor, *A family of Calabi–Yau varieties and potential automorphy II*. Publ. Res. Inst. Math. Sci. **47**(2011), no. 1, 29–98. https://doi.org/10.2977/PRIMS/31

[Ber08] J. Bergström, *Cohomology of moduli spaces of curves of genus three via point counts*. J. Reine Angew. Math. **622**(2008), 155–187. https://doi.org/10.1515/CRELLE.2008.068

[BDPW23] J. Bergström, A. Diaconu, D. Petersen, and C. Westerland, *Hyperelliptic curves, the scanning map, and moments of families of quadratic l-functions*. Preprint, 2023. arXiv:2302.07664.

[BF22] J. Bergström and C. Faber, *Cohomology of moduli spaces via a result of Chenevier and Lannes*. Épijournal Géom. Algébrique, 7:14, 2023, Art. 20. https://doi.org/10.1007/s41468-022-00099-1.

[BFvdG14] J. Bergström, C. Faber, and G. van der Geer, *Siegel modular forms of degree three and the cohomology of local systems*. Selecta Math. (N.S.) **20**(2014), no. 1, 83–124. https://doi.org/10.1007/s00029-013-0118-6

[BHLGR23] J. Bergström, E. W. Howe, E. L. García, and C. Ritzenthaler, *Lower bounds on the maximal number of rational points on curves over finite fields*. Math. Proc. Cambridge Philos. Soc. **176**(2024), 213–238. https://doi.org/10.1017/S0305004123000476

[Bil95] P. Billingsley, *Probability and measure*, 3rd ed., Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, Inc., New York, 1995; A Wiley-Interscience Publication. https://worldcat.org/en/title/30735805.

[Bir68] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*. J. Lond. Math. Soc. **43**(1968), 57–60. https://doi.org/10.1112/jlms/s1-43.1.57

[Bog18] V. I. Bogachev, *Weak convergence of measures*, Mathematical Surveys and Monographs, 234, American Mathematical Society, Providence, RI, 2018. https://doi.org/10.1090/surv/234

[BCD+18] A. Bucur, E. Costa, C. David, J. Guerreiro, and D. Lowry-Duda, *Traces, high powers and one level density for families of curves over finite fields*. Math. Proc. Cambridge Philos. Soc. **165**(2018), no. 2, 225–248. https://doi.org/10.1017/S030500411700041X

[BDFL10] A. Bucur, C. David, B. Feigon, and M. Lalín, *Fluctuations in the number of points on smooth plane curves over finite fields*. J. Number Theory **130**(2010), no. 11, 2528–2541. https://doi.org/10.1016/j.jnt.2010.05.009

[Car32] L. Carlitz, *The arithmetic of polynomials in a Galois field*. Amer. J. Math. **54**(1932), no. 1, pp. 39–50. https://doi.org/10.2307/2371075

[CM09] R. L. Cohen and I. Madsen, *Surfaces in a background space and the homology of mapping class groups*. In: Algebraic geometry—Seattle 2005. Part 1, Proceedings of Symposia in Pure Mathematics, 80, American Mathematical Society, Providence, RI, 2009, pp. 43–76. https://doi.org/10.1090/pspum/080.1/2483932

[CDSS17] A. C. Cojocaru, R. Davis, A. Silverberg, and K. E. Stange, *Arithmetic properties of the Frobenius traces defined by a rational abelian variety (with two appendices by J-P. Serre)*. Int. Math. Res. Not. IMRN **2017**(2017), no. 12, 3557–3602. https://doi.org/10.1093/imrn/rnw058

[Cox13] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, 2nd ed., Pure and Applied Mathematics, John Wiley & Sons, Inc., Hoboken, NJ, 2013. https://doi.org/10.1002/9781118400722

[Del71] P. Deligne, *Formes modulaires et représentations l-adiques*. In: Séminaire Bourbaki. Volume 1968/69: Exposés 347–363, Lecture Notes in Mathematics, 175, Springer, Berlin, 1971, pp. 139–172 (Exp. No. 355). https://doi.org/10.1007/BFb0058810

[Del80] P. Deligne, *La conjecture de Weil. II*. Publ. Math. Inst. Hautes Études Sci. **52**(1980), 137–252. http://www.numdam.org/item/PMIHES_1980__52__137_0/.

[Deu41] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*. Abh. Math. Sem. Hansischen Univ. **14**(1941), 197–272. https://doi.org/10.1007/BF02940746

[FKRS12] F. Fité, K. S. Kedlaya, V. Rotger, and A. V. Sutherland, *Sato–Tate distributions and Galois endomorphism modules in genus 2*. Compos. Math. **148**(2012), no. 5, 1390–1442. https://doi.org/10.1112/S0010437X12000279

[FH91] W. Fulton and J. Harris, *Representation theory: A first course*, Graduate Texts in Mathematics, 129, Readings in Mathematics, Springer-Verlag, New York, 1991. https://doi.org/10.1007/978-1-4612-0979-9

[Hai95] R. M. Hain, *Torelli groups and geometry of moduli spaces of curves*. In: Current topics in complex algebraic geometry (Berkeley, CA, 1992/93), Mathematical Sciences Research Institute Publications, 28, Cambridge University Press, Cambridge, 1995, pp. 97–143. http://library.msri.org/books/Book28/files/hain.pdf.

[HKL+20] T. Hammonds, S. Kim, B. Logsdon, Á. Lozano-Robledo, and S. J. Miller, *Rank and bias in families of hyperelliptic curves via Nagao's conjecture*. J. Number Theory **215**(2020), 339–361. https://doi.org/10.1016/j.jnt.2020.04.017

[How22] E. W. Howe, *Variations in the distribution of principally polarized abelian varieties among isogeny classes*. Ann. H. Lebesgue **5**(2022), 677–702. https://doi.org/10.5802/ahl.133

[Joh83] D. Johnson, *The structure of the Torelli group. I. A finite set of generators for J*. Ann. of Math. (2) **118**(1983), no. 3, 423–442. https://doi.org/10.2307/2006977

[Kab98] A. I. Kabanov, *The second cohomology with symplectic coefficients of the moduli space of smooth projective curves*. Compos. Math. **110**(1998), no. 2, 163–186. https://doi.org/10.1023/A:1000256302432

[KS99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, 45, American Mathematical Society, Providence, RI, 1999. https://doi.org/10.1090/coll/045

[KS09] K. S. Kedlaya and A. V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*. In: Arithmetic, geometry, cryptography and coding theory, Contemporary Mathematics, 487, American Mathematical Society, Providence, RI, 2009, pp. 119–162. https://doi.org/10.1090/conm/487/09529

[Lac16] G. 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, Contemporary Mathematics, 663. American Mathematical Society, Providence, RI, 2016, pp. 185–221. https://doi.org/10.1090/conm/663/13355

[Lau02] K. Lauter, *The maximum or minimum number of rational points on genus three curves over finite fields*. Compos. Math. **134**(2002), no. 1, 87–111; With an appendix by Jean-Pierre Serre. https://doi.org/10.1023/A:1020246226326

[Leo06a] V. K. Leont'ev, *On the roots of random polynomials over a finite field*. Math. Notes **80**(2006), nos. 1–2, 300–304. English translation of [Leo06b]. https://doi.org/10.1007/s11006-006-0139-y

[Leo06b] V. K. Leont'ev, *On the roots of random polynomials over a finite field*. Mat. Zametki **80**(2006), no. 2, 313–316. https://doi.org/10.4213/mzm2812

[LRRS14] R. Lercier, C. Ritzenthaler, F. Rovetta, and J. Sijsling, *Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields*. LMS J. Comput. Math. **17**(2014), no. suppl. A, 128–147. https://doi.org/10.1112/S146115701400031X

[LRR+19] R. Lercier, C. Ritzenthaler, F. Rovetta, J. Sijsling, and B. Smith, *Distributions of traces of Frobenius for smooth plane curves over finite fields*. Exp. Math. **28**(2019), no. 1, 39–48. https://doi.org/10.1080/10586458.2017.1328321

[Loo96] E. Looijenga, *Stable cohomology of the mapping class group with symplectic coefficients and of the universal Abel–Jacobi map*. J. Algebraic Geom. **5**(1996), no. 1, 135–150.

[Ma23] Z. Y. Ma, *Refinements on vertical Sato–Tate*. Preprint, 2023. arXiv:2310.08791.

[MPPR24] J. Miller, P. Patzt, D. Petersen, and O. Randal-Williams. *Uniform twisted homological stability*. https://arxiv.org/abs/2402.00354.

[Pet15] D. Petersen, *Cohomology of local systems on the moduli of principally polarized abelian surfaces*. Pacific J. Math. **275**(2015), no. 1, 39–61. https://doi.org/10.2140/pjm.2015.275.39
[Pet16] D. Petersen, *Tautological rings of spaces of pointed genus two curves of compact type*. Compos. Math. **152**(2016), no. 7, 1398–1420. https://doi.org/10.1112/S0010437X16007478
[PTY21] D. Petersen, M. Tavakol, and Q. Yin, *Tautological classes with twisted coefficients*. Ann. Sci. Éc. Norm. Supér. (4) **54**(2021), no. 5, 1179–1236. https://doi.org/10.24033/asens.2479
[Sch47] H. Scheffé, *A useful convergence theorem for probability distributions*. Ann. Math. Statistics **18**(1947), 434–438. https://doi.org/10.1214/aoms/1177730390
[Ser83] J.-P. Serre, *Nombres de points des courbes algébriques sur* $\boldsymbol{F}_q$. In: Seminar on number theory, 1982–1983 (Talence, 1982/1983), University of Bordeaux I, Talence, France, 1983, p. 8 (Exp. No. 22). https://www.digizeitschriften.de/dms/resolveppn/?PID=GDZPPN002545039.
[Ste95] J. R. Stembridge, *A Maple package for symmetric functions*. J. Symbolic Comput. **20**(1995), nos. 5–6, 755–768. This package is available at https://www.math.lsa.umich.edu/jrs/maple.html. https://doi.org/10.1006/jsco.1995.1077
[Sun12] S. Sun, *L-series of Artin stacks over finite fields*. Algebra Number Theory **6**(2012), no. 1, 47–122. https://doi.org/10.2140/ant.2012.6.47
[vdGvdV92] G. van der Geer and M. van der Vlugt, *Supersingular curves of genus* 2 *over finite fields of characteristic* 2. Math. Nachr. **159**(1992), 73–81. https://doi.org/10.1002/mana.19921590106
[Vlă01] S. G. Vlăduţ, *Isogeny class and Frobenius root statistics for abelian varieties over finite fields*. Mosc. Math. J. **1**(2001), no. 1, 125–139. https://doi.org/10.17323/1609-4514-2001-1-1-125-139
[Wah13] N. Wahl, *Homological stability for mapping class groups of surfaces*. In: Handbook of moduli. Volume III, Advanced Lectures in Mathematics (ALM), 26, International Press, Somerville, MA, 2013, pp. 547–583.
[Wat18] T. Watanabe, *On the completion of the mapping class group of genus two*. J. Algebra **501**(2018), 303–327. https://doi.org/10.1016/j.jalgebra.2018.01.003

Department of Mathematics, Stockholms Universitet, Stockholm, Sweden
e-mail: jonasb@math.su.se

Independent mathematician, San Diego, CA, United States
e-mail: however@alumni.caltech.edu

Faculté des sciences, Institut de Mathématiques, Université de Neuchâtel, Neuchâtel, Switzerland
e-mail: elisa.lorenzo@unine.ch

Laboratoire J.A. Dieudonné, Université Côte d'Azur, Nice, France
e-mail: christophe.ritzenthaler@univ-rennes1.fr