The Normal Distribution as a Limit of Generalized Sato-Tate Measures

Michael Larsen*
University of Pennsylvania
Philadelphia, PA 19104
larsen@math.upenn.edu

§0. Introduction

Let \( X \) denote a curve of genus \( g \) over a finite field \( \mathbb{F}_q \). By the Riemann hypothesis for function fields,

\[
|X(\mathbb{F}_q)| = 1 - T + q,
\]

where

\[
(0.0.1) \quad -2g\sqrt{q} \leq T \leq 2g\sqrt{q}.
\]

We consider this inequality from a naive probabilistic point of view. Suppose \( g = 1 \), for example. Then \( E \) has a model as a projective cubic curve. Let \( F(x, y, z) \) denote the corresponding homogeneous cubic polynomial. There are \( q^2 + q + 1 \) \( \mathbb{F}_q \)-rays through the origin in affine 3-space, and loosely speaking, each ray has a probability \( 1/q \) of lying on the zero-locus of \( F \). Therefore, \( X(\mathbb{F}_q) \) should have about \( q + 1 \) points, with an expected error of \( O(\sqrt{q}) \). Thus (0.0.1) gives the right order of magnitude. On the other hand, rather than satisfying a Gaussian distribution law as one might expect, \( T/\sqrt{q} \) is absolutely bounded by 2. More precisely, in the limit \( q \to \infty \), the values of \( T/\sqrt{q} \) are uniformly distributed with respect to a certain measure \( \mu_1 \), known as the Sato-Tate measure, if \( E \) is drawn at random from the set of isomorphism classes of elliptic curves over \( \mathbb{F}_q \). For each value of \( g \), we obtain in this way a measure \( \mu_g \) supported on \([-2g, 2g]\). The main result of this paper is that the limit of these measures is, in fact, \( \mu = (2\pi)^{-1/2}e^{-x^2/2}dx \). Heuristically speaking, for a random curve of random genus, over a random finite field, \( T/\sqrt{q} \) is normally distributed.

The distribution of \( |X(\mathbb{F}_q)| \), as \( X \) varies over a family of varieties, can be approached via the cohomological theory of exponential sums, due to Deligne [5]. More generally, to a family of exponential sums (suitably defined) one can associate a compact Lie group \( G \), the geometric monodromy group, and a finite-dimensional representation \((\rho, V)\) of \( G \) with character \( \chi \). Under suitable hypotheses, the distribution of values of the sums is the same as the distribution of values of \( \chi(g) \), as \( g \) is drawn randomly from the uniform (Haar) measure on \( G \). For each genus \( g \geq 2 \), we construct such a group \( G_g \) and a symplectic representation \( V_g \). It turns out that \( G_g \) is the full (compact) symplectic group \( \text{Sp}(2g) \) and \( V_g \) is its standard 2g-dimensional representation. It is not easy to explicitly compute the distribution of \( \chi(g) \) as \( g \) ranges over \( \text{Sp}(2g) \), but the moments of the distribution can be read off from the invariant theory of \( \text{Sp}(2g) \). There is a precise sense in which the invariant

* Supported by N.S.A. Grant No. MDA 904-92-H-3026
theory “stabilizes” for large values of $g$. The measure-theoretic counterpart of this fact is the statement that $\mu_g$ converges to $\mu$.

Of course, the heuristic principle suggesting this theorem is not limited to curves. One would also expect, for example, that a “random” hypersurface in $\mathbb{P}^3$ of degree $k \gg 0$ should have $q^2 + q + 1 + T$ points, where $T/q$ is normally distributed. The corresponding $V_k$ in this case is orthogonal. Fortunately, the invariant theory of $\text{SO}(n)$ also stabilizes (though one should be careful to distinguish even and odd values of $n$), and the limit of the Sato-Tate measures associated to the standard representations is again $\mu$. To prove that the Sato-Tate measures of $(G_k, V_k)$ for hypersurfaces of degree $k$ do indeed tend $\mu$, one would need to show somehow that $G_k$ is “as large as possible.” In most known instances, geometric monodromy groups associated with self-dual representations do turn out to be either $\text{Sp}$, $\text{O}$, or $\text{SO}$. See, for instance, [8] 11.1 and [9] 8.13 for a discussion of Kloosterman sums and hypergeometric sums respectively.

This paper is organized as follows. The first section analyzes the geometric monodromy group $(G'_{2g+2}, V'_{2g+2})$ of a subfamily of the curves of genus $g$, namely, the hyperelliptic curves of degree $2g + 2$. We compute the first $2g + 1$ moments of the associated Sato-Tate measure $\mu'_{2g+2}$ explicitly. These turn out to be the same as the first $2g + 1$ moments of $\mu$. To conclude that $\mu$ is actually the weak limit of the $\mu'_{2g+2}$ requires some work. The second section gives an effective version of the Weierstrass approximation theory which justifies this conclusion. At this stage, we still do not know that $G'_{2g+2}$ is $\text{Sp}_{2g}$, though the values of the moments are highly suggestive. The third section is pure invariant theory, devoted to an analysis of the fourth moment of the Sato-Tate measure of a self-dual representation of an infinite compact group. Its value is 3 when $(G, V)$ consists of the standard representation of a symplectic, orthogonal, or special orthogonal group, and with one exception, the converse is also true. With this result in hand, we return to $G'_{2g+2}$ in the fourth section and prove that is exactly $\text{Sp}_{2g}$. Since the full moduli space of curves, $\mathcal{M}_g$, is larger than the family of hyperelliptic curves, we expect the geometric monodromy group $G_g$ for $\mathcal{M}_g$ to be at least at large as $G'_{2g+2}$. We make this precise, and prove that in fact $G_g = G'_{2g+2}$.

The results of this paper are superficially similar to those of Davidoff [4]. However, the apparent similarity is illusory. Let $G_n = U(1)^n$ with its standard $n$-dimensional representation. If the associated Sato-Tate measures are rescaled by a factor of $\sqrt{n}$, by the central limit theorem, they will converge to the normal distribution. This is a completely different phenomenon from the (rather miraculous) fact that the Sato-Tate measures of the standard representations of orthogonal and symplectic groups, without any renormalization, tend to $\mu$. Davidoff considers a special family of hyperelliptic curves which are endowed with many endomorphisms, and as a result, she obtains a commutative monodromy group.

This paper has benefited from discussions with C. Epstein, N. Katz, A. Kouvidakis, G. Kuperberg, A. Lindenstrauss, and R. Pink. It gives me pleasure to acknowledge their assistance.

§1. Hyperelliptic Exponential Sums

In this section we compute the $k^{th}$ moment of the generalized Sato-Tate measure of $H^1$ of the universal hyperelliptic curve of genus $g$ for $k < 2g + 2$. These measures behave
as one would expect if the geometric monodromy group of the sheaf of cohomology groups were $\text{Sp}(2g)$. This cohomological point of view is explained below. We begin with some estimates of exponential sums.

\textbf{(1.1)} Let $p$ denote a fixed odd prime and $n \geq 3$ an integer. Let $R_n/\mathbb{F}_p$ denote the affine variety

$$R_n = \text{Spec} \left( \mathbb{F}_p \left[ t_1, \ldots, t_n, \frac{1}{t_1 - t_2}, \frac{1}{t_1 - t_3}, \ldots, \frac{1}{t_{n-1} - t_n} \right] \right)$$

of ordered $n$-tuples with no repeated elements. We consider the universal hyperelliptic curve $X$ over $R_n$ given by the homogeneous equation

$$y^2 z^{n-2} - \prod_{i=1}^{n} (x - t_iz) = 0.$$

The unique point at $\infty$ on this curve has projective coordinates $(0, 1, 0)$. Let $\mathbb{F}_q$ denote a finite extension of $\mathbb{F}_p$ and $\chi$ the extension by zero of the quadratic character on $\mathbb{F}_q^\times$ For each $n$-tuple $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, and each $x \in \mathbb{F}_q$, the cardinality of the set of solutions $y \in \mathbb{F}_q$ of

$$y^2 = (x - a_1) \cdots (x - a_n)$$

is $1 + \chi((x - a_1) \cdots (x - a_n))$. Summing over $x$, we see that the cardinality of $X_a(\mathbb{F}_q)$ is $q - T + 1$, where

$$(1.1.2) \quad T_a = - \sum_{x \in \mathbb{F}_q} \chi((x - a_1) \cdots (x - a_n)).$$

\textbf{Lemma (1.2)} If $P(x)$ a polynomial over a finite field $\mathbb{F}_q$, then

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) \right| \leq (\deg(P) - 1) \sqrt{q}$$

unless $P(x) = cQ(x)^2$ for some $Q(x) \in \mathbb{F}_q[x], c \in \mathbb{F}_q$.

\textbf{Proof.} If $P(x) = R(x)Q(x)^2$, then

$$\left| \sum_{x \in \mathbb{F}_q} \chi(P(x)) - \sum_{x \in \mathbb{F}_q} \chi(R(x)) \right| \leq \deg(Q).$$

Therefore, without loss of generality, we may assume that $P(x)$ is squarefree. Let $d$ denote the degree of $P$. If $d = 0$, there is nothing to prove. If $d = 1$ or $d = 2$, the sum is always 0 or $\pm 1$ respectively. Otherwise $y^2 z^{d-2} = z^d P(x/z)$ defines a projective hyperelliptic curve $X$ of genus $g = \left\lfloor \frac{d-1}{2} \right\rfloor > 0$. By the Lefschetz trace formula,

$$|X(\mathbb{F}_q)| = q - \text{tr}(F_q : H^1(X, \mathbb{Q}_\ell)) + 1,$$

where $F_q$ denotes the Frobenius element $x \mapsto x^q$, and $H^1(X, \mathbb{Q}_\ell)$ the étale cohomology of $X$ with $\ell$-adic coefficients, $\ell \neq p$. By (1.1.2), $- \sum_{x \in \mathbb{F}_q} \chi(P(x))$ is the trace of Frobenius on $H^1$. By the Riemann hypothesis for curves over finite fields, this has absolute value less than or equal to $2g \sqrt{q}$. 

3
Lemma (1.3) Let \( P(x) \) be a monic polynomial over a finite field \( \mathbb{F}_q \), not a perfect square. Then 
\[
\sum_{(a_1, \ldots, a_n) \in R_n(\mathbb{F}_q)} \chi(P(a_1)P(a_2) \cdots P(a_n)) = O(q^{n/2}).
\]

Proof. For each partition \( \pi \) of a set \( \Sigma \), we write \( V_{\pi, \Sigma} \) for the subvariety of the \( |\Sigma| \)-dimensional affine space \( \mathbb{A}^{|\Sigma|} \) defined by the equations \( x_a = x_b \) whenever \( \{a, b\} \subset \kappa \in \pi \). Setting \( \Sigma_n = \{1, 2, \ldots, n\} \), we consider 
\[
S_{\pi, \Sigma_n} = \sum_{(a_1, \ldots, a_n) \in V_{\pi, \Sigma_n}(\mathbb{F}_q)} \chi(P(a_1)P(a_2) \cdots P(a_n))
\]
and prove by induction on \( n \) that all of such sums are \( O(q^{n/2}) \). If \( \kappa \in \pi \) is a singleton \( \{k\} \), then 
\[
S_{\pi, \Sigma_n} = \left( \sum_{a_k \in \mathbb{F}_q} \chi(P(a_k)) \right) S_{\pi \setminus \{\kappa\}, \Sigma_n \setminus \{k\}} = O(q^{n/2})
\]
by Lemma (1.2) and induction on \( n \). If all the equivalence classes of \( \pi \) have two elements or more, there can be no more than \( n/2 \) of them, so \( \dim(V_{\pi, \Sigma_n}) \leq n/2 \). It follows that 
\( |S_{\pi, \Sigma_n}| \leq q^{n/2} \).

By the inclusion-exclusion principle, the characteristic function on \( R_n \) is a linear combination of the characteristic functions of \( V_{\pi, \Sigma_n} \). The lemma follows.

Proposition (1.4) Let 
\[
F(m) = \begin{cases} (m - 1)!! := (m - 1)(m - 3)(m - 5) \cdots (5)(3)(1) & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases}
\]

For \( m < n \), 
\[
\sum_{a \in R_n(\mathbb{F}_q)} (-T_a)^m = F(m)q^{n+m/2} + O(q^{n+m/2-1}).
\]

Proof. By (1.1.2), 
\[
\sum_{a \in R_n(\mathbb{F}_q)} (-T_a)^m = \sum_{a \in R_n(\mathbb{F}_q)} \sum_{x_1 \in \mathbb{F}_q} \cdots \sum_{x_m \in \mathbb{F}_q} \chi \left( \prod_{i=1}^{n} \prod_{j=1}^{m} (x_j - a_i) \right).
\]

Defining 
\[
P_{x_1, \ldots, x_m}(y) = \prod_{j=1}^{m} (y - x_j) = (-1)^m \prod_{j=1}^{m} (x_j - y),
\]
we obtain 
(1.4.1) 
\[
\sum_{a \in R_n(\mathbb{F}_q)} (-T_a)^m = \sum_{x_1 \in \mathbb{F}_q} \cdots \sum_{x_m \in \mathbb{F}_q} \sum_{a \in R_n(\mathbb{F}_q)} \chi((-1)^m) \chi(P_{x_1, \ldots, x_m}(a_1) \cdots P_{x_1, \ldots, x_m}(a_n)).
\]
If there exists a partition $\pi$ of $\Sigma_m$ into pairs such that $(x_1, \ldots, x_m) \in V_\pi \Sigma_m(\mathbb{F}_q)$, then as a polynomial in $y$, $P_{x_1,\ldots,x_m}(y)$ is a perfect square, but otherwise it is not. Therefore, outside the union of such loci, the inner sum of (1.4.1) is of order $O(q^{n/2})$. There are $F(m)$ partitions $\pi$ of $\Sigma_m$ into pairs, and the loci $V_\pi$ intersect pairwise in sets of lower dimension, so

$$\sum_{a \in R_n(\mathbb{F}_q)} T_a = (-1)^{m-n} F(m) q^{n+m/2} + O(q^{n+m/2-1} + q^{m+n/2}) = F(m) q^{n+m/2} + O(q^{n+m/2-1}).$$

**Remark (1.5)** If $m$ and $n$ are both odd, it is easy to see that

$$\sum_{a \in R_n(\mathbb{F}_q)} T_a = 0.$$

Indeed, if $\lambda \in \mathbb{F}_q$ is chosen such that $\chi(\lambda) = -1$, then

$$T_{\lambda a} = -\sum_{x \in \mathbb{F}_q} \chi((x - \lambda a_1) \cdots (x - \lambda a_n)) = -\sum_{\lambda x \in \mathbb{F}_q} \chi((x - a_1) \cdots (x - a_n)) = -T_{\lambda a}.$$

(1.6) Let $S/\mathbb{F}_p$ denote a geometrically connected variety and $\bar{s}$ a fixed geometric point of $S$. The functor assigning to each finite étale $X/S$ the set $\text{Hom}_{S}(\bar{s}, X)$, is represented by a projective system $\{X_i, \phi_{ij} : X_j \rightarrow X_i\}$ of finite étale covers of $S$. As usual, we define

$$\pi_1^{\text{alg}}(S, \bar{s}) := \varprojlim_i \text{Aut}_X(X_i).$$

Given a second geometric point $\bar{s}'$, there is an isomorphism $\pi_1^{\text{alg}}(S, \bar{s}') \cong \pi_1^{\text{alg}}(S, \bar{s})$ canonical up to inner automorphism (i.e., up to choice of “path”) [11] I 5.1 (a). Let $\tilde{S}$ denote the variety obtained from $S$ by extension of scalars to $\mathbb{F}_p$. There is a short exact sequence

$$0 \rightarrow \pi_1^{\text{alg}}(\tilde{S}, \bar{s}) \rightarrow \pi_1^{\text{alg}}(S, \bar{s}) \rightarrow \hat{\mathbb{Z}} \rightarrow 0$$

([5] 1.1.13). By a smooth $\ell$-adic sheaf $\mathcal{F}$ on $S$, we mean a continuous homomorphism $\pi_1^{\text{alg}}(S, \bar{s}) \rightarrow \text{GL}_n(\mathbb{Q}_\ell)$. We fix an embedding $\iota : \mathbb{Q}_\ell \rightarrow \mathbb{C}$ and say that $\mathcal{F}$ is pure of weight $w \in \mathbb{Z}$ if for every $\mathbb{F}_q$-point $x \in S(\mathbb{F}_q)$, every geometric point $\bar{x}$ of $x$, and every choice of path $\pi_1^{\text{alg}}(S, \bar{x}) \rightarrow \pi_1^{\text{alg}}(S, \bar{s})$, the image of Frobenius under the composition of arrows

$$\pi_1^{\text{alg}}(x, \bar{x}) \rightarrow \pi_1^{\text{alg}}(S, \bar{x}) \rightarrow \pi_1^{\text{alg}}(S, \bar{s}) \rightarrow \text{GL}_n(\mathbb{Q}_\ell) \rightarrow \text{GL}_n(\mathbb{C})$$

has all its eigenvalues of absolute value $q^{w/2}$. We write $\text{tr}(\mathcal{F}_x)$ for the trace of the resulting matrix.
Let $d = \dim(S)$. By Poincaré duality ([11] VI 11.1)

$$H^2_c(\bar{S}, \mathcal{F}) \to \text{Hom}_{\mathbb{Q}_\ell}(H^0(\bar{S}, \mathcal{F}^*(d)), \mathbb{Q}_\ell) = \mathcal{F}^{-1}_{\text{alg}}(\bar{S}, \bar{s})(-d).$$

The right hand side is pure of weight $w + 2d$. Let $G_{\text{geom}}$ denote the Zariski closure of $\pi_{\text{alg}}^{\text{alg}}(\bar{S}, \bar{s})$ in $\text{GL}_n(\mathbb{Q}_\ell)$. The space of $G_{\text{geom}}$-invariants in $\mathbb{Q}_\ell^n$ is the same as the space of $\pi_{\text{alg}}^{\text{alg}}(\bar{S}, \bar{s})$-invariants, so

$$\dim(H^2_c(\bar{S}, \mathcal{F})) = \dim(\mathcal{F}^{G_{\text{geom}}}).$$

Note that by [5] 1.3.9, 3.4.1 (iii), the identity component of $G_{\text{geom}}$ is semisimple. By the Lefschetz trace formula [11] VI 13.4,

$$\sum_{x \in S(\mathbb{F}_q)} \text{tr}(\mathcal{F}_x) = \sum_{i=0}^{2d} (-1)^i \text{tr}(F_q : H^i_c(\bar{S}, \mathcal{F})).$$

By [5] 3.3.1, the $i = 2d$ term dominates the sum for $q \gg 0$. Therefore, if

$$a_n = p^{n(-d-w/2)} \sum_{x \in S(\mathbb{F}_{p^n})} \text{tr}(\mathcal{F}_x)$$

tends to a limit as $n \to \infty$, then $H^2_c(\bar{S}, \mathcal{F})$ must be just $\mathbb{Q}_\ell(-d - w/2)$, and

$$\lim_{n \to \infty} a_n = \dim(\mathcal{F}^{G_{\text{geom}}}).$$

**Proposition (1.8)** Let $X \to R_n$ denote the universal hyperelliptic curve over the base $R_n$, and $\mathcal{F} = R^1\pi_*^\dagger(\mathbb{Q}_\ell)$ the sheaf of $H^1$ of the fibres over $R_n$. Then $\mathcal{F}$ is pure of weight 1 and for $m < n$,

$$\dim \left( (\mathcal{F} \otimes m)^{G_{\text{geom}}} \right) = F(m),$$

where $F(m)$ is defined as in Prop. (1.4).

**Proof.** The purity statement is immediate from [5] 3.4.11. This implies that $\mathcal{F} \otimes m$ is pure of weight $m$ for all positive integers $m$. The proposition now follows immediately from Prop. (1.4) and (1.7.1).

**Proposition (1.9)** Let $G$ denote an algebraic group over $\mathbb{C}$ with semisimple identity component and $(\rho, V)$ a complex representation of $G$. There is a unique compact real form $G^c$ of $G$, and

$$\dim(V^G) = \dim(V^{G^c}).$$

On the other hand, if $\mu$ denotes Haar measure on $G^c$, then

$$\dim(V^{G^c}) = \int_{G^c} \chi_{\rho}(g) \mu, \quad \chi_{\rho} := \text{tr} \rho.$$
We define the generalized Sato-Tate measure for \((G^c, V)\) as the direct image measure

\[ \mu_{S-T} := \chi_{\rho_*} \mu \]

on \( \mathbb{R} \). In particular, we can associate a Sato-Tate measure to every pure sheaf over \( S \). By definition of direct image,

\[
\int_{-\infty}^{\infty} x^n \mu_{S-T} = \int_{G^c} \chi_{\rho}(g)^n \mu = \int_{G^c} \chi_{\rho \otimes^n}(g) \mu = \dim(V \otimes^n G).
\]

Prop. (1.8) can be interpreted as the computation of the first \( n - 1 \) moments of the Sato-Tate measure associated with the family of hyperelliptic curves over \( R_n \).

\section{Moments and Limits of Non-negative Measures}

\textbf{(2.1)} Let \( f : \mathbb{R} \to \mathbb{R}^+ \) denote a positive real valued-function. We say \( f \) is very rapidly decreasing (VRD) if every smooth compactly supported function \( g \) is a uniform limit (on \( \mathbb{R} \)) of functions of the form \( f(x)P(x) \), where \( P(x) \) is a polynomial.

\textit{Lemma (2.2)} If \( f(x) \) is VRD, then so is \( f(\lambda x) \) for all \( x \).

\textit{Proof.} The ring of polynomials and the \( L^\infty \) norm are both invariant under the rescaling \( x \mapsto \lambda x \).

\textit{Lemma (2.3)} If \( f(x) \) is VRD and \( g(x) \) is positive, bounded continuous function, then \( f(x)g(x) \) is VRD.

\textit{Proof.} Approximating a smooth compactly supported function \( h(x) \) by \( f(x)g(x)P(x) \) in the \( L^\infty \) topology is equivalent to approximating \( h(x)/g(x) \) by \( f(x)P(x) \).

\textit{Lemma (2.4)} If \( f(x) \) is VRD, then the moment integrals

\[
\int_{-\infty}^{\infty} f(x)x^n \, dx
\]

converge for all \( n \).

\textit{Proof.} The space of smooth compactly supported functions on \( \mathbb{R} \) is of infinite dimension, and all such spaces are uniform limits of sequences \( f(x)P_n(x) \). Therefore, \( f(x)P(x) \in L^\infty(\mathbb{R}) \) for some polynomial \( P \) of arbitrarily large degree. Therefore \( f(x) = o(x^{-n}) \) for all \( n \), and the lemma follows.
Proposition (2.5) The normal functions \( f(x) = e^{-Kx^2} \) are VRD.

Proof. Without loss of generality we may assume \( K = 1/2 \). Let \( T_n(x) \) denote the \( n \)th Chebyshev polynomial of the first kind. When \( x \in [-1, 1] \) and \( 4|n \), we have

\[
T_n(x) = \cos(n \cos^{-1} x) = \cos(n \sin^{-1} x).
\]

For \( |x| \leq 1 < \frac{\pi}{3} \),

\[
1 - \frac{x^2}{4} \geq \cos x \geq 1 - \frac{x^2}{2}, \quad \frac{x^2}{4} \leq \sin^2 x \leq x^2,
\]

so when \( 4|n \),

\[
1 - 2n^2x^2 \leq T_n(x) \leq 1 - \frac{n^2}{4}x^2
\]

for \( |x| \leq \frac{1}{2n} \). Let \( m \) denote an integer congruent to 2 (mod 4). For \( |x| < m/2 \),

(2.5.1) \[
1 - \frac{2x^2}{m^2} \leq 1 - 2(m-2)^2 \left( \frac{x}{2m} \right)^2 \leq T_{m-2} \left( \frac{x}{m^2} \right) \leq 1 - \frac{(m-2)^2}{4} \left( \frac{x}{m^2} \right)^2 \leq 1 - \frac{x^2}{16m^2}.
\]

We define

\[
Q_m(x) = \left[ \left( 1 - \frac{x^2}{m^4} \right) T_{m-2} \left( \frac{x}{m^2} \right) \right]^{m^3/4}.
\]

As \( (1 - \epsilon)^{1/\epsilon} \geq 1/4 \) for \( 0 \leq \epsilon \leq \frac{1}{2} \), for \( |x| < m^{-1/2} \),

\[
Q_m(x) \geq ((1 - m^{-5})(1 - 2m^{-3}))^{m^3/4} \geq (1 - 4m^{-3})^{m^3/4} \geq \frac{1}{4}.
\]

As \( m^3/4 \) is even, \( Q_m(x) \geq 0 \) for all \( x \), so

\[
I_m = \int_{-m^2}^{m^2} Q_m(x) \geq \frac{1}{2\sqrt{m}}.
\]

In the other direction, (2.5.1) implies

(2.5.2) \[
Q_m(x) \leq \left( 1 - \frac{x^2}{16m^2} \right)^{m^3/4} \leq e^{-mx^2/64}
\]

for \( |x| < m/2 \). For \( m/2 \leq |x| \leq \sqrt{2m^4 - m^2/4} \),

(2.5.3) \[
Q_m(x) \leq \left( 1 - \frac{x^2}{m^4} \right)^{m^3/4} \leq e^{-m/16}.
\]

Finally, we note that the identity \( T_n(\cosh x) = \cosh nx \) implies that for \( |y| \geq 1 \),

\[
T_n(y) < |2y|^n.
\]
For $|x| \geq m^2$, then,

$$0 < Q_m(x)e^{-(x-r)^2/2} < (2^m m^{-2m} x^m)^{m^3/4} e^{-(x-r)^2/2}.$$ 

From the fact that $|x^n e^{-x^2/2}|$ achieves its maximum when $x = \pm \sqrt{n}$, we deduce

$$\sup_{x \in \mathbb{R}} x^n e^{-(x-r)^2/2} = \sup_{x \in \mathbb{R}} (x + r)^n e^{-x^2/2} = \sup_{x \in \mathbb{R}} (1 + r/x)^n e^{-x^2/2}.$$ 

If the maximum is achieved for some $x \geq 2r$, then

$$\sup_{x \in \mathbb{R}} x^n e^{-(x-r)^2/2} \leq n^{n/2} C^{-n/2},$$

where $C = 4e/9 > 1$. Thus, if $r < \sqrt{\frac{m^2}{6C}}$,

$$\sup_{x \in \mathbb{R}} x^n e^{-(x-r)^2/2} \leq \sup_{|x| \leq 2r} x^n e^{-(x-r)^2/2}, \quad n^{n/2} C^{-n/2} \leq n^{n/2} C^{-n/2}.$$ 

We conclude that if $r < \frac{m^2}{6eC}$,

(2.5.4) \[ Q_m(x)e^{-(x-r)^2/2} < (2^m m^{-2m} x^m)^{m^3/4} \sup_{x \in \mathbb{R}} x^{m^4/4} e^{-(x-r)^2/2} \leq C^{-m^4}. \]

For each $n \in \mathbb{N}$, we set $m = 4n + 2$ and define $f_n(x)$ as the product of $Q_m/I_m$ and the characteristic function of the interval $[-m^2, m^2]$. Then $f_n$ is a non-negative measure of integral 1, and the estimates (2.5.2) and (2.5.3) imply that $f_n$ is an approximate identity. Therefore, if $g$ is a smooth compactly supported function, the sequence of convolutions $f_n \ast g$ converges uniformly to $g$. By (2.5.3) and (2.5.4), since $g$ is supported on a subset of $[-r, r]$ for some $r$,

$$e^{-x^2/2}((f_n - Q_{4n+2}/I_{4n+2}) \ast g)$$

tends to zero uniformly on $\mathbb{R}$ as $n \to \infty$. Therefore, $g$ is the uniform limit of the products $e^{-x^2/2}((Q_{4n+2}/I_{4n+2}) \ast g)$ of a fixed Gaussian with a sequence of polynomials.

**Proposition (2.6)** Let $\mu_1, \mu_2, \ldots$ denote a sequence of non-negative measures on the real line and $f(x)$ a smooth positive real-valued VRD function. Suppose that for all $m < n$

(2.6.1) \[ \int_{-\infty}^{\infty} x^m \mu_n = \int_{-\infty}^{\infty} x^m f(x)^4 \, dx. \]

Then $\mu_i$ converges to $f(x)^4 \, dx$ in the weak-* topology.

**Proof.** We note that $f(x)^4$ is VRD, so the right hand side of (2.6.1) converges. Let $g(x)$ by any smooth compactly supported function which takes only non-negative values. Choose $\epsilon > 0$, and let $h(x)$ denote a smooth compactly supported function such that
on $\mathbb{R}$. Letting $\epsilon$ tend to 0, we can write $f(x)^2g(x)$ as a uniform limit of functions $f(x)^2B_n(x)$, where $B_n(x) \in \mathbb{R}[x]$, and $B_n(x) \geq g(x)$ for all $x \in \mathbb{R}$. As $f(x)^2$ is VRD, it is integrable, so $f(x)^4B_n(x)$ converges in the $L^1$ norm to $f(x)^4g(x)$. Therefore (2.6.2)
\[
\lim_{n \to \infty} \int_{-\infty}^{\infty} g(x)\mu_n \leq \lim_{m \to \infty} \lim_{n \to \infty} \int_{-\infty}^{\infty} B_m(x)\mu_n = \lim_{m \to \infty} \int_{-\infty}^{\infty} B_m(x)\mu = \int_{-\infty}^{\infty} g(x)\mu.
\]
On the other hand, the measure of the real line is the same with respect to $\mu$ and with respect to $\mu_n$ for $n \gg 0$, so we must have equality in (2.6.2). Finally, every smooth compactly supported function is the difference of two such functions which are everywhere non-negative, and the proposition follows.

**Corollary (2.7)** If $\mu_n'$ denotes the Sato-Tate measure associated with the family of hyper-elliptic curves over $R_n$, then in the weak-* topology,
\[
\lim_{n \to \infty} \mu_n' = \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx.
\]

**Proof.** By Prop. (1.8) and (1.9.1),
\[
\int_{-\infty}^{\infty} x^m \mu_n' = F(m),
\]
for $m < n$. Applying Prop. (2.6) to $(2\pi)^{-1/8} e^{-x^2/8}$, we deduce (2.7.1) from the integral
\[
\int_{-\infty}^{\infty} x^m e^{-x^2/2} dx = \sqrt{2\pi} F(m),
\]
which is easily checked by integration by parts.

§3. **A Problem in Invariant Theory**

Throughout this section $G$ will always denote a compact Lie group and $V$ a faithful finite dimensional representation.

**(3.1)** Given a fixed $G$ and $V$, we define the sequence of Sato-Tate moments
\[
a_n = a_n(G, V) = \dim \left( V \otimes^n G \right), \quad n \geq 1.
\]
It is possible, in general, that $a_1 = a_2 = \cdots = a_m = 0$, for any desired value of $m$. This is the case, for instance, if $G = \text{SU}(n)$, $V$ is the standard $n$-dimensional representation, and $n > m$. However, if $V$ is self-dual, then $a_{2k} > 0$ for all $k$. Indeed,
\[
a_{2k} = \dim \left( V \otimes^{2k} G \right) = \dim \left( \text{Hom}_G \left( V \otimes^k, V \otimes^k \right) \right) = \sum_{i} m_i^2,
\]
where $m_i$ denote the multiplicities of the irreducible factors of $V \otimes^k$. In particular, $a_{2k}$ is at least as large as the number of summands appearing when $V \otimes^k$ is decomposed into irreducible representations.

Henceforth, we shall always assume $V$ is self-dual.
This section is devoted to the classification of pairs \((G, V)\) such that \(a_4(G, V) = 3\). The complete classification problem seems to be quite difficult. A wide variety of interesting finite groups admit such representations. For example, the irreducible 3-dimensional representations of \(A_5\) satisfy this condition. So do the standard 6, 7, and 8 dimensional representations of the Weyl groups of \(E_6\), \(E_7\), and \(E_8\) respectively. The natural 24-dimensional representation of the automorphism group of the Leech lattice does as well. The 133-dimensional representation of the Harada-Norton group and the 248-dimensional representation of the Thompson group provide even more exotic examples. The equality \(a_4 = 3\) can be readily checked in all these cases with the aid of character tables, such as those in [2].

Fortunately, in our application, finite groups may be ruled out on geometric grounds, so we are not obliged to attempt to classify the solutions. It seems likely that a complete list is attainable, using the classification of finite simple groups and the following lemma:

Lemma (3.3) Let \((G, V)\) denote a solution to the equation \(a_4(G, V) = 3\). Then every non-abelian normal subgroup \(H\) of \(G\) the restriction of \(V\) to \(H\) is irreducible. In particular, the centralizer of \(H\) in \(G\) has order \(\leq 2\).

Proof. First we observe that \(V\) must be an irreducible \(G\)-module. Indeed, if \(V = V' \oplus V''\), then the trivial representation appears with multiplicity \(\geq 2\) in \(V \otimes V\). Therefore, \(a_4 \geq 4\), contrary to hypothesis. Let \(H\) be a normal subgroup of \(G\). As a representation of \(H\), \(V\) decomposes into a direct sum

\[(W_1 \oplus \cdots W_k) \otimes \mathbb{C}^\ell, \quad \dim(W_1) = \cdots = \dim(W_k) = m,\]

where \(H\) acts irreducibly on the \(W_i\) and trivially on \(\mathbb{C}^\ell\) ([3] 49.7). As \(H\) is non-abelian and \(V\) is a faithful \(H\)-module, \(m > 1\). Every element of \(G\) maps an \(H\)-isotypic factor \(W_i \otimes \mathbb{C}^\ell\) into another such factor, \(W_j \otimes \mathbb{C}^\ell\). Therefore,

\[V \otimes V = \bigoplus_{i=1}^{k} \text{Sym}^2(W_i \otimes \mathbb{C}^\ell) \oplus \bigoplus_{i=1}^{k} \Lambda^2(W_i \otimes \mathbb{C}^\ell) \oplus \bigoplus_{i \neq j} (W_i \otimes \mathbb{C}^\ell) \otimes (W_j \otimes \mathbb{C}^\ell)\]

represents \(V \otimes V\) as a direct sum of three \(G\)-modules. If \(k > 1\) or \(\ell > 1\), all three pieces are have dimension \(> 1\). Since there is also at least one \(G\)-invariant in \(V \otimes V\), \(a_4 \geq 4\). Therefore, \(k = \ell = 1\), and \(V\) is an irreducible \(H\)-module. By Schur’s lemma, the centralizer of \(\rho(H)\) in \(\text{GL}(V)\) consists of the scalar matrices. But all traces of elements in \(\rho(G)\) are real, so only scalar matrices \(\pm 1\) are possible. As \(V\) is faithful on \(G\), the centralizer of \(H\) has order \(\leq 2\).

Corollary (3.4) If \(a_4(G, V) = 3\), then the identity component of \(G\) is either a torus or a semisimple group.

Proof. Let \(G^o\) denote the identity component of \(G\). It is a normal subgroup of \(G\). If it is not a torus, then it has a finite centralizer in \(G\), hence a finite center. Therefore, it is semisimple.
Proposition (3.5) If \( a_4(G, V) = 3 \) for an infinite compact group \( G \), then \( G \subset \text{GL}(V) \) is \( N_{\text{SU}(2)}U(1) \subset U(2) \), \( SO(n) \subset U(n) \), \( O(n) \subset U(n) \), or \( \text{Sp}(2n) \subset U(2n) \).

**Proof.** Suppose first that \( G^0 \) is a torus \( T \). Then \( V \) is a direct sum \( \chi_1 \oplus \cdots \chi_n \) of characters of \( T \), and for each \( \chi_i \) there exists \( \chi_j = \chi_i^{-1} \). As \( V \) is irreducible as a \( G \)-representation, all the characters \( \chi_i \) must lie in a single orbit under the action of \( G/T \) on the character group \( X^*(T) \). If some \( \chi_i \) were trivial, then all \( \chi_i \) would be trivial, contrary to the assumption that \( V \) is faithful. It follows that (suitably renumbering the indices), \( V \) is the direct sum

\[
\chi_1 \oplus \chi_1^{-1} \oplus \chi_2 \oplus \cdots \oplus \chi_{n/2}^{-1}.
\]

Therefore, as \( G \)-module, \( V \otimes V \) decomposes into the following three pieces:

\[
\bigoplus_i \left( \chi_i \otimes \chi_i \oplus \chi_i^{-1} \oplus \chi_i^{-1} \right) \oplus \bigoplus_i \left( \chi_i \otimes \chi_i^{-1} \oplus \chi_i^{-1} \otimes \chi_i \right) \oplus \bigoplus_{i \neq j} \left( \chi_i \otimes \chi_j^{-1} \oplus \chi_i^{-1} \otimes \chi_j \right).
\]

If \( n/2 > 1 \), then these pieces are all of dimension \( \geq 2 \). Since \( V^{\otimes 2} \) also has a \( G \)-invariant line, this implies \( a_4 \geq 4 \). We conclude that \( n = 2 \), so \( G \) is contained in \( \text{SU}(2) \). As \( T \) is normal in \( G \), \( G \) can only be the normalizer of a maximal torus.

Suppose, on the contrary, that \( G^0 \) is a semisimple group. As \( G^0 \) is normal in \( G \), the restriction of an irreducible representation of \( G \) to \( G^0 \) is the direct sum of highest weight modules \( V_{\lambda_i} \) of \( G^0 \), where the \( \lambda_i \) lie in the same orbit of the automorphism group \( \Gamma \) of the root system \( \Phi \) of \( G^0 \). We apply this observation to \( V_{\lambda}^{\otimes 2} \). The dual of the Killing form gives a \( \Gamma \)-invariant inner product on the space of characters of \( G \), so it suffices to find submodules \( V_{\mu} \) of \( V_{\lambda}^{\otimes 2} \) of four different lengths.

Given a semisimple Lie algebra \( \mathfrak{g} \) and a representation \( V \), let \( S(\mathfrak{g}, V) \) denote the set of norms \( \| \lambda \|^2 \), where \( V_{\lambda} \) is a submodule of \( V \). If \( (\mathfrak{h}, W) \) is a second pair, then

\[
S(\mathfrak{g} \times \mathfrak{h}, V \boxtimes W) = \{ x + y \mid x \in S(\mathfrak{g}, V), y \in S(\mathfrak{h}, W) \},
\]

so

\[
|S(\mathfrak{g} \times \mathfrak{h}, V \boxtimes W)| \geq |S(\mathfrak{g}, V)| + |S(\mathfrak{h}, W)| - 1.
\]

If \( \mathfrak{g} \) is simple and \( V_{\lambda} \) is faithful and self-dual, then \( |S(\mathfrak{g}, V_{\lambda})| \geq 2 \) because \( 0, 2\lambda \in S(\mathfrak{g}, V_{\lambda}) \). By [10], \( V_{\lambda}^{\otimes 2} \) contains a submodule \( V_{\mu} \) in every Weyl orbit \( W_{\mu} = W(\lambda + w\lambda) \), for fixed \( w \in W \). If \( \text{rk}(\mathfrak{g}) > 1 \), this implies that \( |S(\mathfrak{g}, V_{\lambda})| \geq 3 \) because \( W \) acts irreducibly on the root space, and therefore some \( w\lambda \not\in \{ \pm \lambda \} \). Since \( V \) is self dual, \( W\lambda \) is invariant under multiplication by \(-1\). Suppose there exists \( w \in W \) such that

\[
w\lambda \not\in \{ \lambda, -\lambda \} \cup \lambda^\perp.
\]

Then \( \lambda + \lambda \), \( \lambda + w\lambda \), \( \lambda - w\lambda \), and \( \lambda - \lambda \) are all of different lengths, so \( |S(\mathfrak{g}, V_{\lambda})| \geq 4 \).

We have seen that if \( \mathfrak{g} = \text{Lie}(G^0) \), and \( V \) is a representation of \( G \) such that \( a_4(G, V) = 3 \), then \( |S(\mathfrak{g}, V)| \leq 3 \). In view of the foregoing analysis, this implies that \( \mathfrak{g} = \mathfrak{sl}_2 \times \mathfrak{sl}_2 \) with \( V \) the exterior tensor product of the two standard representations, or \( \mathfrak{g} \) is simple with \( V = V_{\lambda} \), where \( \mu_1, \mu_2 \in W\lambda \) implies \( \mu_1 = \pm \mu_2 \) or \( \mu_1 \perp \mu_2 \). By the classification
of simple Lie algebras, the latter condition implies that \( g \) is of type \( A_1 \), \( B_n \) \((n \geq 2)\), \( C_n \) \((n \geq 2)\), or \( D_n \) \((n \geq 3)\), and \( \lambda \) is a positive integral multiple of the fundamental weight \( \omega_1 = (1,0,\ldots,0) \), in the notation of [1] VI Planches. Note that the Lie algebras \( B_2 \) and \( C_2 \) are the same, but the value of \( \omega_1 \) depends on which name we choose.

Assume that \( n = \text{rk}(g) > 1 \). We recall the Freudenthal formula for the multiplicity \( m_\omega(\lambda) \) of a weight \( \lambda \) appearing in the highest weight module \( V_\omega \) ([1] VIII §9 Ex. 5 (g)):

\[
m_\omega(\lambda) = \frac{2\sum_{\alpha \in \Phi^+} \sum_{i=1}^{\infty} m_\omega(\lambda + i\alpha) \langle \mu + i\alpha, \alpha \rangle}{\langle \omega + \rho, \omega + \rho \rangle - (\lambda + \rho, \lambda + \rho)},
\]

where \( \rho \) denotes the half sum of roots. Applying this formula for \( B_n, C_n, \) and \( D_n \) to \( \omega = k\omega_1 \) and \( \lambda = (k-1,1,0,\ldots,0) \), in each case we get a multiplicity of 1. As \((2k-1,1,0,\ldots,0)\) appears with multiplicity 2 in \( V_{k\omega_1}^{\otimes 2}, V_{(2k-1,1,\ldots,0)} \) is a submodule of \( V_{k\omega_1}^{\otimes 2} \). By [10], we know that there are also submodules \( V_{(2k,0,\ldots,0)}, V_{(k,k,0,\ldots,0)}, \) and \( V_0 \). If \( k > 1 \), the highest weights of these modules are all of different lengths. We conclude that \( \lambda = \omega_1 \). As \( V \) is faithful, this means that \( G^\circ \) is \( SO(2n+1) \), the compact form of \( Sp(2n) \), or \( SO(2n) \), depending on whether \( g \) is of type \( B_n, C_n, \) or \( D_n \). In any case, \( G \) is contained in the normalizer of the image of \( G^\circ \) under its standard representation, so \( G = G^\circ \) in the symplectic case and \( G \) can be either of type \( SO \) or type \( O \) in the orthogonal case.

Finally we consider the \( sl_2 \) cases. When \( g = sl_2, V = V_{k\omega_1} \), then \( |S(g, V^{\otimes 2})| = k + 1 \). When \( k = 1 \), we have the standard representation of \( G^\circ = SU(2) \), so \( a_4(G, V) < 3 \). When \( k = 2 \), we have the solutions \( SO(3) \) and \( O(3) \) enumerated above. Finally, if \( g = sl_2 \times sl_2 \), the condition \( |S(g, V)| \leq 3 \) implies that \( V \) is the exterior tensor product of the standard representations of the two factors. This gives rise to the solutions \( SO(4) \) and \( O(4) \) enumerated above.

§4. Monodromy for the Moduli Spaces of Curves

**Theorem (4.1)** For \( n \geq 5 \), the geometric monodromy \((G'_n, V_n)\) of \( R^1\pi_*\mathbb{Q}_\ell \) for the family of hyperelliptic curves over \( R_n = Sp_{2[(n-1)/2]} \).

**Proof.** Applying Prop. (1.4) for \( m = 4 \), we see that \( a_4(G'_n, V_n) = 3 \). Now \( \dim(V_n) = 2g = 2[(n-1)/2] \), so by Prop. (3.5), \( G'_n \) is finite, symplectic, or orthogonal. On the other hand, the cup product on \( H^1 \) is anti-symmetric, so by Poincaré duality, \( V_n \) is a symplectic representation. Therefore, it suffices to prove that \( G'_n \) is infinite. Now

\[
R_n = \text{Spec} \left( \mathbb{F} \left[ t_1, \ldots, t_n, \frac{1}{t_1-t_2}, \frac{1}{t_1-t_3}, \ldots, \frac{1}{t_{n-1}-t_n} \right] \right)
\]

is an open subvariety of affine space \( \mathbb{A}^n \) over \( \mathbb{F} \), and \( X \) extends naturally to the projective curve over \( \pi : X \to \mathbb{A}^n \) defined by (1.1.1). For every non-singular curve \( Z \subset \mathbb{A}^n \), we define \( Z^\circ = Z \cap R_n \). We choose \( Z \) such that \( Z \setminus Z^\circ \) is a non-empty subset of the smooth locus of \( \mathbb{A}^n \setminus R_n \). The restriction \( X_Z := X \times_{\mathbb{A}^n} Z \) is a Lefschetz pencil, and the restriction of \( R^1\pi_Z_*\mathbb{Q}_\ell \) to \( Z^\circ \) is a smooth \( \ell \)-adic sheaf \( \mathcal{F} \) with finite monodromy. Therefore, there exists a finite étale cover \( Y^\circ \) of \( Z^\circ \) on which \( \mathcal{F} \) is a sheaf with trivial monodromy. The
normalization of $Y^\circ$ over $Z$ is a non-singular curve $Y$ with a Lefschetz pencil $X_Y \to Y$. The fibres over the (non-empty) set $Y \setminus Y^\circ$ have a double point, so there is at least one vanishing cycle of $R^1\pi_{Y*}\mathbb{Q}_\ell$. By the Picard-Lefschetz theorem ([11] V 3.15), the space of $\pi_1$-invariants of $R^1\pi_{Y*}\mathbb{Q}_\ell$ is orthogonal to the space of vanishing cycles under the Poincaré pairing. As the Poincaré pairing is perfect, we have a contradiction, and the theorem holds.

**Remark (4.2)** In the light of this result, the moment computations of Prop. (1.8) give

$$a_m(\text{Sp}(2g), \text{Std}) = \begin{cases} 0 & \text{if } m \text{ is odd,} \\ (m-1)!! & \text{if } m \text{ is even,} \end{cases}$$

for $m \leq 2g+1$. This is a classical result of invariant theory [13] 6.1.A, 6.1.B. The analogous result also holds for orthogonal groups [13] 2.11.A, 2.17.A.

(4.3) For each pair $(g, n)$ of non-negative integers, consider the functor of $n$-pointed curves of genus $g$ over $\mathbb{F}_p$, i.e., the functor assigning to each scheme $S/\mathbb{F}_p$ the set of $n+1$-tuples $(\pi, \sigma_1, \ldots, \sigma_n)$, where $\pi : X \to S$ is a proper smooth morphism and $\sigma_i : S \to X$ are sections of $\pi$ such that for all geometric points $\bar{s}$ on $S$, $X_{\bar{s}}$ is a curve of genus $g$ and $\sigma_i(\bar{s})$ are distinct points. For fixed $g$, when $n$ is sufficiently large, this functor is represented by a quasi-projective variety $\mathcal{M}_{g,n}$ [12] II. By a theorem of Deligne and Mumford [6], the coarse moduli space of curves $M_g$ and therefore the variety $\mathcal{M}_{g,n}$ is geometrically irreducible. Let $Y_{2g+2,n}$ denote the complement of the diagonal on the $n$-fold fibre power of the universal curve on $R_{2g+2}$. From the projection $Y_{2g+2,n} \to R_{2g+2}$ we obtain a universal curve on $Y_{2g+2,n}$, with $n$ canonical sections. The data of curve with sections defines a map $i_{g,n} : Y_{2g+2,n} \to \mathcal{M}_{g,n}$. The universal curve on $\mathcal{M}_{g,n}$ (resp. $Y_{2g+2,n}$) gives rise to a sheaf of relative first cohomology groups, and therefore to a continuous $\ell$-adic representation $\pi_\mathcal{M}$ of $\pi_1^{\text{alg}}(\mathcal{M}_{g,n}, \bar{m})$ (resp. $\pi_Y$ of $\pi_1^{\text{alg}}(Y_{2g+2,n}, \bar{y})$). If we choose $\bar{m}$ to be the image of a fixed geometric point $\bar{y}$ of $Y_{2g+2,n}$, we obtain the commutative diagram

$$\begin{array}{ccc}
\pi_1^{\text{alg}}(Y_{2g+2,n}, \bar{y}) & \xrightarrow{i_{g,n}} & \pi_1^{\text{alg}}(\mathcal{M}_{g,n}, \bar{m}) \\
\rho_Y & \swarrow & \rho_M \\
\text{GL}_{2g}(\mathbb{Q}_\ell) & & \\
\end{array}$$

(4.4) The representation $(\pi_Y, V_Y)$ is obtained by pull-back from the continuous representation of $\pi_1^{\text{alg}}(R_n, \bar{m})$ on the hyperelliptic curve $X_{\bar{m}}$. Therefore, the geometric monodromy group $G_Y$ of the sheaf of relative $H^1$ on $Y_{2g+2,n}$ is a subgroup of $\text{Sp}(2g)$. There are several ways to see that it is actually the full group. One way is to construct a multi-section $R_n \to Y_{2g+2,n}$. Another is to note that the inequality of exponential sums

$$(q+1-2g\sqrt{q}-n)^n \sum_{a \in R_n(\mathbb{F}_q)} T_2^{2k} \leq \sum_{(a, x_1, \ldots, x_n) \in Y_{2g+2,n}(\mathbb{F}_q)} T_2^{2k} \leq (q+1+2g\sqrt{q}-n)^n \sum_{a \in R_n(\mathbb{F}_q)} T_2^{2k}$$

implies

$$\sum_{(a, x_1, \ldots, x_n) \in Y_{2g+2,n}(\mathbb{F}_q)} T_2^{2k} = F(2k)q^{n+2g+k} + O(q^{n+2g+k-1/2}),$$

and therefore

$$\dim(V_Y^{\otimes 2k}G_Y) = F(2k) = \dim(V_Y^{\otimes 2k}\text{Sp}(2g)).$$

It follows from a standard result in invariant theory [7] I Prop. 3.1 (c) that $G_Y = \text{Sp}(2g)$. 

14
Theorem (4.5) Let \( p : X \to \mathcal{M}_{g,n} \) denote the universal curve of genus \( g \). Then the geometric monodromy \( G_{g,n} \) of \( R^1 p_* \mathbb{Q}_\ell \) is \( \text{Sp}(2g) \).

Proof. The map \( i_{g,n} \) realizes the geometric monodromy group \( G'_{2g+2,n} \) of \( H^1 \) of the universal curve on \( Y_{2g+2,n} \) as a subgroup of \( G_{g,n} \). On the other hand, by Poincaré duality, \( G_{g,n} \) is contained in \( \text{Sp}(2g) \). The theorem follows.

Remark (4.6) We do not state a monodromy result about the moduli space \( \mathcal{M}_g \) itself because it does not admit a universal curve. There is an algebraic stack \( \mathcal{M}_g \), and presumably the natural language in which this theorem should be framed is that of smooth \( \ell \)-adic sheaves on stacks. The choice of scheme language was dictated by the lack of adequate references on the foundations of the theory of stacks.

REFERENCES
[1] N. Bourbaki, Groupes et algèbres de Lie, Paris: Masson (1981)
[2] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.
[3] C. W. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley-Interscience, London, 1962.
[4] G. Davidoff, Distribution properties of certain exponential sums, Duke J. of Math. 62 No. 1 (1991) 205–235.
[5] P. Deligne, La Conjecture de Weil, II, Publ. Math. IHES, 52 (1980), 138–252.
[6] P. Deligne, D. Mumford, The irreducibility of the space of curves of given genus, Publ. Math. IHES, 36 (1969) 75–110.
[7] P. Deligne, J. S. Milne, A. Ogus, K. Shih, Hodge Cycles, Motives, and Shimura Varieties, Lecture Notes in Math. 900, Springer-Verlag, Berlin, 1982.
[8] N. Katz, Gauss Sums, Kloosterman Sums, and Monodromy Groups, Annals of Math. Studies 116, Princeton University Press, Princeton, 1988.
[9] N. Katz, Exponential Sums and Differential Equations, Annals of Math. Studies 124, Princeton University Press, Princeton, 1990.
[10] S. Kumar, Proof of the Parthasarathy-Ranga Rao-Varadarajan conjecture, Invent. Math. 93 (1988) 117–130.
[11] J. S. Milne, Étale Cohomology, Princeton University Press, Princeton, 1980.
[12] D. Mumford, Curves and their Jacobians, University of Michigan Press, Ann Arbor, 1976.
[13] H. Weyl, The Classical Groups, Princeton University Press, Princeton, 1939.