HYPERELLIPTIC CURVES WITH MAXIMAL GALOIS ACTION ON THE TORSION POINTS OF THEIR JACOBIANS

AARON LANDESMAN, ASHVIN A. SWAMINATHAN, JAMES TAO, AND YUJIE XU

Abstract. In this article, we show that in each of four standard families of hyperelliptic curves, there is a density-1 subset of members with the property that their Jacobians have adelic Galois representation with image as large as possible. This result constitutes an explicit application of a general theorem on arbitrary rational families of abelian varieties to the case of families of Jacobians of hyperelliptic curves. Furthermore, we provide explicit examples of hyperelliptic curves of genus 2 and 3 over $\mathbb{Q}$ whose Jacobians have such maximal adelic Galois representations.

1. Introduction

1.1. **Background.** Let A be a principally polarized abelian variety (PPAV) of dimension $g \geq 1$ over a number field K. Fix an algebraic closure $\overline{K}$ of K, and let $G_K := \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group. The action of G_K on the torsion points of $A(\overline{K})$ gives rise to the *adelic* Galois representation

$$\rho_A \colon G_K \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}).$$

For prime numbers ℓ, the *mod-ℓ Galois representation* $\rho_{A,\ell} \colon G_K \to \mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is defined by reducing the image of ρ_A modulo ℓ. See [Zyw15, Section 2.2] and [LSTX19, Section 3.1] for more detailed descriptions of these representations.

In 1972, Jean-Pierre Serre proved the celebrated Open Image Theorem (see [Ser72]), which states that for an elliptic curve E/K without complex multiplication, $\rho_E(G_K)$ is an open subgroup of, and hence has finite index in, the profinite group $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$. While the Open Image Theorem implies that the adelic Galois representation maps onto a large subgroup of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$, the image of this representation is not always equal to $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. Indeed, Serre observed in [Ser72, Proposition 22] that for every elliptic curve $E/\mathbb{Q}$, the image of ρ_E has even index in $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$. Nonetheless, in [Ser72, Sections 5.5.6-8], Serre constructs several examples of elliptic curves over $\mathbb{Q}$ whose Galois representations have "maximal image" among all elliptic curves, in the sense that the index of the image in $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$ is equal to 2.

The obstruction faced by elliptic curves over $\mathbb{Q}$ to having surjective adelic Galois representation no longer exists when $\mathbb{Q}$ is replaced by a larger number field. In [Gre10], Greicius constructs an example of an elliptic curve over a cubic extension of $\mathbb{Q}$ whose Galois representation has image equal to $\mathrm{GSp}_2(\widehat{\mathbb{Z}})$. Furthermore, in [Zyw15], Zywina constructs an example of a non-hyperelliptic curve of genus 3 over $\mathbb{Q}$ whose Jacobian has adelic Galois image equal to $\mathrm{GSp}_6(\widehat{\mathbb{Z}})$. While there are explicit examples in genera 1 and 3, to the authors' knowledge, there are no examples in the literature of curves of genus 2 with associated Galois representation having maximal image among such curves. Additionally, there are no known examples of hyperelliptic curves of genus 3 whose Galois image is maximal. Nevertheless, there are a few examples that come close: In [Die02, Theorem 5.4], Dieulefait gives an example of a genus-2 curve over $\mathbb{Q}$ whose Jacobian has mod-ℓ monodromy equal to $\mathrm{GSp}_4(\mathbb{Z}/\ell\mathbb{Z})$

for $\ell \geq 5$. Similarly, in [ALS16, Corollary 1.1], an example of a genus-3 hyperelliptic curve over $\mathbb{Q}$ whose Jacobian has mod-ℓ Galois image equal to $\mathrm{GSp}_6(\mathbb{Z}/\ell\mathbb{Z})$ for primes $\ell \geq 3$ is constructed. However, in both of these cases, it is easy to check that these examples have mod-2 Galois image that is not maximal among all hyperelliptic curves of genus 2 or 3. In Theorem 1.3, we improve on the results of [Die02] and [ALS16], giving explicit examples of hyperelliptic curves of genus 2 and 3 over $\mathbb{Q}$ with maximal adelic Galois image. The reader may wish to also refer to the related recent paper [AD17], which constructs hyperelliptic curves with maximal mod-ℓ Galois image in all genera g with the property that $2g+2$ can be expressed as of sum of two primes in two different ways, with none of the primes being the largest prime less than $2g+2$.[1]

In addition to finding explicit examples of PPAVs with maximal Galois image, there are a number of results in the literature concerning how many members of a given family of PPAVs have maximal adelic Galois image. The first key result in this direction is due to Duke, who proved in [Duk97] that "most" elliptic curves $E/\mathbb{Q}$ in the standard family with Weierstrass equation $y^2 = x^3 + ax + b$ have the property that $\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GSp}_2(\mathbb{Z}/\ell\mathbb{Z})$ for every prime number ℓ; here, the term "most" means a density-1 subset of curves ordered by naïve height. Building upon the work of Duke, Jones proved in [Jon10, Theorem 4] that $[\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) : \rho_E(G_K)] = 2$ for most elliptic curves E in the standard family over $\mathbb{Q}$. In [Zyw10b, Theorem 1.15], Zywina generalized the above results, showing that most members of every non-isotrivial rational family of elliptic curves over an arbitrary number field have maximal adelic Galois image, subject to the constraints that arise from the arithmetic and geometric properties of the family under consideration. Additional results over $\mathbb{Q}$ were obtained in [Gra00], [CH05], and [CGJ11] (see [Zyw10b, p. 6] for a more detailed overview). In Theorem 1.2, we give an explicit version of [LSTX19, Theorem 1.1] – a result that generalizes Zywina's results to rational families of higher-dimensional PPAVs – for many common families of hyperelliptic curves. This yields a generalization of [Zyw10a, Theorem 1.2] and [Jon10, Theorem 4] to hyperelliptic curves of higher genus.

1.2. **Main Results.** In this paper, we primarily consider those PPAVs that arise as Jacobians of hyperelliptic curves belonging to one of the following four standard families; we restrict our consideration to curves of genus at least 2 because the results of Zywina in [Zyw10b] completely handle the case of elliptic curves.

Definition 1.1. Let $g \geq 2$ be an integer, and for $i \in \{1,2,3,4\}$ define $\mathscr{W}_{g,K}^{(i)}$ by

$$\mathscr{W}_{g,K}^{(1)} = \mathbb{A}^{2g+1}_{[a_0,\ldots,a_{2g}]} \setminus \Delta^{(1)}, \quad \mathscr{W}_{g,K}^{(2)} = \mathbb{A}^{2g+2}_{[a_0,\ldots,a_{2g+1}]} \setminus \Delta^{(2)},$$
$$\mathscr{W}_{g,K}^{(3)} = \mathbb{A}^{2g}_{[a_0,\ldots,a_{2g-1}]} \setminus \Delta^{(3)}, \quad \mathscr{W}_{g,K}^{(4)} = \mathbb{A}^{2g+1}_{[a_0,\ldots,a_{2g}]} \setminus \Delta^{(4)},$$

where each $\Delta^{(i)}$ is the discriminant locus, on which the indicated polynomial has at least one multiple root:

$$\begin{aligned} x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0 &\quad \rightsquigarrow \Delta^{(1)} \\ x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_0 &\quad \rightsquigarrow \Delta^{(2)} \\ x^{2g+1} + a_{2g-1}x^{2g-1} + \cdots + a_0 &\quad \rightsquigarrow \Delta^{(3)} \\ x^{2g+2} + a_{2g}x^{2g} + \cdots + a_0 &\quad \rightsquigarrow \Delta^{(4)}. \end{aligned}$$

[1]Note that [AD17] therefore does not address the cases $g = 2, 3$, which we cover in this paper.

Consider the following vanishing loci, and view them as families over $\mathscr{W}_{g,K}^{(i)}$ via projection onto the first factor:

$$V(y^2 - x^{2g+1} - a_{2g}x^{2g} - \cdots - a_0) \hookrightarrow \mathscr{W}_{g,K}^{(1)} \times \mathbb{A}^2_{[x,y]} \to \mathscr{W}_{g,K}^{(1)},$$
$$V(y^2 - x^{2g+2} - a_{2g+1}x^{2g+1} - \cdots - a_0) \hookrightarrow \mathscr{W}_{g,K}^{(2)} \times \mathbb{A}^2_{[x,y]} \to \mathscr{W}_{g,K}^{(2)},$$
$$V(y^2 - x^{2g+1} - a_{2g-1}x^{2g-1} - \cdots - a_0) \hookrightarrow \mathscr{W}_{g,K}^{(3)} \times \mathbb{A}^2_{[x,y]} \to \mathscr{W}_{g,K}^{(3)},$$
$$V(y^2 - x^{2g+2} - a_{2g}x^{2g} - \cdots - a_0) \hookrightarrow \mathscr{W}_{g,K}^{(4)} \times \mathbb{A}^2_{[x,y]} \to \mathscr{W}_{g,K}^{(4)}.$$

For $1 \le i \le 4$, define $\mathscr{Y}_{g,K}^{(i)}$, the *standard families* of genus-g hyperelliptic curves by completing the above smooth affine curve over $\mathscr{W}_{g,K}^{(i)}$ to a smooth projective curve over $\mathscr{W}_{g,K}^{(i)}$. The definition of $\Delta^{(i)}$ ensures that these are indeed genus-g hyperelliptic curves. For a K-valued point $u \in \mathscr{W}_{g,K}^{(i)}(K)$, we denote by A_u the Jacobian (which is necessarily a g-dimensional PPAV) of the fiber over u of the corresponding standard family.

As we show in Section 3.3, the mod-2 Galois image of the Jacobian of a member of $\mathscr{Y}_{g,K}^{(i)}$ always lands in a certain copy of the symmetric group $S_{2g+2-(i \bmod 2)} \subset \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. Denote by $\widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K}$ the intersection of the following two subgroups of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$: (1) the subgroup of those matrices with multiplier landing in $\chi(K) \subset \widehat{\mathbb{Z}}^\times$, where χ denotes the cyclotomic character, and (2) the preimage of $S_{2g+2-(i \bmod 2)}$ under the projection map $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. Let $\mathrm{Ht}\colon \mathbb{P}^r(\overline{K}) \to \mathbb{R}_{>0}$ denote the absolute multiplicative height on projective space, and define a height function $\|-\|$ on the lattice $\mathcal{O}_K^r$ sending $(t_1, \ldots, t_r) \mapsto \max_{\sigma,i} |\sigma(t_i)|$, where σ varies over all field embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$. Having fixed this notation, our first main theorem may be stated as follows:

Theorem 1.2. *Let $B > 0$, $i \in \{1,2,3,4\}$, $g \ge 2$, and let n be an arbitrarily positive integer. Let $\delta_{\mathbb{Q}} = 2$, and let $\delta_K = 1$ for $K \ne \mathbb{Q}$. Then $[\widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K} : \rho_{A_u}(G_K)] \ge \delta_K$ for all $u \in \mathscr{Y}_{g,K}^{(i)}(K)$, and we have the following asymptotic statements, with the implied constants depending only on n, g, and K:*

$$\frac{|\{u \in \mathscr{W}_{g,K}^{(i)}(\mathcal{O}_K) : \|u\| \le B,\ [\widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K} : \rho_{A_u}(G_K)] = \delta_K\}|}{|\{u \in \mathscr{W}_{g,K}^{(i)}(\mathcal{O}_K) : \|u\| \le B\}|} = 1 + O((\log B)^{-n}),$$
$$\frac{|\{u \in \mathscr{W}_{g,K}^{(i)}(K) : \mathrm{Ht}(u) \le B,\ [\widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K} : \rho_{A_u}(G_K)] = \delta_K\}|}{|\{u \in \mathscr{W}_{g,K}^{(i)}(K) : \mathrm{Ht}(u) \le B\}|} = 1 + O((\log B)^{-n}).$$

Furthermore, the statement above applies if we take $i = 2$ and replace $\mathscr{W}_{g,K}^{(2)}$ by any rational family of hyperelliptic curves dominating the moduli of hyperelliptic curves, so long as the map to the moduli of hyperelliptic curves has geometrically connected generic fiber.

The methods employed to prove density-1 results like Theorem 1.2 do not lend themselves well to the construction of explicit examples, which may be useful insofar as they can provide evidence in support of related conjectures. We now give two explicit examples, improving upon the examples of [Die02] and [ALS16] mentioned in Section 1.1. To the authors' knowledge, these are the first examples of hyperelliptic curves in genus $g = 2$ and 3 whose mod-ℓ monodromy is equal to $\mathrm{GSp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ when $\ell > 2$, and equal to S_{2g+2} when $\ell = 2$. Moreover, we show the Galois representations of these curves have index 2 in the group $\widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}}$. Note

that all hyperelliptic curves over $\mathbb{Q}$ have Galois representation strictly contained in $\widetilde{\mathrm{GSp}}_{2g+2,\mathbb{Q}}$, as follows from Corollary 3.10 (since the monodromy of any curve is contained in that of the universal family). Hence, our examples yield curves with maximal monodromy among all hyperelliptic curves of genus 2 and 3.

Theorem 1.3. *Let C_2 and C_3 over $\mathbb{Q}$ be smooth projective models of the affine plane curves cut out by the equations*

$$\begin{aligned} C_2: \quad & y^2 = x^6 + 7471225x^5 + 16548721x^4 + 6639451x^3 + 16857421x^2 + \\ & \qquad 20754195x + 9508695, \text{ and} \\ C_3: \quad & y^2 = x^8 + 10781051650x^7 + 5302830080x^6 + 33362176x^5 + 10656581376x^4 + \\ & \qquad 5522318080x^3 + 4238752256x^2 + 3613465600x + 3725404480. \end{aligned}$$

Then for each $g \in \{2,3\}$, the Jacobian J_{C_g} of C_g is a g-dimensional PPAV over $\mathbb{Q}$ satisfying the condition $[\widetilde{\mathrm{GSp}}_{2g+2,\mathbb{Q}} : \rho_{J_{C_g}}(G_{\mathbb{Q}})] = 2$.

Remark 1.4. In checking the examples declared in Theorem 1.3, we combined the methods developed in [AD17] and [Zyw15] to expedite the verification process. It is also possible to modify the techniques introduced in [Zyw15] to show that the curves cut out by the equations

$$f(x) = x^6 - 2x^4 - 2x^3 - 3x^2 - 2x + 1 \quad \text{and} \tag{1.1}$$

$$f(x) = x^8 - 4x^3 + 4x + 4, \tag{1.2}$$

which are of respective genera 2 and 3, both have maximal monodromy. The reader may contact any one of the authors if further details of the proof of this claim are desired.

The rest of this paper is organized as follows: Section 2 is concerned with proving the group-theoretic Theorem 2.2. In Section 3.2, we use Theorem 2.2 to prove Lemma 3.4, which is employed in the proof of Theorem 1.2 to verify the claimed value of δ_K. In Section 3.4 we compute the monodromy of various families of hyperelliptic curves. We combine these two results to prove Theorem 1.2 in Section 3.5. Finally, in Section 4, we prove Theorem 1.3.

2. Definitions and Properties of Symplectic Groups

This section is devoted to proving Theorem 2.2, which is needed for proving the main results of this paper, Theorems 1.2 and 1.3. We start in Sections 2.1 and 2.2.2 by defining symplectic groups, discussing their basic properties, and introducing some recurring notation. Then, in Section 2.2 we prove a result that is a crucial input to Section 3, where we prove Theorem 1.2. The reader may choose to continue directly to Section 3 after studying the statement of Theorem 2.2.

2.1. **Symplectic Groups.** Let R be a commutative ring, and let g be a positive integer. Let M be a free R-module of rank $2g$, and let $\langle -,- \rangle \colon M \times M \to R$ be a non-degenerate alternating bilinear form on M. Define the *general symplectic group* (otherwise known as the *group of symplectic similitudes*) $\mathrm{GSp}(M) \subset \mathrm{GL}(M)$ to be the subgroup of all R-automorphisms S such that there exists some $m_S \in R^\times$, called the *multiplier* of S, satisfying $\langle Sv, Sw \rangle = m_S \cdot \langle v, w \rangle$ for all $v, w \in M$. If m_S exists, then it is necessarily unique, and one easily checks that the

resulting *mult* map

$$\begin{aligned} \text{mult}\colon \mathrm{GSp}(M) &\to R^\times \\ S &\mapsto m_S \end{aligned}$$

is a group homomorphism; we call its kernel the *symplectic group* $\mathrm{Sp}(M)$.

Choose an R-basis for M, and denote by Ω_{2g} the matrix which expresses the inner product $\langle -, - \rangle$ with respect to this basis. The choice of basis gives rise to an identification $\mathrm{GL}(M) \simeq \mathrm{GL}_{2g}(R)$, and we take $\mathrm{GSp}_{2g}(R)$ to be the image of $\mathrm{GSp}(M)$ and $\mathrm{Sp}_{2g}(R)$ to be the image of $\mathrm{Sp}(M)$ under this identification. Let $\det\colon \mathrm{GL}_{2g}(R) \to R^\times$ be the determinant map, and observe that the diagram

$$\begin{array}{ccc} \mathrm{GSp}(M) & \xrightarrow{\sim} & \mathrm{GSp}_{2g}(R) \\ & \searrow^{\mathrm{mult}^g} & \downarrow \det \\ & & R^\times \end{array}$$

commutes. Note that $\mathrm{GSp}_{2g}(R) \subset \mathrm{GL}_{2g}(R)$ is the subgroup of all invertible matrices S satisfying $S^T \Omega_{2g} S = (\mathrm{mult}\, S)\, \Omega_{2g}$ and that $\mathrm{Sp}_{2g}(R) = \ker(\mathrm{mult}\colon \mathrm{GSp}_{2g}(R) \to R^\times)$.

Let $\mathrm{Mat}_{2g\times 2g}(R)$ be the space of $2g \times 2g$ matrices having entries in R, and consider the Lie algebras $\mathfrak{gsp}_{2g}(R)$ and $\mathfrak{sp}_{2g}(R)$ defined by

$$\begin{aligned} \mathfrak{gsp}_{2g}(R) &:= \{\Lambda \in \mathrm{Mat}_{2g\times 2g}(R) : \Lambda^T \Omega_{2g} + \Omega_{2g}\Lambda = d \cdot \Omega_{2g} \text{ for some } d \in R\}, \\ \mathfrak{sp}_{2g}(R) &:= \{\Lambda \in \mathrm{Mat}_{2g\times 2g}(R) : \Lambda^T \Omega_{2g} + \Omega_{2g}\Lambda = 0\}. \end{aligned}$$

When studying Galois representations associated to PPAVs, we usually take R to be one of the following: the profinite completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$, the ring of ℓ-adic integers $\mathbb{Z}_\ell$ for a prime number ℓ, or the finite cyclic ring $\mathbb{Z}/m\mathbb{Z}$ for a positive integer m. Observe that we have the following isomorphisms of topological groups:

$$\mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \simeq \varprojlim_k \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z}) \quad \text{and} \tag{2.1}$$

$$\prod_{\text{prime } \ell} \mathrm{GSp}_{2g}(\mathbb{Z}_\ell) \simeq \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \simeq \varprojlim_m \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}). \tag{2.2}$$

The isomorphisms (2.1) and (2.2) remain valid if GSp_{2g} is replaced by Sp_{2g}. As for the Lie algebras, note that by sending $\Lambda \mapsto \mathrm{id}_{2g} + \ell^k \Lambda$ we obtain group isomorphisms

$$\begin{aligned} \mathfrak{gsp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) &\simeq \ker(\mathrm{GSp}_{2g}(\mathbb{Z}/\ell^{k+1}\mathbb{Z}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})), \\ \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) &\simeq \ker(\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^{k+1}\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^k\mathbb{Z})) \end{aligned}$$

for every $k \geq 1$, so when it is useful or convenient, we will sometimes use the Lie algebra notation to denote the above kernels.

2.2. **Computing Commutators of Large Subgroups of** $\mathrm{GSp}_{2g}(\mathbb{Z}_2)$**.** The objective of this section is to prove a soon-to-be-useful theorem concerning the commutator of a subgroup of $\mathrm{GSp}_{2g}(\mathbb{Z}_2)$ which is the preimage (under mod-2 reduction) of a subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ that contains a copy of the symmetric group S_{2g+1}.

2.2.1. *Embedding the Symmetric Group, Take 1.* We asserted in the discussion immediately preceding the statement of Theorem 1.2 that the symmetric group S_{2g+1} may be viewed as a subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. We now provide a working description of the way in which this embedding is constructed; the manner in which this description applies to the context of studying hyperelliptic curves is discussed in Section 3.3.

Lemma 2.1. *For every $g \geq 2$, we have an inclusion $S_{2g+2} \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. When $g = 2$, this inclusion is an isomorphism.*

Proof. Let V be a $(2g+2)$-dimensional vector space over $\mathbb{F}_2$, and equip $V \simeq \mathbb{F}_2^{2g+2}$ with the standard inner product. Let $t := (1, \ldots, 1)$ be the vector whose components are all equal to 1. Then the hyperplane $t^\perp \subset V$ of all vectors orthogonal to t actually contains t since $\dim V = 2g+2$ is even. Moreover, if we define $W = t^\perp / \operatorname{span}(t)$, the inner product on V descends to a nondegenerate alternating bilinear form on W. The action of S_{2g+2} given by permuting the coordinates of V fixes both t and $t^\perp$, so it descends to an action on W that preserves the bilinear form. Thus, we obtain an inclusion of S_{2g+2} into the group of symplectic transformations of W with multiplier 1. For a more conceptual explanation of this inclusion in terms of the two-torsion of hyperelliptic curves, see Section 3.3. Upon choosing a suitable basis for W we may identify this group with $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. For $g = 2$, the resulting inclusion is an isomorphism because $\#(S_6) = 720 = \#(\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z}))$. □

We embed $S_{2g+1} \hookrightarrow S_{2g+2}$ as the subgroup fixing the vector $(0, \ldots, 0, 1) \in \mathbb{F}_2^{2g+2}$.

2.2.2. *Notation.* In what follows, we shall (for the most part) study subquotients of $\mathrm{GSp}_{2g}(\mathbb{Z}_2)$ and $\mathrm{GSp}_{2g}(\mathbb{Z}/2^k\mathbb{Z})$ for k a positive integer. We employ the following notational conventions:

- Let $H \subset \mathrm{GSp}_{2g}(\mathbb{Z}_2)$ be a closed subgroup.
- For $m, n \in \mathbb{Z}_{>0} \cup \{\infty\}$ with $m > n$, let $\mathrm{G}\Phi_{2^m \to 2^n} \colon \mathrm{GSp}_{2g}(\mathbb{Z}/2^m\mathbb{Z}) \to \mathrm{GSp}_{2g}(\mathbb{Z}/2^n\mathbb{Z})$ and $\Phi_{2^m \to 2^n} \colon \mathrm{Sp}_{2g}(\mathbb{Z}/2^m\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/2^n\mathbb{Z})$ be the natural projection maps. (When $m = \infty$, $\mathbb{Z}/2^m\mathbb{Z}$ denotes $\mathbb{Z}_2$.)
- Let $H(2^k) = \mathrm{G}\Phi_{2^\infty \to 2^k}(H) \subset \mathrm{GSp}_{2g}(\mathbb{Z}/2^k\mathbb{Z})$ be the mod-2^k reduction of H.
- For any topological group G, let $[G, G]$ be the closure of its commutator subgroup, and let $G^{\mathrm{ab}} := G/[G, G]$ be its abelianization.
- For each positive integer n, let id_n denote the $n \times n$ identity matrix.

2.2.3. *Main Group Theoretic Result.* We can now state the main theorem of this section.

Theorem 2.2. *Let $g \geq 2$. Let $H \subset \mathrm{GSp}_{2g}(\mathbb{Z}_2)$ be a subgroup such that $H = \mathrm{G}\Phi^{-1}_{2^\infty \to 2}(H(2))$ and such that $H(2)$ contains S_{2g+1}. Then we have that*

$$[H, H] = \Phi^{-1}_{2^\infty \to 2}([H(2), H(2)]). \tag{2.3}$$

Moreover, the homomorphism $H \to (H(2))^{\mathrm{ab}} \times (\mathbb{Z}_2)^\times$, defined on the left component by postcomposing reduction mod-2 with the abelianization map $H(2) \to H(2)^{\mathrm{ab}}$ and on the right component by the multiplier map mult*, induces an isomorphism*

$$H^{\mathrm{ab}} \simeq (H(2))^{\mathrm{ab}} \times (\mathbb{Z}_2)^\times. \tag{2.4}$$

The relevance of Theorem 2.2 to studying Galois representations of Jacobians of hyperelliptic curves is described in Lemma 3.4, given at the beginning of Section 3. We prove Theorem 2.2 next in Section 2.3.

2.3. **Proof of Theorem 2.2.**

Proof of Theorem 2.2 assuming Corollary 2.5 and Proposition 2.10. Because we have that

$$[H, H](2) = [H(2), H(2)],$$

in order to prove (2.3), it suffices to prove that $[H, H] \supset \ker \Phi_{2^\infty \to 2}$. To prove this statement, it further suffices to prove the following two statements:

(A) $[H, H] \supset \ker \Phi_{2^\infty \to 4}$,
(B) $[H(4), H(4)] \supset \ker \Phi_{4 \to 2}$.

Statement (A) is proven in Corollary 2.5 and statement (B) is proven in Proposition 2.10. To complete the proof, we only need verify (2.4). Note that (2.3) tells us that the map $H \to (H(2))^{\mathrm{ab}} \times (\mathbb{Z}_2)^\times$ has kernel precisely $[H, H]$, so to prove (2.4), it suffices to check that the map $H \to (H(2))^{\mathrm{ab}} \times (\mathbb{Z}_2)^\times$ is surjective. But this is easy to check by hand: For $\alpha \in (\mathbb{Z}_2)^\times$, let N_α be the matrix which has alternating 1's and α's on the diagonal, taken with respect to a symplectic basis $e_1, \ldots, e_{2g}$ where $\langle e_i, e_j \rangle$ is 1 if $i = 2k, j = 2k+1$ for some integer k, is -1 if $i = 2k+1, j = 2k$, and is 0 otherwise. For $(M_2, \alpha) \in (H(2))^{\mathrm{ab}} \times (\mathbb{Z}_2)^\times$, let $M_2^\infty \in \Phi^{-1}_{2^\infty \to 2}(M_2)$, and observe that $M_2^\infty \cdot N_\alpha \mapsto (M_2, \alpha)$ via the map $H \to (H(2))^{\mathrm{ab}} \times (\mathbb{Z}_2)^\times$. This concludes the proof of our main group-theoretic result, Theorem 2.2. □

2.3.1. *Proving Statement (A).* We begin with the following lemma, in which we compute the commutator subalgebra of $\mathfrak{gsp}_{2g}(\mathbb{Z}/2\mathbb{Z})$.

Lemma 2.3. *Let ℓ be a prime number. We have* $[\mathfrak{gsp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}), \mathfrak{gsp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})] = \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.[2]

Proof. For convenience, let $\mathfrak{g}_\ell := [\mathfrak{gsp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}), \mathfrak{gsp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})]$. That $\mathfrak{g}_\ell \subset \mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is obvious from the definitions of $\mathfrak{gsp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ and $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$, so it suffices to prove that reverse containment. For $\ell \geq 3$, this is immediate from [LSTX19, Proposition 2.10], so we may restrict to the case where $\ell = 2$ (note that this is the case of primary interest to us).[3] Choose a basis for $(\mathbb{Z}/2\mathbb{Z})^{2g}$ with respect to which Ω_{2g} is given by $\Omega_{2g} = \left[\begin{array}{c|c} 0 & \mathrm{id}_g \\ \hline -\mathrm{id}_g & 0 \end{array}\right]$. Then $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ consists of matrices of the form $\left[\begin{array}{c|c} A & B \\ \hline C & -A^T \end{array}\right]$ where $A, B, C \in \mathrm{Mat}_{g\times g}(\mathbb{Z}/2\mathbb{Z})$ and B, C are required to be symmetric. Since we have

$$\left[\left[\begin{array}{c|c} A & 0 \\ \hline 0 & -A^T \end{array}\right], \left[\begin{array}{c|c} D & 0 \\ \hline 0 & -D^T \end{array}\right]\right] = \left[\begin{array}{c|c} AD - DA & 0 \\ \hline 0 & A^TD^T - D^TA^T \end{array}\right], \tag{2.5}$$

all block-diagonal matrices in $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ with every diagonal entry equal to 0 are contained in $\mathfrak{g}_2$. Moreover, for symmetric $B, C, E, F \in \mathrm{Mat}_{g\times g}(\mathbb{Z}/2\mathbb{Z})$, we have

$$\left[\left[\begin{array}{c|c} 0 & B \\ \hline C & 0 \end{array}\right], \left[\begin{array}{c|c} 0 & E \\ \hline F & 0 \end{array}\right]\right] = \left[\begin{array}{c|c} BF - EC & 0 \\ \hline 0 & CE - FB \end{array}\right], \tag{2.6}$$

[2]This result is a variant of [LSTX19, Proposition 2.10].

[3]In essence, the reason why the case of ℓ odd needs to be handled separately is that $\mathfrak{sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is a perfect Lie algebra if and only if ℓ is odd, a result due to Hogeweij [Hog82].

and we can arrange that $BF - EC$ is an elementary matrix with a single nonzero entry on the diagonal. Summing matrices from (2.5) and (2.6), tells us that all block-diagonal matrices in $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ are contained in $\mathfrak{g}_2$. Additionally, note that $\mathfrak{gsp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ also contains $\left[\begin{array}{c|c} \mathrm{id}_g & 0 \\ \hline 0 & 0 \end{array}\right]$, from which we deduce that $\mathfrak{g}_2$ contains

$$\left[\left[\begin{array}{c|c} \mathrm{id}_g & 0 \\ \hline 0 & 0 \end{array}\right], \left[\begin{array}{c|c} 0 & B \\ \hline 0 & 0 \end{array}\right]\right] = \left[\begin{array}{c|c} 0 & B \\ \hline 0 & 0 \end{array}\right], \tag{2.7}$$

where $B \in \mathrm{Mat}_{g\times g}(\mathbb{Z}/2\mathbb{Z})$ is symmetric. One similarly checks that $\mathfrak{g}_2$ contains $\left[\begin{array}{c|c} 0 & 0 \\ \hline C & 0 \end{array}\right]$, for $C \in \mathrm{Mat}_{g\times g}(\mathbb{Z}/2\mathbb{Z})$ symmetric. It follows that $\mathfrak{g}_2 \supset \mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. □

Corollary 2.4. *We have* $[\ker \mathrm{G}\Phi_{2^\infty\to 2}, \ker \mathrm{G}\Phi_{2^\infty\to 2}] = \ker \Phi_{2^\infty\to 4}$.

Proof. Clearly $[\ker \mathrm{G}\Phi_{2^\infty\to 2}, \ker \mathrm{G}\Phi_{2^\infty\to 2}] \subset \ker \Phi_{2^\infty\to 4}$, so it suffices to prove the reverse inclusion. By [LSTX19, Lemma 2.11], we have that $[\ker \mathrm{G}\Phi_{2^\infty\to 2}, \ker \mathrm{G}\Phi_{2^\infty\to 2}] \supset \ker \Phi_{2^\infty\to 8}$. Then, identifying $\mathfrak{gsp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ with $\ker \mathrm{G}\Phi_{8\to 4}$ and $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ with $\ker \Phi_{8\to 4}$, we have by Lemma 2.3 that

$$\begin{aligned} \ker \Phi_{8\to 4} &= [\ker \mathrm{G}\Phi_{8\to 4}, \ker \mathrm{G}\Phi_{8\to 4}] = [\ker \mathrm{G}\Phi_{2^\infty\to 4}, \ker \mathrm{G}\Phi_{2^\infty\to 4}]\,(8) \\ &\subset [\ker \mathrm{G}\Phi_{2^\infty\to 2}, \ker \mathrm{G}\Phi_{2^\infty\to 2}]\,(8) \end{aligned}$$

It follows that $[\ker \mathrm{G}\Phi_{2^\infty\to 2}, \ker \mathrm{G}\Phi_{2^\infty\to 2}] \supset \ker \Phi_{2^\infty\to 4}$. □

Corollary 2.5. *We have* $\ker \Phi_{2^\infty\to 4} \subset [H, H]$.

Proof. The hypothesis that $H = \mathrm{G}\Phi^{-1}_{2^\infty\to 2}(H(2))$ implies that $\ker \mathrm{G}\Phi_{2^\infty\to 2} \subset H$, and hence $[\ker \mathrm{G}\Phi_{2^\infty\to 2}, \ker \mathrm{G}\Phi_{2^\infty\to 2}] \subset [H, H]$. Applying Corollary 2.4 then yields the desired result. □

2.3.2. *Proving Statement (B): Tensor Product Notation.* Just as we did in the proof of Lemma 2.3, we must choose a basis with respect to which our symplectic form has an easy-to-use matrix representation. The goal of this subsection is to choose such a basis and to develop a shorthand notation for this basis. In Sections 2.3.3 and 2.3.4, we use this notation to prove Statement (B), thereby completing the proof of Theorem 2.2.

Recall the notation introduced in the first paragraph of Section 2.1: R is a commutative ring (which we will take to be either $\mathbb{Z}_2$ or $\mathbb{Z}/4\mathbb{Z}$), and M is a free R-module of rank $2g$. We choose a basis $(e_1, \ldots, e_{2g})$ for M so that the symplectic form $\langle -, - \rangle$ is given by

$$\langle e_i, e_j \rangle := \begin{cases} j - i & \text{if } |j - i| = 1 \text{ and } \max\{i, j\} \equiv 0 \,(\mathrm{mod}\, 2) \\ 0 & \text{otherwise} \end{cases}$$

We may alternatively construct M as follows. Let $N_1 \simeq R^2$ have basis (x_1, x_2) and let $N_2 \simeq R^g$ have basis $(y_1, \ldots, y_g)$. Endow N_1 with the alternating form given by $\langle x_i, x_j \rangle = j - i$, and endow N_2 with the symmetric form given by $\langle y_i, y_j \rangle = \delta_{ij}$, where δ_{ij} denotes the Kronecker δ-function as usual. Then if we take $M := N_1 \otimes N_2$, we have that $(x_i \otimes y_j : i \in \{1, 2\},\, j \in \{1, \ldots, g\})$ is a basis for M and that M is equipped with an alternating form defined on simple tensors by

$$\langle a_1 \otimes b_1, a_2 \otimes b_2 \rangle := \langle a_1, a_2 \rangle \cdot \langle b_1, b_2 \rangle.$$

Note that the map sending $x_i \otimes y_j \mapsto e_{2j+i-2}$ gives an identification between our two different constructions of M.

Linear operators on M are R-linear combinations of tensor products of linear operators on N_1 with linear operators on N_2. If we denote by x_{ij} the row-i, column-j elementary matrix acting on N_1 and by y_{mn} the row-m, column-n elementary matrix acting on N_2, then a basis for $\mathrm{End}(M)$ is given by $(x_{ij} \otimes y_{mn} : i,j \in \{1,2\},\, m,n \in \{1,\dots,g\})$. Also notice that any element $\Lambda \in \mathrm{End}(M)$ may be expressed as

$$\Lambda = \sum_{i=1}^{g}\sum_{j=1}^{g} \Lambda_{ij} \otimes y_{ij} \tag{2.8}$$

where $\Lambda_{ij} \in \mathrm{End}(N_1)$ for all $i,j \in \{1,\dots,g\}$.

Proposition 2.6. *Let $\phi \in \mathrm{End}(\mathrm{End}(N_1))$ be defined by*

$$x_{11} \mapsto -x_{22}, \quad x_{22} \mapsto -x_{11}, \quad x_{12} \mapsto x_{12}, \quad x_{21} \mapsto x_{21}.$$

The Lie algebra $\mathfrak{gsp}_{2g}(R)$ consists of those elements $\Lambda \in \mathrm{End}(M)$ with $\Lambda_{ij} \in \mathrm{End}(N_1)$ such that there exists $d \in R$ satisfying

$$\phi(\Lambda_{ji}) = \Lambda_{ij} - (d\delta_{ij}) \cdot \mathrm{id}_2\,.$$

Moreover, $\mathfrak{sp}_{2g}(R)$ admits an analogous description in which d is required to be zero.

Proof. Since $\Omega_{2g}^2 = -\,\mathrm{id}_{2g}$, the defining equation for $\mathfrak{gsp}_{2g}(R)$ is equivalent to

$$\Omega_{2g}\Lambda^T\Omega_{2g} - \Lambda + d \cdot (\mathrm{id}_2 \otimes \mathrm{id}_g) = 0. \tag{2.9}$$

Note that the identity element $\mathrm{End}(N_2)$ is given by $\mathrm{id}_g = y_{11} + \cdots + y_{gg}$. Substituting this in along with the expansion (2.8) for Λ as well as $(x_{12} - x_{21}) \otimes \mathrm{id}_g$ for Ω_{2g} on the left-hand side of (2.9) yields that

$$\sum_{i=1}^{g}\sum_{j=1}^{g} \big[(x_{12}-x_{21})(\Lambda_{ji})^T(x_{12}-x_{21}) - \Lambda_{ij} + (d\delta_{ij}) \cdot \mathrm{id}_2\,\big] \otimes y_{ij} = 0,$$

which is equivalent to the following condition:

$$(x_{12}-x_{21})(\Lambda_{ji})^T(x_{12}-x_{21}) = \Lambda_{ij} - (d\delta_{ij}) \cdot \mathrm{id}_2$$

The desired result then follows upon observing that $(x_{12}-x_{21})(\Lambda_{ji})^T(x_{12}-x_{21}) = \phi(\Lambda_{ji})$. □

Remark 2.7. When $R = \mathbb{Z}/2\mathbb{Z}$, minus signs may be ignored, so the operator ϕ may be concisely described as transposition across the anti-diagonal. It follows from Proposition 2.6 that the following is a basis for $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$:

$$\big(\mathrm{id}_2 \otimes y_{ii}, x_{12} \otimes y_{ii}, x_{21} \otimes y_{ii} : i \in \{1,\dots,g\}\big) \cup$$
$$\big(x_{12} \otimes (y_{ij}+y_{ij}), x_{11} \otimes y_{ij} + x_{22} \otimes y_{ji}, x_{21} \otimes (y_{ij}+y_{ji}), x_{22} \otimes y_{ij} + x_{11} \otimes y_{ji} : 1 \le i < j \le g\big).$$

In Section 2.3.4, it will be convenient to define a function ind that assigns to each of the above basis elements the value of i (e.g., $\mathrm{ind}(\mathrm{id}_2 \otimes y_{ii}) = i$ and $\mathrm{ind}(x_{12} \otimes (y_{ij}+y_{ij})) = i$).

2.3.3. *Proving Statement (B): Describing the Action of S_{2g+2}.* We now seek to describe the embedding $S_{2g+2} \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ from Lemma 2.1 in terms of the tensor product notation that we just introduced in Section 2.3.2. To this end, we set $R = \mathbb{Z}/2\mathbb{Z}$, so that $M \simeq \mathbb{F}_2^{2g}$.

Lemma 2.8. *Recall notation from the proof of Lemma 2.1. The map $\psi : M \to t^\perp/\langle t\rangle$ of symplectic vector spaces defined by*

$$x_1 \otimes y_n \mapsto \sum_{i=1}^{2n} e_i \quad \text{and} \quad x_2 \otimes y_n \mapsto e_{2n+1} + \sum_{i=1}^{2n-1} e_i \quad \text{for each} \quad n \in \{1, \dots, g\}$$

is an isomorphism.

Proof. The lemma follows immediately from the observation that ψ identifies the symplectic forms of M and $t^\perp/\langle t\rangle$. □

Recall that the group S_{2g+2} is generated by the adjacent transpositions T_k for $k \in \{1, \dots, 2g+1\}$ whose cycle types are given by $T_k = (k, k+1)$. We now compute the action of T_k on M for each k:

Lemma 2.9. *When viewed as operators on M, the transpositions T_k are given by*

$$T_{2n} = \mathrm{id}_{2g} + (x_{11} + x_{12} + x_{21} + x_{22}) \otimes y_{nn},$$
$$T_{2n+1} = \mathrm{id}_{2g} + x_{12} \otimes (y_{nn} + y_{(n+1)n} + y_{n(n+1)} + y_{(n+1)(n+1)}),$$

according as $k = 2n$ or $k = 2n+1$, where any term with an out-of-range index is zero.

Proof. The result for $k = 2n$ follows from the observation that T_{2n} swaps $x_1 \otimes y_n$ with $x_2 \otimes y_n$ and keeps all the other basis vectors fixed. As for $k = 2n+1$, we break into three cases:

(1) Suppose $n = 0$. The transposition T_1 sends

$$\psi(x_2 \otimes y_1) = (e_1 + e_3) \mapsto (e_1 + e_2) + (e_1 + e_3) = \psi(x_1 \otimes y_1) + \psi(x_2 \otimes y_2)$$

and fixes all other $\psi(x_i \otimes y_j)$. Thus, T_1 is given by $T_1 = \mathrm{id}_{2g} + x_{12} \otimes y_{11}$.

(2) Suppose $n = g$. The transposition T_{2g+1} sends

$$\psi(x_2 \otimes y_g) = e_{2g+1} + \sum_{i=1}^{2g-1} e_i \mapsto \sum_{i=1}^{2g+1} e_i + \sum_{i=1}^{2g-1} e_i = e_{2g} + e_{2g+1} = \psi(x_1 \otimes y_g) + \psi(x_2 \otimes y_g)$$

and fixes all other $\psi(x_i \otimes y_j)$. Thus, T_g is given by $T_{2g+1} = \mathrm{id}_{2g} + x_{12} \otimes y_{gg}$.

(3) Finally, suppose $n \in \{1, \dots, g-1\}$. The transposition T_{2n+1} sends

$$\begin{aligned}\phi(x_2 \otimes y_n) = e_{2n+1} + \sum_{i=1}^{2n-1} e_i \;\mapsto\; & \sum_{i=1}^{2n+2} e_i + \left(e_{2n+1} + \sum_{i=1}^{2n-1} e_i\right) + \sum_{i=1}^{2n} e_i \\ & = \psi(x_1 \otimes y_{n+1}) + \psi(x_2 \otimes y_n) + \psi(x_1 \otimes y_n),\end{aligned}$$

$$\begin{aligned}\psi(x_2 \otimes y_{n+1}) = e_{2n+3} + \sum_{i=1}^{2n+1} e_i \;\mapsto\; & e_{2n+3} + \sum_{i=1}^{2n+1} e_i + \sum_{i=1}^{2n+2} e_i + \sum_{i=1}^{2n} e_i \\ & = \psi(x_2 \otimes y_{n+1}) + \psi(x_1 \otimes y_{n+1}) + \psi(x_1 \otimes y_n),\end{aligned}$$

and fixes all other $\psi(x_i \otimes y_n)$. Thus, T_{2n+1} is given by

$$T_{2n+1} = \mathrm{id}_{2g} + x_{12} \otimes (y_{nn} + y_{(n+1)n} + y_{n(n+1)} + y_{(n+1)(n+1)}).$$

The result for $k = 2n+1$ follows immediately from points (1)–(3) above. □

2.3.4. *Finishing the Proof of Statement (B).*

Proposition 2.10. *We have* $[H(4), H(4)] \supset \ker \Phi_{4\to 2}$.

Proof. The assumption that $H = \mathrm{G}\Phi^{-1}_{2^\infty\to 2}(H(2))$ implies that $\ker \mathrm{G}\Phi_{4\to 2} \subset H(4)$. Recall that we may identify $\ker \mathrm{G}\Phi_{4\to 2}$ with $\mathfrak{gsp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, so that each $S \in \ker \mathrm{G}\Phi_{4\to 2}$ may be expressed as $S = \mathrm{id}_{2g} + 2\Lambda$ where $\Lambda \in \mathfrak{gsp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. The assumption that $H(2)$ contains S_{2g+1} tells us that for any $M_2 \in S_{2g+1} \subset \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, we may lift M_2 to an element $M_4 \in H(4)$. In particular, we have that

$$\mathrm{id}_{2g} + 2(\Lambda + M_2\Lambda M_2^{-1}) = (\mathrm{id}_{2g} + 2\Lambda)^{-1} M_4 (\mathrm{id}_{2g} + 2\Lambda) M_4^{-1} \in [H(4), H(4)].$$

To complete the proof, it suffices to show that matrices of the form $\Lambda + M_2\Lambda M_2^{-1}$ span all of $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. Let $V = \mathrm{span}(\Lambda + M_2\Lambda M_2^{-1} : \Lambda \in \mathfrak{gsp}_{2g}(\mathbb{Z}/2\mathbb{Z}) \text{ and } M_2 \in S_{2g+1})$.

It suffices to restrict our consideration to matrices M_2 corresponding to transpositions $T_k \in S_{2g+1}$. Note that $T_k = (T_k)^{-1}$, so that if we write $T_k = \mathrm{id}_{2g} + N_k$, then we have

$$\Lambda + T_k\Lambda(T_k)^{-1} = N_k\Lambda + \Lambda N_k + N_k\Lambda N_k. \tag{2.10}$$

As in Lemma 2.9, we will have to treat the cases $k = 2n$ and $k = 2n+1$ separately. In what follows, we induct on the value of the ind function that V contains the seven types of basis elements listed in Remark 2.7. First, however, we perform some calculations that serve to greatly simplify this inductive argument. Combining Lemma 2.9 with (2.10) and taking $\Lambda = x_{11} \otimes \mathrm{id}_g$, we find that

$$\Lambda + T_{2n}\Lambda T_{2n} = \mathrm{id}_2 \otimes y_{nn} \in V, \tag{2.11}$$

$$\Lambda + T_{2n-1}\Lambda T_{2n-1} = x_{12} \otimes (y_{(n-1)(n-1)} + y_{(n-1)n} + y_{n(n-1)} + y_{nn}) \in V. \tag{2.12}$$

Repeating this calculation for $k = 2n$ but taking $\Lambda = x_{12} \otimes y_{nn}$, we find that

$$\Lambda + T_{2n}\Lambda T_{2n} = (x_{12} + x_{21}) \otimes y_{nn} \in V. \tag{2.13}$$

Now fix n, ℓ with $\ell > n$, and take $\Lambda = M \otimes y_{n\ell} + \phi(M) \otimes y_{\ell n}$ for any $M \in \mathrm{Mat}_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$. By Proposition 2.6, all such Λ are elements of $\mathfrak{gsp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. We find that

$$\begin{aligned}\Lambda + T_{2n}\Lambda T_{2n} = (x_{11} + x_{12} + x_{21} + x_{22})M \otimes y_{n\ell} + \\ \phi(M)(x_{11} + x_{12} + x_{21} + x_{22}) \otimes y_{\ell n} \in V,\end{aligned} \tag{2.14}$$

$$\Lambda + T_{2n-1}\Lambda T_{2n-1} = x_{12}M \otimes (y_{n\ell} + y_{(n-1)\ell}) + \phi(M)x_{12} \otimes (y_{\ell n} + y_{\ell(n-1)}) \in V. \tag{2.15}$$

Taking $M = x_{11}$ in (2.14), so that $\phi(M) = x_{22}$, yields that

$$(x_{11} + x_{21}) \otimes y_{n\ell} + (x_{21} + x_{22}) \otimes y_{\ell n} \in V, \tag{2.16}$$

and taking $M = x_{22}$ in (2.14), so that $\phi(M) = x_{11}$, yields that

$$(x_{12} + x_{22}) \otimes y_{n\ell} + (x_{11} + x_{12}) \otimes y_{\ell n} \in V. \tag{2.17}$$

Taking $M = x_{22}$ in (2.15), so that $\phi(M) = x_{11}$, yields that

$$x_{12} \otimes (y_{n\ell} + y_{\ell n}) \in V \tag{2.18}$$

and taking $M = x_{21}$ in (2.18), so that $\phi(M) = x_{21}$, yields that

$$x_{11} \otimes y_{n\ell} + x_{22} \otimes y_{\ell n} \in V. \tag{2.19}$$

We are now ready to carry out the induction. For the base case, we need to check that all basis vectors with ind-value equal to 1 are in V; this follows immediately upon taking $n = 1$ in (2.11)–(2.19). Next, suppose for some $N \in \{1, \dots, g\}$ we have that all basis vectors with ind-value less than N are in V. Taking $n = N$ in (2.11)–(2.19) and applying the inductive hypothesis yields that all basis vectors with ind-value equal to N are in V. □

3. Proof of Theorem 1.2

In this section, we prove the first main result of this paper, namely Theorem 1.2. We begin in Section 3.1 with a description of the relevant background material on Galois representations of PPAVs. Then, in Section 3.2, we prove a group-theoretic Lemma, useful for determining δ_K. In Section 3.3, we describe the particular manner in which we embed S_{2g+2} as a subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. In Section 3.4 we determine the monodromy groups of the four families of hyperelliptic curves introduced in Definition 1.1 and the monodromy of the universal family over the moduli stack of hyperelliptic curves. Finally, in Section 3.5, we complete the proof of Theorem 1.2.

3.1. **Background.** Let K be a number field, let $r \geq 0$ be an integer, and let $U \subset \mathbb{P}^r_K$ be an open subscheme. For an integer $g \geq 0$, let A be a family of g-dimensional PPAVs over U, by which we mean that A is an abelian scheme over U, meaning that $A \to U$ is a proper smooth group scheme with geometrically connected fibers of dimension g, and A is equipped with a principal polarization over U. Because the base U is rational, we call $A \to U$ a *rational family*. By construction, the fiber A_u of the morphism $A \to U$ over any K-valued point $u \in U(K)$ is a g-dimensional PPAV over K.

Recall that the action of the étale fundamental group $\pi_1(U)$ on the torsion points of a chosen geometric generic fiber of $A \to U$ gives rise to a continuous linear representation whose image is constrained by the Weil pairing to lie in the general symplectic group $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. We denote the resulting *adelic representation* by

$$\rho_A \colon \pi_1(U) \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}).^4 \tag{3.1}$$

We now define the monodromy groups associated to ρ_A. We call the image of $\rho_A \colon \pi_1(U) \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ the *monodromy* of the family $A \to U$, and we denote it by H_A. We write $H_A(m)$ for the mod-m reductions and $H_{A,\ell}$ for the ℓ-adic reductions of the above-defined monodromy groups.

Remark 3.1. Let $u \in U(K)$ be a K-valued point. Precomposing the adelic representation with the induced map $\pi_1(u) \to \pi_1(U)$ gives a representation $\pi_1(u) \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ whose image we denote by H_{A_u}. Because $\pi_1(u) \simeq G_K$, the representation ρ_{A_u} obtained by restricting ρ_A to A_u is the same as the adelic representation ρ_{A_u} discussed in Section 1.1.

Remark 3.2. For a commutative ring R, recall from the definition of the general symplectic group that we have a multiplier map $\mathrm{mult} \colon \mathrm{GSp}_{2g}(R) \to R^\times$. If χ denotes the cyclotomic character, then for a PPAV A it follows from G_K-invariance of the Weil pairing that $\chi = \mathrm{mult} \circ \rho_A$. More generally, if $A \to U$ is a family of PPAVs with U normal and integral, and if ϕ denotes the map $\pi_1(U) \to \pi_1(\operatorname{Spec} K)$ induced by the structure map $U \to \operatorname{Spec} K$, then we have that $\chi \circ \phi = \mathrm{mult} \circ \rho_A$

[4]The map in (3.1) is well-defined up to the choice of base-point, and choosing a different base-point would only alter the image of ρ_A by an inner automorphism. For this reason, when it will not lead to confusion, we may omit the base-point from our notation.

3.2. **Computing δ_K.** In this section, we prove Lemma 3.4, which is used to compute the value of δ_K in the proof of Theorem 1.2, given in Section 2.3. In order to state Lemma 3.4, we need the following definition, in which we introduce notation used throughout the paper to denote various lifts of S_{2g+i}:

Definition 3.3. For $i \in \{1, 2\}$, we define

$$\widetilde{\mathfrak{S}}_{2g+i} := (\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z}))^{-1}(S_{2g+i}) \qquad \text{and} \qquad \mathfrak{S}_{2g+i} := \Phi_{2^\infty \to 2}^{-1}(S_{2g+i}).$$

The next lemma applies Theorem 2.2 to determine how large the commutator subgroup of $\widetilde{\mathrm{G}\mathfrak{S}}_{2g+i,K}$, is as a subgroup of $\widetilde{\mathfrak{S}}_{2g+i}$:

Lemma 3.4. *Let $g \geq 2$, let $i \in \{1, 2\}$ and let $H \subset \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ be a closed subgroup. Suppose that*

- $H_2 = \mathrm{G}\Phi_{2^\infty \to 2}^{-1}(S_{2g+i})$, *and*
- $H(\ell) \supset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ *for $\ell \geq 3$.*

Then

$$[H, H] = \Phi_{2^\infty \to 2}^{-1}(A_{2g+i}) \times \prod_{\ell \geq 3} \mathrm{Sp}_{2g}(\mathbb{Z}_\ell),$$

where A_{2g+i} denotes the alternating group on $2g + i$ letters.

Proof. By Theorem 2.2,

$$[H, H]_2 = [H_2, H_2] = \Phi_{2^\infty \to 2}^{-1}(A_{2g+i}).$$

Also, note that for $\ell \geq 3$,

$$\begin{aligned}[H, H](\ell) &= [H(\ell), H(\ell)] \\ &\supset [\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})] \\ &= \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}),\end{aligned}$$

the last equality following from [O'M78, 3.3.6]. We now appeal to the fact that a closed subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ mapping onto $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ must in fact be all of $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ for $g > 1$. This fact was shown in [Wei96, Theorem B] (except for the case where $g = 3$ and $\ell = 2$), as well as in [Vas03, Theorem 1.3], and then again in [LSTX19, Proposition 2.5]. Applying this fact to $[H, H] \subset \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ gives the result. □

Corollary 3.5. *For H as in Lemma 3.4, we have $[\widetilde{\mathfrak{S}}_{2g+i} : [H, H]] = 2$. In particular, $[\widetilde{\mathfrak{S}}_{2g+i} : [\widetilde{\mathrm{G}\mathfrak{S}}_{2g+i,K}, \widetilde{\mathrm{G}\mathfrak{S}}_{2g+i,K},]] = 2$.*

3.3. **Embedding the Symmetric Group, Take 2.** In Section 2.2.1 we constructed the well-known embedding $S_{2g+2} \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. Beginning with

$$\begin{aligned}V &\simeq \mathbb{F}_2^{2g+2} \\ t &= (1, \ldots, 1) \in V \\ W &= t^\perp / \operatorname{span}(t),\end{aligned}$$

we observed that the action of S_{2g+2} on the basis vectors of V descends to a symplectic action on W. Our goal in this section is to relate this embedding with the mod-2 Galois representation attached to a family of hyperelliptic curves, by proving the following result:

Theorem 3.6. *Given a family $\mathcal{C} \to \mathcal{U}$ of hyperelliptic curves (where $\mathcal{U}$ is any stack), and a geometric generic point $\overline{\eta} \hookrightarrow \mathcal{U}$, the monodromy group $\rho_2(\pi_1(\mathcal{U}, \overline{\eta})) \subset \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ is in fact contained in $S_{2g+2} \subset \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. As a subgroup of S_{2g+2}, the monodromy group is given by the action of $\pi_1(\mathcal{U})$ on the Weierstrass points of $\mathcal{C}_{\overline{\eta}}$.*

This has an immediate consequence for our standard families:

Corollary 3.7. *For $i \in \{1, 2, 3, 4\}$, we have $H_{\mathscr{Y}_{g,K}^{(i)}} \subset \widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K}$.*

Proof. We have $\mathrm{mult}(H_{\mathscr{Y}_{g,K}^{(i)}}) = \chi(K)$ as subgroups of $\widehat{\mathbb{Z}}^\times$, by Remark 3.2. Therefore, it suffices to show that $H_{\mathscr{Y}_{g,K}^{(i)}}(2) \subset S_{2g+2-(i \bmod 2)}$. By Theorem 3.6, we need only check that the monodromy action on the Weierstrass points of $\mathscr{Y}_{g,K}^{(i)} \to \mathscr{W}_{g,K}^{(i)}$ is contained in $S_{2g+2-(i \bmod 2))}$. The nontrivial cases $i = 1, 3$ follow by observing that, when the defining equation is $y^2 = f(x)$ with $\deg f(x) = 2g + 1$, one Weierstrass point always lies over infinity, hence is fixed under monodromy. □

We prove Theorem 3.6 in three steps:

(1) In subsection 3.3.1, we prove the statement when $\mathcal{U}$ is $\mathrm{Spec}\,\overline{k}$. The key points are that the constructions are functorial in $\mathcal{C}$ and that the isomorphism with $\mathrm{Jac}_{C/U}[2]$ follows from standard facts about divisors on hyperelliptic curves.
(2) In subsection 3.3.2, we prove the statement when $\mathcal{U}$ is a scheme by explicitly constructing the algebraic space of Weierstrass points over $\mathcal{U}$, the corresponding group space $t^\perp/\operatorname{span}(t)$ over $\mathcal{U}$, and the map from the latter to $\mathrm{Jac}_{C/U}[2]$. Step (1) implies that this map is an isomorphism.
(3) In subsection 3.3.3, we interpret the (functorial) constructions of step (2) as giving rise to corresponding objects and maps over the moduli space $\mathscr{X}_g$ of hyperelliptic curves, corresponding to the universal family $\mathscr{C}_g \to \mathscr{X}_g$.

3.3.1. *A single hyperelliptic curve.* Let k be an algebraically closed field of characteristic zero, let C be a hyperelliptic curve over k, and let J be the Jacobian of C. The set of Weierstrass points $\{P_1, \ldots, P_{2g+2}\}$ of C is uniquely determined because $g \geq 2$. With this setup, define V to be the free vector space over $\mathbb{F}_2$ spanned by $P_1, \ldots, P_{2g+2}$, so that

$$t = P_1 + \cdots + P_{2g+2}$$
$$t^\perp = \mathrm{span}_{\mathbb{F}_2}(P_i - P_j : i, j \in \{1, \ldots, 2g+2\}).$$

The map

$$\begin{array}{ccc} \mathrm{span}_{\mathbb{Z}}(P_1, \ldots, P_{2g+2}) & \xrightarrow{\quad\phi\quad} & \mathrm{Pic}_C \\ \sum_i a_i \cdot P_i & \longmapsto & \mathcal{O}_C\left(\sum_i a_i \cdot P_i\right), \end{array}$$

is such that $\phi(\mathrm{span}_{\mathbb{Z}}(P_i - P_j)) \subset \mathrm{Pic}^0_C \simeq J$. Furthermore, it can be checked that

- The resulting map $\mathrm{span}_{\mathbb{Z}}(P_i - P_j) \to J$ annihilates $2 \cdot (P_i - P_j)$ and t. Hence it descends to a map $W := t^\perp/\operatorname{span}(t) \to J[2]$ of $\mathbb{F}_2$ vector spaces.
- This latter map is an isomorphism.

The second bullet point implies that the action of $\mathrm{Aut}(C)$ on $J[2]$, *a priori* contained in $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, is in fact contained in the subgroup $S_{2g+2} \subset \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ which is determined by the vector space isomorphism $J[2] \simeq W$. For details, see [Yel15, Proposition 1.2.1(a)].

3.3.2. *Schematic families of hyperelliptic curves.* Let $C \to U$ be a family of hyperelliptic curves of genus g, where U is a scheme. Because all constructions in 3.3.1 were functorial, they can be carried out in families. Let us indicate how this is done.

(1) Let P be the fixed point locus of the hyperelliptic involution. Then we have a diagram

$$\begin{array}{ccc} P & \xhookrightarrow{\text{closed emb.}} & C \\ & \searrow^{\text{étale}} & \downarrow \\ & & U \end{array}$$

For any geometric point $u \hookrightarrow U$, the fiber P_u consists of the Weierstrass points of C_u.

(2) Let G be the group algebraic space over U which represents the sheaf associated to the following presheaf on $\mathrm{Sch}_{/U}$, in the étale topology:

$$T \mapsto \mathrm{span}_{\mathbb{Z}}(\mathrm{Hom}_U(T, P)).$$

Representability follows by taking an étale cover of U which trivializes P. For $u \to U$ a geometric point, the fiber G_u equals $\mathrm{span}_{\mathbb{Z}}(P_u)$.

There is a section $t\colon U \to G$ which is first defined on a sufficiently fine étale cover $U' \to U$ for which $U' \times_U P$ is a trivial $(2g+2)$-cover of U', by "adding all the Weierstrass points," i.e. summing the $(2g+2)$ basis elements of

$$\mathrm{span}_{\mathbb{Z}}(\mathrm{Hom}_U(U', P)) \simeq \mathrm{span}_{\mathbb{Z}}(\mathrm{Hom}_{U'}(U', U' \times_U P)).$$

The section on U' can then be descended to U.

We can also define a group subspace $G^0 \hookrightarrow G$ via the sub-presheaf given by requiring that the coefficients of the $\mathbb{Z}$-linear combination sum to zero.

(3) Define a map $\Phi : G \to \mathrm{Pic}_{C/U}$ of group spaces over U as follows: given $f \in G(T)$, we may find an étale cover $\sigma : T' \to T$ for which $\sigma^* f = \sum_i f_i$, for some $f_i \in \mathrm{Hom}_U(T', P)$. Each f_i gives a section of the pulled-back family $C_{T'} \to T'$, whose image determines a relative effective Cartier divisor D_i. A standard descent argument shows that $\sum_i D_i$ descends to a divisor D on C_T, which does not depend on the chosen étale cover σ. We may therefore define $\Phi(f) := D$. This assignment is natural in T, so it gives a natural transformation of functors $G \to \mathrm{Pic}_{C/U}$. The fiber Φ_u is the map ϕ defined in 3.3.1. The map Φ restricts to a map $G^0 \to \mathrm{Pic}^0_{C/U} \simeq \mathrm{Jac}_{C/U}$.

(4) Subsection 3.3.1 allows us to describe the kernel and image of Φ as follows. First, $2 \cdot G^0$ maps to zero, so Φ descends to a map $G^0/(2 \cdot G^0) \to \mathrm{Jac}_{C/U}$. Second, the inclusion $G^0 \hookrightarrow G$ gives an injection $G^0/(2 \cdot G^0) \hookrightarrow G/(2 \cdot G)$, and the image of $t \in G(U)$ in the quotient $G/(2 \cdot G)$ in fact lies in $G^0/(2 \cdot G^0)$ because t is a sum of an even number of terms; we abuse notation by denoting the latter section with the same symbol t. This t spans the kernel of the descended map $G^0/(2 \cdot G^0) \to \mathrm{Jac}_{C/U}$, the image of which is equal to $\mathrm{Jac}_{C/U}[2]$. Thus, we have that

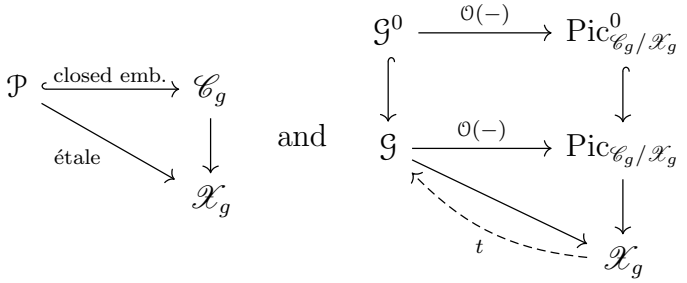
$$G^0/(2 \cdot G^0 + \mathrm{span}(t)) \to \mathrm{Jac}_{C/U}[2]$$

is an isomorphism of group stacks over U.

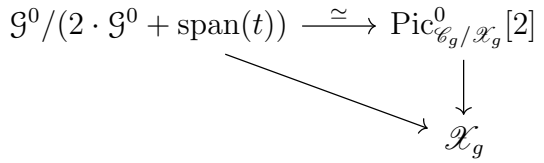
This proves Theorem 3.6 when $\mathcal{U} := U$ is a scheme, because the action of $\pi_1(U)$ on the fiber of $G^0/(2G^0 + \mathrm{span}(t))$ over a chosen geometric generic point $\overline{\eta} \in U$ (as an $\mathbb{F}_2$-vector space)

is obtained from the action of $\pi_1(U)$ on the fiber of $P_{\overline{\eta}}$ (as a set of size $(2g+2)$) via the procedure of Section 2.2.1.

3.3.3. *The universal family over $\mathscr{X}_g$.* The constructions of subsection 3.3.2 are functorial in the chosen family $C \to U$, and behave well under base change $V \to U$, so we obtain the analogous constructions over the moduli stack of hyperelliptic curves:

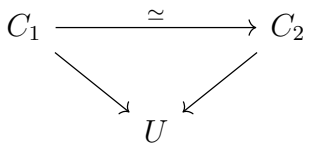


where t is a section of $\mathcal{G} \to \mathscr{X}_g$, for which we have the following isomorphism of group stacks over $\mathscr{X}_g$:



Here, t is interpreted as a section of $\mathcal{G}^0/(2\cdot\mathcal{G}^0)$ over $\mathscr{X}_g$ just as in step (4) of subsection 3.3.2.

Remark 3.8. By way of example, let us explain the definition of $\mathcal{P}$, and prove that it is a stack. By definition, $\mathcal{P}(U)$ is the groupoid whose objects are pairs $(C \to U, f)$ where $C \to U$ is a hyperelliptic family over U (i.e. an object of $\mathscr{X}_g(U)$) and f is a section of the étale cover $P \to U$ constructed in subsection 3.3.2 from the family $C \to U$. A morphism $(C_1 \to U, f_1) \simeq (C_2 \to U, f_2)$ is an isomorphism σ of families



for which the resulting isomorphism $P_1 \simeq P_2$ of the associated spaces of Weierstrass points identifies the sections f_1 and f_2.

The descent condition is easy to check. Given an étale cover $V \to U$, a descent datum for $\mathcal{P}$ is given by a family $\widetilde{C} \to V$ and a section $\widetilde{f}$ of the resulting space of Weierstrass points, denoted $\widetilde{P} \to V$, along with gluing isomorphisms that take place over $V \times_U V$, which satisfy a cocycle condition on $V \times_U V \times_U V$. The cocycle condition first allows us to realize $\widetilde{C}$ as the pullback of a family $C \to U$, because $\mathscr{X}_g$ is known to be a stack. By functoriality, the pullback to V of the resulting space of Weierstrass points $P \to U$ is canonically identified with $\widetilde{P} \to V$. So effectiveness of the descent datum follows from the fact that $P \to U$ is an étale sheaf over $\mathrm{Sch}_{/U}$, and, as such, satisfies a gluing axiom.

In a similar way, the following points are formal consequences of subsection 3.3.2:

- All stacks appearing in the three commutative diagrams above are algebraic.
- All maps to $\mathscr{X}_g$ appearing above are representable.

- The isomorphism in the third diagram, which gives the desired statement about monodromy for the universal family $\mathscr{C}_g \to \mathscr{X}_g$, can be checked on pullback to schemes U, but this is exactly the conclusion of subsection 3.3.2.

To finish the proof of Theorem 3.6, we need only note that any hyperelliptic family $\mathcal{C} \to \mathcal{U}$, with $\mathcal{U}$ a Deligne-Mumford stack, is pulled back from the universal family $\mathscr{C}_g \to \mathscr{X}_g$ via a map $\mathcal{U} \to \mathscr{X}_g$. In this case, all constructions above can be pulled back along the same map $\mathcal{U} \to \mathscr{X}_g$. Therefore, to $\mathcal{C} \to \mathcal{U}$, we can associate a stack of Weierstrass points, whose $\mathbb{Z}$-span maps to $\mathrm{Pic}_{\mathcal{C}/\mathcal{U}}$, giving rise to an isomorphism analogous to that of the third commutative diagram above. This gives the desired result, by the same reasoning as in the last paragraph of subsection 3.3.2.

3.4. **Monodromy of Hyperelliptic Families $\mathscr{W}_{g,K}^{(i)}$ and $\mathscr{X}_{g,K}$.** We now show that the containment in Corollary 3.7 is an equality for the families $\mathscr{Y}_{g,K}^{(i)} \to \mathscr{W}_{g,K}^{(i)}$.

Lemma 3.9. *Let $g \geq 2$, and let $i \in \{1,2,3,4\}$.*

(i) For any algebraically closed field L which is a subfield of $\mathbb{C}$, we have $H_{\mathscr{Y}_{g,L}^{(i)}} = \widetilde{\mathbb{S}}_{2g+2-(i \bmod 2)}$.

(ii) For any number field K, we have $H_{\mathscr{Y}_{g,K}^{(i)}} = \widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K}$.

Proof. (i) $\Leftrightarrow$ (ii): we have a map of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_{\mathscr{Y}_{g,\overline{K}}^{(i)}} & \longrightarrow & H_{\mathscr{Y}_{g,K}^{(i)}} & \xrightarrow{\text{mult}} & \chi(K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \widetilde{\mathbb{S}}_{2g+2-(i \bmod 2)} & \longrightarrow & \widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K} & \xrightarrow[\text{mult}]{} & \chi(K) & \longrightarrow & 0. \end{array} \tag{3.2}$$

By the Five Lemma, the second vertical map is an isomorphism if and only if the first is.

Proof of (i): By Corollary 3.7, and because L is a subfield of $\mathbb{C}$, we have containments

$$H_{\mathscr{Y}_{g,\mathbb{C}}^{(i)}} \subset H_{\mathscr{Y}_{g,L}^{(i)}} \subset \widetilde{\mathbb{S}}_{2g+2-(i \bmod 2)}.$$

Therefore, it suffices to show that $H_{\mathscr{Y}_{g,\mathbb{C}}^{(i)}} = \widetilde{\mathbb{S}}_{2g+2-(i \bmod 2)}$. For $i \in \{1,2\}$, this follows from [A'C79, Théorème 1], since the étale fundamental group is the profinite completion of the topological fundamental group. To complete the proof we need only show that, when $i \in \{3,4\}$, we have $H_{\mathscr{Y}_{g,\mathbb{C}}^{(i)}} = H_{\mathscr{Y}_{g,\mathbb{C}}^{(i-2)}}$.

For this, it suffices to construct a deformation retract

$$\phi : \mathscr{W}_{g,\mathbb{C}}^{(i-2)} \times [0,1] \to \mathscr{W}_{g,\mathbb{C}}^{(i-2)}$$

of $\mathscr{W}_{g,\mathbb{C}}^{(i-2)}$ onto $\mathscr{W}_{g,\mathbb{C}}^{(i)}$, which is done as follows. Let $n := 2g + 2 - (i \bmod 2)$. Then $\mathscr{W}_{g,\mathbb{C}}^{(i-2)}$ parameterizes unordered n-tuples of distinct points in $\mathbb{A}^1_{\mathbb{C}}$, and $\mathscr{W}_{g,\mathbb{C}}^{(i)}$ parameterizes those which sum to zero. At time $t \in [0,1]$, we define

$$\phi_t \colon \{z_i\}_{i=1}^n \mapsto \left\{ z_i - t \cdot \frac{z_1 + \cdots + z_n}{n} \right\}_{i=1}^n,$$

where the n-tuple on the right sums to zero by construction. This ϕ is continuous, as desired. In fact, ϕ is regular: its coordinate functions are obtained by expressing the elementary

symmetric polynomials in the right hand side n-tuple as polynomials in (the elementary symmetric polynomials of the z_i) and t. □

Corollary 3.10. *Let $g \geq 2$. We have that $H_{\mathscr{C}_{g,K}} = \widetilde{\mathrm{GS}}_{2g+2,K}$, where $\mathscr{C}_{g,K} \to \mathscr{X}_{g,K}$ is the universal family over the moduli stack of hyperelliptic curves.*

Proof. A priori, we have the containments

$$H_{\mathscr{Y}^{(2)}_{g,K}} \subset H_{\mathscr{C}_{g,K}} \subset \widetilde{\mathrm{GS}}_{2g+2,K},$$

the latter following from Corollary 3.6. But Lemma 3.9 implies that $H_{\mathscr{Y}^{(2)}_{g,K}} = \widetilde{\mathrm{GS}}_{2g+2,K}$. □

3.5. **Finishing the Proof.** We are now in position to complete the proof of Theorem 1.2. The main input to the proof is the following general theorem from [LSTX19].

Theorem 3.11 ([LSTX19, Theorem 1.1])**.** *Let $B, n > 0$, and suppose that the rational family $A \to U$ is non-isotrivial and has big monodromy, meaning that H_A is open in $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. Let $\delta_{\mathbb{Q}}$ be the index of the closure of the commutator subgroup of H_A in $H_A \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, and let $\delta_K = 1$ for $K \neq \mathbb{Q}$. Then $[H_A : H_{A_u}] \geq \delta_K$ for all $u \in U(K)$, and we have the following asymptotic statements:*

$$\frac{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B,\, [H_A : H_{A_u}] = \delta_K\}|}{|\{u \in U(K) \cap \mathcal{O}_K^r : \|u\| \leq B\}|} = 1 + O((\log B)^{-n}), \text{ and}$$

$$\frac{|\{u \in U(K) : \mathrm{Ht}(u) \leq B,\, [H_A : H_{A_u}] = \delta_K\}|}{|\{u \in U(K) : \mathrm{Ht}(u) \leq B\}|} = 1 + O((\log B)^{-n}),$$

where the implied constants depend only on $A \to U$ and n.

Proof of Theorem 1.2. First, we explain how Theorem 3.11 applies to the standard families $\mathscr{Y}^{(i)}_{g,K} \to \mathscr{W}^{(i)}_{g,K}$. By Lemma 3.9(ii), these families have big monodromy, so Theorem 3.11 applies. Lemma 3.9(ii) says that $H_{\mathscr{Y}^{(i)}_{g,K}} = \widetilde{\mathrm{GS}}_{2g+2-(i \bmod 2),K}$. With this in mind, Corollary 3.5 implies that $\delta_{\mathbb{Q}} = 2$ in the statement of Theorem 3.11.

Next, we apply Theorem 3.11 to a rational family $C \to U$ represented by a map $U \to \mathscr{X}_{g,K}$ with connected geometric generic fiber. This hypothesis implies that $\pi_1(U) \to \pi_1(\mathscr{X}_{g,K})$ is a surjection, cf. [LSTX19, Corollary 5.3], so the monodromy group of $C \to U$ is equal to that of the universal family over $\mathscr{X}_{g,K}$, and Corollary 3.10 implies that the universal family over $\mathscr{X}_{g,K}$ has monodromy group $\widetilde{\mathrm{GS}}_{2g+2,K}$. At this point, Corollary 3.5 implies $\delta_{\mathbb{Q}} = 2$, as before. □

4. Verification of the Examples

The objective of this section is to prove our second main result, namely Theorem 1.3. To verify that the example curves stated in Theorem 1.3 have maximal monodromy among members of $\mathscr{X}_{g,\mathbb{Q}}$, we shall rely on two different sets of criteria, one adapted from [AD17], and the other adapted from [Zyw15]. We introduce these criteria in Section 4.1; then, in Section 4.2, we apply these criteria to check the example curves.

4.1. **Criteria for Having Maximal Monodromy.** Let $g \in \{2,3\}$, and let C be a genus-g hyperelliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $y^2 = f(x)$, where $f(x) \in \mathbb{Q}[x]$ is a polynomial of degree $2g+2$; note that C is a $\mathbb{Q}$-valued point of $\mathscr{W}^{(2)}_{g,\mathbb{Q}}$.

Let J denote the Jacobian of C. We want to write down criteria for the associated monodromy group H_J to be as large as possible in $H_{\mathscr{X}_{g,\mathbb{Q}}} \simeq \widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}}$, which by Theorem 1.2 is equivalent to having index 2 in $\widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}}$. We shall rely on the following lemma, which gives us two conditions under which maximal monodromy is attained:

Lemma 4.1. *Suppose C is a hyperelliptic curve over $\mathbb{Q}$ with Jacobian J satisfying*

$$(H_J)_2 = \mathrm{G}\Phi^{-1}_{2^\infty \to 2}(S_{2g+2}), \text{ and} \tag{4.1}$$

$$H_J(\ell) \supset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z}) \text{ for every prime number } \ell \geq 3. \tag{4.2}$$

Then, $[\widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}} : H_J] = 2$.

Proof. Since the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ is equal to the maximal cyclotomic extension $\mathbb{Q}^{\mathrm{cyc}}$, we have that

$$\rho_J(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}})) = \rho_J(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})) = [H_J, H_J]. \tag{4.3}$$

Using (4.3), we find that

$$\begin{aligned}
[\widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}} : H_J] &= [\widetilde{\mathrm{S}}_{2g+2} : \rho_J(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}}))] \\
&= [\widetilde{\mathrm{S}}_{2g+2} : [\widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}}, \widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}}]] \cdot [[\widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}}, \widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}}] : \rho_J(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}}))] \\
&= 2 \cdot [[\widetilde{\mathrm{S}}_{2g+2}, \widetilde{\mathrm{S}}_{2g+2}] : [H_J, H_J]],
\end{aligned}$$

where in the last step above we used the result of Corollary 3.5. Thus, to prove that H_J is maximal, it suffices to show that the inclusion $[H_J, H_J] \subset [\widetilde{\mathrm{S}}_{2g+2}, \widetilde{\mathrm{S}}_{2g+2}]$ is an equality. The result then follows from Lemma 3.4. □

Criterion (4.2) may be broken down into two different sets of criteria by means of the following two propositions, adapted from [AD17] and [Zyw15] respectively. The first set of criteria has the advantage that it implies the image is surjective at all but finitely many primes, although notably it does omit a finite list of primes ℓ.

We first recall definitions from [AD17].

Definition 4.2 ([AD17, Definition 1.2, Definition 1.3])**.** Let $t \geq 1$ be an integer and p a prime. A polynomial $f(x) := x^m + a_{m-1}x^{m-1} + \cdots + a_0 \in \mathbb{Z}_p[x]$ is *t-Eisenstein* if $v(a_i) \geq t$ for $i > 0$ and $v(a_0) = t$, for v the p-adic valuation. Further, suppose $q_1, \ldots, q_k$ are prime numbers and $f(x) \in \mathbb{Z}_p[x]$ is monic and squarefree. We say $f(x)$ is of *type* $t - \{q_1, \ldots, q_k\}$ if it can be factored as $f(x) = h(x)\prod_{i=1}^k g_i(x - \alpha_i)$ over $\mathbb{Z}_p[x]$ for $\alpha_i \in \mathbb{Z}_p$ with $\alpha_i \not\equiv \alpha_j \bmod p$ for all $i \neq j$, $g_i(x)$ a t-Eisenstein polynomial of degree q_i, and $h(x) \bmod p$ a separable polynomial with $h(\alpha_i) \not\equiv 0 \bmod p$ for all i.

The next proposition follows immediately upon combining the main results of [AD17]:

Proposition 4.3 ([AD17])**.** *Suppose $f \in \mathbb{Z}[x]$ satisfies the following properties:*

(1) There exist primes q_1, q_2, and q_3 such that

$$q_1 \leq q_2 < q_3 < q_1 + q_2 = 2g + 2.$$

(2) There exist two distinct primes $p_{t_1}, p_{t_2} > g$ so that f has type $1 - \{2\}$ at p_{t_1} and p_{t_2}.

(3) *There exists a prime* $p_2 > 2g+2$ *which is a primitive root modulo* q_1, q_2, *and* q_3 *so that* f *has type* $1 - \{q_1, q_2\}$ *at* $p_2 > 2g+2$.
(4) *There exist a prime* $p_3 > 2g+2$ *which is a primitive root modulo* q_3 *such that* f *has type* $2 - \{q_3\}$ *at* p_3.
(5) *Writing* $f = x^{2g+2} + a_{2g+1}x^{2g+1} + \cdots + a_1 x + a_0$ *we have* $a_0 \equiv 2^{2g} \bmod 2^{2g+2}$, $a_{2g+1} \equiv 2 \bmod 2^{2g+2}$, *and* $a_i \equiv 0 \bmod 2^{2g+2-i}$ *for* $1 \leq i \leq 2g$.
(6) *For all primes* $p \notin \{2, p_2, p_3\}$ *we have that* $p^2 \nmid \operatorname{disc} f$, *the discriminant of* f.

Let J *denote the Jacobian of the regular proper model for the affine curve* $y^2 = f(x)$. *Then* $H_J(\ell) \supset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ *for every* $\ell > g$ *so long as* $\ell \notin \{2, 3, q_1, q_2, q_3, p_2, p_3\}$.

Proof. We now demonstrate why Proposition 4.3 follows immediately from the results of [AD17]. It suffices to verify the hypotheses of [AD17, Theorem 6.2]. Their hypotheses (G+ε), (2T), (p_2) and (p_3) are respectively (1), (2), (3), and (4) above. Next, we note that f satisfies their condition (adm): We have to show f is admissible (in the terminology of [AD17, Definition 4.6]) at all primes p. f is admissible at p_2 by [AD17, Lemma 4.10] and at p_3 by [AD17, Lemma 4.11]. Further, f is admissible at all primes with semistable reduction by [AD17, Lemma 4.9] so it suffices to show f is semistable at all primes $p \notin \{p_2, p_3\}$. At $p = 2$ this follows from [AD17, Lemma 7.7], using (5) above, while at all odd primes this follows from [AD17, Lemma 7.5], using (6) above. To conclude the proof, we only need check that all primes $\ell > g$ with $\ell \notin \{2, 3, q_1, q_2, q_3, p_2, p_3\}$ satisfy either [AD17, Theorem 6.2(i) or (iii)]. If $\ell \neq p_2, p_3$ then ℓ satisfies [AD17, Theorem 6.2(i)] because we have seen $J/\mathbb{Q}_\ell$ is semistable above. If $\ell = p_2$ or p_3 then ℓ satisfies [AD17, Theorem 6.2(iii)] by (3) and (4) above. □

The second set of criteria has the advantage that it is simpler to state and works for every odd prime ℓ. The following criteria have, in essence, appeared in several papers including [AdRDW16, Theorem 1.1], [Hal08, Theorem 1.1], and [Zyw15, Proposition 2.2].

Proposition 4.4. *Let* $g \geq 2$, *and let* $\ell \geq 3$ *be prime. Consider a subgroup* $H(\ell) \subset \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ *satisfying the following conditions:*

(A) $H(\ell)$ *contains a transvection, by which we mean an element with determinant* 1 *that fixes a codimension-*1 *subspace.*
(B) *The action of* $H(\ell)$ *on* $(\mathbb{Z}/\ell\mathbb{Z})^{2g}$ *is irreducible, in the sense that there are no nontrivial invariant subspaces.*
(C) *The action of* $H(\ell)$ *on* $(\mathbb{Z}/\ell\mathbb{Z})^{2g}$ *is primitive, in the sense that there does not exist a decomposition* $(\mathbb{Z}/\ell\mathbb{Z})^{2g} \simeq V_1 \oplus \cdots \oplus V_k$ *with* $H(\ell)$ *permuting the* V_i*'s.*

Then we have that $H(\ell) \supset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$.

4.2. **Checking the Criteria.** The remainder of the paper is devoted to using the criteria introduced in Section 4.1 to verify the examples declared in Theorem 1.3.

4.2.1. *Criterion* (4.1)*: The* 2*-adic Component.* The following lemma allows us to verify criterion (4.1):

Lemma 4.5. *Let* $g \in \{2, 3\}$, *and let* $H_2 \subset \mathcal{S}_{2g+2}$ *be a closed subgroup. If* $H_2(2) = S_{2g+2}$, *then we have that* $H_2 = \mathcal{S}_{2g+2}$.

Proof. When $g = 2$, the inclusion $S_6 \subset \mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z})$ is an equality, so the lemma follows from [LSTX17, Theorem 1]. For the rest of the proof, we take $g = 3$. Note that an easy generalization of the argument given in [Ser98, Lemma 3, Section IV.3.4] shows that, if

$H \subset \mathrm{Sp}_6(\mathbb{Z}_2)$ is a closed subgroup satisfying $\mathcal{S}_8(8) = H(8)$, then $H_2 = \Phi^{-1}_{2^\infty \to 2}(H(2))$. So it suffices to show that $\mathcal{S}_8(8) = H(8)$. Indeed, the following `magma` code verifies that there are no strict subgroups of $\mathcal{S}_8(8)$ with mod-2 reduction equal to $\mathcal{S}_8(2) = S_8$.

```
G := GL(6,quo<Integers()|8>);
e := elt<G| 1,0,0,0,0,0,1,1,0,0,0,0,0,0,1,0,0,0,
     0,0,0,1,0,0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,0,1>;
f := elt<G|1,1,0,0,0,0,0,0,1,1,0,0,0,1,1,1,1,0,0,
     1,1,0,1,1,1,0,1,1,1,1,1,1,1,1,1,1,1,0,0,1>;
H := sub<G|e,f>;
maximals := MaximalSubgroups(H);
grp, f := ChangeRing(G, quo<Integers()|2>);
for K in maximals do
    if #f(K`subgroup) eq #H then
        assert false;
    end if;
end for;
```

□

Recall from the discussion in Section 3.3.1 that $H_J(2) = S_{2g+2}$ if and only if the polynomial $f(x)$ has Galois group S_{2g+2}. A simple `magma` computation that this is the case for the polynomials $f(x)$ associated to the curves stated in Theorem 1.3. Then Lemma 4.5 tells us that $(H_J)_2 = \mathcal{S}_{2g+2}$, thus verifying the criterion (4.1).

4.2.2. *Criterion* (4.2)*: The Genus-*2 *Example.* We now verify the genus-2 example. We first apply Proposition 4.3. To verify the conditions (1)-(6) on the polynomial $f(x)$, we make the following choices:

$$q_1 = q_2 = 3,\ q_3 = 5,\ p_{t_1} = 3,\ p_{t_2} = 5,\ p_2 = 17,\ p_3 = 7.$$

Condition (1) is clearly satisfied and conditions (2)-(4) are satisfied upon observing that $f(x)$ admits the following factorizations:

$$\begin{aligned}(x^4 + x^3 + x^2 + x + 1)(x^2 - 3) \bmod 3^2\\ (x^4 + x^2 + x + 1)(x^2 - 5) \bmod 5^2\\ (x^3 - 17)((x-1)^3 - 17) \bmod 17^2\\ (x-1)(x^5 - 7^2) \bmod 7^3.\end{aligned}$$

Condition (5) is verified by reducing f modulo $2^{2g+2} = 2^6 = 64$. Finally, the computer verifies that the prime factorization of $\mathrm{disc}\, f$ is given by

$$\mathrm{disc}\, f = 3{\cdot}5{\cdot}7^8{\cdot}17^4{\cdot}421{\cdot}6397{\cdot}10343494117334526221444592 7{\cdot}48996528304396107289766658 49.$$

Hence, Proposition 4.3 tells us that condition (4.2) holds for every odd prime ℓ satisfying $\ell \notin \{3, 5, 7, 17\}$.

To deal with the four remaining primes ℓ, we utilize the criteria given in Proposition 4.4. First, we show the existence of a transvection (condition (A) of Proposition 4.4). Indeed, this follows from [AD17, Lemma 2.9], which says that if there is a prime $p \nmid 2\ell$ such that $f(x)$ has type $1 - \{2\}$ when viewed as a polynomial in $\mathbb{Z}_p[x]$, then $J[\ell]$ contains a transvection. For $\ell \in \{5, 7, 17\}$ this follows by taking $p = 3$ while for $\ell = 3$ this follows by taking $p = 5$.

To complete the proof, it suffices to verify conditions (B) and (C) of Proposition 4.4. For p be a prime of good reduction of J, let $\mathrm{Frob}_p \in G_{\mathbb{Q}}$ denote the corresponding Frobenius element, and let $\mathrm{ch}_p(T) \in \mathbb{Z}[t]$ denote the characteristic polynomial of $\rho_J(\mathrm{Frob}_p) \in \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. The next proposition gives us a criterion to check irreducibility and primitivity together (conditions (B) and (C)):

Proposition 4.6 ([Zyw15, Proof of Lemma 7.2])**.** *Fix a prime $\ell \geq 3$. Suppose there exists $p \neq \ell$ of good reduction such that $\mathrm{ch}_p(T)$ is irreducible modulo ℓ and $\ell \nmid \mathrm{tr}(\mathrm{Frob}_p)$. Then $H(\ell)$ acts irreducibly and primitively on $(\mathbb{F}_\ell)^{2g}$.*

A simple `magma` calculation shows that for $\ell \in \{3, 17\}$, we can apply Proposition 4.6 with

$$\mathrm{ch}_{401}(T) = T^4 - 49T^3 + 1257T^2 - 19649T + 160801.$$

Likewise, for $\ell = 5$, we can use

$$\mathrm{ch}_{61}(T) = T^4 + 6T^3 + 54T^2 + 366T + 3721,$$

and for $\ell = 7$, we can use

$$\mathrm{ch}_{277}(T) = T^4 + 31T^3 + 765T^2 + 8587T + 76729.$$

This completes the verification that the curve C_2 in Theorem 1.3 has maximal monodromy.

4.2.3. *Criterion* (4.2)*: The Genus-*3 *Example.* We now verify the genus-3 example. We begin again by applying Proposition 4.3. To verify the conditions (1)-(6) on the polynomial $f(x)$, we make the following choices:

$$q_1 = 3,\ q_2 = 5,\ q_3 = 7,\ p_{t_1} = 5,\ p_{t_2} = 13,\ p_2 = 17,\ p_3 = 19.$$

Condition (1) is clearly satisfied and conditions (2)-(4) are satisfied upon observing that $f(x)$ admits the following factorizations:

$$\begin{aligned}(x^6 + x^3 + x^2 + 1)(x^2 + 5) &\bmod 5^2\\ (x^6 + 51x^5 + 12x^4 + 70x^3 + 82x^2 + 41x + 158)((x-10)^2 + 143(x-10) + 78) &\bmod 13^2\\ ((x-1)^3 + 17)(x^5 + 17) &\bmod 17^2\\ (x+1)(x^7 + 361) &\bmod 19^3.\end{aligned}$$

Condition (5) is verified by reducing f modulo $2^{2g+2} = 2^8 = 256$. Finally, the computer verifies that the prime factorization of $\mathrm{disc}\, f$ is given by

$$\begin{aligned}\mathrm{disc}\, f = 2^{44} \cdot 5 \cdot 13 \cdot 17^6 \cdot 19^{12} \cdot 409 \cdot 71347 \cdot 249200273817326443 \cdot 22598623764098539015 27\cdot\\ 76378336963241484055881774103 \cdot 37005571802283225722722192361 51.\end{aligned}$$

Hence, Proposition 4.3 tells us that condition (4.2) holds for every odd prime ℓ satisfying $\ell \notin \{3, 5, 7, 13, 17, 19\}$.

To deal with the four remaining primes ℓ, we again utilize the criteria given in Proposition 4.4. First, we show the existence of a transvection (condition (A) of Proposition 4.4). This follows from [AD17, Lemma 2.9], which says that if there is a prime $p \nmid 2\ell$ such that $f(x)$ has type $1 - \{2\}$ when viewed as a polynomial in $\mathbb{Z}_p[x]$, then $J[\ell]$ contains a transvection. For $\ell \in \{3, 7, 13, 17, 19\}$ this follows by taking $p = 5$ while for $\ell = 5$ this follows by taking $p = 13$.

To complete the proof, it suffices to verify conditions (B) and (C) of Proposition 4.4. A simple `magma` calculation shows that for $\ell = 3$, we can apply Proposition 4.6 with

$$\mathrm{ch}_{101}(T) = T^6 + 10T^5 + 60T^4 + 222T^3 + 6060T^2 + 102010T + 1030301.$$

Likewise, for $\ell = 5$, we can use

$$\mathrm{ch}_{89}(T) = T^6 - 3T^5 + 93T^4 + 40T^3 + 8277T^2 - 23763T + 704969,$$

for $\ell \in \{7, 17\}$, we can use

$$\mathrm{ch}_{127}(T) = T^6 - 12T^5 + 8T^4 + 548T^3 + 1016T^2 - 193548T + 2048383,$$

and for $\ell \in \{13, 19\}$, we can use

$$\mathrm{ch}_{103}(T) = T^6 - 7T^5 + 55T^4 - 191T^3 + 5665T^2 - 74263T + 1092727.$$

This completes the verification that the curve C_3 in Theorem 1.3 has maximal monodromy.

5. Conjecture Regarding Maximal Adelic Image of Hyperelliptic Curves

As we saw in Section 3.3, the mod-2 monodromy of a hyperelliptic curve $y^2 = f(x)$ always lies in the subgroup $S_{2g+2} \subset \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$. Further, the mod-2 monodromy will be all of S_{2g+2} if and only if the spitting field of $f(x)$ is as large as possible; i.e., has Galois group S_{2g+2} over the base field K. In Lemma 4.5, we saw that for $g = 2$ or 3, if the mod-2 monodromy is surjective modulo 2, then it is surjective 2-adically. We conjecture that this pattern continues to hold in higher genera:

Conjecture 5.1. *Let $g \geq 2$ and let $H \subset \mathcal{S}_{2g+2}$ be a closed subgroup. If $H(2) = S_{2g+2}$ then $H = \mathcal{S}_{2g+2}$.*

To conclude, we make some remarks on the consequences of this conjecture.

Remark 5.2. As described in the proof of Lemma 4.1, via an easy generalization of the argument given in [Ser98, Lemma 3, Section IV.3.4], to prove Conjecture 5.1, it suffices to check $\mathcal{S}_{2g+2}(8) = H(8)$.

Remark 5.3. Note that Conjecture 5.1, if true, has the following useful consequence: If C is a hyperelliptic curve over $\mathbb{Q}$ with Jacobian J satisfying $H_J(2) = S_{2g+2}$ and $H_J(\ell) \supset \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ for every $\ell \geq 3$, then the C has maximal adelic Galois image. That is, $[\widetilde{\mathrm{GS}}_{2g+2,\mathbb{Q}} : H_J] = 2$.

Indeed, granting Conjecture 5.1, this claim follows immediately from Lemma 4.1.

Remark 5.4. As follows from Remark 5.3, Conjecture 5.1, would imply that the examples of hyperelliptic curves with maximal mod-ℓ image constructed in [ALS16, Theorem 7.1] in fact have maximal adelic image.

Acknowledgments

This research was supervised by Ken Ono and David Zureick-Brown at the Emory University Mathematics REU and was supported by the National Science Foundation (grant number DMS-1557960). We would like to thank David Zureick-Brown for suggesting the problem that led to the present article and for offering us his invaluable advice and guidance. We would like to thank Samuele Anni and Vladimir Dokchitser for helpful correspondence regarding applying their work. We thank Jackson Morrow and David Zureick-Brown for reading early drafts and providing helpful feedback, and we thank the anonymous referee for providing a number of useful suggestions. We used `Magma` and *Mathematica* for explicit calculations.

References

[A'C79] N. A'Campo. Tresses, monodromie et le groupe symplectique. *Comment. Math. Helv.*, 54(2):318–327, 1979.

[AD17] S. Anni and V. Dokchitser. Constructing hyperelliptic curves with surjective galois representations. *arXiv preprint arXiv:1701.05915v1*, 2017.

[AdRDW16] S. Arias-de Reyna, L. Dieulefait, and G. Wiese. Classification of subgroups of symplectic groups over finite fields containing a transvection. *Demonstr. Math.*, 49(2):129–148, 2016.

[ALS16] S. Anni, P. Lemos, and S. Siksek. Residual representations of semistable principally polarized abelian varieties. *Res. Number Theory*, 2:2:1, 2016.

[CGJ11] A. C. Cojocaru, D. Grant, and N. Jones. One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations. *Proc. Lond. Math. Soc. (3)*, 103(4):654–675, 2011.

[CH05] A. C. Cojocaru and C. Hall. Uniform results for Serre's theorem for elliptic curves. *Int. Math. Res. Not.*, (50):3065–3080, 2005.

[Die02] L. Dieulefait. Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. *Experiment. Math.*, 11(4):503–512 (2003), 2002.

[Duk97] W. Duke. Elliptic curves with no exceptional primes. *C. R. Acad. Sci. Paris Sér. I Math.*, 325(8):813–818, 1997.

[Gra00] D. Grant. A formula for the number of elliptic curves with exceptional primes. *Compositio Math.*, 122(2):151–164, 2000.

[Gre10] A. Greicius. Elliptic curves with surjective adelic Galois representations. *Experiment. Math.*, 19(4):495–507, 2010.

[Hal08] C. Hall. Big symplectic or orthogonal monodromy modulo l. *Duke Math. J.*, 141(1):179–203, 2008.

[Hog82] G. M. D. Hogeweij. Almost-classical Lie algebras. I, II. *Nederl. Akad. Wetensch. Indag. Math.*, 44(4):441–452, 453–460, 1982.

[Jon10] N. Jones. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010.

[LSTX17] Aaron Landesman, Ashvin A. Swaminathan, James Tao, and Yujie Xu. Lifting subgroups of symplectic groups over $\mathbb{Z}/\ell\mathbb{Z}$. *Res. Number Theory*, 3:Paper No. 14, 12, 2017.

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

[O'M78] O. T. O'Meara. *Symplectic groups*, volume 16 of *Mathematical Surveys*. American Mathematical Society, Providence, R.I., 1978.

[Ser72] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser98] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Vas03] A. Vasiu. Surjectivity criteria for p-adic representations. I. *Manuscripta Math.*, 112(3):325–355, 2003.

[Wei96] Thomas Weigel. On the profinite completion of arithmetic groups of split type. In *Lois d'algèbres et variétés algébriques (Colmar, 1991)*, volume 50 of *Travaux en Cours*, pages 79–101. Hermann, Paris, 1996.

[Yel15] J. Yelton. *Hyperelliptic Jacobians and their associated l-adic Galois representations*. PhD thesis, The Pennsylvania State University, 2015.

[Zyw10a] D. Zywina. Elliptic curves with maximal Galois action on their torsion points. *Bull. Lond. Math. Soc.*, 42(5):811–826, 2010.

[Zyw10b] D. Zywina. Hilbert's irreducibility theorem and the larger sieve. *arXiv:1011.6465v1*, November 2010.

[Zyw15] D. Zywina. An explicit Jacobian of dimension 3 with maximal Galois action. *arXiv:1508.07655v1*, August 2015.

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address, Aaron Landesman: aaronlandesman@stanford.edu

Department of Mathematics, Princeton University, Princeton, NJ 08544
E-mail address, Ashvin A. Swaminathan: ashvins@math.princeton.edu

Department of Mathematics, Harvard College, Cambridge, MA 02138
E-mail address, James Tao: jamestao@college.harvard.edu

Department of Mathematics, Harvard University, Cambridge, MA 02138
E-mail address, Yujie Xu: yujiex@math.harvard.edu