A CHARACTERIZATION OF THE $U(\Omega, m)$ SETS OF A HYPERELLIPTIC CURVE AS Ω AND m VARY

CHRISTELLE VINCENT

Abstract. In this article we consider a certain distinguished set $U(\Omega, m) \subseteq \{1, 2, \dots, 2g+1, \infty\}$ that can be attached to a marked hyperelliptic curve of genus g equipped with a small period matrix Ω for its polarized Jacobian. We show that as Ω and the marking m vary, this set ranges over all possibilities prescribed by an argument of Poor.

1. Introduction and Statement of Results

Let X be a hyperelliptic curve of genus g defined over $\mathbb{C}$, and let $J(X)$ be its polarized Jacobian. In Definition 2.2, we associate to $J(X)$ a *small period matrix* Ω, which is an element of the Siegel upper half-space $\mathbb{H}_g$ with the property that there is an isomorphism

$$J(X)(\mathbb{C}) \cong \mathbb{C}^g / L_\Omega, \tag{1.1}$$

where L_Ω is the rank $2g$ lattice generated by the columns of Ω and the standard basis $\{e_i\}$ of $\mathbb{C}^g$.

After this choice we may define an analytic theta function

$$\vartheta(z, \Omega) \colon \mathbb{C}^g \to \mathbb{C}, \tag{1.2}$$

whose exact definition is given in Definition 2.13. While this function is not well-defined on $J(X)(\mathbb{C})$, it is quasi-periodic with respect to the lattice L_Ω, and so its zero set on the Jacobian is well-defined. In this article we study how a certain combinatorial characterization of this zero set depends on the choice of small period matrix (since the theta function itself depends on the small period matrix) and on a further choice we now make.

Since X is hyperelliptic, there is a morphism $\pi \colon X \to \mathbb{P}^1$ of degree two, branched at $2g+2$ points. Suppose further that X is given a *marking of its branch points*, denoted m, by which we mean that the branch points of π are numbered $1, 2, \dots, 2g+1, \infty$. As we explain in Proposition 2.8, this choice gives a bijection between sets

$$S \subseteq \{1, 2, \dots, 2g+1, \infty\}, \quad \#S \equiv 0 \pmod 2, \tag{1.3}$$

up to the equivalence $S \sim S^c$, where ^{c} denotes taking the complement within $\{1, 2, \dots, 2g+1, \infty\}$, and the two-torsion in $J(X)(\mathbb{C})$.

Then we have the following theorem, which we will repeat and make more precise in Theorem 2.14:

Theorem 1.1 (Riemann Vanishing Theorem)**.** *Let X be a hyperelliptic curve, m be a marking of its branch points, and let Ω be a small period matrix associated to its polarized Jacobian. Then there is a distinguished set Θ on $J(X)(\mathbb{C})$ (defined in Definition 2.12) and the zero set of the theta function $\vartheta(z, \Omega)$, considered as a subset of $J(X)(\mathbb{C})$, is exactly the set Θ translated by an element of the two-torsion of $J(X)$.*

Under the correspondence given above, this two-torsion point corresponds to a set which we denote $T(\Omega, m)$. Note that the set $T(\Omega, m)$ is only well-defined up to the equivalence $S \sim S^c$, where as before ^{c} denotes the complement.

This theorem gives rise to the following distinguished set:

Definition 1.2. Let X be a hyperelliptic curve of genus g, Ω a choice of small period matrix associated to its Jacobian via the process described in Definition 2.2, and m a marking of the branch points of X. Let $U(\Omega, m) \subset \{1, 2, \dots, 2g+1, \infty\}$ be defined up to the equivalence $S \sim S^c$ by the following formula:

$$U(\Omega, m) = \begin{cases} T(\Omega, m) & \text{if } g \text{ is odd, and} \\ T(\Omega, m) \circ \{\infty\} & \text{if } g \text{ is even,} \end{cases} \tag{1.4}$$

where $\circ$ here denotes the symmetric difference of sets (see Definition 2.6). To fix one set in this equivalence class, we take $U(\Omega, m)$ to be the set containing ∞.

Remark. We note that Mumford [Mum07b] adopts the opposite convention and chooses $U(\Omega, m)$ to be the member of the equivalence class that does not contain ∞. In this respect we follow the convention adopted by Poor [Poo94].

The significance of this set $U(\Omega, m)$ is especially salient in computational applications; we invite the reader to consult Section 2.3 for a further account of its role. This set first appeared in work of Mumford [Mum07b], where given a marked hyperelliptic curve X, the author constructs a certain small period matrix Ω and computes the set $U(\Omega, m)$ explicitly. In this example, it is the case that

$$\#U(\Omega, m) = g + 1, \tag{1.5}$$

where as before g is the genus of the curve. In the theorems following this computation (in particular Mumford's version of Theorem 2.15, Theorem 9.1 of [Mum07b], which is the most important of those from our point of view), the set $U(\Omega, m)$ is always assumed to have this cardinality.

However, in later work of Poor [Poo94], the same set $U(\Omega, m)$ is shown to have the property that

$$\#U(\Omega, m) \equiv g + 1 \pmod 4 \tag{1.6}$$

(see [Poo94, Proposition 1.4.9]). This raises the following interesting question: Does the set $U(\Omega, m)$ always have cardinality $g + 1$, or do other cardinalities occur? We answer this question completely:

Theorem 1.3. *Let $g \geq 1$ and X be a hyperelliptic curve of genus g defined over $\mathbb{C}$. Then for any set $U \subseteq \{1, 2, \ldots, 2g + 1, \infty\}$ containing ∞ such that*

$$\#U \equiv g + 1 \pmod 4, \tag{1.7}$$

there exists a small period matrix Ω associated to the Jacobian of X via the process described in Definition 2.2, and a marking m of the branch points of X such that

$$U = U(\Omega, m). \tag{1.8}$$

In other words, every possible set U occurs as the set $U(\Omega, m)$ for a given hyperelliptic curve X, and Poor's characterization of $U(\Omega, m)$ is sharp.

Acknowledgments

The author would like to thank Sorina Ionica for many discussions that led her to understand the set $U(\Omega, m)$ more deeply, and the referees for their careful reading of the manuscript and thoughtful comments.

2. Preliminaries

Let X be a hyperelliptic curve, by which we mean a smooth complete curve of genus g defined over $\mathbb{C}$ admitting a map $\pi\colon X \to \mathbb{P}^1$ of degree 2. Throughout we denote its Jacobian variety by $J(X)$.

2.1. The small period matrix of the Jacobian of a curve.

We give here standard facts about abelian varieties and Jacobians. We refer the reader to [BL04] for further background and proofs.

We begin by giving an analytic space associated to polarized abelian varieties of dimension g:

Definition 2.1. Let $g \geq 1$. The *Siegel upper half-space* $\mathbb{H}_g$ is the set of symmetric $g \times g$ complex matrices M such that the imaginary part of M (obtained by taking the imaginary part of each entry in M) is positive definite.

Although much of the discussion below would apply to general polarized abelian varieties, in this article we focus our attention to Jacobians of curves equipped with their principal polarization. To simplify matters, at this time we restrict our attention to these objects. In this setting, the connection between this space and Jacobians is through the following object:

Definition 2.2. Let X be a curve of genus g defined over $\mathbb{C}$, and let $J(X)$ be its principally polarized Jacobian. To $J(X)$, we can associate matrices $\Omega \in \mathbb{H}_g$ in the following manner: Let A_i, B_i, $i = 1, \ldots, g$, be a basis for the homology group $H_1(J(X), \mathbb{Z}) \cong H_1(X, \mathbb{Z})$, which is a $2g$-dimensional vector space over $\mathbb{C}$. Assume further that this basis is symplectic with respect to the cup product. There exists a unique basis $\omega_1, \omega_2, \ldots, \omega_g$ of $\Omega^1(J(X)) \cong \Omega^1(X)$, the space of holomorphic 1-forms on $J(X)$ or X, such that

$$\int_{B_i} \omega_j = \delta_{ij}, \tag{2.1}$$

where δ_{ij} is the Kronecker delta function. Then the matrix given by $\int_{A_i} \omega_j$ belongs to $\mathbb{H}_g$ and is called a *small period matrix* for $J(X)$.

Let $\mathrm{Sp}_{2g}(\mathbb{Z})$ be the group of $2g \times 2g$ matrices with coefficients in $\mathbb{Z}$ and symplectic with respect to the bilinear form given by the matrix

$$\begin{pmatrix} 0 & \mathbb{1}_g \\ -\mathbb{1}_g & 0 \end{pmatrix}, \tag{2.2}$$

where $\mathbb{1}_g$ is the $g \times g$ identity matrix. We note that two elements of $\mathbb{H}_g$ can be associated to isomorphic polarized abelian varieties if and only if they differ by a matrix in $\mathrm{Sp}_{2g}(\mathbb{Z})$, where the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on $\mathbb{H}_g$ is given in the following manner: Let

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}), \tag{2.3}$$

where A, B, C and D are four $g \times g$ matrices. Then

$$\gamma \cdot \Omega = (A\Omega + B)(C\Omega + D)^{-1}, \tag{2.4}$$

where on the right multiplication and addition are the usual operation on $g \times g$ matrices.

We can further define an Abel-Jacobi map for a principally polarized Jacobian variety $J(X)$:

Definition 2.3. Let X be a curve of genus g defined over $\mathbb{C}$, let $J(X)$ be its principally polarized Jacobian, and fix A_i, B_i, $i = 1, \ldots, g$, a symplectic basis for the homology group $H_1(X, \mathbb{Z})$. Let $\omega_1, \omega_2, \ldots, \omega_g$ be the basis of $\Omega^1(X)$ described in Definition 2.2, Ω be the small period matrix attached to $J(X)$ via this choice of symplectic basis for homology and let L_Ω be the rank $2g$ lattice generated by the columns of Ω and the standard basis $\{e_i\}$ of $\mathbb{C}^g$. Then there is an isomorphism called the *Abel-Jacobi map*

$$AJ\colon J(X) \to \mathbb{C}^g/L_\Omega, \tag{2.5}$$

given by the map

$$D = \sum_{k=1}^{s} P_k - \sum_{k=1}^{s} Q_k \mapsto \left(\sum_{k=1}^{s} \int_{Q_k}^{P_k} \omega_i \right)_i, \tag{2.6}$$

where the P_ks and Q_ks are points on X. This map is well-defined since the value of each integral on X is well-defined up to the value of integrating the differentials ω_i along the basis elements A_i, B_i, and thus up to elements of L_Ω.

We will in fact need a slightly modified version of this Abel-Jacobi map for our purposes:

Definition 2.4. Let X be a curve of genus g defined over $\mathbb{C}$, let $J(X)$ be its principally polarized Jacobian, and fix A_i, B_i, $i = 1, \ldots, g$, a symplectic basis for the homology group $H_1(X, \mathbb{Z})$. Let Ω be the small period matrix attached to $J(X)$ via this choice of symplectic basis for homology and let L_Ω be the rank $2g$ lattice generated by the columns of Ω and the standard basis $\{e_i\}$ of $\mathbb{C}^g$. This gives rise to an isomorphism

$$\mathbb{C}^g/L_\Omega \to \mathbb{R}^{2g}/\mathbb{Z}^{2g}, \tag{2.7}$$

given by writing an element of $\mathbb{C}^g/L_\Omega$ as a linear combination of the columns of Ω and the standard basis $\{e_i\}$ of $\mathbb{C}^g$ and sending the element to the coefficients of the linear combination. Composing this isomorphism with the Abel-Jacobi map defined in Definition 2.3, we obtain the *modified Abel-Jacobi map*

$$AJ_c\colon J(X) \to \mathbb{R}^{2g}/\mathbb{Z}^{2g}, \tag{2.8}$$

which gives the coordinates of a point of $J(X)$ under the Abel-Jacobi map.

In this paper we will need to know how a change of symplectic basis for $H_1(X, \mathbb{Z})$ affects the image of the Abel-Jacobi map and the coordinates of a point of $J(X)$ under the Abel-Jacobi map. We have

Proposition 2.5 (adapted from Section 1.4 of [Poo94])**.** *Let X be a curve of genus g defined over $\mathbb{C}$, let $J(X)$ be its principally polarized Jacobian, and let A_i, B_i be a symplectic basis for $H_1(X, \mathbb{Z})$ from which arises the small period matrix Ω, the Abel-Jacobi map AJ and the modified Abel-Jacobi map AJ_c. Let $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ act on the elements A_i, B_i. Since $\mathrm{Sp}_{2g}(\mathbb{Z})$ preserves the cup pairing, the images $\tilde{A}_i$, $\tilde{B}_i$ gives rise to a second Abel-Jacobi map $\widetilde{AJ}$. If*

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{2.9}$$

where A, B, C and D are $g \times g$ matrices, then

$$\widetilde{AJ} = (C\Omega + D)^{-T} AJ, \tag{2.10}$$

where M^{-T} is the inverse of the transpose of the matrix M. Furthermore, we have

$$\widetilde{AJ}_c = \gamma^{-T} AJ_c. \tag{2.11}$$

2.2. **The two-torsion on the Jacobian of a hyperelliptic curve.**

We now turn our attention to the two-torsion of the Jacobian of a hyperelliptic curve of genus g defined over $\mathbb{C}$. As a group, it is isomorphic to C_2^{2g}, where C_2 is the cyclic group with two elements.

Throughout, let $B = \{1, 2, \ldots, 2g+1, \infty\}$. When $S \subseteq B$, we let S^c be the complement of S in B.

Definition 2.6. Let S_1 and S_2 be any two subsets of B. We define

$$S_1 \circ S_2 = (S_1 \cup S_2) - (S_1 \cap S_2), \tag{2.12}$$

the *symmetric difference* of S_1 and S_2.

This binary operation on subsets in turns gives rise to the following group:

Proposition 2.7. *The set*

$$\{S \subseteq B : \#S \equiv 0 \pmod 2\}/\{S \sim S^c\} \tag{2.13}$$

is a commutative group under the operation $\circ$, of order 2^{2g}, with identity $\emptyset \sim B$. Since $S \circ S = \emptyset$ for all $S \subseteq B$, this is a group of exponent 2. Therefore this group, which we denote G_B, is isomorphic to C_2^{2g}.

If the hyperelliptic curve X is equipped with a marking of its branch points (recall that this means that we label the $2g+2$ branch points of the degree two map $\pi\colon X \to \mathbb{P}^1$, $P_1, P_2, \ldots, P_{2g+1}, P_\infty$), there is in fact an explicit isomorphism between G_B and $J(X)[2]$, the two-torsion on the Jacobian of X:

Proposition 2.8 (Corollary 2.11 of [Mum07b]). *To each set $S \subseteq B$ such that $\#S \equiv 0 \pmod 2$, associate the divisor class of the divisor*

$$e_S = \sum_{i \in S} P_i - (\#S)P_\infty. \tag{2.14}$$

This association is a group isomorphism between $J(X)[2]$ and G_B.

We may now compose the isomorphism of Proposition 2.8 with the modified Abel-Jacobi map given in Definition 2.4.

Definition 2.9. We denote by $\eta_{\Omega,m}$ the isomorphism

$$\eta_{\Omega,m} \colon \{S \subseteq B : \#S \equiv 0 \pmod 2\}/\{S \sim S^c\} \to (\frac{1}{2}\mathbb{Z})^{2g}/\mathbb{Z}^{2g} \tag{2.15}$$

given by composing the isomorphism $G_B \to J(X)[2]$ given in Proposition 2.8 and the map AJ_c given in Definition 2.4.

Remark. We note that in Poor's work [Poo94], this is the *class* of the map η, which is an equivalence class of maps to $(\frac{1}{2}\mathbb{Z})^{2g}$. In this work we will not need the distinction between the "true" η-map and its class, and therefore by a slight abuse of notation we consider the map above to be the η-map.

This map $\eta_{\Omega,m}$ will allow us to give a more concrete definition of the set $U(\Omega, m)$, which we will use in our proof in Section 3. We first need one more notion.

Definition 2.10. If $x \in \mathbb{C}^{2g}$, let $x = (x_1, x_2)$, with $x_i \in \mathbb{C}^g$; in other words let x_1 denote the vector of the first g entries of x, and x_2 denote the vector of the last g entries of x. Furthermore, for $x_i \in \mathbb{C}^g$, let x_i^T denote the transpose of x_i. Then for $\xi \in (\frac{1}{2}\mathbb{Z})^{2g}$, we define

$$e_*(\xi) = \exp(4\pi i \xi_1^T \xi_2) \tag{2.16}$$

to be the *parity* of ξ. Note that e_* is also well-defined on $(\frac{1}{2}\mathbb{Z})^{2g}/\mathbb{Z}^{2g}$.

Proposition 2.11. *[Lemma 1.4.13 of [Poo94]] Let X be a hyperelliptic curve of genus g equipped with a marking m of its branch points, and let $J(X)$ be equipped with a choice of small period matrix Ω via the process described in Definition 2.2. Then the set $U(\Omega, m)$ of Definition 1.2 is given by*

$$\{i \in \{1, 2, \dots, 2g+1\} : e_*(\eta_{\Omega,m}(\{i, \infty\})) = -1\} \cup \{\infty\}. \tag{2.17}$$

In other words, if we consider the distinguished elements $D_i = P_i - P_\infty \in J(X)[2]$ for $i = 1, 2, \dots, 2g+1, \infty$, the set $U(\Omega, m)$ can be made to contain ∞ as well as i such that the coordinates of D_i under the Abel-Jacobi map are odd, for $i = 1, 2, \dots, 2g+1$.

2.3. **Mumford and Poor's vanishing theorem.**

We now turn our attention to explaining the significance of the set $U(\Omega, m)$. As we explained briefly in the introduction, the set connects the vanishing set of an analytic theta function to a distinguished divisor Θ on the Jacobian $J(X)$ of a marked hyperelliptic curve X.

We begin by defining this divisor:

Definition 2.12. Let X be a curve of genus g defined over $\mathbb{C}$ and P_∞ be a basepoint on X. Then we define the *theta divisor* Θ on $J(X)$ to be the subset of divisor classes of the form

$$\sum_{i=1}^{g-1} Q_i - (g-1)P_\infty. \tag{2.18}$$

Note that if X is a marked hyperelliptic curve and we choose P_∞ to be the branch point of X labeled ∞, this gives a unique choice of theta divisor on $J(X)$. We therefore call it "the" theta divisor on the marked curve X.

We now define the theta function whose zeroes we will study:

Definition 2.13. For $z \in \mathbb{C}^g$ and $\Omega \in \mathbb{H}_g$, we define the *theta function*

$$\vartheta(z, \Omega) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^T \Omega n + 2\pi i n^T z). \tag{2.19}$$

Remark. As noted in the introduction, this function is quasi-periodic for the lattice L_Ω in the coordinate z. Indeed, if $k \in \mathbb{Z}^g$, by [Mum07a, p. 120], we have

$$\vartheta(z + k, \Omega) = \vartheta(z, \Omega) \tag{2.20}$$

and

$$\vartheta(z + \Omega k, \Omega) = \exp(-i\pi k^T \Omega k - 2\pi i k^T z)\vartheta(z, \Omega). \tag{2.21}$$

However, since the automorphy factor is non-zero, the zero set of ϑ is well-defined as a subset of $\mathbb{C}^g/L_\Omega$.

For the convenience of the reader, we repeat the Riemann Vanishing Theorem now that all terms have been defined:

Theorem 2.14 (Riemann Vanishing Theorem, or Theorem 5.3 of [Mum07b])**.** *Let X be a hyperelliptic curve, m be a marking of its branch points, and let Ω be a small period matrix associated to its Jacobian via the process described in Definition 2.2. If $\Theta \in J(X)$ is as in Definition 2.12, then the zero set of the theta function $\vartheta(z, \Omega)$, considered as a subset of $J(X)(\mathbb{C})$ is a translate of Θ by a two-torsion point of $J(X)$.*

From the introduction, we recall that this gives rise to the set $U(\Omega, m)$ in the following manner: Given a marking m and a small period matrix Ω, the Riemann Vanishing Theorem singles out a divisor on the Jacobian of X (the zero locus of the function ϑ). As this is a translate of Θ by a two-torsion point, this gives in turn a distinguished two-torsion point on $J(X)$. Recall that Proposition 2.8 gives an isomorphism between the group G_B defined in Proposition 2.7 and the two-torsion of $J(X)$. Therefore, via this isomorphism, we obtain an element of the group G_B. Finally, since the elements of G_B are equivalence classes of certain subsets of B (where the equivalence consists in taking the complement in $B = \{1, 2, \ldots, 2g+1, \infty\}$), we obtain a certain (equivalence class of) subset of B, which we denote by $T(\Omega, m)$ here.

We then define the set $U(\Omega, m)$ to be the element of the equivalence class of

$$\begin{cases} T(\Omega, m) & \text{if } g \text{ is odd, and} \\ T(\Omega, m) \circ \{\infty\} & \text{if } g \text{ is even} \end{cases} \tag{2.22}$$

that contains ∞, as noted in Definition 1.2.

This definition is motivated by the proof of Proposition 6.2 of [Mum07b]: Under the correspondence given in part a) of this Proposition, the set $T(\Omega, m)$ when g is odd, or $T(\Omega, m) \circ \{\infty\}$ when g is even, corresponds to the translate $\Theta + e_{T(\Omega,m)}$ and to the characteristic $\delta + \eta_{T(\Omega,m)}$ (in our notation $\eta_{T(\Omega,m)}$ is $\eta_{\Omega,m}(T(\Omega, m))$). Since $\eta_{T(\Omega,m)} = \delta$ and $\delta \in \frac{1}{2} L_\Omega$, $T(\Omega, m)$ when g is odd, or $T(\Omega, m) \circ \{\infty\}$ when g is even, corresponds to 0 and is therefore the set $U(\Omega, m)$ defined here.

We end by giving part of the Vanishing Criterion for hyperelliptic small period matrices, which highlights how truly central the set $U(\Omega, m)$ is to the computational theory of hyperelliptic curves.

Theorem 2.15 (Main Theorem 2.6.1 of [Poo94])**.** *Let X be a hyperelliptic curve of genus g, with a marking of its branch points m and let Ω be a small period matrix associated to its Jacobian $J(X)$ via the process described in Definition 2.2. Then for $S \subseteq B$ with $\#S \equiv 0 \pmod 2$, we have*

$$\vartheta(AJ(e_S), \Omega) = 0 \tag{2.23}$$

if and only if

$$\#(S \circ U(\Omega, m)) \neq g + 1. \tag{2.24}$$

We stress that here we have only stated part of the Vanishing Criterion for hyperelliptic matrices, and that the important part of this Vanishing Criterion for computational purposes is a strengthening of the statement which allows one to give a converse for general curves.

This converse then allows the detection of hyperelliptic small period matrices among all small period matrices. We refer the reader to Poor's work [Poo94], notably Definition 1.4.11 for a complete account of this converse with proofs, or to [BILV16] for a shorter exposition.

3. The proof

The proof of Theorem 1.3 has two main parts. In the first part, for a fixed $g \geq 1$ we count the number of different sets U satisfying $U \subseteq \{1, 2, \ldots, 2g+1, \infty\}$, $\infty \in U$ and $\#U \equiv g+1 \pmod 4$ (this is Proposition 3.4). In the second part, we count how many different sets $U(\Omega, m)$ arise as we vary among all possible small period matrices Ω that can be associated to the Jacobian of a hyperelliptic curve X via the process described in Definition 2.2 and all possible markings m of its branch points (this is Proposition 3.11). Since these two numbers are equal, we conclude that every allowable set U must arise $U(\Omega, m)$ for some choice of Ω and m.

3.1. Counting the allowable sets U.

Counting the sets such that $U \subseteq \{1, 2, \ldots, 2g+1, \infty\}$, $\#U \equiv g+1 \pmod 4$, and $\infty \in U$ is equivalent to counting the sets satisfying the following two conditions:

- $\tilde{U} \subseteq \{1, 2, \ldots, 2g+1\}$, and
- $\#\tilde{U} \equiv g \pmod 4$.

We turn to this task.

Definition 3.1. Let $n \geq 1$, $d \geq 0$ and $m \geq 2$ be integers. We define the sum

$$S(n, d, m) = \sum_{\substack{0 \leq k \leq n \\ k \equiv d \pmod m}} \binom{n}{k}. \tag{3.1}$$

This is the number of subsets of $\{1, \ldots, n\}$ of any cardinality $k \equiv d \pmod m$.

We are interested in computing the quantity $S(2g+1, g, 4)$. We first note the following well-known result:

Proposition 3.2. *Let n be any positive integer, then*

$$S(n, 0, 2) = S(n, 1, 2) = 2^{n-1}. \tag{3.2}$$

In other words, for any n, of the 2^n subsets of $\{1, \ldots, n\}$, half of them have even cardinality, and half have odd cardinality.

Lemma 3.3. *We have*

$$S(n, d, 4) = S(n-1, d, 4) + S(n-1, d-1, 4). \tag{3.3}$$

Proof. This follows from Pascal's identity, which says that for $n \geq 1$ and $k \geq 0$, we have

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{3.4}$$

Here we use the usual convention that $\binom{n}{k} = 0$ if $k < 0$. □

This is enough to show

Proposition 3.4. *Let $g \geq 1$, then*

$$S(2g+1, g, 4) = 2^{g-1}(2^g + 1). \tag{3.5}$$

Proof. The proof is done by induction on g. The case of $g = 1$ is the claim that $S(3, 1, 4) = 3$. Indeed, of the subsets of $\{1, 2, 3\}$, three of them have cardinality congruent to 1 modulo 4 (and therefore actually equal to 1, since there are no subsets of $\{1, 2, 3\}$ of cardinality greater than or equal to 5).

We know assume that $S(2g-1, g-1, 4) = 2^{g-2}(2^{g-1}+1)$ and $g \geq 2$. We have

$$\begin{aligned} S(2g+1, g, 4) &= S(2g, g, 4) + S(2g, g-1, 4) && (3.6)\\ &= (S(2g-1, g, 4) + S(2g-1, g-1, 4)) && (3.7)\\ &\quad + (S(2g-1, g-1, 4) + S(2g-1, g-2, 4)) \\ &= S(2g-1, g, 4) + S(2g-1, g-2, 4) && (3.8)\\ &\quad + 2S(2g-1, g-1, 4). \end{aligned}$$

We now note that if g is even, then

$$S(2g-1, g, 4) + S(2g-1, g-2, 4) = S(2g-1, 0, 2), \tag{3.9}$$

and if g is odd, then

$$S(2g-1, g, 4) + S(2g-1, g-2, 4) = S(2g-1, 1, 2). \tag{3.10}$$

In either case, by Proposition 3.2,

$$S(2g-1, g, 4) + S(2g-1, g-2, 4) = 2^{2g-2}. \tag{3.11}$$

Furthermore, by induction $S(2g-1, g-1, 4) = 2^{g-2}(2^{g-1} + 1)$.

Therefore we have

$$\begin{aligned} S(2g+1, g, 4) &= 2^{2g-2} + 2 \cdot 2^{g-2}(2^{g-1} + 1) && (3.12)\\ &= 2^{g-1}(2^{g-1} + 2^{g-1} + 1) && (3.13)\\ &= 2^{g-1}(2^g + 1). && (3.14) \end{aligned}$$

This completes the proof. □

3.2. **Counting the different sets $U(\Omega, m)$ for a hyperelliptic curve.** Here we show that in fact, given a hyperelliptic curve X with a marking m of its branch points, every allowable U-set is realized as $U(\Omega, m)$ as we vary the small period matrix Ω associated to its Jacobian $J(X)$ by Definition 2.2. This certainly implies our main theorem. Thus we begin by fixing a marking m on the branch points of X.

The proof is carried out by considering the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ on Ω and considering which matrices fix the set $U(\Omega, m)$. We will see in Proposition 3.9 that they are exactly a subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ denoted $\Gamma_{1,2}$:

Definition 3.5. Let $\Gamma_{1,2}$ be the subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$ containing the matrices that fix the parity of every element of $(\frac{1}{2}\mathbb{Z})^{2g}$. In other words, $\gamma \in \Gamma_{1,2}$ if and only if

$$e_*(\gamma\xi) = e_*(\xi) \tag{3.15}$$

for all $\xi \in (\frac{1}{2}\mathbb{Z})^{2g}$, where e_* is as in Definition 2.10 and $\gamma\xi$ is the usual matrix-vector multiplication.

We will need two further characterizations of these matrices below. First, we have:

Proposition 3.6. *Let $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ with*

$$\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \tag{3.16}$$

where A, B, C and D are four $g \times g$ matrices. Then $\gamma \in \Gamma_{1,2}$ if and only if the diagonals of the matrices A^TC and B^TD have all even entries.

Proof. This can be verified directly, or found in [Mum07a, page 189]. □

The second characterization of these matrices relies on an important property of the vectors $\eta_{\Omega,m}(\{i, \infty\})$ for $i = 1, 2, \ldots, 2g+1$:

Proposition 3.7. *Let X be a marked hyperelliptic curve, $J(X)$ its Jacobian, and Ω a small period matrix associated to $J(X)$ via the process outlined in Definition 2.2. Furthermore, given this data, let $\eta_{\Omega,m}$ be the map given in Definition 2.9. Then the set*

$$\{\eta_{\Omega,m}(\{i, \infty\}) : i = 1, \ldots, 2g+1\} \tag{3.17}$$

contains a basis of the $\mathbb{F}_2$-vector space $(\frac{1}{2}\mathbb{Z})^{2g}/\mathbb{Z}^{2g}$.

Proof. By the proof Lemma 1.4.13 of [Poo94], the set

$$\{\eta_{\Omega,m}(\{i, \infty\}) : i = 1, \ldots, 2g+1\} \tag{3.18}$$

is an azygetic basis of $(\frac{1}{2}\mathbb{Z})^{2g}/\mathbb{Z}^{2g}$, and by Definition 1.4.12 of *ibid*, therefore spans the vector space $(\frac{1}{2}\mathbb{Z})^{2g}/\mathbb{Z}^{2g}$. Therefore it contains a basis of the space. □

We can now prove the following:

Lemma 3.8. *A matrix $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ belongs to $\Gamma_{1,2}$ if and only if it fixes the parity of $\eta_{\Omega,m}(\{i,\infty\})$ for $i = 1, 2, \ldots, 2g+1$.*

Proof. It is clear that if $\gamma \in \Gamma_{1,2}$, then it will fix the parity of $\eta_{\Omega,m}(\{i,\infty\})$ for $i = 1, 2, \ldots, 2g+1$. Therefore we assume that $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$ fixes the parity of $\eta_{\Omega,m}(\{i,\infty\})$ for $i = 1, 2, \ldots, 2g+1$ and show that $\gamma \in \Gamma_{1,2}$.

We first establish some notation: For $\xi \in (\frac{1}{2}\mathbb{Z})^{2g}$, let

$$q(\xi) = \xi_1^T \xi_2 \tag{3.19}$$

be the quadratic form associated to the parity function e_* defined in Definition 2.10. We note that

$$q(\xi) \equiv q(\zeta) \pmod{(\frac{1}{2}\mathbb{Z})^{2g}}, \tag{3.20}$$

if and only if

$$e_*(\xi) = e_*(\zeta). \tag{3.21}$$

Let also

$$b(\xi, \zeta) = \xi^T J \zeta, \tag{3.22}$$

be the bilinear form associated to the matrix J, where as before

$$J = \left(\begin{smallmatrix} 0 & \mathbb{1}_g \\ -\mathbb{1}_g & 0 \end{smallmatrix} \right), \tag{3.23}$$

and $\mathbb{1}_g$ is the $g \times g$ identity matrix.

A quick computation shows that for any $\xi, \zeta \in (\frac{1}{2}\mathbb{Z})^{2g}$

$$q(\xi + \zeta) \equiv q(\xi) + q(\zeta) + b(\xi, \zeta) \pmod{(\frac{1}{2}\mathbb{Z})^{2g}}. \tag{3.24}$$

Now let $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$. We have then that

$$b(\gamma\xi, \gamma\zeta) = b(\xi, \zeta), \tag{3.25}$$

by definition of b and $\mathrm{Sp}_{2g}(\mathbb{Z})$. Therefore, for any $\xi, \zeta \in (\frac{1}{2}\mathbb{Z})^{2g}$

(3.26)

$$q(\gamma(\xi + \zeta)) = q(\gamma\xi + \gamma\zeta) \equiv q(\gamma\xi) + q(\gamma\zeta) + b(\gamma\xi, \gamma\zeta) \pmod{(\frac{1}{2}\mathbb{Z})^{2g}}$$

$$\equiv q(\gamma\xi) + q(\gamma\zeta) + b(\xi, \zeta) \pmod{(\frac{1}{2}\mathbb{Z})^{2g}}. \tag{3.27}$$

As a result, if

$$q(\gamma\xi) \equiv q(\xi) \pmod{(\frac{1}{2}\mathbb{Z})^{2g}} \tag{3.28}$$

and

$$q(\gamma\zeta) \equiv q(\zeta) \pmod{(\frac{1}{2}\mathbb{Z})^{2g}}, \tag{3.29}$$

then

$$q(\gamma(\xi+\zeta)) \equiv q(\xi+\zeta) \pmod{(\frac{1}{2}\mathbb{Z})^{2g}}. \tag{3.30}$$

From this discussion we conclude that if $e_*(\gamma\xi) = e_*(\xi)$ and $e_*(\gamma\zeta) = e_*(\zeta)$, it follows that

$$e_*(\gamma(\xi+\zeta)) = e_*(\xi+\zeta). \tag{3.31}$$

The result now follows from the fact that the set

$$\{\eta_{\Omega,m}(\{i,\infty\}) : i = 1, \ldots, 2g+1\} \tag{3.32}$$

contains a basis of the $\mathbb{F}_2$-vector space $(\frac{1}{2}\mathbb{Z})^{2g}/\mathbb{Z}^{2g}$ by Proposition 3.7. Therefore if a matrix γ fixes the parity of each element of this basis, it must fix the parity of each element of the vector space. □

We are now in a position to show:

Proposition 3.9. *Let X be a marked hyperelliptic curve, $J(X)$ its Jacobian, and Ω a small period matrix associated to $J(X)$ via the process outlined in Definition 2.2. Furthermore, given this data, let $\eta_{\Omega,m}$ be the map given in Definition 2.9 and $U(\Omega, m)$ be the set defined in Definition 1.2.*

Let $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$. Then the matrix $\gamma \cdot \Omega$ is another small period matrix for $J(X)$, to which we may similarly attach a map $\eta_{\gamma\cdot\Omega,m}$ and a set $U(\gamma \cdot \Omega, m)$.

In that case, we have

$$U(\gamma \cdot \Omega, m) = U(\Omega, m) \tag{3.33}$$

if and only if

$$\gamma \in \Gamma_{1,2}. \tag{3.34}$$

Proof. Recall from Proposition 2.11 that $U(\Omega, m)$ can be described as the set

$$\{i \in \{1, 2, \ldots, 2g+1\} : e_*(\eta_{\Omega,m}(\{i,\infty\})) = -1\} \cup \{\infty\}. \tag{3.35}$$

Since $\eta_{\Omega,m}(\{i,\infty\}) \in (\frac{1}{2}\mathbb{Z})^{2g}/\mathbb{Z}^{2g}$ is none other than $AJ_c(e_{\{i,\infty\}})$, by Proposition 2.5, we have

$$\eta_{\gamma\cdot\Omega,m}(\{i,\infty\}) = \gamma^{-T}\eta_{\Omega,m}(\{i,\infty\}), \tag{3.36}$$

Therefore we have that

$$U(\gamma \cdot \Omega, m) = U(\Omega, m) \tag{3.37}$$

if and only if multiplication by γ^{-T} does not change the parity of any $\eta_{\Omega,m}(\{i,\infty\})$ for $i = 1, 2, \ldots, 2g+1$. By Lemma 3.8, this is the case if and only if $\gamma^{-T} \in \Gamma_{1,2}$.

To finish the proof we must show that $\gamma^{-T} \in \Gamma_{1,2}$ if and only if $\gamma \in \Gamma_{1,2}$. Note that since $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$, we have

$$\gamma^{-T} = \begin{pmatrix} D & -C \\ -B & A \end{pmatrix}. \tag{3.38}$$

By Proposition 3.6, it suffices thus to show that the diagonals of the matrices

$$D^T(-B) = (-B^T D)^T \tag{3.39}$$

and

$$(-C)^T A = (-A^T C)^T \tag{3.40}$$

have all even entries if and only if the diagonals of the matrices $A^T C$ and $B^T D$ have all even entries, which is true. □

As a direct consequence we now have:

Theorem 3.10. *The number of different sets $U(\Omega, m)$ that arise, as Ω varies over all small period matrices that can be attached to the polarized Jacobian of a marked hyperelliptic curve X with the process outlined in Definition 2.2, is equal to the cardinality of the quotient group*

$$\mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma_{1,2}. \tag{3.41}$$

Proof. As described in Section 2, the group $\mathrm{Sp}_{2g}(\mathbb{Z})$ acts transitively on the set of small period matrices that can be associated to $J(X)$ via the process described in Definition 2.2. This action changes $U(\Omega, m)$ if and only if $\gamma \in \Gamma_{1,2}$ by Proposition 3.9, which completes the proof. □

We now compute the cardinality of this quotient group, which will give us the number of different sets $U(\Omega, m)$ attached to a fixed hyperelliptic curve X with a marking of its branch points m as Ω is allowed to vary over all possible small period matrices that can be associated to its Jacobian $J(X)$ via the process described in Definition 2.2.

Proposition 3.11. *We have that*

$$\#\,\mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma_{1,2} = 2^{g-1}(2^g + 1). \tag{3.42}$$

Proof. To compute the cardinality of this quotient group, we use the following facts: First, by the Third Group Isomorphism Theorem,

$$\mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma_{1,2} \cong \frac{\mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma(2)}{\Gamma_{1,2}/\Gamma(2)}, \tag{3.43}$$

where

$$\Gamma(2) = \left\{\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z}) : \gamma \equiv \mathbb{1}_{2g} \pmod 2\right\}. \tag{3.44}$$

Furthermore, we have

$$\mathrm{Sp}_{2g}(\mathbb{Z})/\Gamma(2) \cong \mathrm{Sp}_{2g}(\mathbb{F}_2), \tag{3.45}$$

where $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ is the group of matrices with coefficients in $\mathbb{F}_2$ and symplectic with respect to the bilinear form given by the matrix

$$\begin{pmatrix} 0 & \mathbb{1}_g \\ \mathbb{1}_g & 0 \end{pmatrix}, \tag{3.46}$$

and

$$\Gamma_{1,2}/\Gamma(2) \cong \mathrm{SO}_{2g}(\mathbb{F}_2, +1), \tag{3.47}$$

where $\mathrm{SO}_{2g}(\mathbb{F}_2, +1)$ is the special orthogonal group of matrices with entries in $\mathbb{F}_2$ and preserving the quadratic form

$$Q(x_1, x_2, \ldots, x_{2g-1}, x_{2g}) = \sum_{i=1}^{g} x_i x_{g+i}. \tag{3.48}$$

(These last two facts are implicit in the discussion in [Mum07a], Appendix to Chapter 5.)

There are therefore

$$\frac{\#\,\mathrm{Sp}_{2g}(\mathbb{F}_2)}{\#\,\mathrm{SO}_{2g}(\mathbb{F}_2, +1)} \tag{3.49}$$

different sets $U(\Omega, m)$ as Ω varies over all small period matrices that can be associated to $J(X)$ via the process described in Definition 2.2.

We have

$$\#\,\mathrm{Sp}_{2g}(\mathbb{F}_2) = 2^{g^2} \prod_{i=1}^{g} (2^{2i} - 1), \tag{3.50}$$

(see for example [Gro02, Theorem 3.12]) and

$$\#\,\mathrm{SO}_{2g}(\mathbb{F}_2, +1) = 2 \cdot 2^{g(g-1)} (2^g - 1) \prod_{i=1}^{g-1} (2^{2i} - 1), \tag{3.51}$$

(see for example [KL90, Table 2.1C]). Computing the quotient gives the result we sought.

□

References

[BILV16] Jennifer S. Balakrishnan, Sorina Ionica, Kristin Lauter, and Christelle Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *London Mathematical Society Journal of Computation and Mathematics*, 19(suppl. A):283–300, 2016.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin, second edition, 2004.

[Gro02] Larry C. Grove. *Classical groups and geometric algebra*, volume 39 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 2002.

[KL90] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, 1990.

[Mum07a] David Mumford. *Tata lectures on theta. I.* Modern Birkhäuser Classics. Birkhäuser, Boston, MA, 2007.

[Mum07b] David Mumford. *Tata lectures on theta. II.* Modern Birkhäuser Classics. Birkhäuser, Boston, MA, 2007.

[Poo94] Cris Poor. The hyperelliptic locus. *Duke Mathematical Journal*, 76(3):809–884, 1994.

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Avenue, Burlington VT 05401

E-mail address: `christelle.vincent@uvm.edu`