TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 350, Number 8, August 1998, Pages 3083–3106
S 0002-9947(98)02056-X

EQUATIONS FOR THE JACOBIAN OF A HYPERELLIPTIC CURVE

PAUL VAN WAMELEN

Abstract. We give an explicit embedding of the Jacobian of a hyperelliptic curve, $y^2 = f(x)$, into projective space such that the image is isomorphic to the Jacobian over the splitting field of f. The embedding is a modification of the usual embedding by theta functions with half integer characteristics.

1. Introduction

The Jacobian J of a curve defined over a field K is a projective group variety also defined over K. In general it is hard to give an explicit description of the Jacobian. In the case where the curves are hyperelliptic there is a relatively explicit description of the Jacobian as an *abstract* variety defined over K. On the other hand, if K is a subfield of $\mathbb{C}$, then $J(\mathbb{C})$ carries the structure of an abelian torus $\mathbb{C}^g/\Lambda$, and this torus can be embedded into projective space by theta functions. For a hyperelliptic curve $y^2 = f(x)$ the equations defining this variety in projective space are given by the Frobenius identities for half-integer characteristic theta functions. This description can be very useful because it is so explicit, but in general it is not isomorphic to the Jacobian over K (only over $\mathbb{C}$) and we therefore lose any arithmetic information. We can now ask whether we might not be able to modify this description in such a way that the resulting variety would be isomorphic to the Jacobian over a smaller field. This paper gives one answer to this question.

The main result is Theorem 9, which gives a variety defined by theta functions which is isomorphic to the Jacobian of a hyperelliptic curve over the splitting field of f. The description is a modification of the usual embedding of the complex points of the Jacobian into projective space using theta functions. It describes the Jacobian as an explicit projective variety and not just as an abstract variety.

This work is a generalization of work done by D. Grant and others on the genus 2 case; see [Gra90] and [GG93]. For other work in this direction see [Fly90]. For a potential application of these ideas see [Pil90].

The idea of the paper is as follows. Let C be the curve $y^2 = \prod_{i=1}^{2g+1}(x - a_i)$ and set $F = \mathbb{Q}(a_1, \ldots, a_{2g+1})$. The Jacobian, J, of a curve is an abelian variety whose points parameterize divisors of degree zero on the curve modulo linear equivalence. Let $\mathrm{cl}(D)$ denote the linear equivalence class of the divisor D. Then

$$\Theta = \{\mathrm{cl}(P_1 + \cdots + P_{g-1} - (g-1)\infty) | P_i \in C\}$$

Received by the editors December 5, 1995.
1991 *Mathematics Subject Classification.* Primary 14H40; Secondary 14H42.
Key words and phrases. Jacobian, hyperelliptic curve, theta function, theta constant, Thomae's identity.

is a divisor on the Jacobian. Now $[2]^*\Theta$ is very ample and the dimension of $\mathcal{L}([2]^*\Theta)$ is 2^{2g}. It is well-known that a basis for this space can be given by quotients of theta functions with half integer characteristics evaluated at $2z$. We will modify this basis to get a new basis $\{t_A(2z)\}$. Denote the image of the embedding $J \to \mathbb{P}^{2^{2g}-1}$ induced by this basis, by T. We can explicitly write down a set of equations for T, and using some new theta-constant identities we can check that these equations have coefficients in F. It then remains to show that T is isomorphic to J over F.

We will describe a certain affine variety Z birationally equivalent to J. The coefficients of two polynomials $\mathbf{U}$ and $\mathbf{V}$ give explicit coordinate functions of Z over F. We will show that these coordinates can be expressed as rational functions of the $t_A(2z)$ with coefficients in F. From this we will deduce that T is isomorphic to J over F.

We now give a brief outline of the paper. Sections 2 to 5 introduce the objects we will be working with, and we try to state all the main results that will be used in the rest of the paper. Section 2 describes the Jacobian of a hyperelliptic curve, and we introduce the variety Z. Section 3 introduces theta functions and states some of the many beautiful identities that they satisfy. For theta functions associated to hyperelliptic curves there is a very useful way of describing the half-integer characteristics. This leads to elegant ways of stating the special results which hold for theta functions associated to hyperelliptic curves and with half-integer characteristics. The statements of these results are started in Section 4 and continued in Section 5. This last section contains proofs of a few mild generalizations of results on theta-constants. In particular, Theorem 2 is a generalization of Thomae's identities.

Section 6 starts with the definition of the modified embedding. For every theta function with half-integer characteristic we define a function t_A which is just this theta function multiplied by a complicated-looking constant. The first result is that the variety, T, obtained from the embedding into projective space defined by the t_A is defined over F. The final section of the paper is devoted to showing that T is isomorphic, over F, to the Jacobian. Along the way to proving this we find a nice description of the $\mathbf{V}$ polynomial analogous to Mumford's description of the $\mathbf{U}$ polynomial.

Acknowledgement: I would like to thank the reviewer for his careful reading of the paper and his suggestions. In particular the reviewer suggested substantial improvements to the proofs of Theorems 4, 6 and 9.

2. The Jacobian of a hyperelliptic curve

In this section we want to describe the background on hyperelliptic curves and their Jacobians. We will follow [Mum83], [Mum84], especially chapters II and IIIa.

Let C be a hyperelliptic curve defined over $\mathbb{C}$ of positive genus g; that is, an affine part of C is given by the solutions of the equation

$$y^2 = \prod_{i=1}^{2g+1} (x - a_i) = f(x) \tag{1}$$

where the a_i are distinct points in $\mathbb{C}$. Since the a_i are assumed distinct this curve will be non-singular. We only need to add one point at infinity to make the curve into a non-singular projective curve. We will still think of points on this projective

curve as solutions (x, y) to (1) and refer to the point at infinity as ∞. The hyperelliptic curve comes equipped with an involution sending $P = (x, y)$ to $\imath P = (x, -y)$. We can think of x and y as functions on the curve, and as such we can show that x has a pole of order 2 and y has a pole of order $2g + 1$ at ∞ (and neither one has a pole anywhere else). Also, y has a simple zero at each finite branch point a_i while $x - a_i$ has a double zero at each such branch point. Note that we are using a_i to refer to both the actual point $(a_i, 0)$ on the curve and to just its x-coordinate.

To any complete non-singular curve we can associate an abelian (and therefore projective [Mil86a, Thm 7.1]) variety called the Jacobian of the curve. The Jacobian can be defined over the same field as the curve ([Mil86b, Thm 1.1]). The points of the Jacobian form a group, and correspond to the divisors of degree zero modulo linear equivalence. Let $\mathrm{cl}(D)$ denote the linear equivalence class of the divisor D. One can show that any divisor of degree zero is linearly equivalent to a divisor of the form $\sum_{i=1}^{g} P_i - g \cdot \infty$. This shows that the the map I from the symmetric product of the curve with itself g times, $C^{(g)}$, to J given by

$$I(\sum_{i=1}^{g} P_i) = \mathrm{cl}(\sum_{i=1}^{g} P_i - g \cdot \infty)$$

is surjective. In fact, it is a birational map ([Mil86b, Thm 5.1.(a)]. Even better, J is the unique abelian variety birationally equivalent to $C^{(g)}$ [Mil86b, Remark 5.6.(a)]).

Thinking of points in $C^{(g)}$ as effective divisors of degree g, we define $Z \subset C^{(g)}$ to be those divisors $D = \sum P_i$ such that $P_i \neq \infty$ and $P_i \neq \imath P_j$ for all i and j with $i \neq j$. Then it can be shown that I is injective on Z. In fact, if $I(\sum P_i) = I(\sum Q_i)$ with only $\sum P_i \in Z$, then $\sum P_i = \sum Q_i$. We denote the complement of the image of Z under I in J by Θ, so that I is a bijection between Z and $J - \Theta$. It follows that Θ is given by the set $\{\mathrm{cl}(\sum_{i=1}^{g-1} P_i - (g-1)\infty)\}$.

We need to show that Z is a variety. We begin by associating to a divisor $D = \sum_{i=1}^{g} P_i$ in Z two polynomials $\mathbf{U}$ and $\mathbf{V}$ as follows. Set x_i equal to the x-coordinate of the point P_i. Similarly let $y_i = y(P_i)$. We define $\mathbf{U}(x)$, a monic polynomial of degree g, by

$$\mathbf{U}(x) = \prod_{i=1}^{g} (x - x_i).$$

We let the polynomial $\mathbf{V}(x)$ be the unique polynomial of degree at most $g-1$ such that, if P_i has order $n_i = \mathrm{ord}_{P_i}(D)$ in D, $\mathbf{V}(x) - \sqrt{f(x)}$ has a zero of multiplicity n_i at x_i. Here $\sqrt{f(x)}$ denotes a branch of the square root that equals y_i at x_i. In particular, if all the P_i are distinct, we have

$$\mathbf{V}(x) = \sum_{i=1}^{g} y_i \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}. \tag{2}$$

By construction, $\mathbf{U}(x)$ divides $f(x) - \mathbf{V}(x)^2$.

Conversely, to any two given polynomials $\mathbf{U}$ and $\mathbf{V}$ such that $\mathbf{U}$ divides $f - \mathbf{V}^2$, $\mathbf{U}$ is monic of degree g and $\mathbf{V}$ is of degree $\leq g - 1$, we can associate a divisor in Z. The zeros of $\mathbf{U}$ give g x-coordinates and the value of $\mathbf{V}$ at such a coordinate gives one of the square roots of $f(x)$, so a y-coordinate. This gives g points making up an effective divisor in Z.

For an arbitrary $\mathbf{U}$ and $\mathbf{V}$ with the right degrees we can use the Euclidean algorithm to find the remainder of $f(x) - \mathbf{V}(x)^2$ divided by $\mathbf{U}$. The requirement that this remainder be zero can be expressed as a set of algebraic equations in the coefficients of $\mathbf{U}$ and $\mathbf{V}$. So we see that the variety of solutions to these equations is bijective as a set to Z. That is, we have shown that, using the coefficients of the $\mathbf{U}$ and $\mathbf{V}$ polynomials, we can give Z a variety structure. We even see that Z is defined over the same field as the curve. In the proof of [Mum84, Prop IIIa.1.3] Mumford shows that the above-mentioned bijection is a morphism. Following the argument, it is clear that this morphism is defined over the same field as the curve. So it finally follows that Z is birationally equivalent to $C^{(g)}$ over F.

We want to describe $J(\mathbb{C})$ analytically, so view $C(\mathbb{C})$ as a compact Riemann surface of genus g. Then it is known that the dimension of the vector space of holomorphic 1-forms is equal to the genus of the curve. So let φ_i, $i = 1, 2, \ldots, g$, be a basis for this vector space and set $\overline{\varphi} = {}^t(\varphi_1, \ldots, \varphi_g)$, a vector of holomorphic 1-forms. We can now define a mapping

$$\text{Int} : C \to \mathbb{C}^g \tag{3}$$

by

$$P \mapsto \int_\infty^P \overline{\varphi}. \tag{4}$$

To remove the dependency of this mapping on the path of integration, we define Λ to be the image of the map from the first homology group of C, $H_1(C, \mathbb{Z})$, to $\mathbb{C}^g$ which sends a closed path, $\sigma \in H_1(C, \mathbb{Z})$, on the Riemann surface to $\int_\sigma \overline{\varphi}$. Then Λ turns out to be a lattice in $\mathbb{C}^g$ and so we get the complex torus $\mathbb{C}^g/\Lambda$. We then see that Int is a well-defined mapping from C into $\mathbb{C}^g/\Lambda$. We extend this mapping additively to the divisors of degree zero on C. The Abel part of the Abel-Jacobi theorem then states that two divisors map to the same thing under Int if and only if they are linearly equivalent. The Jacobi part says that the map is onto. So there is a bijection between $J(\mathbb{C})$ and $\mathbb{C}^g/\Lambda$ as sets.

We now want to describe a variety structure on $\mathbb{C}^g/\Lambda$. Let $A_1, \ldots, A_g, B_1, \ldots, B_g$ be a symplectic homology basis. That is, the A_i and B_i are closed paths on the Riemann surface so that the A_i's are disjoint, the B_i's are disjoint and A_i intersects B_j only if $i = j$ and then so that the intersection multiplicity of A_i with B_i equals plus one. Let ω_1 and ω_2 be the $g \times g$ matrices with entries

$$\omega_{1\,ij} = \int_{B_j} \varphi_i$$

and

$$\omega_{2\,ij} = \int_{A_j} \varphi_i.$$

Then $\Omega = (\omega_1, \omega_2)$ is a $\mathbb{Z}$-basis for the lattice $\Lambda = \Omega\mathbb{Z}^{2g}$. It can now be shown that the so-called Riemann relations hold:

$$\omega_2\, {}^t\omega_1 - \omega_1\, {}^t\omega_2 = 0 \tag{5}$$

and

$$i(\omega_2\, {}^t\overline{\omega}_1 - \omega_1\, {}^t\overline{\omega}_2) > 0, \tag{6}$$

where the bar denotes complex conjugation and > 0 means positive definite. The space of symmetric $g \times g$ matrices with positive definite imaginary part is called the

Siegel upper-half space of degree g and is denoted by $\mathfrak{h}_g$. The Riemann relations are equivalent to saying that $\omega_2^{-1}\omega_1 \in \mathfrak{h}_g$. Set

$$J = \begin{pmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{pmatrix}.$$

If we define

$$E(\Omega x, \Omega y) = {}^t x\, J y,$$

for any $x, y \in \mathbb{R}^{2g}$, then E is a Riemann form for the torus $\mathbb{C}^g/\Lambda$. The existence of a Riemann form on a torus is a necessary and sufficient condition for the torus to be embeddable into projective space. Chow's theorem [Har77, Appendix B, Thm 2.2] then says that $\mathbb{C}^g/\Lambda$ is complex analytically isomorphic to the complex points of an abelian variety. Theta functions allow us to make this explicit.

3. Theta functions

The rest of the theory is simplified by normalizing a few of our choices. We will only be working with hyperelliptic curves, and for these there is a specific and traditional choice of a homology basis for C. Recall that the a_i are the branch points of the double cover of $\mathbb{P}$ by the Riemann surface C. Consider "cuts" between a_{2i-1} and a_{2i} for $i = 1, \ldots, g$ and between a_{2g+1} and ∞. Let A_i be a path clockwise around a_{2i-1} and a_{2i} for $i = 1, \ldots, g$. Let the B_i be clockwise paths around all the a_j for $j = 2i, 2i+1, \ldots, 2g+1$. As each of these paths circles an even number of branch points, lifting these paths to the Riemann surface C we obtain closed paths on C. See Figure 1. So $A_1, \ldots, A_g, B_1, \ldots, B_g$ form a symplectic basis.

The natural choice of a basis for the holomorphic 1-forms, in the case of a hyperelliptic curve, is $x^{i-1}dx/y$ for $i = 1, \ldots, g$. We now normalize this. Let λ be the $g \times g$ matrix with entries

$$\lambda_{ij} = \int_{A_j} \frac{x^{i-1}dx}{y},$$

and set

$$\overline{\varphi} = \lambda^{-1\,t}\left(\frac{dx}{y}, \ldots, \frac{x^{g-1}dx}{y}\right).$$

Thus $\int_{A_j} \varphi_i = \delta_{ij}$. If we define τ to be the $g \times g$ matrix with entries $\tau_{ij} = \int_{B_j} \varphi_i$, then we have seen that τ is in $\mathfrak{h}_g$. Note that now $\Lambda = \tau\mathbb{Z}^g + \mathbb{Z}^g$.

As we pointed out, $\mathbb{C}^g/\Lambda$ has the structure of an algebraic variety. This is made explicit by using theta functions to embed $\mathbb{C}^g/\Lambda$ into projective space—the theta identities then give explicit equations satisfied by the image. We now introduce these functions.

For $c \in \mathbb{R}^{2g}$ let c' be the first g entries and c'' the second g entries of c. For such a c, $z \in \mathbb{C}^g$ and $\tau \in \mathfrak{h}_g$ the classical multi-variable theta function is defined by

$$\theta[c](z, \tau) = \sum_{m \in \mathbb{Z}^g} \exp(\pi i\, {}^t(m + c')\tau(m + c') + 2\pi i\, {}^t(m + c')(z + c'')).$$

The vector c is called the characteristic of the theta function. We usually think of theta functions with different characteristics as distinct functions. We will often suppress the variable τ and think of a theta function as just depending on z. These functions satisfy many identities, of which we note a few of the more important ones.

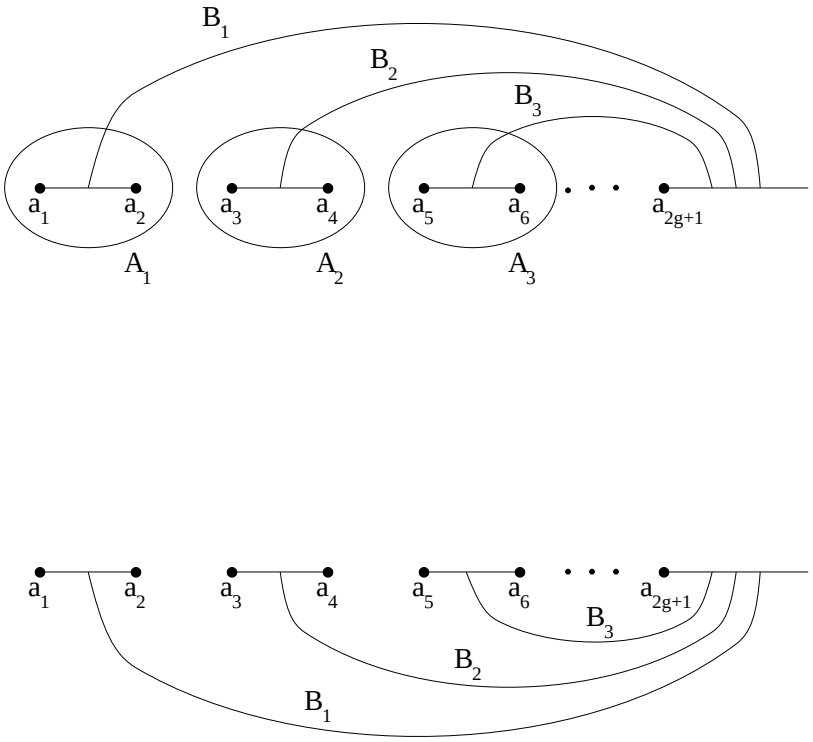

FIGURE 1. The clockwise paths making up the traditional homology basis

Quasi-periodicity: For k in $\mathbb{Z}^{2g}$,

$$\begin{aligned}\theta[c](z+\tau k'+k'',\tau)\\ = \exp(-\pi i\,{}^t k'\,\tau k' - 2\pi i\,{}^t k'\,z)\exp(2\pi i({}^t c'\,k'' - {}^t c''\,k'))\theta[c](z,\tau).\end{aligned} \tag{7}$$

Characteristics modulo $\mathbb{Z}$: For k in $\mathbb{Z}^{2g}$

$$\theta[c+k](z,\tau) = \exp(2\pi i\,{}^t c'\,k'')\theta[c](z,\tau). \tag{8}$$

Relating different characteristics: For r in $\mathbb{R}^{2g}$,

$$\theta[c+r](z,\tau) = \exp(\pi i\,{}^t r'\,\tau r' + 2\pi i\,{}^t r'(z+r''+c''))\theta[c](z+\tau r'+r'',\tau). \tag{9}$$

In particular, we can write every theta function in terms of the theta function with zero characteristic.

Symmetry in the z variable: For $c \in \frac{1}{2}\mathbb{Z}^{2g}$,

$$\theta[c](-z,\tau) = (-1)^{4\,{}^t c'\,c''}\theta[c](z,\tau). \tag{10}$$

This shows that theta functions with half-integer characteristics are either even or odd functions. These identities all follow more or less directly from the definition.

The final type of identity we will use are identities giving algebraic relations between different theta functions. In a sense the 'only' identity here is the Riemann theta identity. It is so general, though, that in applying the identity we almost always specialize some of the variables to gives us the identity we need. We won't state the most general form (see [Mum83, Thm II.6.1]), but just what we will use.

Riemann identity: For a, b, c, d in $\mathbb{R}^{2g}$ and x, y, u, v in $\mathbb{C}^g$

(11)
$$\begin{aligned}\theta[\tfrac{a+b+c+d}{2}](\tfrac{x+y+u+v}{2})\cdot\theta[\tfrac{a+b-c-d}{2}](\tfrac{x+y-u-v}{2})\\ \cdot\theta[\tfrac{a-b+c-d}{2}](\tfrac{x-y+u-v}{2})\cdot\theta[\tfrac{a-b-c+d}{2}](\tfrac{x-y-u+v}{2})\\ = 2^{-g}\sum_{\alpha\in\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}}\exp(-2\pi i\,{}^t(a+b+c+d)'\alpha'')\theta[a+\alpha](x)\cdot\theta[b+\alpha](y)\\ \cdot\theta[c+\alpha](u)\cdot\theta[d+\alpha](v).\end{aligned}$$

4. Half-integer characteristics

We now indicate some of the special identities and results we can obtain for theta functions with half-integer characteristics, using the fact that τ comes from a hyperelliptic curve. First we describe a very convenient way of labeling the half-integer characteristics.

Let
$$B = \{1, 2, \ldots, 2g+1, \infty\}$$
be an index set for the branch points. For $i = 1, \ldots, g$ define column vectors $\eta_i = {}^t(\eta_i', \eta_i'') \in \mathbb{R}^{2g}$ as follows:

$$\begin{aligned}\eta'_{2i-1} &= {}^t(0,\ldots,0,\overset{\text{position } i}{\overset{\downarrow}{\tfrac{1}{2}}},0,\ldots,0),\\ \eta''_{2i-1} &= {}^t(\tfrac{1}{2},\ldots,\tfrac{1}{2},0,0,\ldots,0),\\ \eta'_{2i} &= {}^t(0,\ldots,0,\tfrac{1}{2},0,\ldots,0),\\ \eta''_{2i} &= {}^t(\tfrac{1}{2},\ldots,\tfrac{1}{2},\tfrac{1}{2},0,\ldots,0),\end{aligned}$$

and

$$\begin{aligned}\eta'_{2g+1} &= {}^t(0,\ldots,0),\\ \eta''_{2g+1} &= {}^t(\tfrac{1}{2},\ldots,\tfrac{1}{2}),\\ \eta_\infty &= {}^t(0,\ldots,0).\end{aligned}$$

This defines η_j for any $j \in B$. We extend this to η_T for any $T \subset B$ by setting
$$\eta_T = \sum_{j\in T}\eta_j.$$

For any $T \subset B$ let T^c denote the complement of T in B. Note that $\eta_B \in \mathbb{Z}^{2g}$, so that if we view η_T as an element of $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ then $\eta_T = \eta_{T^c}$. Also if we let $\circ$ denote the symmetric difference of sets, that is $T \circ S = (T \cup S) - (T \cap S)$, then $\circ$ makes the set of subsets of B into a group. In fact we have a group isomorphism

$$\{T \subset B | \#(T) \equiv 0 \mod 2\}/T \sim T^c \cong \frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}.$$

The reason for this choice of the η_j's is the following. Let $U = \{1, 3, \ldots, 2g+1\}$ be the odd branch points. Then for $S \subset B$ with $\#S$ even ([Mum84, Def. IIIa.2.3 and (5.8)])

$$\operatorname{Int}(\sum_{i\in S} a_i) = \tau\eta'_S + \eta''_S.$$

It follows from Riemann's vanishing theorem that $\theta[\eta_U](z)$ has a simple zero at Θ; moreover, by (9), $\theta[\eta_{U\circ S}](z)$ differs by an exponential from $\theta[\eta_U](z+\tau\eta'_S+\eta''_S)$, so we see that $\theta[\eta_{U\circ S}](z)$ has a simple zero on $T_{\sum_{i\in S}a_i-\#(S)\infty}\Theta$, where for a point $Q\in J$ we let T_Q denote the translation-by-Q map. It is important to note that the correct choice of η (to make all of this true), depends on the particular choice of symplectic basis for the homology group.

We can also use η to identify the 'even' and 'odd' characteristics. For $\eta\in\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ define

$$e_*(\eta)=(-1)^{4\,{}^t\eta'\,\eta''}.$$

Then (10) becomes

$$\theta[c](-z,\tau)=e_*(c)\theta[c](z,\tau).$$

We say that c is an even (respectively odd) characteristic if $e_*(c)=1$ (respectively $e_*(c)=-1$). Then ([Mum84, Prop. IIIa.6.3.b])

$$e_*(\eta_{U\circ T})=(-1)^{\left(\frac{\#T-g-1}{2}\right)}\text{ for }T\subset B,\ \#T\equiv g+1 \mod 2. \tag{12}$$

We will also need the following definition and evaluation. For $\eta,\zeta\in\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$ define

$$e_2(\eta,\zeta)=(-1)^{4({}^t\zeta'\,\eta''-{}^t\eta'\,\zeta'')}. \tag{13}$$

For $S_1,S_2\in B$ with $\#S_1$ and $\#S_2$ both even ([Mum84, Prop. IIIa.6.3.a])

$$e_2(\eta_{S_1},\eta_{S_2})=\frac{e_*(\eta_{S_1}+\eta_{S_2})}{e_*(\eta_{S_1})e_*(\eta_{S_2})}=(-1)^{\#(S_1\cap S_2)}. \tag{14}$$

By a theta-constant we mean a theta function evaluated at $z=0$. We will denote a theta-constant, $\theta[c](0)$, by $\vartheta[c]$. We can use η to describe exactly which of the theta-constants are zero—this is the fundamental Vanishing Property (see [Mum84, Cor IIIa.6.7]). It states that for any $S\subset B$ with $\#S\equiv g+1 \mod 2$,

$$\vartheta[\eta_{U\circ S}]=0\iff \#S\neq g+1. \tag{15}$$

In fact this solves the "Schottky problem for hyperelliptic curves": this property characterizes hyperelliptic period matrices (see [Mum84, Sec. IIIa.9]).

Recall that our purpose for introducing theta functions was to embed $\mathbb{C}^g/\Lambda$ into projective space. Note that from (7), theta functions with half-integer characteristics evaluated at $2z$ will change by a factor independent of the characteristic under $z\mapsto z+\lambda$ for $\lambda\in\Lambda$. Therefore it is not a function on $\mathbb{C}^g/\Lambda$, but the map

$$z\mapsto\left(\theta[c](2z)\right)_{c\in\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}} \tag{16}$$

is a well-defined map from $\mathbb{C}^g/\Lambda$ into $2^{2g}-1$ dimensional projective space. It can be shown that this map is injective (see [Mum83, Thm II.1.3], [Lan82, Thm VI.6.1] or [LB92, Thm 4.5.3]) and therefore the image is a projective variety bijective to $\mathbb{C}^g/\Lambda$ as a set. In this way $\mathbb{C}^g/\Lambda$ becomes a variety isomorphic to $J(\mathbb{C})$ over $\mathbb{C}$.

Note that if we take $x=y=2z$, $u=v=0$ and the a_i in $\frac{1}{2}\mathbb{Z}^{2g}$ with $a_1+a_2+a_3+a_4\in\mathbb{Z}^{2g}$ in (11), we get quadratic equations satisfied by the image of the above map. These equations can be simplified. In the case that τ comes from a hyperelliptic curve the Riemann identities simplifies to the following, more elegant looking equations called the Frobenius theta identities (for a proof see [Mum84,

Thm IIIa.7.1]). For all $z_i \in \mathbb{C}^{2g}$, $i = 1, 2, 3$ or 4, such that $z_1 + z_2 + z_3 + z_4 = 0$, and for all $a_i \in \mathbb{R}^{2g}$, $i = 1, 2, 3$ or 4, such that $a_1 + a_2 + a_3 + a_4 = 0$, we have

$$\sum_{j \in B} \varepsilon_U(j)\theta[a_1 + \eta_j](z_1)\theta[a_2 + \eta_j](z_2)\theta[a_3 + \eta_j](z_3)\theta[a_4 + \eta_j](z_4) = 0, \tag{17}$$

where, for any $A \subset B$,

$$\varepsilon_A(k) = \begin{cases} 1 & \text{if } k \in A, \\ -1 & \text{if } k \notin A. \end{cases}$$

We won't use this, but it follows easily from Theorem 7.5.2 in [LB92] that the Frobenius Identities with $z_1 = z_2 = 2z$, $z_3 = z_4 = 0$ and all possible choices of $a_i \in \frac{1}{2}\mathbb{Z}^{2g}$ give all the equations satisfied by the image of the above mentioned embedding. Note though, that these equations have coefficients in the field generated by the ratios of the theta constants, $\mathbb{Q}(\vartheta[\eta_A]/\vartheta[\eta_U])_{A \subset B}$. Later (Lemma 2) we will see that this field is actually the field generated by $\mathbb{Q}$ and the square roots of differences of the a_i's. The purpose of a large part of this paper is to show that we can modify the above embedding in such a way that the image is defined over the smaller field generated by $\mathbb{Q}$ and only the a_i's. We will also show that it is isomorphic to the Jacobian over this same field.

5. Theta-constants

In this section we prove a slight generalization of a form of Thomae's identity [Mum84, Thm IIIa.8.1]. These are identities relating the roots a_i of the hyperelliptic equation to the theta-constants with half-integer characteristics.

We first prove a technical-looking lemma that will, nevertheless, turn out to be crucial in allowing us to define the square roots of differences of the a_i's in a meaningful way. Recall (14)

$$e_2(\eta_{A_1}, \eta_{A_2}) = (-1)^{4({}^t\eta'_{A_1}\,\eta''_{A_2} + {}^t\eta'_{A_2}\,\eta''_{A_1})} = (-1)^{\#(A_1 \cap A_2)}$$

for subsets A_1 and A_2 of B with an even number of elements. By abuse of notation we let $e_2(A_1, A_2) = e_2(\eta_{A_1}, \eta_{A_2})$ and $e_2(i, A) = e_2(\eta_{\{i,\infty\}}, \eta_A)$.

Lemma 1. *Let V and V' be subsets of B with $g + 1$ elements such that $\{i, j\} \subseteq V \cap V'$ and $\{k, \infty\} \subseteq V^c \cap V'^c$. Then*

$$\begin{aligned} &\vartheta[\eta_{U \circ V \circ \{i,\infty\}}]\vartheta[\eta_{U \circ V \circ \{j,k\}}]\vartheta[\eta_{U \circ V' \circ \{j,\infty\}}]\vartheta[\eta_{U \circ V' \circ \{i,k\}}] \\ &\quad = \vartheta[\eta_{U \circ V \circ \{j,\infty\}}]\vartheta[\eta_{U \circ V \circ \{i,k\}}]\vartheta[\eta_{U \circ V' \circ \{i,\infty\}}]\vartheta[\eta_{U \circ V' \circ \{j,k\}}]. \end{aligned}$$

Proof. Let $A_1 = V$, $A_2 = V \circ \{i, j, k, \infty\}$, $A_3 = V' \circ \{i, j\}$, $A_4 = V' \circ \{k, \infty\}$ and set $\eta = \eta_{U \circ A_1} + \eta_{U \circ A_2} + \eta_{U \circ A_3} + \eta_{U \circ A_4}$. Since $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$ we have $\eta \in \mathbb{Z}^{2g}$. We set $a_i = \eta_{U \circ A_i}$ for $i = 1, 2, 3$ and $a_4 = \eta_{U \circ A_4} - \eta$, and apply the Frobenius identities (17) (with $z_i = 0$, $i = 1, \ldots, 4$). By the fundamental Vanishing Property (15) the identity reduces to

$$\begin{aligned} &-\varepsilon_U(i)\vartheta[a_1 + \eta_i]\vartheta[a_2 + \eta_i]\vartheta[a_3 + \eta_i]\vartheta[a_4 + \eta_i] \\ &\quad = \varepsilon_U(j)\vartheta[a_1 + \eta_j]\vartheta[a_2 + \eta_j]\vartheta[a_3 + \eta_j]\vartheta[a_4 + \eta_j]. \end{aligned}$$

Note that by equation (8), $\vartheta[\eta_{A_1}+\eta_{A_2}] = (-1)^{4\,{}^t\eta'_{A_1\circ A_2}\,\eta''_{A_1\cap A_2}}\vartheta[\eta_{A_1\circ A_2}]$ also, $\varepsilon_U(k) = -e_*(\eta_k)$, so that we get the required equation up to the sign:

$$\begin{aligned}
&-\varepsilon_U(i)\varepsilon_U(j)(-1)^{4\,{}^t(\,\eta_{U\circ V}+\eta_{U\circ V'}+\eta_k)'(\eta_i+\eta_j)''}(-1)^{2\,{}^t(\,\eta_{U\circ V'\circ\{i,k\}}+\eta_{U\circ V'\circ\{j,k\}})'\eta''}\\
&\quad = -e_*(\eta_i)e_*(\eta_j)(-1)^{4\,{}^t(\,\eta_{U\circ V}+\eta_{U\circ V'}+\eta_k)'(\eta_i+\eta_j)''}\\
&\qquad\quad \cdot(-1)^{4\,{}^t(\,\eta_i+\eta_j)'(\eta_{U\circ V}+\eta_{U\circ V'}+\eta_i+\eta_j+\eta_k)''}\\
&\quad = -e_2(i,j)e_2(\{i,j\},V\circ V'\circ\{k,\infty\})\\
&\quad = 1.
\end{aligned}$$

□

We now state a theorem from Mumford [Mum84, Thm IIIa.7.6] of which we will now only use a small part. We state it in full here, although we will only see the real use for it later. Recall that $\mathbf{U}$ is one of the polynomials associated to the divisor D, used to define the variety structure on Z.

Theorem 1. *For any finite branch point a_k, $k \in B - \{\infty\}$ and any $V \subset B$ such that $\#(V) = g+1$, $k \in V$ and $\infty \notin V$,*

$$\mathbf{U}(a_k) = \pm\prod_{\substack{i\in V\\ i\neq k}}(a_k-a_i)\cdot\left(\frac{\vartheta[\eta_{U\circ V}+\eta_k]\theta[\eta_U+\eta_k](z)}{\vartheta[\eta_{U\circ V}]\theta[\eta_U](z)}\right)^2$$

where $z = \mathrm{Int}(D)$ and the sign is given by -1 to the power

$$4\,{}^t\eta'_U\,\eta''_k + 4\,{}^t\eta''_{U\circ V}\,\eta'_k.$$

Here and for the rest of the paper an explicit multiplication sign, $\cdot$, will denote the end of the scope of a $\prod$ sign.

Note that immediately from this theorem, for V and V' with $\#(V) = \#(V') = g+1$ and $k \in V\cap V'$, $\infty\notin V$, $\infty\notin V'$,

$$\pm\prod_{\substack{i\in V\\ i\neq k}}(a_k-a_i)\cdot\vartheta[\eta_{U\circ V}+\eta_k]^2\vartheta[\eta_{U\circ V'}]^2 = \prod_{\substack{i\in V'\\ i\neq k}}(a_k-a_i)\cdot\vartheta[\eta_{U\circ V'}+\eta_k]^2\vartheta[\eta_{U\circ V}]^2$$

where the sign is given by

$$(-1)^{4\,{}^t(\,\eta''_V-\eta''_{V'})\eta'_k}.$$

Following [Gra85], but changing the sign, we make the following definition.

Definition 1.

$$\langle a_i-a_j\rangle = (-1)^{4\,{}^t\eta''_i\,\eta'_j}(a_j-a_i) = \begin{cases} a_j-a_i & \text{if } i<j,\\ a_i-a_j & \text{if } j<i.\end{cases} \tag{18}$$

The second equality can easily be checked from the definition of the η_i.

We obtain

$$\prod_{\substack{i\in V\\ i\neq k}}\langle a_k-a_i\rangle\cdot\vartheta[\eta_{U\circ V}+\eta_k]^2\vartheta[\eta_{U\circ V'}]^2 = \prod_{\substack{i\in V'\\ i\neq k}}\langle a_k-a_i\rangle\cdot\vartheta[\eta_{U\circ V'}+\eta_k]^2\vartheta[\eta_{U\circ V}]^2. \tag{19}$$

In particular, for V such that $\#(V) = g+1$, $i,j \in V$ and $\infty, k \notin V$, we have

$$\frac{\langle a_k - a_j\rangle}{\langle a_k - a_i\rangle} = \frac{\vartheta[\eta_{U\circ V\circ\{j,\infty\}}]^2\vartheta[\eta_{U\circ V\circ\{i,k\}}]^2}{\vartheta[\eta_{U\circ V\circ\{i,\infty\}}]^2\vartheta[\eta_{U\circ V\circ\{j,k\}}]^2}. \tag{20}$$

We now want to pick 'compatible' square roots for $\langle a_i - a_j\rangle$.

Definition 2. Fix a square root for $\langle a_1 - a_2\rangle$ and for any V such that $\#(V) = g+1$, $j, 2 \in V$ and $1, \infty \notin V$ define

$$\sqrt{\langle a_1 - a_j\rangle} = \sqrt{\langle a_1 - a_2\rangle}\frac{\vartheta[\eta_{U\circ V\circ\{j,\infty\}}]\vartheta[\eta_{U\circ V\circ\{1,2\}}]}{\vartheta[\eta_{U\circ V\circ\{2,\infty\}}]\vartheta[\eta_{U\circ V\circ\{1,j\}}]}. \tag{21}$$

For any V such that $\#(V) = g+1$, $1, i \in V$ and $\infty, j \notin V$ define

$$\sqrt{\langle a_j - a_i\rangle} = \sqrt{\langle a_j - a_1\rangle}\frac{\vartheta[\eta_{U\circ V\circ\{i,\infty\}}]\vartheta[\eta_{U\circ V\circ\{1,j\}}]}{\vartheta[\eta_{U\circ V\circ\{1,\infty\}}]\vartheta[\eta_{U\circ V\circ\{i,j\}}]}. \tag{22}$$

Lemma 1 and (20) show that this definition is well-defined and meaningful.

With this definition we can now prove some identities which are usually only stated without the square roots. For instance the final corollary in this section is a generalization of Thomae's identity. First let's generalize (20): For V such that $\#(V) = g+1$, $i,j \in V$ and $\infty, k \notin V$ we have

$$\frac{\sqrt{\langle a_k - a_j\rangle}}{\sqrt{\langle a_k - a_i\rangle}} = \frac{\vartheta[\eta_{U\circ V\circ\{j,\infty\}}]\vartheta[\eta_{U\circ V\circ\{i,k\}}]}{\vartheta[\eta_{U\circ V\circ\{i,\infty\}}]\vartheta[\eta_{U\circ V\circ\{j,k\}}]}. \tag{23}$$

To see this, note that if V is such that $\#(V) = g+1$, $1, i, j \in V$ and $\infty, k \notin V$, then from the definition we obtain

$$\begin{aligned}\frac{\sqrt{\langle a_k - a_j\rangle}}{\sqrt{\langle a_k - a_i\rangle}} &= \frac{\sqrt{\langle a_k - a_j\rangle}}{\sqrt{\langle a_k - a_1\rangle}}\frac{\sqrt{\langle a_k - a_1\rangle}}{\sqrt{\langle a_k - a_i\rangle}} \\ &= \frac{\vartheta[\eta_{U\circ V\circ\{j,\infty\}}]\vartheta[\eta_{U\circ V\circ\{1,k\}}]}{\vartheta[\eta_{U\circ V\circ\{1,\infty\}}]\vartheta[\eta_{U\circ V\circ\{j,k\}}]}\frac{\vartheta[\eta_{U\circ V\circ\{1,\infty\}}]\vartheta[\eta_{U\circ V\circ\{i,k\}}]}{\vartheta[\eta_{U\circ V\circ\{i,\infty\}}]\vartheta[\eta_{U\circ V\circ\{1,k\}}]} \\ &= \frac{\vartheta[\eta_{U\circ V\circ\{j,\infty\}}]\vartheta[\eta_{U\circ V\circ\{i,k\}}]}{\vartheta[\eta_{U\circ V\circ\{i,\infty\}}]\vartheta[\eta_{U\circ V\circ\{j,k\}}]}.\end{aligned}$$

Now use Lemma 1 to see that this holds for any V, even if $1 \notin V$. Next we generalize (19).

Lemma 2. *For V and V', subsets of B, with $\#(V) = \#(V') = g+1$ and $k \in V'$, $k \notin V$, $\infty \notin V'$, $\infty \in V$,*

$$\prod_{\substack{i\in V\\ i\neq\infty}} \sqrt{\langle a_k - a_i\rangle}\cdot\vartheta[\eta_{U\circ V}]\vartheta[\eta_{U\circ V'}] = \prod_{\substack{i\in V'\\ i\neq k}} \sqrt{\langle a_k - a_i\rangle}\cdot\vartheta[\eta_{U\circ V\circ\{k,\infty\}}]\vartheta[\eta_{U\circ V'\circ\{k,\infty\}}].$$

Proof. We will use induction on $\#(V - V') = \#(V' - V)$. The base case is when $V' = V\circ\{k,\infty\}$, in which case the identity holds trivially. Otherwise note that if $j \in V - V'$, $j \neq \infty$, $j' \in V' - V$, $j' \neq k$, then by the induction hypothesis

$$\begin{aligned}&\prod_{\substack{i\in V\circ\{j,j'\}\\ i\neq\infty}} \sqrt{\langle a_k - a_i\rangle}\cdot\vartheta[\eta_{U\circ V\circ\{j,j'\}}]\vartheta[\eta_{U\circ V'}] \\ &\quad= \prod_{\substack{i\in V'\\ i\neq k}} \sqrt{\langle a_k - a_i\rangle}\cdot\vartheta[\eta_{U\circ V\circ\{j,j',k,\infty\}}]\vartheta[\eta_{U\circ V'\circ\{k,\infty\}}].\end{aligned}$$

Now let $V = V \circ \{j', \infty\}$ and $i = j'$ in (23) to get

$$\frac{\sqrt{\langle a_k - a_j\rangle}}{\sqrt{\langle a_k - a_{j'}\rangle}} \frac{\vartheta[\eta_{U\circ V}]}{\vartheta[\eta_{U\circ V\circ\{j,j'\}}]} = \frac{\vartheta[\eta_{U\circ V\circ\{k,\infty\}}]}{\vartheta[\eta_{U\circ V\circ\{j,j',k,\infty\}}]}.$$

Multiplying these two expressions gives the required equation. □

Theorem 2. *Let $V, V' \subseteq B$ with $\#(V) = \#(V') = g+1$, $\infty \in V$, $\infty \notin V'$, $C \subseteq V - V'$ and $C' \subseteq V' - V$ with $\#(C) = \#(C')$. Set $W = V - V'$, $W' = V' - V$. Then*

$$\prod_{\substack{i\in W-C\\ k\in C'}} \sqrt{\langle a_k - a_i\rangle} \cdot \prod_{\substack{i\in W'-C'\\ k\in C}} \sqrt{\langle a_k - a_i\rangle} \cdot \vartheta[\eta_{U\circ V}]\vartheta[\eta_{U\circ V'}]$$
$$= \prod_{\substack{i\in W-C\\ k\in C}} \sqrt{\langle a_k - a_i\rangle} \cdot \prod_{\substack{i\in W'-C'\\ k\in C'}} \sqrt{\langle a_k - a_i\rangle} \cdot \vartheta[\eta_{U\circ V\circ(C\cup C')}]\vartheta[\eta_{U\circ V'\circ(C\cup C')}],$$

where we are using the convention $\langle a_\infty - a_i\rangle = \langle a_k - a_\infty\rangle = 1$.

Proof. We will prove this by induction on the number of non-infinity elements in $C \cup C'$. The base case is just $C = C' = \emptyset$, in which case the identity holds trivially. To do the induction step we will consider two cases: $\infty \notin C$ and $\infty \in C$.

The case $\infty \notin C$. For any $k \in C$ Lemma 2, with $V = V \circ (C \cup C')$ and $V' = V' \circ (C \cup C')$, gives

$$\frac{\prod_{\substack{i\in V'\circ(C\cup C')\\ i\neq k}} \sqrt{\langle a_k - a_i\rangle}}{\prod_{\substack{i\in V\circ(C\cup C')\\ i\neq\infty}} \sqrt{\langle a_k - a_i\rangle}} = \frac{\vartheta[\eta_{U\circ V\circ(C\cup C')}]\vartheta[\eta_{U\circ V'\circ(C\cup C')}]}{\vartheta[\eta_{U\circ V\circ(C\cup C')\circ\{k,\infty\}}]\vartheta[\eta_{U\circ V'\circ(C\cup C')\circ\{k,\infty\}}]},$$

which we can rewrite as

$$\frac{\prod_{i\in W'\circ((C\circ\{k,\infty\})\cup C')} \sqrt{\langle a_k - a_i\rangle}}{\prod_{i\in W\circ(C\cup C')} \sqrt{\langle a_k - a_i\rangle}} = \frac{\vartheta[\eta_{U\circ V\circ(C\cup C')}]\vartheta[\eta_{U\circ V'\circ(C\cup C')}]}{\vartheta[\eta_{U\circ V\circ((C\circ\{k,\infty\})\cup C')}]\vartheta[\eta_{U\circ V'\circ((C\circ\{k,\infty\})\cup C')}]}.$$

By the induction hypothesis we have

$$\prod_{\substack{i\in W-(C\circ\{k,\infty\})\\ j\in C'}} \sqrt{\langle a_j - a_i\rangle} \cdot \prod_{\substack{i\in W'-C'\\ j\in C\circ\{k,\infty\}}} \sqrt{\langle a_j - a_i\rangle} \cdot \vartheta[\eta_{U\circ V}]\vartheta[\eta_{U\circ V'}]$$
$$= \prod_{\substack{i\in W-(C\circ\{k,\infty\})\\ j\in C\circ\{k,\infty\}}} \sqrt{\langle a_j - a_i\rangle} \cdot \prod_{\substack{i\in W'-C'\\ j\in C'}} \sqrt{\langle a_j - a_i\rangle}$$
$$\cdot \vartheta[\eta_{U\circ V\circ((C\circ\{k,\infty\})\cup C')}]\vartheta[\eta_{U\circ V'\circ((C\circ\{k,\infty\})\cup C')}].$$

Multiplying by the previous equation and simplifying the product terms, we complete this case.

The case $\infty \in C$. For any $k \in C'$ Lemma 2, with $V = V' \circ (C \cup C')$ and $V' = V \circ (C \cup C')$, gives

$$\frac{\prod_{\substack{i\in V\circ(C\cup C')\\ i\neq k}} \sqrt{\langle a_k - a_i\rangle}}{\prod_{\substack{i\in V'\circ(C\cup C')\\ i\neq\infty}} \sqrt{\langle a_k - a_i\rangle}} = \frac{\vartheta[\eta_{U\circ V\circ(C\cup C')}]\vartheta[\eta_{U\circ V'\circ(C\cup C')}]}{\vartheta[\eta_{U\circ V\circ(C\cup C')\circ\{k,\infty\}}]\vartheta[\eta_{U\circ V'\circ(C\cup C')\circ\{k,\infty\}}]},$$

and again we can can rewrite this as

$$\frac{\prod_{i\in W\circ(C\cup(C'-k))}\sqrt{\langle a_k-a_i\rangle}}{\prod_{i\in W'\circ(C\cup C')}\sqrt{\langle a_k-a_i\rangle}}=\frac{\vartheta[\eta_{U\circ V\circ(C\cup C')}]\vartheta[\eta_{U\circ V'\circ(C\cup C')}]}{\vartheta[\eta_{U\circ V\circ((C-\infty)\cup(C'-k))}]\vartheta[\eta_{U\circ V'\circ((C-\infty)\cup(C'-k))}]}.$$

By the induction hypothesis we have

$$\begin{aligned}&\prod_{\substack{i\in W-C\\ j\in C'-k}}\sqrt{\langle a_j-a_i\rangle}\cdot\prod_{\substack{i\in W'-(C'-k)\\ j\in C}}\sqrt{\langle a_j-a_i\rangle}\cdot\vartheta[\eta_{U\circ V}]\vartheta[\eta_{U\circ V'}]\\ &\quad=\prod_{\substack{i\in W-C\\ j\in C}}\sqrt{\langle a_j-a_i\rangle}\cdot\prod_{\substack{i\in W'-(C'-k)\\ j\in C'-k}}\sqrt{\langle a_j-a_i\rangle}\\ &\qquad\cdot\vartheta[\eta_{U\circ V\circ((C-\infty)\cup(C'-k))}]\vartheta[\eta_{U\circ V'\circ((C-\infty)\cup(C'-k))}].\end{aligned}$$

Again the product of the last two expressions simplifies to the required identity. □

The next corollary will be used frequently and is the inspiration for the definition of f_A in the next chapter.

Corollary 1. *For sets A_1 and A_2 such that $\#(A_1)=\#(A_2)=g+1$,*

$$\begin{aligned}(-1)^{2^t\eta'_{A_1\circ A_2}\eta''_B}&\prod_{\substack{i\in A_1\cap A_2\\ k\in A_2-A_1}}\sqrt{\langle a_k-a_i\rangle}\cdot\prod_{\substack{i\in A_1^c\cap A_2^c\\ k\in A_1-A_2}}\sqrt{\langle a_k-a_i\rangle}\cdot\vartheta[\eta_{U\circ A_1}]^2\\ &=\prod_{\substack{i\in A_1\cap A_2\\ k\in A_1-A_2}}\sqrt{\langle a_k-a_i\rangle}\cdot\prod_{\substack{i\in A_1^c\cap A_2^c\\ k\in A_2-A_1}}\sqrt{\langle a_k-a_i\rangle}\cdot\vartheta[\eta_{U\circ A_2}]^2.\end{aligned}$$

Proof. First note that the identity does not change if we replace A_1 by its complement. So we can assume $\infty\in A_1$ and then apply the theorem with $V=A_1$, $V'=A_1^c$, $C=A_1-A_2$ and $C'=A_2-A_1$. All that remains is to find the sign relating $\vartheta[\eta_{U\circ A^c}]$ to $\vartheta[\eta_{U\circ A}]$, for $A=A_1$ and A_2. Note that $U\circ A^c=(U\circ A)^c$ and from (8) it therefore follows that

$$\vartheta[\eta_{U\circ A^c}]=(-1)^{2^t\eta'_{U\circ A}(\eta_B-2\eta_{U\circ A})''}\vartheta[\eta_{U\circ A}].$$

Finally, if $\#A=g+1$ then from (12) we see that the $(-1)^{4^t\eta'_{U\circ A}\eta''_{U\circ A}}$ term drops out. □

6. Definition of the embedding

We now define the functions t_A, and then show that if we use them to embed the torus associated to $J(\mathbb{C})$ into projective space, the image variety is defined over the field generated by $\mathbb{Q}$ and the roots a_i of the hyperelliptic equation.

Definition 3. For any subset A of B such that $\#(A)\equiv g+1 \bmod 2$, let $t_A=f_A\theta[\eta_{A\circ U}](z)$ where

$$f_A=\frac{\prod_{\substack{i\in A\cap U\\ k\in U-A}}\sqrt{\langle a_k-a_i\rangle}\cdot\prod_{\substack{i\in A^c\cap U^c\\ k\in A-U}}\sqrt{\langle a_k-a_i\rangle}}{\prod_{\substack{i\in(A\circ C)\cap(U\circ C)\\ k\in(U\circ C)-(A\circ C)}}\sqrt{\langle a_k-a_i\rangle}\cdot\prod_{\substack{i\in(A\circ C)^c\cap(U\circ C)^c\\ k\in(A\circ C)-(U\circ C)}}\sqrt{\langle a_k-a_i\rangle}}\frac{\vartheta[\eta_{U\circ U\circ C}]}{\vartheta[\eta_{U\circ A\circ C}]},$$

and C is chosen as follows:

1. If $\#(A)\le g+1$ let $g+1-\#(A)=2n$. Pick sets $C'_U\subseteq(A\cup U)^c$ with $\#(C'_U)=n$ and $C_U\subseteq U-A$ with $\#(C_U)=n$.

2. If $\#(A) > g+1$ let $\#(A) - (g+1) = 2n$. Pick sets $C'_U \subseteq A - U$ with $\#(C'_U) = n$ and $C_U \subseteq U \cap A$ with $\#(C_U) = n$.
3. In either case set $C = C_U \cup C'_U$ and note that $\#(A \circ C) = \#(U \circ C) = g+1$ (so that the theta-constants in the definition are non-zero).

We will now show that only the sign of f_A depends on the choice of C. First, for *any* A contained in B, define

$$f'_A = \exp(\pi i\, {}^t\eta'_{U\circ A}\,\eta''_B)\frac{\sqrt{\prod_{\substack{i\in A\cap U\\ k\in U-A}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in A^c\cap U^c\\ k\in A-U}}\sqrt{\langle a_k - a_i\rangle}}}{\sqrt{\prod_{\substack{i\in A\cap U\\ k\in A-U}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in A^c\cap U^c\\ k\in U-A}}\sqrt{\langle a_k - a_i\rangle}}}$$

where we can pick either square root. Note that by Corollary 1, for A and C as in Definition 3

$$\begin{aligned}
&\frac{\vartheta[\eta_{U\circ U\circ C}]}{\vartheta[\eta_{U\circ A\circ C}]}\\
&\quad = \pm e^{\pi i\, {}^t\eta'_{U\circ A}\,\eta''_B}\frac{\sqrt{\prod_{\substack{i\in (U\circ C)\cap(A\circ C)\\ k\in (U\circ C)-(A\circ C)}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in (U\circ C)^c\cap(A\circ C)^c\\ k\in (A\circ C)-(U\circ C)}}\sqrt{\langle a_k - a_i\rangle}}}{\sqrt{\prod_{\substack{i\in (U\circ C)\cap(A\circ C)\\ k\in (A\circ C)-(U\circ C)}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in (U\circ C)^c\cap(A\circ C)^c\\ k\in (U\circ C)-(A\circ C)}}\sqrt{\langle a_k - a_i\rangle}}}\\
&\quad = \pm e^{\pi i\, {}^t\eta'_{U\circ A}\,\eta''_B}\frac{\prod_{\substack{i\in (U\circ C)\cap(A\circ C)\\ k\in (U\circ C)-(A\circ C)}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in (U\circ C)^c\cap(A\circ C)^c\\ k\in (A\circ C)-(U\circ C)}}\sqrt{\langle a_k - a_i\rangle}}{\sqrt{\prod_{\substack{i\in (U\circ A)^c\\ k\in U\circ A}}\sqrt{\langle a_k - a_i\rangle}}}.
\end{aligned}$$

Substituting this into f_A, we get

$$\begin{aligned}
f_A &= \pm e^{\pi i\, {}^t\eta'_{U\circ A}\,\eta''_B}\frac{\prod_{\substack{i\in A\cap U\\ k\in U-A}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in A^c\cap U^c\\ k\in A-U}}\sqrt{\langle a_k - a_i\rangle}}{\sqrt{\prod_{\substack{i\in (U\circ A)^c\\ k\in U\circ A}}\sqrt{\langle a_k - a_i\rangle}}}\\
&= \pm e^{\pi i\, {}^t\eta'_{U\circ A}\,\eta''_B}\frac{\sqrt{\prod_{\substack{i\in A\cap U\\ k\in U-A}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in A^c\cap U^c\\ k\in A-U}}\sqrt{\langle a_k - a_i\rangle}}}{\sqrt{\prod_{\substack{i\in A\cap U\\ k\in A-U}}\sqrt{\langle a_k - a_i\rangle}\cdot\prod_{\substack{i\in A^c\cap U^c\\ k\in U-A}}\sqrt{\langle a_k - a_i\rangle}}}\\
&= \pm f'_A.
\end{aligned}$$

As we wanted, this shows that only the sign of f_A depends on the choice of C.

We should point out here that the functions t_A are generalizations of the functions t_{e_i} and $t_{e_{ij}}$ defined in [GG93] for the genus 2 case. It can be shown that $t_{e_i}(z) = \pm t_{\{i,\infty\}}(2z)/t_\emptyset(2z)$ and $t_{e_{ij}}(z) = \pm t_{\{i,j\}}(2z)/t_\emptyset(2z)$; see our Theorems 4 and 5 and the definitions of t_{e_i} and $t_{e_{ij}}$.

From now on we will denote $\mathbb{Q}(a_1, a_2, ..., a_{2g+1})$ by F. The next lemma will be used several times to show that things are defined over F.

Lemma 3. *For any A_1, A_2, A_3, A_4 and D subsets of B such that $A_1 \circ A_2 \circ A_3 \circ A_4 = \emptyset$,*

$$\frac{f'_{A_1}f'_{A_2}f'_{A_3}f'_{A_4}}{f'_{A_1\circ D}f'_{A_2\circ D}f'_{A_3\circ D}f'_{A_4\circ D}} \in F.$$

Proof. It's easy to see that the exponential terms contribute at most a sign. Indeed, we just use the identity $e^{\pi i({}^t\eta'_A\,\eta''_B \pm {}^t\eta'_{A'}\,\eta''_B)} = \pm e^{\pi i\,{}^t\eta'_{A\circ A'}\,\eta''_B}$ repeatedly.

It remains to show that each $\langle a_k - a_j\rangle$ occurs to an integer power. Let $p_{jk}(U,A)$ denote the number of times $\langle a_j - a_k\rangle$ occurs in

$$\prod_{\substack{i\in A\cap U\\ l\in U-A}} \langle a_i - a_l\rangle.$$

So $p_{jk}(U,A)$ is zero unless j is in U *and* k is in U *and* precisely one of j and k is in A, in which case the answer is 1. If 1 corresponds to true and 0 to false, then *and* corresponds to multiplication, so

$$p_{jk}(U,A) = \left(\frac{1-(-1)^{\delta_j(U)}}{2}\right)\left(\frac{1-(-1)^{\delta_k(U)}}{2}\right)\left(\frac{1-(-1)^{\delta_j(U)+\delta_k(A)}}{2}\right),$$

where, for any $A \subset B$,

$$\delta_j(A) = \begin{cases} 1 & \text{if } j \in A,\\ 0 & \text{if } j \notin A.\end{cases}$$

Now let $p_{jk}(A)$ be the power of $\langle a_k - a_j\rangle$ occurring in ${f'_A}^4$ and note that

$$p_{jk}(A) = p_{jk}(U,A) + p_{jk}(U^c,A^c) - p_{jk}(A,U) - p_{jk}(A^c,U^c).$$

Using $\delta_j(A^c) = 1 - \delta_j(A)$, we can simplify to get

$$p_{jk}(A) = \frac{1}{2}((-1)^{\delta_j(U)+\delta_k(U)} - (-1)^{\delta_j(A)+\delta_k(A)}),$$

It will be sufficient to show that

$$\sum_{i=1}^4 p_{jk}(A_i) - \sum_{i=1}^4 p_{jk}(A_i\circ D) \equiv 0 \bmod 4$$

if $A_1\circ A_2\circ A_3\circ A_4 = \emptyset$. Since $(-1)^{\delta_j(A\circ D)} = (-1)^{\delta_j(A)+\delta_j(D)}$, we see that

(24)
$$\sum_{i=1}^4 p_{jk}(A_i) - \sum_{i=1}^4 p_{jk}(A_i\circ D) = \frac{(-1)^{\delta_j(D)+\delta_k(D)}-1}{2}\sum_{i=1}^4 (-1)^{\delta_j(A_i)+\delta_k(A_i)}.$$

As $A_1\circ A_2\circ A_3\circ A_4 = \emptyset$, we see that j and k are each in 0, 2 or 4 of the A_i. This implies that $\sum_{i=1}^4 \delta_j(A_i) + \delta_k(A_i)$ is even, or, equivalently, an even number of $\delta_j(A_i) + \delta_k(A_i)$ are equal to one. So $\sum_{i=1}^4 (-1)^{\delta_j(A_i)+\delta_k(A_i)} \equiv 0 \bmod 4$, which completes the proof. □

From the Riemann identities (11) and the fundamental Vanishing Property we can deduce the following (see [Mum84, Proof of Thm. IIIa.7.1]). For any A_1, A_2, A_3 and A_4 subsets of B such that $A_1\circ A_2\circ A_3\circ A_4 = \emptyset$,

$$\sum_{\substack{S\subset B-\{\infty\}\\ \#S \text{ even}}} s_j\theta[\eta_{U\circ A_1\circ S}](z)\theta[\eta_{U\circ A_2\circ S}](z)\vartheta[\eta_{U\circ A_3\circ S}]\vartheta[\eta_{U\circ A_4\circ S}] = 0, \tag{25}$$

where s_j is a sign.

Lemma 4. *If we substitute $f_A^{-1}t_A$ for $\theta[\eta_{U\circ A}]$ in the above identities we get quadratic identities in the t_A with coefficients in $F = \mathbb{Q}(a_1, a_2, ..., a_{2g+1})$.*

Proof. The general term in the sum is

$$f_{A_1\circ S}^{-1} f_{A_2\circ S}^{-1} \vartheta[\eta_{U\circ A_3\circ S}]\vartheta[\eta_{U\circ A_4\circ S}]t_{A_1\circ S}t_{A_2\circ S}.$$

If $\#(A) = g+1$, then, by Corollary 1, we can replace $\vartheta[\eta_{U\circ A}]$ by $\pm {f'_A}^{-1}\vartheta[0]$, so to prove the claim it is enough to show that

$$\frac{f'_{A_1\circ S}f'_{A_2\circ S}f'_{A_3\circ S}f'_{A_4\circ S}}{f'_{A_1\circ S'}f'_{A_2\circ S'}f'_{A_3\circ S'}f'_{A_4\circ S'}}$$

is in F. This follows from Lemma 3. □

For some ordering of $\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}$, define

$$\mathcal{F}(z) = (t_A(2z))_{\eta_{U\circ A}\in\frac{1}{2}\mathbb{Z}^{2g}/\mathbb{Z}^{2g}}.$$

Note that, as in (16), $\mathcal{F}$ is a well-defined map from $\mathbb{C}^g/(\tau, \mathbf{1})\mathbb{Z}^{2g}$ into projective space. Let's call the image variety T. Note that because the embedding $\mathcal{F}$ is just the map (16) with each coordinate multiplied by a constant, T is isomorphic to J over $\mathbb{C}$.

Theorem 3. *The variety T is defined over $F = \mathbb{Q}(a_1, a_2, \ldots, a_{2g+1})$.*

Proof. Theorem 7.5.2 in [LB92] shows that the equations defining T are generated by the quadratic Riemann relations (25). The previous lemma says that these have coordinates in F. □

7. The isomorphism

In this final section we will show that the variety T defined above is isomorphic to the Jacobian over the field F. We first need to write the $\mathbf{V}$ polynomial in terms of theta functions in the same way as Theorem 1 gives the $\mathbf{U}$ polynomial in terms of theta functions. In this case the expression is a bit more involved, and so we first define a function Y and show that at a_l and a_m it can be written in terms of theta functions in a very similar way to that of $\mathbf{U}$ at a_k. We can then write $\mathbf{V}$ at a_k in terms of the Y's. Having $\mathbf{U}$ and $\mathbf{V}$ in terms of theta functions with coefficients in F means that we have an injective rational map from T to J. The final theorem shows that from this we can deduce that T and J are isomorphic over F.

Let $D = \sum_{i=1}^g P_i$ be an effective divisor of degree g. Let $x_i = x(P_i)$ be the x-coordinate of the point P_i. Similarly let $y_i = y(P_i)$. Define

$$Y_{lm} = \sum_{i=1}^{g} -y_i \prod_{\substack{n=1\\ n\neq i}}^{g} \frac{(x_n - a_l)(x_n - a_m)}{x_i - x_n}.$$

Note that this function is symmetric in the P_i, and so we think of it as a function of effective divisors of degree g, or as a function on the Jacobian.

Theorem 4. *For $z = \sum_{i=1}^g \int_\infty^{P_i} \overline{\varphi}$,*

$$Y_{lm}(P_1, \ldots, P_g) = c_{lm}\frac{t_l(z)t_m(z)t_{lm}(z)}{t_\emptyset(z)^3}$$

for some constant c_{lm}.

Proof. Since t_S differs by a non-zero constant from $\theta[\eta_{U\circ S}](z)$ and $\theta[\eta_{U\circ S}](z)$ has a simple zero at $T_{\sum_{i\in S} a_i - \#(S)\infty}\Theta$, we see that

$$h = \frac{t_l(z)t_m(z)t_{lm}(z)}{t_\emptyset(z)^3}$$

has divisor

$$T_{a_l-\infty}\Theta + T_{a_m-\infty}\Theta + T_{a_l+a_m-2\infty}\Theta - 3\Theta.$$

Now Y_{lm} clearly vanishes on $T_{a_l-\infty}\Theta$ and $T_{a_m-\infty}\Theta$. Suppose we can show that it has a pole of order 3 at Θ and no other poles; then Y_{lm}/h will have a simple pole at

$$T_{a_l+a_m-2\infty}\Theta$$

and no other pole. The theorem would then follow because $\mathcal{L}(T_{a_l+a_m-2\infty}\Theta)$ (being isomorphic to $\mathcal{L}(\Theta)$) has dimension 1 by the Riemann-Roch Theorem on Abelian varieties ([Lan82, Thm 4.1]), and so Y_{lm}/h must be a constant.

Before showing that Y_{lm} has a pole of order 3 at Θ and no other poles, let's recall some facts about divisors and their pullbacks.

Let $\pi : C^g \to C^{(g)}$ be the natural projection from C^g, the product of C with itself g times, to $C^{(g)}$, the symmetric product. Since $C^{(g)}$ is gotten by modding out C^g by a finite group of automorphisms, π is a finite morphism (and hence proper), surjective and of degree $g!$. Recall from the introduction that the map $I : C^{(g)} \to J$ is a surjective birational map between projective varieties, and hence proper. So the composite $\phi : C^g \to J$ is a proper surjective morphism of degree $g!$. Since C^g and J are non-singular and of the same dimension, if D is a prime divisor on J, then $\phi^{-1}(D) = \bigcup_{i=1}^r D_i \cup \bigcup_{i=1}^s E_i$, where the D_i and E_i are irreducible divisors, $\phi(D_i)$ is dense in D, and $\phi(E_i)$ is not (see [Iit82, Sec. 2.15c]).

Furthermore

$$\phi^*(D) = \sum_{i=1}^r e_i D_i,$$

where

$$\sum_{i=1}^r e_i(\deg \phi|_{D_i}) = \deg \phi = g!$$

([Iit82, Thm. 2.28]). Also, by [Iit82, Prop. 2.15]

$$\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^*(f))$$

for any function f on J. Finally, if D is a divisor on V, $\pi : V \times W \to V$ is the projection and f is a function on V, then $\mathrm{ord}_{D\times W}\,\pi^* f = \mathrm{ord}_D\, f$.

We can now begin by proving that Y_{lm} is regular on J off Θ. Let Q be a point on $J - \Theta$. Then Q can be uniquely represented as $\sum_{i=1}^g P_i - g\infty$, with $P_i \neq \infty$ and $P_i \neq \overline{P_j}$ for $i \neq j$. Thus we see directly from the definition of Y_{lm} that if it is not regular at Q we must have $P_i = P_j$ for some $i \neq j$. So we need only show that Y_{lm} does not have a pole at the irreducible divisor $D = \{2P_1 + P_2 + \cdots + P_{g-1} - g\infty | P_i \in C\}$. Set $D' = \Delta \times \underbrace{C \times \cdots \times C}_{g-2}$, where Δ is the diagonal divisor in $C \times C$, and note that $D' \in \phi^{-1}(D)$ and $\phi(D')$ is dense in D. So it would be sufficient to show that

$\phi^*(Y_{lm})$ is regular on D'. But

$$\sum_{i=3}^{g} -y_i \prod_{\substack{n=1 \\ n\neq i}}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_i-x_n}$$

is regular on an open subset of D', hence has no pole on D'. So we need only check that

(26)

$$\begin{aligned}
&\sum_{i=1}^{2} y_i \prod_{\substack{n=1 \\ n\neq i}}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_i-x_n} \\
&= \left(\frac{y_1(x_2-a_l)(x_2-a_m) - y_2(x_1-a_l)(x_1-a_m)}{x_1-x_2} \right) \prod_{n=3}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_1-x_n} \\
&\quad + \frac{y_2(x_1-a_l)(x_1-a_m)}{x_2-x_1} \left(\prod_{n=3}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_2-x_n} - \prod_{n=3}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_1-x_n} \right)
\end{aligned}$$

has no pole on D'. First note that

$$\begin{aligned}
&\frac{y_1(x_2-a_l)(x_2-a_m) - y_2(x_1-a_l)(x_1-a_m)}{x_1-x_2} \\
&\quad = \frac{y_1^2(x_2-a_l)^2(x_2-a_m)^2 - y_2^2(x_1-a_l)^2(x_1-a_m)^2}{x_1-x_2} \\
&\qquad \cdot \frac{1}{y_1(x_2-a_l)(x_2-a_m) + y_2(x_1-a_l)(x_1-a_m)}.
\end{aligned}$$

By writing y_1^2 and y_2^2 in terms of x_1 and x_2 we see that the first term on the right is a polynomial in x_1 and x_2, and therefore this expression has no pole on Δ. Also, the term

$$\prod_{n=3}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_2-x_n} - \prod_{n=3}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_1-x_n}$$

is zero when $x_1 = x_2$ and is therefore divisible by $x_1 - x_2$. So both terms in (26) are regular on D'. So Y_{lm} has poles only at Θ.

It remains to show that Y_{lm} has a pole of order 3 at Θ. Note that $T_i = \underbrace{C \times \cdots \times C}_{i-1} \times \infty \times C \times \cdots \times C$ is a divisor on C^g such that $\phi(T_i)$ is dense in Θ. So

$$\phi^*(\Theta) = \sum_{i=1}^{g} e_i T_i + \sum_j f_j W_j, \ e_i \leq 1.$$

where W_j are other prime divisors on C^g such that $\phi(W_j)$ is dense in Θ. We have

$$\sum_{i=1}^{g} e_i (\deg \phi|_{T_i}) + \sum_j f_j (\deg \phi|_{W_j}) = \deg \phi = g!$$

But $\phi|_{T_i}$ is a map of order $(g-1)!$, so all $e_i = 1$, there are no W_j, and $\phi^*(\Theta) = \sum_{i=1}^{g} T_i$. So it suffices to show that $\phi^*(Y_{lm})$ has a pole of order 3 at T_1. Let

$2 \le i \le g$. We first claim that

$$y_i \prod_{\substack{n=1\\ n\neq i}}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_i-x_n} = \frac{(x_1-a_l)(x_1-a_m)}{x_i-x_1}\left(y_i \prod_{\substack{n=1\\ n\neq 1,i}}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_i-x_n}\right)$$

has a pole of order 2 at T_1. It suffices to show that $\frac{(x_1-a_l)(x_1-a_m)}{x_i-x_1}$ has a pole of order 2 at T_1, or that the same is true of each of x_1-a_l, x_1-a_m and x_i-x_1. But this follows because x has a pole of order 2 at ∞ on C and so x_1 has a pole of order 2 at T_1.

It remains to show that $y_1 \prod_{n=2}^{g} \frac{(x_n-a_l)(x_n-a_m)}{x_1-x_n}$ has a pole of order 3 at T_1, or from above that y_1 has a pole of order $2g+1$ at T_1. But this is true since y has a pole of order $2g+1$ at ∞ on C. □

Theorem 5. *For a finite branch point a_k, we have*

$$\mathbf{U}(a_k) = (-1)^g \frac{t_k^2}{t_\emptyset^2}.$$

Proof. By Theorem 1, for any $V \subset B$ such that $\#(V) = g+1$, $\infty \notin V$, $k \in V$,

$$\begin{aligned}
\mathbf{U}(a_k) &= (-1)^{4\,{}^t\eta'_U\,\eta''_k}(-1)^{4\,{}^t\eta'_k\,\eta''_{U\circ V}} \\
&\quad \cdot \prod_{\substack{i\in V\\ i\neq k}}(a_k-a_i)\cdot\left(\frac{\theta[\eta_{U\circ\{k,\infty\}}](z)\vartheta[\eta_{U\circ V\circ\{k,\infty\}}]}{\theta[\eta_U](z)\vartheta[\eta_{U\circ V}]}\right)^2 \\
&= (-1)^{4({}^t\eta'_U\,\eta''_k+{}^t\eta'_k\,\eta''_U)}(-1)^{4\,{}^t\eta'_k\,\eta''_k} \\
&\quad \cdot \prod_{\substack{i\in V\\ i\neq k}}(-1)^{4\,{}^t\eta'_k\,\eta''_i}(a_k-a_i)\cdot\frac{t_k^2}{t_\emptyset^2}\left(\frac{f'_\emptyset f'_V}{f'_{\{k,\infty\}}f'_{V\circ\{k,\infty\}}}\right)^2
\end{aligned}$$

By (14) we see that

$$(-1)^{4({}^t\eta'_U\,\eta''_k+{}^t\eta'_k\,\eta''_U)} = \left.\begin{cases}(-1)^{\#(U\cap\{k,\infty\})} & \text{if } \#(U) \text{ is even}\\ (-1)^{\#((U\cup\infty)\cap\{k,\infty\})} & \text{if } \#(U) \text{ is odd}\end{cases}\right\} = (-1)^g\varepsilon_U(k).$$

Also, from the definition of η_k, $(-1)^{4\,{}^t\eta'_k\,\eta''_k} = \varepsilon_U(k)$. By Definition 1,

$$(-1)^{4\,{}^t\eta'_k\,\eta''_i}(a_k-a_i) = \langle a_k-a_i\rangle.$$

To simplify the f' term, first note that the exponential terms in the definition of f' cancel. To count the $\langle a_i-a_j\rangle$ terms we will use the function p_{ij} of Lemma 3. So we need to evaluate

$$2p_{ij}(\emptyset)+2p_{ij}(V)-2p_{ij}(\{k,\infty\})-2p_{ij}(V\circ\{k,\infty\}).$$

Note that by (24) this expression is zero if $i\neq k$ and $j\neq k$, for then $\delta_i(\{k,\infty\})+\delta_j(\{k,\infty\})=0$. It remains only to calculate

$$\begin{aligned}
&2p_{ik}(\emptyset)+2p_{ik}(V)-2p_{ik}(\{k,\infty\})-2p_{ik}(V\circ\{k,\infty\}) \\
&\quad = -(2+2(-1)^{\delta_i(V)+\delta_k(V)}) \\
&\quad = \begin{cases}-4 & \text{if } i\in V,\\ 0 & \text{if } i\notin V.\end{cases}
\end{aligned}$$

Thus we get

$$\left(\frac{f'_\emptyset f'_V}{f'_{\{k,\infty\}} f'_{V\circ\{k,\infty\}}}\right)^2 = (\prod_{\substack{i\in V\\ i\neq k}} \langle a_k - a_i\rangle)^{-1}.$$

Combining the above calculations, we get the desired equality. □

Theorem 6. *The c_{lm} of Theorem 4 are all 1 or -1.*

Proof. Squaring both sides of the statement of Theorem 4 and applying Theorem 5 twice, we get

$$\begin{aligned}\sum_i \prod_{j\neq l,m} (x_i - a_j)\cdot \prod_{\substack{n=1\\ n\neq i}}^{g} \frac{(x_n-a_l)(x_n-a_m)}{(x_i-x_n)^2}\\ -2\sum_{i<j}\frac{y_i y_j}{(x_i-x_j)^2}\prod_{\substack{n=1\\ n\neq i,j}}^{g}\frac{(x_n-a_l)(x_n-a_m)}{(x_i-x_n)(x_j-x_n)} = c_{lm}^2\frac{t_{lm}^2(z)}{t_\emptyset^2(z)}.\end{aligned} \tag{27}$$

We now want to evaluate this identity at a specific z. Pick a set $W\subset B-\{l,m,\infty\}$ with $\#W = g-1$ and let $T = B-(W\cup\{l,m,\infty\})$. Then letting $D = a_l+\sum_{i\in W} a_i - g\infty$ and $z = \mathrm{Int}(D)$, we find that the left side of (27) is

$$\prod_{j\neq l,m}(a_l-a_j)\cdot\prod_{n\in W}\frac{(a_n-a_l)(a_n-a_m)}{(a_l-a_n)^2} = \prod_{j\in T}(a_l-a_j)\cdot\prod_{j\in W}(a_m-a_j). \tag{28}$$

The right side of (27) becomes

$$c_{lm}^2\frac{f_{\{l,m\}}^2}{f_\emptyset^2}\left(\frac{\theta[\eta_{U\circ\{l,m\}}](\tau\eta'_{W\cup\{l\}}+\eta''_{W\cup\{l\}})}{\theta[\eta_U](\tau\eta'_{W\cup\{l\}}+\eta''_{W\cup\{l\}})}\right)^2. \tag{29}$$

Now rewrite the theta functions as theta-constants using (9). We get

$$\begin{aligned}c_{lm}^2\frac{f_{\{l,m\}}^2}{f_\emptyset^2}\frac{\vartheta[\eta_{U\circ(W\cup\{m\})}]^2}{\vartheta[\eta_{U\circ(W\cup\{l\})}]^2}e^{4\pi i\eta'_{W\cup\{l\}}\eta''_{\{l,m\}}}\\ = c_{lm}^2\left(\frac{f'_{\{l,m\}}f'_{W\cup\{l,\infty\}}}{f'_\emptyset f'_{W\cup\{m,\infty\}}}\right)^2 e^{4\pi i\eta'_{W\cup\{l\}}\eta''_{\{l,m\}}}.\end{aligned}$$

We want to evaluate the f' term. First note that the exponential terms in the definition of f' cancel. We will again use the function p_{ij} of Lemma 3 to count the $\langle a_i - a_j\rangle$ terms. So we need to evaluate

$$2p_{ij}(\{l,m\}) + 2p_{ij}(W\circ\{l,\infty\}) - 2p_{ij}(\emptyset) - 2p_{ij}(W\circ\{m,\infty\}).$$

By the same argument as in (24) this expression is zero unless $\#(\{i,j\}\cap\{l,m\}) = 1$. So assume first that $j = l$ and $i\neq m$ (so $i\neq l$ as well); then

$$\begin{aligned}&-\big(2p_{il}(\emptyset) + 2p_{il}(W\circ\{m,\infty\}) - 2p_{il}(\{l,m\}) - 2p_{il}(W\circ\{m,\infty\}\circ\{l,m\})\big)\\ &\quad = (2+2(-1)^{\delta_i(W\circ\{m,\infty\})+\delta_l(W\circ\{m,\infty\})})\\ &\quad = \begin{cases}0 & \text{if } i\in W\circ\{m,\infty\},\\ 4 & \text{if } i\notin W\circ\{m,\infty\},\end{cases}\end{aligned}$$

and for $j = m$ and $i \neq l$ (so $i \neq m$ as well),

$$\begin{aligned}
&-\big(2p_{im}(\emptyset) + 2p_{im}(W \circ \{m,\infty\}) - 2p_{im}(\{l,m\}) - 2p_{im}(W \circ \{m,\infty\} \circ \{l,m\})\big) \\
&\quad = (2 + 2(-1)^{\delta_i(W\circ\{m,\infty\})+\delta_m(W\circ\{m,\infty\})}) \\
&\quad = \begin{cases} 4 & \text{if } i \in W \circ \{m,\infty\}, \\ 0 & \text{if } i \notin W \circ \{m,\infty\}. \end{cases}
\end{aligned}$$

We have shown that

$$\begin{aligned}
\frac{(f'_{\{l,j\}} f'_{V\circ\{l,j\}})^2}{(f'_\emptyset f'_V)^2} &= \prod_{i\in W} \langle a_i - a_m\rangle \cdot \prod_{i\in T} \langle a_i - a_l\rangle \\
&= (-1)^{4\,{}^t\eta'_{W\cup\{l,m\}}\,\eta''_l + 4\,{}^t\eta'_W\,\eta''_m} \prod_{i\in T}(a_i - a_l) \cdot \prod_{i\in W}(a_i - a_m).
\end{aligned}$$

So the right side of (27) becomes

$$\begin{aligned}
&c_{lm}^2 (-1)^{4\,{}^t\eta'_{W\cup\{l\}}\,\eta''_{\{l,m\}}} (-1)^{4\,{}^t\eta'_{W\cup\{l,m\}}\,\eta''_l + 4\,{}^t\eta'_W\,\eta''_m} \prod_{i\in T}(a_i - a_l) \cdot \prod_{i\in W}(a_i - a_m) \\
&\quad = c_{lm}^2 (-1)^{4\,{}^t\eta'_m\,\eta''_l + {}^t\eta'_l\,\eta''_m} (-1)^{2g-1} \prod_{i\in T}(a_l - a_i) \cdot \prod_{i\in W}(a_m - a_i) \\
&\quad = c_{lm}^2 \prod_{i\in T}(a_l - a_i) \cdot \prod_{i\in W}(a_m - a_i).
\end{aligned}$$

So comparing with (28) we see that

$$c_{lm}^2 = 1. \quad \square$$

Theorem 7. *For a set $V \subset B$ such that $\#V = g$ and $l \notin V$,*

$$\mathbf{V}(a_l) = \sum_{j\in V} \frac{-Y_{lj}}{\prod_{i\in V-\{j\}}(a_j - a_i)}.$$

Proof. By the definition of Y_{lj}, on changing the order of summation we get

$$\sum_{j\in V} \frac{Y_{jl}}{\prod_{i\in V-\{j\}}(a_j - a_i)} = \sum_{n=1}^{g} \frac{-y_n \prod_{\substack{k=1\\k\neq n}}^{g}(x_k - a_l)}{\prod_{\substack{k=1\\k\neq n}}^{g}(x_n - x_k)} \sum_{j\in V} \frac{\prod_{\substack{k=1\\k\neq n}}^{g}(x_k - a_j)}{\prod_{i\in V-\{j\}}(a_j - a_i)}.$$

Let $s_m(n)$ be the m-th elementary symmetric function in the x_k for $k = 1,\dots,g$, $k \neq n$. So $s_1(n) = x_1 + x_2 + \cdots + \widehat{x_n} + \cdots + x_g$ and $s_{g-1}(n) = x_1 x_2 \cdots \widehat{x_n} \cdots x_g$. Then if we expand the numerator of the inner sum and rearrange the order of summation the inner sum becomes

(30)

$$(-1)^{g-1}\left(\sum_{j\in V} \frac{a_j^{g-1}}{\prod_{i\in V-\{j\}}(a_j - a_i)} + \sum_{m=1}^{g-1}(-1)^m s_m(n) \sum_{j\in V} \frac{a_j^{g-1-m}}{\prod_{i\in V-\{j\}}(a_j - a_i)}\right).$$

To simplify this expression we will show that for a non-negative integer $c \leq g-1$,

$$\sum_{j\in V} \frac{a_j^c}{\prod_{i\in V-\{j\}}(a_j - a_i)} = \begin{cases} 0 & \text{if } 0 \leq c \leq g-2, \\ 1 & \text{if } c = g-1. \end{cases} \tag{31}$$

Consider the following polynomial in w:

$$\sum_{j\in V}\frac{a_j^c\prod_{i\in V-\{j\}}(w-a_i)}{\prod_{i\in V-\{j\}}(a_j-a_i)}.$$

It has degree $g-1$ and it equals $a_{j_0}^c$ at $w=a_{j_0}$ for any $j_0\in V$. That is, this polynomial equals the polynomial w^c at g distinct points, and therefore it must be identically w^c. In particular, for $c<g-1$, the leading coefficient must be zero, and for $c=g-1$, the leading coefficient must be 1. This proves (31).

So we see that (30) simplifies to $(-1)^{g-1}$. By (2) we then get

$$\sum_{j\in V}\frac{Y_{jl}}{\prod_{i\in V-\{j\}}(a_j-a_i)}=\sum_{n=1}^{g}\frac{-y_n\prod_{\substack{k=1\\k\neq n}}^{g}(a_l-x_k)}{\prod_{\substack{k=1\\k\neq n}}^{g}(x_n-x_k)}=-\mathbf{V}(a_l).\quad\square$$

Theorem 8. *The coefficients of* $\mathbf{U}$ *and* $\mathbf{V}$ *are rational functions of the* $t_S(2z)$*'s with coefficients in* F*.*

Proof. We will show that for any finite branch point a_l we can write both $\mathbf{U}(a_l)$ and $\mathbf{V}(a_l)$ as rational functions of the $t_S(2z)$'s with coefficients in F. This will be enough to prove the theorem, because we can clearly recover the coefficients of $\mathbf{U}$ and $\mathbf{V}$ (over F) if we have the values of these polynomials at all the finite branch points.

Immediately from Riemann's theta formula (11) we find the following: For any $c_i\in\frac{1}{2}\mathbb{Z}^{2g}$ such that $\sum_{i=1}^4 c_i\in\mathbb{Z}^{2g}$ and with

$$\begin{aligned}
z_1'&=\frac{z_1+z_2+z_3+z_4}{2},\quad c_1'=\frac{c_1+c_2+c_3+c_4}{2},\\
z_2'&=\frac{z_1+z_2-z_3-z_4}{2},\quad c_2'=\frac{c_1+c_2-c_3-c_4}{2},\\
z_3'&=\frac{z_1-z_2+z_3-z_4}{2},\quad c_3'=\frac{c_1-c_2+c_3-c_4}{2},\\
z_4'&=\frac{z_1-z_2-z_3+z_4}{2},\quad c_4'=\frac{c_1-c_2-c_3+c_4}{2},
\end{aligned}$$

the following identity holds:

$$\begin{aligned}
&\theta[c_1'](z_1')\cdot\theta[c_2'](z_2')\cdot\theta[c_3'](z_3')\cdot\theta[c_4'](z_4')\\
&\quad=2^{-g}\sum_{\substack{S\subset B-\{\infty\}\\ \#(S)\text{ even}}}\pm\theta[c_1+\eta_S](z_1)\\
&\qquad\cdot\theta[c_2+\eta_S](z_2)\cdot\theta[c_3+\eta_S](z_3)\cdot\theta[c_4+\eta_S](z_4).
\end{aligned}\tag{32}$$

Note that if we set

$$\begin{aligned}
z_1&=2z,\quad & z_2&=0,\quad & z_3&=0,\quad & z_4&=0,\\
c_1&=\eta_U+\eta_l,\quad & c_2&=\eta_U+\eta_l,\quad & c_3&=\eta_U,\quad & c_4&=-\eta_U,
\end{aligned}$$

in (32), then we obtain $\theta[\eta_{U\circ\{l,\infty\}}](z)^2\theta[\eta_U](z)^2$ in terms of theta functions with half-integral characteristics evaluated at $2z$. If we replace $\theta[\eta_{U\circ A}]$ by $\pm t_A {f'_A}^{-1}$ and the non-zero $\vartheta[\eta_{U\circ A}]$ by ${f'_A}^{-1}\vartheta[0]$, then we have expressed $t_{\{l,\infty\}}(z)^2t_\emptyset(z)^2$ in terms of the $t_S(2z)$ with coefficients, ignoring the $2^{-g}\vartheta[0]^3$ for now, of the form

$$\frac{f'_{\{l,\infty\}}f'_{\{l,\infty\}}f'_\emptyset f'_\emptyset}{f'_{\{l,\infty\}\circ S}f'_{\{l,\infty\}\circ S}f'_S f'_S}.$$

By Lemma 3 these coefficients are in F. Similarly if we set

$$\begin{array}{cccc} z_1 = 2z, & z_2 = 0, & z_3 = 0, & z_4 = 0, \\ c_1 = \eta_U, & c_2 = \eta_U, & c_3 = \eta_U, & c_4 = -\eta_U, \end{array}$$

we obtain $t_\emptyset(z)^4$ in terms of the $t_S(2z)$. When dividing these two expressions the $2^{-g}\vartheta[0]^3$ terms cancel and we get $\mathbf{U}(a_l) = \pm t_l^2/t_\emptyset^2$ as a rational function of the $t_S(2z)$ with coefficients in F.

If we set

$$\begin{array}{cccc} z_1 = 2z, & z_2 = 0, & z_3 = 0, & z_4 = 0, \\ c_1 = \eta_U + \eta_l, & c_2 = \eta_U + \eta_m, & c_3 = \eta_U + \eta_l + \eta_m, & c_4 = -\eta_U, \end{array}$$

in (32) and replace theta functions and theta-constants by t's and f''s respectively, then we have expressed $t_{\{l,m\}}(z)t_{\{l,\infty\}}(z)t_{\{m,\infty\}}(z)t_\emptyset(z)$ in terms of the $t_S(2z)$ with coefficients of the form

$$\frac{f'_{\{l,m\}}f'_{\{l,\infty\}}f'_{\{m,\infty\}}f'_\emptyset}{f'_{\{l,m\}\circ S}f'_{\{l,\infty\}\circ S}f'_{\{m,\infty\}\circ S}f'_S}.$$

Again Lemma 3 says that these coefficients are in F. If we divide this by the expression for $t_\emptyset(z)^4$ in terms of the $t_S(2z)$, we get $Y_{lm} = \pm t_l(z)t_m(z)t_{lm}(z)/t_\emptyset(z)^3$ as a rational function of the $t_S(2z)$ with coefficients in F. As Theorem 7 shows that $\mathbf{V}(a_l)$ is a rational function of the Y_{lj} with coefficients in F, the proof is complete. □

Theorem 9. *The variety T is isomorphic to the Jacobian over F.*

Proof. We have already pointed out that J and T are isomorphic and that they are both defined over F. So we only need to show that there exists an isomorphism $\phi : J \to T$ defined over F. Let ϕ now be the isomorphism (of abelian varieties) from J to T which, as a rational map, is just the expression of the $t_A(2z)/t_\emptyset(2z)$ as rational functions in the coefficients of $\mathbf{U}$ and $\mathbf{V}$ (under the identification of $F(J)$ with $F(Z)$). By the previous theorem (Theorem 8) the inverse rational map ψ, obtained by writing the coefficients of $\mathbf{U}$ and $\mathbf{V}$ as rational functions in the $t_A(2z)/t_\emptyset(2z)$, is defined over F. So by uniqueness of inverses of morphisms we see that ψ is an isomorphism defined over F, and therefore, so is ϕ. □

References

[Fly90] E. V. Flynn. The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field. *Math. Proc. Cambridge Philos. Soc.*, 107:425–441, 1990. MR **91b:**14025

[GG93] D. M. Gordon and D. R. Grant. Computing the Mordell-Weil rank of Jacobians of curves of genus 2. *Trans. Amer. Math. Soc.*, 337:807–824, 1993. MR **93h:**11057

[Gra85] D. R. Grant. *Theta Functions and Division Points on Abelian Varieties of Dimension Two*. PhD thesis, MIT, 1985.

[Gra90] D. R. Grant. Formal groups in genus 2. *J. Reine Angew. Math.*, 411:96–121, 1990. MR **91m:**14045

[Har77] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, 1977. MR **57:**3116

[Iit82] Shigeru Iitaka. *Algebraic Geometry*. Springer-Verlag, 1982. MR **84j:**14001

[Lan82] S. Lang. *Introduction to Algebraic and Abelian Functions*. Springer-Verlag, 1982. MR **84m:**14032

[LB92] H. Lange and Ch. Birkenhake. *Complex Abelian Varieties*. Springer-Verlag, 1992. MR **94j:**14001

[Mil86a] J.S. Milne. Abelian varieties. In G. Cornell and J.H. Silverman, editors, *Arithmetic Geometry*. Springer-Verlag, 1986, pp. 103–150. MR **89b:**14029

[Mil86b] J.S. Milne. Jacobian varieties. In G. Cornell and J.H. Silverman, editors, *Arithmetic Geometry*. Springer-Verlag, 1986, pp. 167–212. MR **89b:**14029

[Mum83] D. Mumford. *Tata Lectures on Theta I*, volume 28 of *Progr. Math.* Birkhäuser, 1983. MR **85h:**14026

[Mum84] D. Mumford. *Tata Lectures on Theta II*, volume 43 of *Progr. Math.* Birkhäuser, 1984. MR **86b:**14017

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990. MR **91a:**11071

Department of Mathematics, University of California, San Diego, San Diego, California 92093

Current address: Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803-4918

E-mail address: wamelen@math.lsu.edu