

1 Preliminaries

Here X will denote a smooth curve of genus g (that is, isomorphic to its own Riemann Surface).

Rather than constantly talking about linear equivalence of divisors, we will always talk about line bundles. Recall that to a divisor D we may associate a line bundle Δ whose space of global sections $H^0(\Delta)$ is isomorphic to $L(D)$. We denote the dimension of $H^0(\Delta)$ by $h^0(\Delta)$. If $f \in M(X)$ then $D + \text{div}(f)$ also gives Δ . There is a group isomorphism between divisors up to linear equivalence under addition and line bundles up to isomorphism under tensor product \otimes . We denote the group of line bundles under tensor product by $\text{Pic}(X)$.

We can define the degree of a line bundle by the degree of any underlying divisor since principal divisors have degree zero.

Example 1.

The holomorphic 1-forms on X form a line bundle ω_X which we call *the* canonical bundle. The degree of this line bundle is $2g - 2$ (since the degree of *any* canonical divisor is $2g - 2$).

•

When we speak about the Jacobian $J(X)$, we talk about line bundles of degree zero. These form a group under tensor product and the identity is the trivial bundle \mathcal{O}_X .

Facts about $J(X)$ can be found in Mumford's Abelian Varieties [4], we will use these two facts:

1) The n -torsion in $J(X)$, that is, the line bundles L such that $L^{\otimes n} \cong \mathcal{O}_X$ is denoted $J(X)[n]$. Since it is n -torsion, it is a $\mathbf{Z}/n\mathbf{Z}$ module, and it is free of rank $2g$.

2) There is a canonical nondegenerate alternating bilinear pairing

$$e_n : J(X)[n] \times J(X)[n] \rightarrow \mu_n$$

(the n -th roots of unity). How this pairing is defined is not so important, we only note that there is a canonical one. Here nondegenerate means that if we fix $v \in J(X)[n]$ and find that $e_n(v, w) = 1$ for all $w \in J(X)[n]$ then $v \cong \mathcal{O}_X$. Equivalently, the map $J(X)[n] \rightarrow \text{Hom}(J(X)[n], \mathbf{Z}/n\mathbf{Z})$ by $v \mapsto e_n(v, \cdot)$ is an isomorphism.

Definition. If $\vartheta \in \text{Pic}(X)$ is such that $\vartheta^{\otimes 2} \cong \omega_X$, we say that ϑ is a theta characteristic on X . We furthermore say that it is odd or even according to $h^0(\vartheta)$.

Theorem. The set $TC(X)$ of theta characteristics on X is in bijection with $J(X)[2]$, the 2-torsion in the jacobian of X . More precisely, for each theta

characteristic ϑ on X , there is a bijective map of sets $\phi_\vartheta : TC(X) \rightarrow J(X)[2]$ where $\vartheta' \mapsto \vartheta' \otimes \vartheta^{-1}$.

Proof. Note first that we have a map of the prescribed sets. If ϑ' is any theta characteristic then $(\vartheta' \otimes \vartheta^{-1})^{\otimes 2} \cong \vartheta'^{\otimes 2} \otimes (\vartheta^{\otimes 2})^{-1} \cong \omega_X \otimes \omega_X^{-1} \cong \mathcal{O}_X$.

This map is onto because if $v \in J(X)[2]$ then $(v \otimes \vartheta)^{\otimes 2} \cong \mathcal{O}_X \otimes \omega_X \cong \omega_X$ and so $v \cong \phi_\vartheta(v \otimes \vartheta)$. Finally this map is 1 – 1 since it is just restriction of a translation map on $Pic(X)$ to $TC(X)$. □

Note that this is an entirely non-canonical bijection (i.e. it depends very explicitly on being given a theta characteristic), so it only allows us to discover information in the category of sets: for instance that there are $\#J(X)[2] = 2^{2g}$ theta characteristics on X . For better information, we need a better identification.

As we saw in class, the derivative of the Abel-Jacobi map $X \rightarrow J(X)$ is the canonical embedding $X \rightarrow \mathbb{P}^{g-1}$ and that the set W_{g-1} in $Pic^{g-1}(X)$ forms a divisor. We can use the map ϕ_ϑ to push W_{g-1} into $J(X)$ as a *symmetric theta divisor*. Combining these two viewpoints, an odd theta characteristic takes on the meaning of a hyperplane in \mathbb{P}^{g-1} bitangent to X . The geometric meaning of an even theta characteristic is more subtle, and Dolgachev's Topics in Classical Algebraic Geometry [1] is a suggested reference, as we will be concentrating on the algebra for the remainder of this note.

Moreover, symmetric divisors on *abelian varieties* such as the Jacobian can be associated to quadratic functions in a natural way. See Polishchuk [6] for more details on this.

2 Theta Characteristics and Quadratic Forms on $J(X)[2]$

Definition. Let V be a vector space over a field k . A quadratic form is a map $q : V \rightarrow k$ such that $q(cv) = c^2q(v)$ for any $c \in k$. Moreover, if we define the map $b_q : V \times V \rightarrow k$ by $b_q(v, w) = q(v + w) - q(v) - q(w)$, we require that b_q be bilinear.

Example 2. $q_\vartheta(v) = h^0(v \otimes \vartheta) + h^0(\vartheta) \pmod 2$ is a quadratic form on $J(X)[2]$. Scalar multiplication follows trivially because $q_\vartheta(0v) = h^0(\vartheta) + h^0(\vartheta) \equiv 0 = 0^2q(v) \pmod 2$ for all v and likewise for 1.

It is a deep deformation-theoretic result of Mumford that that

$$b_\vartheta(v, w) = h^0(v \otimes w \otimes \vartheta) + h^0(v \otimes \vartheta) + h^0(w \otimes \vartheta) + h^0(\vartheta) \pmod 2$$

is a bilinear form. Thus we have a quadratic form on the $\mathbf{Z}/2\mathbf{Z}$ vector space $J(X)[2]$. But much more is in fact true! •

Theorem (Mumford). *For all theta characteristics ϑ , we have the following relation between the Weil Pairing $e_2 : J(X)[2] \times J(X)[2] \rightarrow \mu_2$ and the bilinear form b_ϑ given by the equation*

$$e_2(v, w) = (-1)^{b_\vartheta(v, w)}.$$

For this reason we will hereon write $\langle \cdot, \cdot \rangle$ for $b_\vartheta(\cdot, \cdot)$.

We see that of particular interest to us will be determining what quadratic forms have the same bilinear form. So let us suppose that q, q' are quadratic forms such that $b_q = b_{q'} = B$, thus

$$q(v+w) - q(v) - q(w) = B(v, w) = q'(v+w) - q'(v) - q'(w).$$

This of course tells us that

$$\begin{aligned} (q - q')(v+w) &:= q(v+w) - q'(v+w) \\ &= q(v) - q'(v) + q(w) - q'(w) \\ &= (q - q')(v) + (q - q')(w). \end{aligned}$$

It's tempting to say this means that $q - q'$ is linear on V , but scalars pull out of $q - q'$ by squaring, as with any quadratic form. We do however say that such a form is *additive*. Hence, we say in general that q and q' have the same bilinear form if and only if their difference is additive.

If ϑ, ϑ' are two theta characteristics then $q_\vartheta(v) - q_{\vartheta'}(v) = a(v)$ for a function $a : J(X)[2] \rightarrow \mathbf{Z}/2\mathbf{Z}$ such that $a(v+w) = a(v) + a(w)$ and $a(cv) = c^2 a(v)$. However, if $c \in \mathbf{Z}/2\mathbf{Z}$, it is well known that $c^2 = c$. Thus a is actually a linear map, and so there exists some $\eta \in J(X)[2]$ such that $a(v) = \langle v, \eta \rangle$ for all $v \in J(X)[2]$.

But we know more. Since $q_\vartheta(v) = h^0(v \otimes \vartheta) + h^0(\vartheta)$, we have

$$\begin{aligned} q_{\vartheta'}(v) - q_\vartheta(v) &= h^0(v \otimes \vartheta') + h^0(\vartheta') + h^0(v \otimes \vartheta) + h^0(\vartheta) \\ &= h^0(v \otimes \vartheta' \otimes \vartheta^{-1} \otimes \vartheta) + h^0(\vartheta' \otimes \vartheta^{-1} \otimes \vartheta) + h^0(v \otimes \vartheta) + h^0(\vartheta) \\ &= h^0((v \otimes \vartheta' \otimes \vartheta^{-1}) \otimes \vartheta) + h^0((\vartheta' \otimes \vartheta^{-1}) \otimes \vartheta) + h^0(v \otimes \vartheta) + h^0(\vartheta) \\ &= \langle v, \vartheta' \otimes \vartheta^{-1} \rangle \end{aligned}$$

Note that we use the fact we showed earlier, that $\vartheta' \otimes \vartheta^{-1}$ is a 2-torsion point in $J(X)$. In fact, we see this respects the earlier bijection since $q_{\vartheta+v}(w) = q_\vartheta(w) + \langle w, v \rangle$. We can now prove the aim of this section.

Theorem. *The map $\vartheta \rightsquigarrow q_\vartheta$ is a canonical bijection between $TC(X)$ and the quadratic forms on $J(X)[2]$ whose bilinear form is $\langle \cdot, \cdot \rangle$*

Proof. The identification $\vartheta \rightsquigarrow q_\vartheta$ is injective because if $q_{\vartheta'} - q_\vartheta = \langle \cdot, \vartheta' \otimes \vartheta^{-1} \rangle$ were constantly zero then the non degeneracy condition would show that $\vartheta' \otimes \vartheta^{-1} \cong \mathcal{O}_X$. But this is of course equivalent to $\vartheta' \cong \vartheta$. Surjectivity then follows from the fact that $q - q' = \langle \cdot, \eta \rangle$ for some η in the $2g$ -dimensional vector space $J(X)[2]$. Thus we are embedding a $2g$ dimensional space into a $2g$ dimensional space, so $\vartheta \rightsquigarrow q_\vartheta$ is a surjection. \square

Now we use this identification to derive some facts about theta characteristics.

3 Intrinsic information about theta characteristics

Let us recall some facts about quadratic forms over a field k of characteristic 2. Let q be a quadratic form on a vector space V/k . And not yet assume the characteristic of k is 2.

We note that $b_q(v, v) = q(2v) - 2q(v) = 4q(v) - 2q(v) = 2q(v)$, so we can recover the quadratic form from its bilinear form precisely when the characteristic of k is not 2. In the case of characteristic 2, we note that for any quadratic form q , $b_q(v, v) = 0$ so it is *alternating* or *symplectic*.

Now we note that $\mathbf{Z}/2\mathbf{Z}$ is certainly a field of characteristic 2, so $(J(X)[2], \langle \cdot, \cdot \rangle)$ is a "symplectic space". A classical theorem about symplectic spaces follows.

Theorem. *A nondegenerate symplectic space is always even dimensional. Moreover, all symplectic spaces of dimension $2g$ are isomorphic to the space $V = k^{2g}$ with basis $e_1, \dots, e_g, f_1, \dots, f_g$ such that the matrix for $V \rightarrow V^\vee$ with respect to that basis (and dual basis) given by $v \mapsto \langle \cdot, v \rangle$ is $\begin{pmatrix} 0_g & I_g \\ -I_g & 0_g \end{pmatrix}$*

Proof. <http://www.math.harvard.edu/~elkies/M55a.99/pfaff.html>

Note that Elkies is being careful enough to work over any field.

□

We call such a basis a *symplectic basis*. Using this basis, we make the following definition:

Definition. *If q is a non degenerate quadratic form over a $\mathbf{Z}/2\mathbf{Z}$ vector space V and $\{e_1, \dots, e_g, f_1, \dots, f_g\}$ is a symplectic basis for V with respect to b_q then we define the Arf invariant as*

$$\text{Arf}(q) = \sum_{i=1}^g q(e_i)q(f_i)$$

Remark. *The Arf invariant can apparently be defined in a coordinate-free way. With q we can define the Clifford algebra $C(q) = T^\bullet V / \langle x \otimes x = q(x) \rangle$. Within the Clifford algebra is the even Clifford algebra $C_0(q)$ made up of the tensor product of an even number of vectors. The even part of the center is a 2-dimensional separable algebra, which is of the form $k[T]/(T^2 - T - \text{Arf}(q))$. Here $k = \mathbf{Z}/2\mathbf{Z}$ but it should be clear how to generalize this to perfect fields of characteristic 2.*

Theorem. *The Arf invariant is independent of the choice of symplectic basis. Moreover $\text{Arf}(q + \langle v, \cdot \rangle) = \text{Arf}(q) + q(v)$*

Proof. For the proof that it is invariant of the symplectic basis, see Gross-Harris [3]. Once we have established that, it suffices to pick a symplectic basis such

that $e_1 = v$. It follows then that

$$\begin{aligned} \text{Arf}(q + \langle e_1, \cdot \rangle) &= \sum_{i=1}^g (q(e_i) + \langle e_1, e_i \rangle)(q(f_i) + \langle e_1, f_i \rangle) \\ &= \left(\sum_{i=1}^g q(e_i)q(f_i) \right) + q(e_1)\langle e_1, f_1 \rangle \\ &= \text{Arf}(q) + q(e_1) = \text{Arf}(q) + q(v) \end{aligned}$$

□

Corollary. *On a non degenerate symplectic space (V, \langle, \rangle) of dimension $2g$, $\# \text{Arf}^{-1}(0) = 2^{g-1}(2^g + 1)$ and $\# \text{Arf}^{-1}(1) = 2^{g-1}(2^g - 1)$*

Proof. Start with a symplectic basis $\{e_1, \dots, e_g, f_1, \dots, f_g\}$. We wish to define q_0 such that

$$q_0\left(\sum_{i=1}^g \alpha_i e_i + \beta_i f_i\right) = \sum_{i=1}^g \alpha_i \beta_i.$$

We note that

$$q_0\left(c \sum_{i=1}^g \alpha_i e_i + \beta_i f_i\right) = \sum_{i=1}^g c \alpha_i c \beta_i = c^2 \sum_{i=1}^g \alpha_i \beta_i$$

while

$$b_{q_0}\left(\sum_{i=1}^g \alpha_i e_i + \beta_i f_i, \sum_{i=1}^g \alpha'_i e_i + \beta'_i f_i\right) = \sum_{i=1}^g \alpha'_i \beta_i + \sum_{i=1}^g \alpha_i \beta'_i.$$

Thus it is clear by checking on the given symplectic basis that q_0 is a quadratic form on V with bilinear form \langle, \rangle . The purpose of this form is that it's been cooked up to have Arf invariant zero. Therefore by the theorem above, the forms of Arf invariant zero are exactly those of the form $q_0 + \langle v, \cdot \rangle$ such that $q_0(v) = 0$. We are thus reduced to counting the zeros of this form. If $g = 0$, $V = 0$ and q_0 is identically zero. If $g = 1$ there is exactly $1 = 2^{1-1}(2^1 - 1)$ vector on which q_0 is nonzero. If it's true for g , then for V of dimension $2(g + 1)$, there are exactly $2^{g-1}(2^g - 1)$ vectors with $\alpha_{g+1} = \beta_{g+1} = 0$ which q_0 sends to 1. This will not change if $\alpha_{g+1} = 0, \beta_{g+1} = 1$ or vice versa. This gives us $3(2^{g-1}(2^g - 1))$ vectors sent to 1. On the other hand if we want vectors with $\alpha_{g+1} = \beta_{g+1} = 1$ which are sent to 1, those are exactly the vectors which are sent to zero in dimension g . There are exactly $2^{g-1}(2^g + 1)$ of these, so in total we have $2^{g-1}(3(2^g - 1) + (2^g + 1)) = 2^{g-1}(2^{g+2} - 2) = 2^g(2^{g+1} - 1)$ vectors sent to 1, proving the claim.

□

Now we connect these results back to our knowledge of theta characteristics:

Theorem. *If ϑ is a theta characteristic, $\text{Arf}(q_\vartheta) = h^0(\vartheta) \bmod 2$.*

Proof. This can be found in Polishchuk [6, Theorem 17.11]. It uses the fact that for $v \in J(X)[2]$, the mod 2 multiplicity on the divisor $\phi_{\vartheta}(W_{g-1}) = W_{g-1} \otimes \vartheta^{-1}$ at v is $h^0(v \otimes \vartheta)$. \square

Corollary. *A curve X of genus g has precisely $2^{g-1}(2^g - 1)$ odd theta characteristics and $2^{g-1}(2^g + 1)$ even theta characteristics.*

Let's conclude with a discussion about why this might be interesting to someone who, like myself, works over non-algebraically closed fields.

4 Rational Points and Maps to projective space

We begin with perhaps the hardest question in the history of mathematics:

When does a set of Diophantine equations (that is, polynomials over the integers set equal to zero) have an integer solution (which we will hereon call a "rational point")?

Throughout the ages, many people have asked this question. Most notable among them is Hilbert who asked the following as the 10th of his famous 23 problems in 1900.

Question. *Given a set of Diophantine Equations, is there an algorithm to find a rational point?*

This answer is no in general [2]. To this day, this is an extremely hard question and the study is mainly geared towards finding cohomological obstructions to rational points. Producing them is in general very hard.

A related question is what degree of a field extension you need to produce rational points, and for what degrees d can you get a rational point over infinitely many fields of degree d ?

One way to approach this is to use the equations to define a variety. If the resulting variety is a curve C , we have a canonical convenient way to provide an upper bound to d . A curve can be normalized (the same process as obtaining the Riemann Surface over the complex numbers) to a smooth (well, at least regular, but let's not dwell on this) curve X . This is enough to admit a canonical bundle, which is always rational. Therefore we always have a rational map $X \rightarrow \mathbb{P}^{g-1}$ of degree $2g - 2$. We know that over any field, \mathbb{P}^{g-1} has infinitely rational points and the pullback of any of these will produce a divisor of degree $2g - 2$. Hence there are infinitely many rational points that can be produced over a field of degree at most $2g - 2$ (not the same field though!).

Now: can we sharpen this? One avenue explored by Shahed Sharif [7] is to ask about maps of degree $g - 1$ given by *rational* theta characteristics. Notice that although you always have theta characteristics over \mathbf{C} , it might not be so over a smaller field, and I've tried to write these notes with a certain sensitivity to that. In particular, the rational theta characteristics will be in setwise bijection with the rational points of $J(X)[2]$.

References

- [1] I.Dolgachev , "Topics in Classical Algebraic Geometry", <http://www.math.lsa.umich.edu/~idolga/topics1.pdf> 2009.
- [2] K.Eisentraeger, "Hilbert's Tenth Problem and Arithmetic Geometry", Ph.D. thesis, 2003.
- [3] B. Gross and J. Harris, "On Some Geometric Constructions Related to Theta Characteristics", In: Contributions to Automorphic Forms, Geometry, and Number Theory, Johns Hopkins Press (2004), 279-311.
- [4] D. Mumford, with C.P. Ramanujam and Y. Manin, "Abelian Varieties: Second edition", American Mathematical Society, Providence 2008.
- [5] D. Mumford, "Theta characteristics of an algebraic curve", Annales scientifiques de l.N.S. 4eme srie, tome 4, **2** (1971), p. 181-192.
- [6] A. Polishchuk, "Abelian Varieties, Theta Functions and the Fourier Transform", Cambridge University Press, Cambridge Tracts in Mathematics (No. 153), 2003.
- [7] S. Sharif, "Rationality of Theta Characteristics", in progress