BITANGENTS AND THETA CHARACTERISTICS ON A SMOOTH PLANE QUARTIC

SAMEER KAILASA

Contents

Date: -.

1. Introduction

Let $C \subset \mathbb{P}^2_{\mathbb{C}}$ be a smooth quartic plane curve. A beautiful fact of enumerative algebraic geometry is that any such C has precisely 28 bitangent lines. In fact, much more is true: one can get a handle on the configuration of these lines via bijections

$$\mathrm{Bit}(C) \leftrightarrow \mathrm{OTC}(C) \leftrightarrow \mathrm{OQW}(C)$$

where $\mathrm{Bit}(C)$ is the set of bitangents to C, $\mathrm{OTC}(C)$ is the set of odd theta characteristics on C, and $\mathrm{OQW}(C)$ is the set of odd quadratic forms on the 2-torsion $J(C)[2]$ of the Jacobian variety of C, whose associated bilinear form is (essentially) the Weil pairing; we will define all these fancy objects shortly! The key idea is that via these bijections, one can pass from statements about the configuration of the bitangents to linear algebraic questions about a particular symplectic space over $\mathbb{F}_2$. In this note, we will try to give some idea of how this contraption works; it's a lovely example of deep machinery touching base with down-to-earth geometry.

2. Preliminaries on Curves

2.1. Notation and Facts.

We review some basic facts on curves to jog the reader's memory and fix notation. Most, if not all, of these facts, are proved somewhere in [1] or [2]. For concreteness' sake, we work over $\mathbb{C}$ throughout; let X be a smooth connected projective curve, and let K denote the sheaf of rational functions on X.

§**1**: Given a divisor D on X, we associate the sheaf $\mathcal{O}(D)$ such that

$$\mathcal{O}(D)(U) := \{f \in K(U)^{\times} \,:\, D|_U + \mathrm{div}(f) \geq 0\}$$

and recall that the association $D \mapsto \mathcal{O}(D)$ induces in this setting an isomorphism $\mathrm{Cl}(X) \to \mathrm{Pic}(X)$, where $\mathrm{Cl}(X)$ denotes the divisor class group and $\mathrm{Pic}(X)$ denotes the Picard group of isomorphism classes of invertible sheaves. The degree of $\mathcal{L} \in \mathrm{Pic}(X)$ is defined to be the degree of the corresponding divisor class under the aforementioned isomorphism. For an element $\mathcal{L} \in \mathrm{Pic}(X)$, we write $h^0(X, \mathcal{L})$ to denote $\dim(H^0(X, \mathcal{L}))$, i.e. the dimension of the space of global sections of $\mathcal{L}$. Recall that $h^0(X, \mathcal{L})$ is finite for all $\mathcal{L} \in \mathrm{Pic}(X)$.

§**2**: We denote by $|D|$ the complete linear system associated to a divisor D, i.e. the set of all effective divisors E such that $E \sim D$. For each $E \in |D|$, we have $E - D = \mathrm{div}(f)$ for some $f \in K(X)^{\times}$, and the map $|D| \to H^0(X, \mathcal{O}(D))$ given by $E \mapsto f$ is defined up to scaling f by a constant, so we have an honest map $|D| \to \mathbb{P}H^0(X, \mathcal{O}(D))$. This honest map is a bijection and, in particular, $|D|$ is nonempty iff $h^0(X, \mathcal{O}(D)) > 0$.

§**3**: For any morphism $f : X \to Y$ of smooth projective curves, the induced inclusion $K(Y) \hookrightarrow K(X)$ of function fields is a finite field extension; accordingly, we define the degree of f to be the degree $[K(X) : K(Y)]$ of this field extension. A curve X of genus ≥ 2 is called hyperelliptic if it admits a morphism $X \to \mathbb{P}^1$ of degree 2. One can show that X is hyperelliptic iff it admits a degree 2 invertible sheaf $\mathcal{L}$ with $h^0(X, \mathcal{L}) = 2$.

2.2. Smooth Quartic Plane Curves.

In this section, we establish some relevant facts on smooth quartic plane curves. Throughout, let $C \subset \mathbb{P}^2_{\mathbb{C}}$ denote a smooth connected quartic plane curve.

Lemma 2.1. *Let ω_C denote the canonical sheaf of rational 1-forms on C. Then $\omega_C \cong \mathcal{O}_C(1)$, where $\mathcal{O}_C(1) = \iota^\star \mathcal{O}(1)$ for $\iota : C \hookrightarrow \mathbb{P}^2$ and $\mathcal{O}(1)$ the invertible sheaf associated to the hyperplane divisor class on $\mathbb{P}^2$.*

Proof. This is a consequence of the *adjunction formula*, which states that if X is a smooth projective variety and $Y \hookrightarrow X$ is a smooth codimension 1 subvariety, then

$$K_Y = (K_X + Y)|_Y$$

where K_Z denotes the canonical divisor class on Z and $|_Y$ denotes restriction to Y. On $\mathbb{P}^2$, let H denote the hyperplane divisor; then $K_X \sim -3 \cdot H$ by a standard computation and C, thought of as a divisor, has $C \sim 4 \cdot H$ since C is a quartic. It follows that $K_C = H|_C$, so the canonical class of C is the hyperplane section, which corresponds to the sheaf $\mathcal{O}_C(1)$. □

Corollary 2.2. *The effective canonical divisors on C are precisely the divisors $C.L$ where $L \subset \mathbb{P}^2$ is a line.*

Proof. This follows immediately from the above lemma and the isomorphism $\mathrm{Cl}(C) \cong \mathrm{Pic}(C)$. □

Corollary 2.3. *If D is any effective divisor of degree 2 on C, then $h^0(C, \mathcal{O}(D)) = 1$.*

Proof. If $D = P + Q$ for points $P, Q \in C$ (not necessarily distinct), then let L be the line through P and Q (if $P = Q$, the tangent to C at P). We know $C.L \sim K_C$, by the previous corollary. Moreover, the lemma implies that K_C is very ample. Accordingly, the result of [1][Prop. IV.3.1] implies $\dim |D| = \dim |K_C| - 2$. But $\dim |K_C| = h^0(C, \omega_C) - 1 = 2$, where we have used the degree-genus formula. Hence $h^0(C, \mathcal{O}(D)) = 1 + \dim |D| = 1$. □

Corollary 2.4. *A smooth quartic plane curve is not hyperelliptic.*

Proof. If C were hyperelliptic, it would admit a degree 2 invertible sheaf $\mathcal{L}$ with $h^0(C, \mathcal{L}) = 2$. But the above corollary shows this cannot happen.

□

2.3. **Bitangent-Theta Characteristic Correspondence.** We now describe the objects of interest in this note, as well as the important bijection between them.

Definition 2.5. A **bitangent** to a curve $C \subset \mathbb{P}^2$ is a line L such that the divisor $C.L$ equals $2P + 2Q$ for some $P, Q \in C$, not necessarily distinct. Let $\mathrm{Bit}(C)$ denote the set of bitangents to C.

Definition 2.6. A **theta characteristic** on a curve C is an invertible sheaf $\mathcal{L}$ such that $\mathcal{L} \otimes \mathcal{L} \cong \omega_C$. Equivalently, a theta characteristic may be thought of as a divisor class D such that $2D \sim K_C$. A theta characteristic is said to be **odd** (resp. **even**) if $h^0(C, \mathcal{L})$ is odd (resp. even). Let $\mathrm{TC}(C)$ denote the set of theta characteristics on C, and let $\mathrm{OTC}(C)$ denote the set of odd theta characteristics on C.

Proposition 2.7. *Let $C \subset \mathbb{P}^2$ be a smooth quartic plane curve. There is a bijection*

$$Bit(C) \leftrightarrow OTC(C)$$

given by

$$L \mapsto \frac{1}{2}(C.L)$$

Proof. If $L \in \mathrm{Bit}(C)$, then $C.L \sim K_C$ by Corollary 2.2, so $\frac{1}{2}(C.L)$ is indeed a theta characteristic. Moreover, by Corollary 2.3, it follows that $\frac{1}{2}(C.L)$ is an odd theta characteristic.

We first show the map is surjective. Suppose D is an odd theta characteristic on C, given as a divisor with $2D \sim K_C$. Since $h^0(C, \mathcal{O}(D)) > 0$, it follows that $|D|$ is nonempty; choose $E \sim D$ an effective divisor. Writing $E = P + Q$, since $2E = 2P + 2Q$ is canonical, it follows from Corollary 2.2 that $2E = C.L$ for some line L.

To see that the map is injective, suppose two bitangents L_1 and L_2 yield the same theta characteristic. It would follow that there exist points $P, Q, R, S \in C$ with $\{P, Q\} \neq \{R, S\}$ as sets, such that $P + Q \sim R + S$. But then $P + Q - R - S = \mathrm{div}(f)$ for some rational function f, and such an f would yield a hyperelliptic map $C \to \mathbb{P}^1$. □

3. Theta Characteristics and Quadratic Forms

In this section, we will establish a correspondence between theta characteristics on a curve X and quadratic forms on a particular $\mathbb{F}_2$-vector space. Our exposition here is based upon [6]. We refer to the following facts on abelian varieties, whose proofs can be found in [3].

§**1**: Associated to every smooth projective curve X of genus g, there is an abelian variety called the Jacobian of X, denoted $J(X)$, which is isomorphic as a group with the subgroup $\mathrm{Pic}^0(X) \subset \mathrm{Pic}(X)$ of degree 0 line bundles. The n-torsion in $J(X)$, denoted $J(X)[n]$ (and consisting of invertible sheaves $\mathcal{L}$ such that $\mathcal{L}^{\otimes n} \cong \mathcal{O}_X$), is free of rank $2g$ as a $\mathbb{Z}/n\mathbb{Z}$ module, i.e. $J(X)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

§**2**: For each n, there is a canonical nondegenerate alternating bilinear form

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

where μ_n is the multiplicative group of nth roots of unity. This is called the Weil pairing on $J(X)[n]$. We will be concerned specifically with $n = 2$, in which case we can construct e_2 explicitly as a form taking values in the additive group $\mathbb{Z}/2\mathbb{Z}$. If f is a rational function on X and $D = \sum n_p P$ is a divisor with $\mathrm{Supp}(D)$ disjoint from $\mathrm{Supp}(\mathrm{div}(f))$, we set

$$f(D) := \prod_{p \in X} f(p)^{n_p}$$

The classic *Weil reciprocity law* says that for rational functions f, g on X with $\mathrm{Supp}(\mathrm{div}(f))$ and $\mathrm{Supp}(\mathrm{div}(g))$ disjoint, we have $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$. Now, suppose $D_1, D_2 \in J(X)[2]$, so that $2D_1 \sim (f)$ and $2D_2 = (g)$ for some rational functions f and g. It follows that

$$\left(\frac{f(D_2)}{g(D_1)}\right)^2 = \frac{f(\mathrm{div}(g))}{g(\mathrm{div}(f))} = 1$$

We finally set

$$e_2(D_1, D_2) := \begin{cases} 0 & \text{if } f(D_2) = g(D_1) \\ 1 & \text{if } f(D_2) = -g(D_1) \end{cases}$$

Remark 3.1. Since any two theta characteristics on X differ by an element of $J(X)[2]$, it follows that there are (non-canonical) bijections $J(X)[2] \to \mathrm{TC}(X)$ and, in particular, we see that any curve has precisely 2^{2g} theta characteristics.

We now cite the following deep theorem of Mumford:

Theorem 3.2. *For any $\theta \in TC(X)$, the map $q_\theta : J(X)[2] \to \mathbb{Z}/2\mathbb{Z}$ given by*

$$q_\theta(\mathcal{L}) := h^0(X, \mathcal{L} \otimes \theta) + h^0(X, \theta) \pmod 2$$

is a quadratic form. Moreover, for any θ, the associated bilinear form $b_\theta(v, w) := q_\theta(v + w) - q(v) - q(w)$ recovers the Weil pairing, i.e. $b_\theta = e_2$ for all $\theta \in TC(X)$. In particular, it follows that for any $v, w \in J(X)[2]$ and $\theta \in TC(X)$, we have

$$e_2(v, w) \equiv h^0(X, v \otimes w \otimes \theta) + h^0(X, v \otimes \theta) + h^0(X, w \otimes \theta) + h^0(X, \theta) \pmod 2$$

Proof. See [4]. □

Accordingly, we define the set $\mathrm{QW}(X)$ to be the set of quadratic forms on $J(X)[2]$ whose associated bilinear form is the Weil pairing e_2. The theorem above gives us a map $\mathrm{TC}(X) \to \mathrm{QW}(X)$, and in fact this is a bijection.

Proposition 3.3. *Let X be a smooth projective curve of genus g. There is a bijection*

$$TC(X) \leftrightarrow QW(X)$$

given by

$$\theta \mapsto q_\theta$$

Proof. If $\theta, \theta' \in \mathrm{TC}(X)$ are distinct, a quick computation shows that $q_{\theta'}(v) - q_\theta(v) = e_2(v, \theta' \otimes \theta^{-1})$. If $q_{\theta'} = q_\theta$, then nondegeneracy of the Weil pairing would imply $\theta' \cong \theta$; hence the map $\mathrm{TC}(X) \to \mathrm{QW}(X)$ is injective. More generally, for any q, $q' \in \mathrm{QW}(X)$, we have $q - q'$ is a linear functional on $J(X)[2]$ (using that we're in characteristic 2), and hence $q - q' = e_2(\cdot, v)$ for some $v \in J(X)[2]$. If $q \in \mathrm{QW}(X)$, we may write $q = q_\theta + e_2(\cdot, v)$ for some $v \in J(X)[2]$, and so $q = q_{\theta'}$ where $\theta' = v \otimes \theta$. □

4. Symplectic Spaces over $\mathbb{F}_2$

Definition 4.1. Let k be a field. A **symplectic space (over k)** is a pair (V, b) consisting of a finite-dimensional k-vector space V and a nondegenerate alternating bilinear form b on V. We say q is a **quadratic form on (V, b)** if q is a quadratic form on V having the property that the associated bilinear form $b_q(v, w) := q(v + w) - q(v) - q(w)$ agrees with b, i.e. $b_q = b$.

The above considerations tell us that $(J(X)[2], e_2)$ is a symplectic space over $\mathbb{F}_2$. In this section, we will record some linear algebra of symplectic spaces (especially over $\mathbb{F}_2$) and bring it to bear on our particular symplectic space of interest.

Remark 4.2. If q is a quadratic form on V, then the associated bilinear form is $b_q(v, w) := q(v + w) - q(v) - q(w)$. Moreover, if $\mathrm{char}(k) \neq 2$, then we can recover q from b_q via the equation $b_q(v, v) = q(2v) - 2q(v) = 2q(v)$. Thus, if $\mathrm{char}(k) \neq 2$, there is at most one quadratic form from which a bilinear form can arise; however, if $\mathrm{char}(k) = 2$, then as we have seen, there can be many q yielding the same b_q.

Proposition 4.3. *A symplectic space is always even-dimensional. Moreover, any symplectic space (V, b) of dimension $2n$ admits a basis of the form*

$$\{e_1, \cdots, e_n, f_1, \cdots, f_n\}$$

such that $b(e_i, e_j) = b(f_i, f_j) = 0$ and $b(e_i, f_j) = \delta_{ij}$ for all pairs $1 \leq i \leq j \leq n$. Such a basis is called a symplectic basis.

Proof. The proof is a straightforward induction on dimension; see [5] for details. □

Definition 4.4. Let (V, b) be a symplectic space of dimension $2n$. A subspace $W \subset V$ is called **isotropic** if $b(v, w) = 0$ for all $v, w \in W$. Since b yields an injection $W \to \mathrm{Ann}(W) \subset V^\star$, it follows that $\dim(W) \leq n$ for any isotropic subspace W. A maximal isotropic subspace, i.e. an isotropic subspace $L \subset V$ with $\dim(L) = n$, is called **Lagrangian**.

Lemma 4.5. *Any basis of a Lagrangian subspace $L \subset V$ extends to a symplectic basis for (V, b).*

Proof. See [5].

□

From here on, suppose we are working with a symplectic space (V, b) over $\mathbb{F}_2$.

Definition 4.6. Suppose q is a nondegenerate quadratic form on (V, b) and let $\{e_1, \cdots, e_n, f_1, \cdots, f_n\}$ be a symplectic basis for (V, b). The **Arf invariant** of q is the element of $\mathbb{Z}/2\mathbb{Z}$ given by

$$\mathrm{Arf}(q) := \sum_{i=1}^{n} q(e_i)q(f_i)$$

Proposition 4.7. (*a*) *The Arf invariant is well-defined, i.e. does not depend on the choice of symplectic basis.*

(*b*) *If q is a quadratic form on (V, b), then for any $v \in V$, the map $w \mapsto q(w) + b(v, w)$ is also a quadratic form, denoted $q + v^\star$. Moreover, we have $Arf(q + v^\star) = Arf(q) + q(v)$.*

(*c*) *If q_0, q_1, and q_2 are all quadratic forms on (V, b), then*

$$Arf(q_0 + q_1 + q_2) = Arf(q_0) + Arf(q_1) + Arf(q_2) + \langle v_1, v_2 \rangle$$

where $q_0 + q_1 = b(\cdot, v_1)$ and $q_0 + q_2 = b(\cdot, v_2)$.

Proof. We just sketch the first part. Let $\mathrm{Sp}(V)$ denote the group of symplectic transformations of V, i.e. linear maps $T : V \to V$ such that $b(v, w) = b(Tv, Tw)$ for all pairs $v, w \in V$. In particular, any two symplectic bases differ by an element of $\mathrm{Sp}(V)$. One can show that $\mathrm{Sp}(V)$ is generated by the "transvection" maps $T_u : V \to V$ given by

$$T_u(v) = v + b(v, u)u.$$

It then suffices to show that the Arf invariant is preserved under the action of transvections, which is a straightforward computation. We omit the proofs of parts (*b*) and (*c*), which are also quick computations. □

Definition 4.8. A quadratic form q on (V, b) is called **odd** (resp. **even**) if $\mathrm{Arf}(q) = 1$ (resp. $\mathrm{Arf}(q) = 0$).

Returning to the situation of $(J(X)[2], e_2)$, we note that this definition agrees with the correspondence $\mathrm{TC}(X) \leftrightarrow \mathrm{QW}(X)$, due to the following theorem, again deep and again due to Mumford.

Theorem 4.9. *If $\theta \in TC(X)$, then $Arf(q_\theta) \equiv h^0(X, \theta) \pmod 2$.*

Proof. See [4]. □

Corollary 4.10. *The bijection $TC(X) \leftrightarrow QW(X)$ restricts to a bijection $OTC(X) \leftrightarrow OQW(X)$, where $OQW(X)$ denotes the set of odd quadratic forms on $(J(X)[2], e_2)$. In particular, in the case where $X = C$ is a smooth quartic plane curve, we have bijections*

$$Bit(C) \leftrightarrow OTC(C) \leftrightarrow OQW(C)$$

We can now count the number of odd/even theta characteristics on X by counting the odd/even quadratic forms on $(J(X)[2], e_2)$; this proceeds by a short combinatorial argument!

Lemma 4.11. *Let (V, b) be a symplectic space over $\mathbb{F}_2$ of dimension $2n$. The number of odd (resp. even) quadratic forms on (V, b) is $2^{n-1}(2^n-1)$ (resp. $2^{n-1}(2^n+1)$).*

Proof. Choose a symplectic basis $\{e_1, \cdots, e_n, f_1, \cdots, f_n\}$. We define on V a quadratic form

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

By a quick computation in these coordinates, one can check that q_0 is in fact a quadratic form over (V, b), and furthermore note that $\mathrm{Arf}(q_0) = 0$. We know that any other quadratic form on (V, b) is of the form $q = q_0 + b(\cdot, v)$ for some $v \in V$. By Proposition 4.5, we see that $\mathrm{Arf}(q) = \mathrm{Arf}(q_0 + v^\star) = q_0(v)$, hence the even quadratic forms on (V, b) are in bijection with the zeroes of q_0. We should therefore count these zeroes.

We proceed by induction on n to show that the number of zeroes of q_0 is $2^{n-1}(2^n+1)$. The base cases $n = 0$ and $n = 1$ are easy to check by hand. Suppose the result is true for $n = k$. For $n = k + 1$, we do casework on the pair $(\alpha_{k+1}, \beta_{k+1})$. If $\alpha_{k+1}\beta_{k+1} = 0$ (and there are three such pairs), then the corresponding solutions are in bijection with those for the $n = k$ case, which thus contributes $3 \cdot 2^{k-1}(2^k+1)$ zeroes to the count. If $\alpha_{k+1} = \alpha_{k+1} = 1$, then the corresponding solutions are in bijection with the non-solutions for the $n = k$ case, which thus contributes $2^{k-1}(2^k - 1)$ zeroes to the count. We conclude there are a total of

$$3 \cdot 2^{k-1}(2^k + 1) + 2^{k-1}(2^k - 1) = 2^{k-1}(2^{k+2} + 2) = 2^k(2^{k+1} + 1)$$

as desired. □

Corollary 4.12. *On a smooth projective curve X of genus g, there are $2^{g-1}(2^g-1)$ odd theta characteristics and $2^{g-1}(2^g + 1)$ even theta characteristics.*

Corollary 4.13. *A smooth quartic plane curve has precisely 28 bitangent lines.*

Proof. By Corollary 4.10, using that a quartic plane curve has genus 3, it follows there are $2^2(2^3 - 1) = 28$ bitangents. □

5. Application: Conics Through Bitangency Points

Let $C \subset \mathbb{P}^2$ be a smooth quartic plane curve. At this point, we have a little machine set up that allows us to convert statements about quadratic forms on the symplectic space $(J(C)[2], e_2)$ to statements about the the bitangent lines to C. Broadly speaking, we can turn geometry into combinatorics and vice versa! We have used this machine above to count the bitangents to C; in this section, we will use it to say a bit more about their configuration. Namely, we will answer the question:

Question 5.1. *Given* $L_1, \cdots, L_4 \in Bit(C)$*, when does there exist a conic* Q *such that*

$$Q.C = \sum_{i=1}^{4} \frac{1}{2}(L_i \cdot C)?$$

Conversely, how many conics Q *exist such that the above equation holds for some* $L_1, \cdots, L_4 \in Bit(C)$*?*

The main reference for this section is [7].

Lemma 5.2. *Suppose* $L_1, \cdots, L_4 \in Bit(C)$*. There is a conic* $Q \subset \mathbb{P}^2$ *such that* $Q.C = \sum_{i=1}^{4} \frac{1}{2}(L_i \cdot C)$ *iff the quadratic forms* $Q_1, \cdots, Q_4$ *on* $(J(X)[2], e_2)$ *corresponding to* $L_1, \cdots, L_4$ *satisfy*

$$Q_1 + Q_2 + Q_3 + Q_4 = 0$$

Proof. Let $\iota : C \to \mathbb{P}^2$ denote the inclusion. From Lemma 2.1, we have $\iota^\star \mathcal{O}(2) = \omega_C^{\otimes 2}$, corresponding to the divisor class $2K_C$. Hence, an effective divisor E on C is cut by a conic iff $E \sim 2K_C$. Given $L_1, \cdots, L_4 \in \mathrm{Bit}(C)$ and setting $D_i = \frac{1}{2}(L_i.C)$, it follows that a conic cuts the divisor $D_1 + \cdots + D_4$ iff $D_1 + \cdots D_4 \sim 2K_C$. To convert this to a statement about quadratic forms, recall from the proof of Proposition 3.3 that we have the identity $q_D - q_{D'} = e_2(\cdot, D - D')$. Thus, we have

$$Q_1 + Q_2 + Q_3 + Q_4 = e_2(\cdot, D_1 - D_2) + e_2(\cdot, D_3 - D_4) = e_2(\cdot, 2K_C - D_1 - D_2 - D_3 - D_4)$$

and it follows that $D_1 + \cdots D_4 \sim 2K_C$ iff $Q_1 + Q_2 + Q_3 + Q_4 = 0$. □

To study Question 5.1, we should therefore study the corresponding object on $(J(C)[2], e_2)$, i.e. quadruples of odd quadratic forms summing to zero.

Definition 5.3. Let (V, b) be a symplectic space over $\mathbb{F}_2$. A **syzygetic tetrad** is a collection $Q_1, \cdots, Q_4$ of distinct odd quadratic forms on (V, b) such that

$$Q_1 + Q_2 + Q_3 + Q_4 = 0$$

We wish to count the syzygetic tetrads on (V, b) in the case when $\dim(V) = \dim(J(C)[2]) = 6$. To do this, we introduce an additional bit of terminology.

Definition 5.4. Let (V, b) be a symplectic space over $\mathbb{F}_2$. A **syzygetic triad** is a collection Q_1, Q_2, Q_3 of distinct odd quadratic forms on (V, b) such that $Q_1 + Q_2 + Q_3$ is odd.

Corollary 5.5. *Suppose* Q_1, Q_2, Q_3 *are odd quadratic forms on* (V, b)*. Write* $Q_1 + Q_2 = b(\cdot, v_2)$ *and* $Q_1 + Q_3 = b(\cdot, v_3)$*. Then* $Q_1 + Q_2 + Q_3$ *is odd iff* $b(v_2, v_3) = 0$*.*

Proof. This follows directly from part (c) of Proposition 4.7. □

Lemma 5.6. *Assume* $\dim(V) = 6$*, and let* Q_1, Q_2, Q_3, Q_4 *be odd quadratic forms on* (V, b)*. Then, the following are equivalent:*

- *(i)* Q_1, Q_2, Q_3, Q_4 *is a syzygetic tetrad*
- *(ii) all four collections* Q_i, Q_j, Q_k *with* $1 \le i < j < k \le 4$ *are syzygetic triads*
- *(iii) three of the four collections* Q_i, Q_j, Q_k *with* $1 \le i < j < k \le 4$ *are syzygetic triads*

Proof. The implications $(i) \implies (ii) \implies (iii)$ are immediate. Suppose (iii) is true, and assume without loss of generality that the three known syzygetic triads are those containing Q_1. Write $Q_1 + Q_i = b(\cdot, v_i)$ for $2 \leq i \leq 4$. By Proposition 4.7, it follows that $Q_1(v_i) = 0$ for all $2 \leq i \leq 4$. Moreover, by Corollary 5.5, it follows that $b(v_i, v_j) = 0$ for all pairs $2 \leq i \leq j \leq 4$; hence $W := \langle v_2, v_3, v_4 \rangle$ is isotropic.

Suppose $\dim(W) = 3$, so that W is Lagrangian. Extending v_2, v_3, v_4 to a symplectic basis for V (Lemma 4.5), it would follows that $\mathrm{Arf}(Q_1) = 0$, contradiction that Q_1 is odd. Hence v_2, v_3, v_4 are linearly dependent, and it follows that $v_2 + v_3 + v_4 = 0$ (as these vectors are nonzero and pairwise distinct). We deduce that

$$Q_1 + Q_2 + Q_3 + Q_4 = b(\cdot, v_2 + v_3 + v_4) = 0$$

as desired. □

Definition 5.7. For any nonzero $v \in V$, we have the associated **Steiner set** S_v of odd quadratic forms Q such that $Q(v) = 0$. Equivalently, by Proposition 4.5, S_v is the set of odd quadratic forms Q such that $Q + v^\star$ is also odd. We say $Q, Q' \in S_v$ are **paired** if $Q = Q' + v^\star$ or, equivalently, $Q + Q' = b(\cdot, v)$. Note that the pairs partition each S_v.

Lemma 5.8. *If* $\dim(V) = 2n$*, each Steiner set* S_v *has* $2^{n-2}(2^{n-1} - 1)$ *pairs of odd quadratic forms. Equivalently,* $|S_v| = 2^{n-1}(2^{n-1} - 1)$.

Proof. If $\{Q, Q + v^\star\} \subset S_v$ is a pair, we obtain an odd quadratic form on

$$\langle v \rangle^\perp := \{w \in V \,:\, b(w, v) = 0\}$$

by restriction, which then descends to an odd quadratic form on $\langle v \rangle^\perp / \langle v \rangle$ since $Q(v) = 0$. One can check that this map yields a bijection between pairs in S_v and odd quadratic forms on the $2n - 2$ dimensional space $\langle v \rangle^\perp / \langle v \rangle$. By Lemma 4.11, the result follows. □

Lemma 5.9. *Assume* $\dim(V) = 6$ *and* Q_1, Q_2, Q_3 *are odd quadratic forms belonging to the Steiner set* S_v*. Then* Q_1, Q_2, Q_3 *is a syzygetic triad iff some two of them are paired in* S_v.

Proof. If some two are paired, e.g. $Q_1 + Q_2 = b(\cdot, v)$, then $Q_1 + Q_2 + Q_3 = Q_3 + v^\star$ is odd, since $Q_3 \in S_v$. Conversely, suppose $Q_1 + Q_2 + Q_3$ is odd. If e.g. $Q_1 + Q_2 \neq v^\star$ and $Q_1 + Q_3 \neq v^\star$, then $Q_1, Q_2, Q_3, Q_1 + v^\star$ is a collection of four odd forms with the property that each set of 3 containing Q_1 is a syzygetic triad. It follows from Lemma 5.6 that $Q_2 + Q_3 = b(\cdot, v)$, so Q_2 and Q_3 are paired. □

Proposition 5.10. *Assume* $\dim(V) = 6$*. Then there are precisely 1260 syzygetic triads and 315 syzygetic tetrads on* (V, b).

Proof. There are 63 distinct Steiner sets (one for each nonzero vector in V) and, by Lemma 5.8, each Steiner set consists of 6 disjoint pairs. By Lemma 5.9, it follows that there are $60 = 6 \cdot 10$ syzygetic triads contained in each Steiner set; indeed, there are 6 ways to choose a pair and $12 - 2 = 10$ ways to choose a third quadratic form. On the other hand, each syzygetic triad Q_1, Q_2, Q_3 is contained in exactly three distinct Steiner sets, namely the sets $S_{v_{ij}}$ for each v_{ij} coming from $Q_i + Q_j = b(\cdot, v_{ij})$. Thus, the total number of syzygetic triads is $63 \cdot 60/3 = 1260$. By Lemma 5.6, each syzygetic triad Q_1, Q_2, Q_3 is contained in a unique syzygetic tetrad (namely, $Q_1, Q_2, Q_3, Q_1 + Q_2 + Q_3$) and there are four triads in each tetrad: thus, the total number of syzygetic tetrads is $1260/4 = 315$. □

Having established the key enumerative result, we apply it to the case $(V, b) = (J(C)[2], e_2)$ and translate back into the language of geometry.

Proposition 5.11. (*a*) *For any pair $L, M \in Bit(C)$, there are exactly five other pairs $L', M' \in Bit(C)$ such that there exists a conic $Q \subset \mathbb{P}^2$ with*

$$Q.C = \frac{1}{2}(L + M + L' + M').C$$

(*b*) *There are exactly 315 conics $Q \subset \mathbb{P}^2$ such that $Q.C = \sum_{i=1}^{4} \frac{1}{2}(L_i \cdot C)$ for some $L_1, \cdots, L_4 \in Bit(C)$.*

Proof. The pairs of bitangents alluded to in part (a) are precisely those other pairs in the Steiner set S_v with $Q_L + Q_M = e_2(\cdot, v)$. Part ($b$) follows from the bijection between such conics and syzygetic tetrads. □

References

[1] *Algebraic Geometry*, Robin Hartshorne
[2] *Fundamentals of Algebraic Geometry*, Ravi Vakil
[3] *Abelian Varieties*, David Mumford
[4] *Theta characteristics of an algebraic curve*, David Mumford
[5] http://www.math.harvard.edu/ elkies/M55a.99/pfaff.html
[6] http://stankewicz.net/Theta.pdf
[7] http://mat.uab.es/ gac/Bitangents.ps