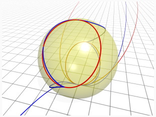


Propriétés géométriques et arithmétiques explicites des courbes

Advisors: Sylvain Duquesne, Christophe Ritzenthaler

Türkü Özlüm Çelik

August 31, 2018

Université de Rennes I, IRMAR

- Chapter 1: Theta Constants
- Chapter 2: (Kummer-Based) Hyperelliptic Curve Cryptography

Gabriel Gallin

Arnaud Tisserand

- Chapter 3: p-Rank Computations

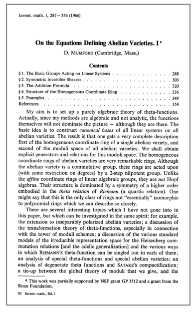
Y.Elias, B. Gunes, C., E. Ozman, R. Newton, R. Pries, L. Thomas

Outline of the Defense

Introduction and Motivation

Motivation

D. Mumford (1966) showed that a principally polarized abelian variety can be written as an intersection of explicit quadrics in a projective space. The coefficients of these quadrics are determined by theta constants.



Invent. math. 1, 287—354 (1966)

On the Equations Defining Abelian Varieties. I*

D. Mumford (Cambridge, Mass.)

Contents

My aim is to set up a purely algebraic theory of theta-functions. Actually, since my methods are algebraic and not analytic, the functions themselves will not dominate the picture — although they are there. The basic idea is to construct *canonical bases* of all linear systems on all abelian varieties. The result is that one gets a very complete description first of the homogeneous coordinate ring of a single abelian variety, and second of the moduli space of all abelian varieties. We shall obtain explicit generators and relations for this moduli space. The homogeneous coordinate rings of abelian varieties are very remarkable rings. Although the abelian variety is a commutative group, these rings are acted upon (with some restriction on degrees) by a 2-step nilpotent group. Unlike the *affine* coordinate rings of linear algebraic groups, they are *not* Hopf algebras. Their structure is dominated by a symmetry of a higher order embodied in the *theta relation* of *Riemann* (a quartic relation). One might say that this is the only class of rings not "essentially" isomorphic to polynomial rings which we can describe so closely.

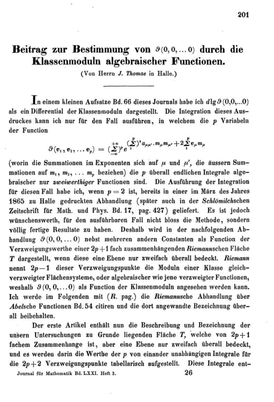
There are several interesting topics which I have not gone into in this paper, but which can be investigated in the same spirit: for example, the extension to inseparably polarized abelian varieties; a discussion of the transformation theory of theta-functions, especially in connection with the tower of moduli schemes; a discussion of the various standard models of the irreducible representation space for the Heisenberg commutation relations [and the adelic generalization] and the various ways in which Riemann's theta-function can be singled out in each of them; an analysis of special theta-functions and special abelian varieties; an analysis of degenerate theta functions and Satake's compactification; a tie-up between the global theory of moduli that we give, and the

* This work was partially supported by NSF grant GP 3512 and a grant from the Sloan Foundation.

A bit of history - 1870

The Jacobian variety of an algebraic curve is an abelian variety.

In the case of hyperelliptic curves, C. J. Thomae found a formula to compute the fourth power of theta constants in terms of the geometry of the curve.



201

Beitrag zur Bestimmung von $\vartheta(0, 0, \dots 0)$ durch die Klassenmoduln algebraischer Functionen.

(Von Herrn *J. Thomae* in Halle.)

In einem kleinen Aufsatze Bd. 66 dieses Journals habe ich $d \lg \vartheta(0,0,\dots 0)$ als ein Differential der Klassenmoduln dargestellt. Die Integration dieses Ausdruckes kann ich nur für den Fall ausführen, in welchem die p Variabeln der Function

$$\vartheta(v_1, v_2, \dots v_p) = (\sum_{-\infty}^{+\infty})^p e^{(\sum_1^p)^2 a_{\mu\mu'} . m_\mu m_{\mu'} + 2\sum_1^p v_\mu m_\mu}$$

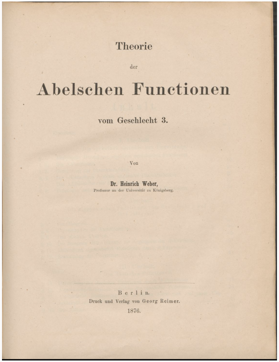
(worin die Summationen im Exponenten sich auf μ und μ', die äussern Summationen auf $m_1, m_2, \dots m_p$ beziehen) die p überall endlichen Integrale algebraischer nur *zweiwerthiger* Functionen sind. Die Ausführung der Integration für diesen Fall habe ich, wenn $p = 2$ ist, bereits in einer im März des Jahres 1865 zu Halle gedruckten Abhandlung (später auch in der *Schlömilch*schen Zeitschrift für Math. und Phys. Bd. 17, pag. 427) geliefert. Es ist jedoch wünschenswerth, für den ausführbaren Fall nicht bloss die Methode, sondern völlig fertige Resultate zu haben. Deshalb wird in der nachfolgenden Abhandlung $\vartheta(0, 0, \dots 0)$ nebst mehreren andern Constanten als Function der Verzweigungswerthe einer $2p+1$ fach zusammenhängenden *Riemann*schen Fläche T dargestellt, wenn diese eine Ebene nur zweifach überall bedeckt. *Riemann* nennt $2p-1$ dieser Verzweigungspunkte die Moduln einer Klasse gleichverzweigter Flächensysteme, oder algebraischer wie jene verzweigter Functionen, weshalb $\vartheta(0, 0, \dots 0)$ als Function der Klassenmoduln angesehen werden kann. Ich werde im Folgenden mit (*R.* pag.) die *Riemann*sche Abhandlung über *Abel*sche Functionen Bd. 54 citiren und die dort angewandte Bezeichnung überall beibehalten.

Der erste Artikel enthält nun die Beschreibung und Bezeichnung der unsern Untersuchungen zu Grunde liegenden Fläche T, welche von $2p+1$ fachem Zusammenhange ist, aber eine Ebene nur zweifach überall bedeckt, und es werden darin die Werthe der p von einander unabhängigen Integrale für die $2p+2$ Verzweigungspunkte tabellarisch aufgestellt. Diese Integrale ent-

Journal für Mathematik Bd. LXXI. Heft 3. 26

A bit of history - 1876

In the case of non-hyperelliptic curves of genus 3, H. M. Weber found a formula to compute the fourth power of the quotients of theta constants in terms of the geometry of the curve.



Theorie

der

Abelschen Functionen

vom Geschlecht 3.

Von

Dr. Heinrich Weber,

Professor an der Universität zu Königsberg.

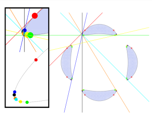
Berlin.

Druck und Verlag von Georg Reimer.

1876.

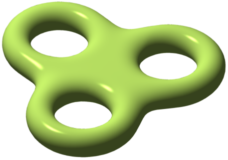
Weber's formula

Let $\mathcal{C}$ be a non-hyperelliptic curve of genus 3. Let p_1, p_2 be even characteristics, and let $\beta_i's$ and $\beta_{ij}'s$ be certain bitangents of the curve. Let τ be a Riemann matrix of $\mathcal{C}$. Then



the characteristics p_i's are 2×3 arrays with $0, 1$ entries

$$\left(\frac{\vartheta[p_1](\tau)}{\vartheta[p_2](\tau)}\right)^4 = \pm \frac{[\beta_1,\beta_2,\beta_3]\cdot[\beta_1,\beta_{12},\beta_{13}]\cdot[\beta_{12},\beta_2,\beta_{23}]\cdot[\beta_{13},\beta_{23},\beta_3]}{[\beta_{23},\beta_{13},\beta_{12}]\cdot[\beta_{23},\beta_3,\beta_2]\cdot[\beta_3,\beta_{13},\beta_1]\cdot[\beta_2,\beta_1,\beta_{12}]}$$



- Link between intrinsic and extrinsic geometry of $\mathcal{C}$.
- Combinatorial structure on the geometry of $\mathcal{C}$.

The Result

How about higher genera?

Let $\mathcal{C}$ be a non-hyperelliptic curve of genus g. Let τ be a Riemann matrix. Note $\text{Jac}(\mathcal{C}) \cong \mathbb{C}^g/\mathbb{Z}^g + \tau\mathbb{Z}^g$.

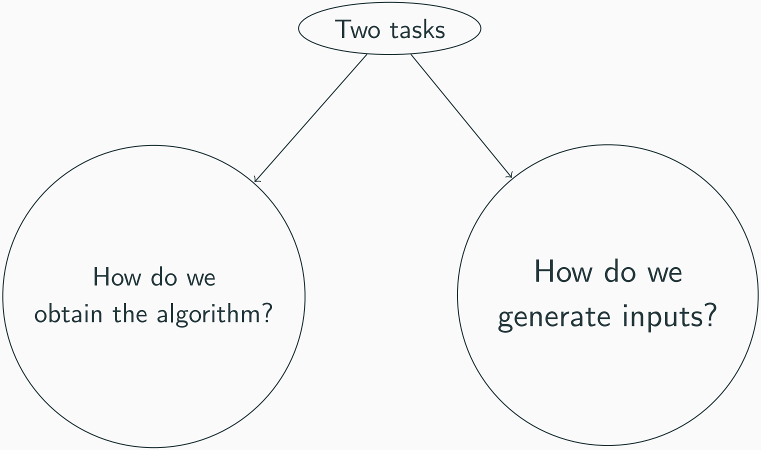
Theorem (heuristical)

The fourth power of quotients of even theta constants can be computed algebraically in an algorithmic way. (The algorithm is implemented in Magma.)

INPUT

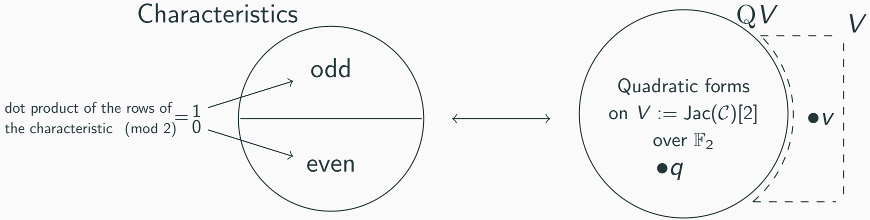
- Two even theta characteristics.
- The equations of the canonical model of the curve in $\mathbb{P}^{g-1}$.
- The equations of multitangents in $\mathbb{P}^{g-1}$ which are labelled with the appropriate characteristics.

How about higher genera?



The Algorithm

Characteristics, quadratic forms...



- V is a symplectic vector space of dimension $2g$ equipped with the Weil pairing.
- $\mathbb{Q}V \sqcup V$ is a vector space of dimension $2g+1$.

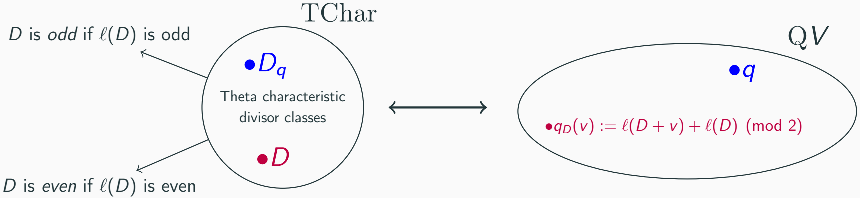
Fixing a symplectic basis $\{e_1, \ldots, e_g, f_1, \ldots, f_g\}$

$$\begin{bmatrix} q(e_1) & \ldots & q(e_g) \\ q(f_1) & \ldots & q(f_g) \end{bmatrix} = \begin{bmatrix} \epsilon \\ \epsilon' \end{bmatrix} =: [q] \qquad \longleftarrow \qquad q$$

Note that the *Arf invariant* $a(q) = \epsilon \cdot \epsilon'$.

Quadratic forms, theta characteristic divisors...

Let κ be the canonical divisor. We call a divisor (class) D *theta characteristic divisor (class)* if $2D \sim \kappa$.



Riemann theorem!

$$a(q) = \mathrm{mult}_0(\{z \mid \vartheta[q](z,\tau)\}) = \ell(D_q) \pmod 2.$$

Odd theta characteristic divisors, multitangents...

Let $\Phi : \mathcal{C} \to \mathbb{P}^{g-1}$ be the canonical embedding.

Let D be an effective theta characteristic divisor. Then

$$D \sim P_1 + \cdots + P_{g-1},$$

where P_i are the points on $\mathcal{C}$ for $i = 1, \ldots, g-1$.

Since $2D \sim \kappa$, there is a hyperplane H_D such that

$$H_D \cdot \Phi(\mathcal{C}) = 2 \cdot \phi(P_1) + \cdots + 2 \cdot \Phi(P_{g-1}).$$

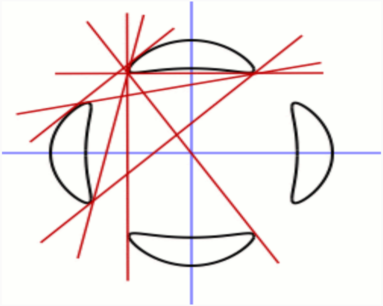
We call such a hyperplane *multitangent*.

g=3, there are 28 multitangents, namely bitangents

The canonical model of $\mathcal{C}$ is a plane quartic.

Example

Trott Curve

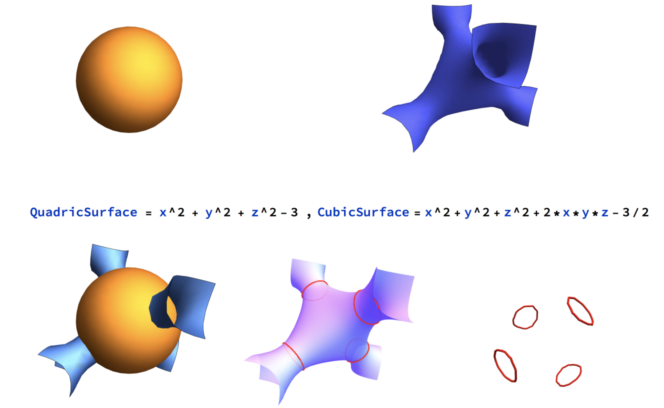


g=4, there are 120 or infinitely many multitangents, namely tritangents

The canonical model of $\mathcal{C}$ is an intersection of a cubic and a quadric surface in $\mathbb{P}^3$.

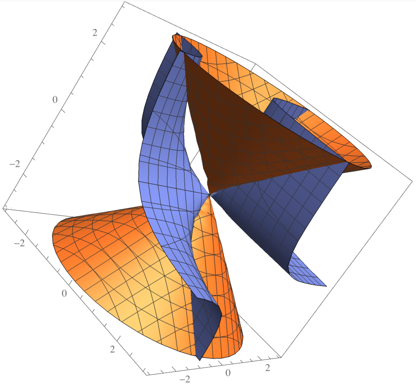
g=4, smooth quadric, 120 tritangents

The canonical model is either lying on a smooth quadric:

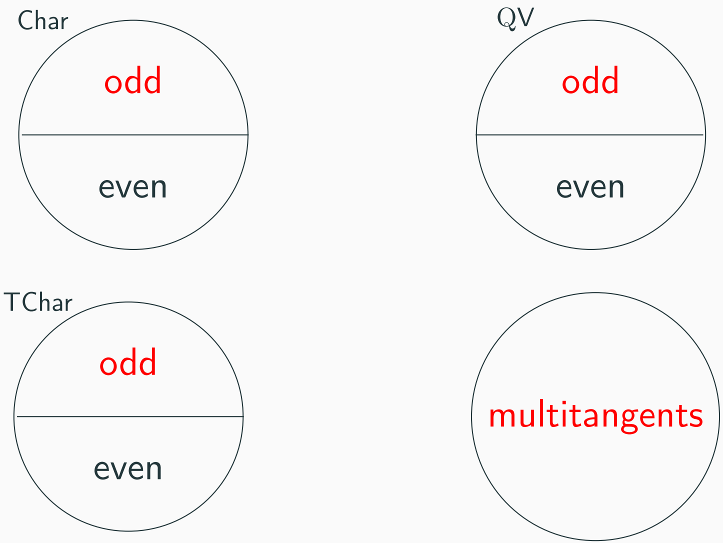


g=4, cone, infinitely many tritangents

Or the canonical model is lying on a singular quadric (cone):



Correspondence



The algorithm

Let p_1, p_2 be two even theta characteristics.

Consider the Riemann-Roch spaces $\mathcal{L}(D_{p_i} + \kappa)$ for $i = 1, 2$. Let $\{t_i^{(1)}, \ldots, t_i^{(2g-2)}\}$ be a basis of sections. Note that $t_i^{(j)}$'s are given by family of rational functions $\left(t_{i,\alpha}^{(j)}\right)_\alpha$ on an open cover $\{U_\alpha\}$ of $\mathcal{C}$.

Let S be an arbitrary generic effective divisor of degree $2g-3$ on $\mathcal{C}$.

For each $i = 1, 2$ and $k = 1, \ldots, 2g-3$, we may assume that there is α_k such that S_k is not a pole of $t_{i,\alpha_k}^{(j)}$ for any $j = 1, \ldots, 2g-2$.

We define $\chi_{i,S}$ as the family of the following rational functions

$$\chi_{i,S,\alpha}(P) = \begin{vmatrix} t_{i,\alpha}^{(1)}(P) & \cdots & t_{i,\alpha}^{(2g-2)}(P) \\ t_{i,\alpha_1}^{(1)}(S_1) & \cdots & t_{i,\alpha_1}^{(2g-2)}(S_1) \\ \vdots & & \vdots \\ t_{i,\alpha_{2g-3}}^{(1)}(S_{2g-3}) & \cdots & t_{i,\alpha_{2g-3}}^{(2g-2)}(S_{2g-3}) \end{vmatrix}, \quad 1 \le i \le 2,$$

on U_α for all α.

The algorithm

$\chi_{i,S} := (\chi_{i,S,\alpha})_\alpha$ is a section of $\mathcal{L}(D_{p_i} + \kappa)$ for $i = 1, 2$.

Take two odd theta characteristics $q_1, \overline{q}_1$ such that

$$p_1 + p_2 = q_1 + \overline{q}_1.$$

Write $D_{q_1} \sim A_1 + \cdots + A_{g-1}$ and $D_{\overline{q}_1} \sim B_1 + \cdots + B_{g-1}$.

If we set

$$S = A_2 + \cdots + A_{g-1} + A_1 + \cdots + A_{g-1}$$

and

$$S' = A_2 + \cdots + A_{g-1} + B_1 + \cdots + B_{g-1}$$

then

$$(-1)^{a(q_0+p_1+p_2)} \cdot \frac{\vartheta[p_1](0)^4}{\vartheta[p_2](0)^4} = \frac{\chi_{1,S}(A_1)^2 \cdot \chi_{2,S'}(A_1)^2}{\chi_{2,S}(A_1)^2 \cdot \chi_{1,S'}(A_1)^2}.$$

A special basis

Consider

$$\Big\{\{r_i, \overline{r}_i\} \mid i = 1, \dots, g-1\Big\} \text{ and } \Big\{\{s_i, \overline{s}_i\} \mid i = 1, \dots, g-1\Big\}$$

be sets of $g-1$ many distinct pairs of odd theta characteristics such that

$$p_1 + q_1 = p_2 + \overline{q}_1 = r_1 + \overline{r}_1 = \cdots = r_{g-1} + \overline{r}_{g-1}$$
$$p_1 + \overline{q}_1 = p_2 + q_1 = s_1 + \overline{s}_1 = \cdots = s_{g-1} + \overline{s}_{g-1}$$

We denote by $\sqrt{q}$ a (fixed) section $\mathcal{L}(D_q)$ for a quadratic form q. We write $\sqrt{q}(P) = \sqrt[P]{q}$.

A special basis

(Assume that) we can choose the following expressions

$$t_1^{(j)} = \sqrt{q_1 r_j \overline{r}_j} \text{ for } j \in \{1, \ldots, g-1\},\ t_1^{(j)} = \sqrt{\overline{q}_1 s_j \overline{s}_j} \text{ for } j \in \{g, \ldots, 2g-2\},$$

and

$$t_2^{(j)} = \sqrt{q_1 s_j \overline{s}_j} \text{ for } j \in \{1, \ldots, g-1\},\ t_2^{(j)} = \sqrt{\overline{q}_1 r_j \overline{r}_j} \text{ for } j \in \{g, \ldots, 2g-2\}$$

Warning

Certain choices may fail to be a basis! Note that we have

$$2 \times \binom{2^{g-2}(2^{g-1}-1)}{g-1}$$

choices for such candidates.

Pause: an open question

Fix $v \in \mathrm{Jac}(\mathcal{C})[2]$.

Can we always find a basis of $\mathcal{L}(\kappa + v)$ by the span of $\mathcal{L}(D) \otimes \mathcal{L}(D + v)$ when $D, D + v$ run through effective respresentatives of all the odd divisors?

An ambiguity - $\frac{0}{0}$

$$t_1^{(j)} = \sqrt{q_1 r_j \overline{r}_j} \text{ for } j \in \{1, \dots, g-1\},\ t_1^{(j)} = \sqrt{\overline{q}_1 s_j \overline{s}_j} \text{ for } j \in \{g, \dots, 2g-2\},$$

and

$$t_2^{(j)} = \sqrt{q_1 s_j \overline{s}_j} \text{ for } j \in \{1, \dots, g-1\},\ t_2^{(j)} = \sqrt{\overline{q}_1 r_j \overline{r}_j} \text{ for } j \in \{g, \dots, 2g-2\}$$

$$S = A_2 + \cdots + A_{g-1} + A_1 + \cdots + A_{g-1}$$
$$S' = A_2 + \cdots + A_{g-1} + B_1 + \cdots + B_{g-1}$$

Recall that $D_{q_1} \sim A_1 + \cdots + A_{g-1}$ and $D_{\overline{q}_1} \sim B_1 + \cdots + B_{g-1}$, so that

$$\sqrt[A_i]{q_1} = 0 \text{ for } i = 1, \dots, g-1$$
$$\sqrt[B_i]{\overline{q}_1} = 0 \text{ for } i = 1, \dots, g-1$$

$$(-1)^{a(q_0+p_1+p_2)} \cdot \frac{\vartheta[p_1](0)^4}{\vartheta[p_2](0)^4} = \frac{\chi_{1,S}(A_1)^2 \cdot \chi_{2,S'}(A_1)^2}{\chi_{2,S}(A_1)^2 \cdot \chi_{1,S'}(A_1)^2}.$$

Resolving the ambiguity $0/0$

We reset $S = S_2 + \cdots + S_{g-1} + A_1 + \cdots + A_{g-1}$.

After some cancelations in the expressions of $\chi_{1,S}(P), \chi_{2,S}(P)$, we let $S_i = A_i$ for $i = 2, \ldots, g-1$. And we have that

$$\frac{\chi_{1,S}(A_1)}{\chi_{2,S}(A_1)} = 1.$$

Hence

sections of the same line bundle corresponding to 3κ

$$\pm \frac{\vartheta[p_1](0)^4}{\vartheta[p_2](0)^4} = \frac{\chi^2_{2,S'}(A_1)}{\chi^2_{1,S'}(A_1)}.$$

Consider $\frac{\chi_{2,S'}(P)}{\chi_{1,S'}(P)}$

After some simplifications, we have

$$\frac{\chi_{2,S'}(A_1)}{\chi_{1,S'}(A_1)} = \frac{\begin{vmatrix} \sqrt[B_1]{s_1\overline{s}_1} & \cdots & \sqrt[B_1]{s_{g-1}\overline{s}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[B_{g-1}]{s_1\overline{s}_1} & \cdots & \sqrt[B_{g-1}]{s_{g-1}\overline{s}_{g-1}} \end{vmatrix} \begin{vmatrix} \sqrt[A_1]{r_1\overline{r}_1} & \cdots & \sqrt[A_1]{r_{g-1}\overline{r}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[A_{g-1}]{r_1\overline{r}_1} & \cdots & \sqrt[A_{g-1}]{r_{g-1}\overline{r}_{g-1}} \end{vmatrix}}{\begin{vmatrix} \sqrt[B_1]{r_1\overline{r}_1} & \cdots & \sqrt[B_1]{r_{g-1}\overline{r}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[B_{g-1}]{r_1\overline{r}_1} & \cdots & \sqrt[B_{g-1}]{r_{g-1}\overline{r}_{g-1}} \end{vmatrix} \begin{vmatrix} \sqrt[A_1]{s_1\overline{s}_1} & \cdots & \sqrt[A_1]{s_{g-1}\overline{s}_{g-1}} \\ \vdots & & \vdots \\ \sqrt[A_{g-1}]{s_1\overline{s}_1} & \cdots & \sqrt[A_{g-1}]{s_{g-1}\overline{s}_{g-1}} \end{vmatrix}}.$$

From sections to functions...

Let $\{r_g, \overline{r}_g\}$ and $\{s_g, \overline{s}_g\}$ be any other two pairs of quadratic forms different than any $\{r_i, \overline{r}_i\}$ and $\{s_i, \overline{s}_i\}$ for $i = 1, \ldots, g-1$ respectively such that $p_1 + q_1 = r_g + \overline{r}_g$ and $p_1 + \overline{q}_1 = s_g + \overline{s}_g$. Now,

$$\frac{\chi_{2,S'}(A_1)}{\chi_{1,S'}(A_1)} = \frac{d_{2,S'} \begin{vmatrix} \frac{\sqrt[B_1]{s_1\overline{s}_1}}{\sqrt[B_1]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[B_1]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[B_1]{s_g\overline{s}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[B_{g-1}]{s_1\overline{s}_1}}{\sqrt[B_{g-1}]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[B_{g-1}]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[B_{g-1}]{s_g\overline{s}_g}} \end{vmatrix} \begin{vmatrix} \frac{\sqrt[A_1]{r_1\overline{r}_1}}{\sqrt[A_1]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[A_1]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[A_1]{r_g\overline{r}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[A_{g-1}]{r_1\overline{r}_1}}{\sqrt[A_{g-1}]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[A_{g-1}]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[A_{g-1}]{r_g\overline{r}_g}} \end{vmatrix}}{d_{1,S'} \begin{vmatrix} \frac{\sqrt[B_1]{r_1\overline{r}_1}}{\sqrt[B_1]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[B_1]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[B_1]{r_g\overline{r}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[B_{g-1}]{r_1\overline{r}_1}}{\sqrt[B_{g-1}]{r_g\overline{r}_g}} & \cdots & \frac{\sqrt[B_{g-1}]{r_{g-1}\overline{r}_{g-1}}}{\sqrt[B_{g-1}]{r_g\overline{r}_g}} \end{vmatrix} \begin{vmatrix} \frac{\sqrt[A_1]{s_1\overline{s}_1}}{\sqrt[A_1]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[A_1]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[A_1]{s_g\overline{s}_g}} \\ \vdots & & \vdots \\ \frac{\sqrt[A_{g-1}]{s_1\overline{s}_1}}{\sqrt[A_1]{s_g\overline{s}_g}} & \cdots & \frac{\sqrt[A_{g-1}]{s_{g-1}\overline{s}_{g-1}}}{\sqrt[A_{g-1}]{s_g\overline{s}_g}} \end{vmatrix}}$$

where $d_{1,S'} = \sqrt[B_1]{r_g\overline{r}_g} \cdots \sqrt[B_{g-1}]{r_g\overline{r}_g}\,\sqrt[A_1]{s_g\overline{s}_g} \cdots \sqrt[A_{g-1}]{s_g\overline{s}_g}$ and $d_{2,S'} = \sqrt[B_1]{s_g\overline{s}_g} \cdots \sqrt[B_{g-1}]{s_g\overline{s}_g}\,\sqrt[A_1]{r_g\overline{r}_g} \cdots \sqrt[A_{g-1}]{r_g\overline{r}_g}$.

Focusing on $\frac{\sqrt[B_1]{s_1\bar{s}_1}}{\sqrt[B_1]{s_g\bar{s}_g}}$

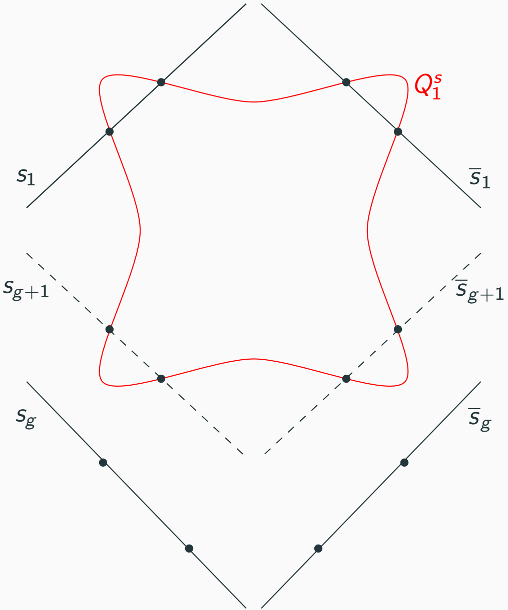
Let $\{s_{g+1}, \bar{s}_{g+1}\}$ be another pair of quadratic forms with $p_1 + \bar{q}_1 = s_1 + \bar{s}_1 = \cdots = s_{g+1} + \bar{s}_{g+1}$.

Observe that $s_1 + \bar{s}_1 + s_{g+1} + \bar{s}_{g+1} = 0$. We call such a tetrad a *syzygetic tetrad*.

$$\text{syzygetic}\left\{\begin{array}{r|l} s_1 & \bar{s}_1 \\ s_{g+1} & \bar{s}_{g+1} \\ s_g & \bar{s}_g \end{array}\right. \quad \left.\begin{matrix} s_1,\ \bar{s}_1 \\ s_{g+1},\ \bar{s}_{g+1} \end{matrix}\right\}\text{syzygetic}$$

Since $D_{s_1} + D_{\bar{s}_1} + D_{s_{g+1}} + D_{\bar{s}_{g+1}} \sim 2\kappa$, it is cut out by a (unique generically) quadric $\mathbb{P}^{g-1}$. Call $\mathcal{Q}_1^s, \mathcal{Q}_g^s$ such quadrics corresponding to $s_1, \bar{s}_1$ and $s_g, \bar{s}_g$ respectively.

g=3



Now...

$$\operatorname{div}\left(\frac{\sqrt{s_{\mathbf{1}}\overline{s}_{\mathbf{1}}}}{\sqrt{s_g\overline{s}_g}}\right) = \operatorname{div}\left(\frac{\mathcal{Q}^s_{\mathbf{1}}}{\mathcal{Q}^s_g}\right).$$

Hence there is a constant $c \in \mathbb{C}$ such that

$$\frac{\sqrt{s_{\mathbf{1}}\overline{s}_{\mathbf{1}}}}{\sqrt{s_g\overline{s}_g}} = c \cdot \frac{\mathcal{Q}^s_{\mathbf{1}}}{\mathcal{Q}^s_g}.$$

Those constants will be cancelled out in the expression.

$c \cdot \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}$

$$\frac{\chi_{2,S'}(A_1)}{\chi_{1,S'}(A_1)} = \frac{d_{2,S'}\left|\begin{array}{ccc||ccc} \frac{\sqrt[B_1]{s_1\bar{s}_1}}{\sqrt[B_1]{s_g\bar{s}_g}} & \cdots & \frac{\sqrt[B_1]{s_{g-1}\bar{s}_{g-1}}}{\sqrt[B_1]{s_g\bar{s}_g}} & \frac{\sqrt[A_1]{r_1\bar{r}_1}}{\sqrt[A_1]{r_g\bar{r}_g}} & \cdots & \frac{\sqrt[A_1]{r_{g-1}\bar{r}_{g-1}}}{\sqrt[A_1]{r_g\bar{r}_g}} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\sqrt[B_{g-1}]{s_1\bar{s}_1}}{\sqrt[B_{g-1}]{s_g\bar{s}_g}} & \cdots & \frac{\sqrt[B_{g-1}]{s_{g-1}\bar{s}_{g-1}}}{\sqrt[B_{g-1}]{s_g\bar{s}_g}} & \frac{\sqrt[A_{g-1}]{r_1\bar{r}_1}}{\sqrt[A_{g-1}]{r_g\bar{r}_g}} & \cdots & \frac{\sqrt[A_{g-1}]{r_{g-1}\bar{r}_{g-1}}}{\sqrt[A_{g-1}]{r_g\bar{r}_g}} \end{array}\right|}{d_{1,S'}\left|\begin{array}{ccc||ccc} \frac{\sqrt[B_1]{r_1\bar{r}_1}}{\sqrt[B_1]{r_g\bar{r}_g}} & \cdots & \frac{\sqrt[B_1]{r_{g-1}\bar{r}_{g-1}}}{\sqrt[B_1]{r_g\bar{r}_g}} & \frac{\sqrt[A_1]{s_1\bar{s}_1}}{\sqrt[A_1]{s_g\bar{s}_g}} & \cdots & \frac{\sqrt[A_1]{s_{g-1}\bar{s}_{g-1}}}{\sqrt[A_1]{s_g\bar{s}_g}} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\sqrt[B_{g-1}]{r_1\bar{r}_1}}{\sqrt[B_{g-1}]{r_g\bar{r}_g}} & \cdots & \frac{\sqrt[B_{g-1}]{r_{g-1}\bar{r}_{g-1}}}{\sqrt[B_{g-1}]{r_g\bar{r}_g}} & \frac{\sqrt[A_{g-1}]{s_1\bar{s}_1}}{\sqrt[A_1]{s_g\bar{s}_g}} & \cdots & \frac{\sqrt[A_g-1]{s_{g-1}\bar{s}_{g-1}}}{\sqrt[A_{g-1}]{s_g\bar{s}_g}} \end{array}\right|},$$

where $d_{1,S'} = \sqrt[B_1]{r_g\bar{r}_g} \cdots \sqrt[B_{g-1}]{r_g\bar{r}_g}\, \sqrt[A_1]{s_g\bar{s}_g} \cdots \sqrt[A_{g-1}]{s_g\bar{s}_g}$ and $d_{2,S'} = \sqrt[B_1]{s_g\bar{s}_g} \cdots \sqrt[B_{g-1}]{s_g\bar{s}_g}\, \sqrt[A_1]{r_g\bar{r}_g} \cdots \sqrt[A_{g-1}]{r_g\bar{r}_g}$.

By taking the square, we get...

$$
\left(\frac{\chi_{2,S'}(A_1)}{\chi_{1,S'}(A_1)}\right)^2 = \frac{d_{1,S'}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(B_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(B_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(B_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(A_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_{(g)}^r}(A_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(A_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_g^r}(A_{g-1}) \end{vmatrix}^2}{d_{2,S'}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(B_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_g^r}(B_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^r}{\mathcal{Q}_g^r}(B_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^r}{\mathcal{Q}_g^r}(B_{g-1}) \end{vmatrix}^2 \begin{vmatrix} \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(A_1) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(A_1) \\ \vdots & & \vdots \\ \frac{\mathcal{Q}_1^s}{\mathcal{Q}_g^s}(A_{g-1}) & \cdots & \frac{\mathcal{Q}_{(g-1)}^s}{\mathcal{Q}_g^s}(A_{g-1}) \end{vmatrix}^2}
$$

where

$$
d_{1,S'} = \sqrt[B_1]{r_g \overline{r}_g} \cdots \sqrt[B_{g-1}]{r_g \overline{r}_g} \sqrt[A_1]{s_g \overline{s}_g} \cdots \sqrt[A_{g-1}]{s_g \overline{s}_g},
$$

and

$$
d_{2,S'} = \sqrt[B_1]{s_g \overline{s}_g} \cdots \sqrt[B_{g-1}]{s_g \overline{s}_g} \sqrt[A_1]{r_g \overline{r}_g} \cdots \sqrt[A_{g-1}]{r_g \overline{r}_g}.
$$

Generating Input

g=4, when the curve is lying on a cone

Consider $\mathcal{P} := \{P_1, \dots, P_8\} \subseteq \mathbb{P}^2$ eight points in general position. Let

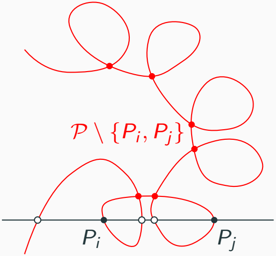
- $\{s, t\}$ be any basis of the space of plane cubics through $\mathcal{P}$,
- $\{s^2, st, t^2, w\}$ be a basis of the space of plane sextics vanishing doubly on $\mathcal{P}$,
- $\{s^3, s^2t, st^2, t^3, sw, tw, r\}$ be a basis of the space of plane nonics vanishing triply on $\mathcal{P}$.

$$
\begin{array}{ccccl}
\mathbb{P}^2 \overset{\psi}{\dashrightarrow} \mathbb{P}(1:1:2:3) & \supseteq & X := \psi(\mathbb{P}^2) & & \textit{del Pezzo surface of degree 1} \\
\pi \Big\downarrow \quad (s:t:w:r) \mapsto (s:t:w) & & & & \\
\mathbb{P}(1:1:2) & \supseteq & \mathcal{C}' := \mathrm{BranchCurve}(\pi|_X) & & \\
\phi \Big\downarrow \quad (s:t:w) \mapsto (s^2:st:t^2:w) & & \Big\downarrow & & \\
\mathbb{P}^3 & \supseteq & \mathcal{C} & &
\end{array}
$$

Tritangents of $\mathcal{C}$

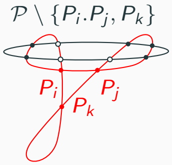
Every tritangent of $\mathcal{C}$ is the image of exactly two exceptional curves on the del Pezzo surface X under $\phi \circ \pi$, which are conjugate under the Bertini involution of X.

- the point P_i and the sextic vanishing triply at P_i and doubly at the other seven points.
- the line through $\{P_i, P_j\}$ and the quintic vanishing at all eight points and doubly at the six points in $\mathcal{P}\backslash\{P_i, P_j\}$.

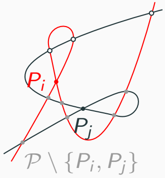


Tritangents

- the conic through $\mathcal{P} \setminus \{P_i, P_j, P_k\}$ and the quartic vanishing at $\mathcal{P}$ and doubly at P_i, P_j, P_k.



- the cubic vanishing doubly at P_i, non-vanishing at P_j, and vanishing simply at $\mathcal{P}\setminus\{P_i, P_j\}$ and the cubic vanishing doubly at P_j, non-vanishing at P_i, and vanishing simply at $\mathcal{P}\setminus\{P_i, P_j\}$.



An example

Consider the configuration $\mathcal{P} = \{P_1, \ldots, P_8\} \subseteq \mathbb{P}^2(\mathbb{Q})$ of the following 8 points:

$$P_1 = (2 : -3 : 1), \quad P_5 = (1/2 : 0 : 1) \quad P_2 = (3/2 : 1 : 1), \quad P_6 = (2/3 : 2/3 : 1)$$
$$P_3 = (0 : -3/2 : 1), \quad P_7 = (-3 : 2 : 1) \quad P_4 = (3/2 : 3/2 : 1), \quad P_8 = (1/3 : 1 : 1)$$

The defining equations of $\mathcal{C}$ are

$$\begin{aligned}
&x_0^3 + 2425564030663/162140107530 x_0^2 x_1 + 15669691012720998280286400529/149429031846570347991915600 x_0^2 x_2 \\
&+21170944847941843110793728964 7/448287095539711043975746800 x_0 x_1 x_2 + 9910047994802558384716635818134607/7644191553143152721874434433600 x_0 x_2^2 \\
&+905783995186184025726770668993123/395389218266025140786608677600 x_1 x_2^2 + 92368472409963092742435769596441128153/55863751870370160091458366840748800 x_2^3 \\
&-29830449072973532706572819/236073482149263407485060 x_0^2 x_3 - 1011526537873326300399754441310551/637015962761929393489536202800 x_0 x_1 x_3 \\
&-36690171700015844095035636292739030279/54311980985082100088917856650728 00 x_0 x_2 x_3 - 331206537690486038353064612628955433/175577524736256789080553415 89675 x_1 x_2 x_3 \\
&-1062182808186693286084865785168875289650763/79382391407795997489962339280704044800 x_2^2 x_3 + 1162135044692003397844695454373200491311/1715051666217814760585606095570766400 x_0 x_3^2 \\
&+24403529360323237608442590572012473543277/798386120480706871307092492765701600 x_1 x_3^2 - 2260119208090704069704104349128528879254888149/112802378190478112433236484117880447660800 x_2 x_3^2 \\
&+13204897029090296036812705006873263119397966616189/53430726469556465922543014643836038708665600 x_3^3, \\
&x_1^2 - x_0 x_2
\end{aligned}$$

An example

We can compute the list of the equations of tritangents:

$$
\begin{gathered}
x_0 + 4073720176917559726/1133376368146185855x_1 + 32745301196096220457845 4/2415791728703595149932 5x_2 - 1127351626887499587081295 81/1373136018595123483221633x_3,\\
x_0 + 350578164144253479/46203319572275680x_1 + 186379990531145373070 81/236357701603933468608 0x_2 + 131316444954786724427554199/335864293979189458891968 0x_3,\\
x_0 + 211479792266371/218188348090920x_1 + 1316618230054501981871/7069040652128098896 0x_2 - 575772344090809694948314 9/334836892222467617707 20x_3,\\
x_0 + 17373590988118142/4158176266996215x_1 + 2145420612977287913 77/177263054262048645 45x_2 - 151002672179443423189734 4/251890800106371125184 45x_3,\\
x_0 + 4864890585953831/378366090117870x_1 - 512579666106105329/131671399361018760x_2 + 185271228743717938285 09/801878822108604248 40x_3,\\
x_0 + 149286535172373/30708550083235x_1 + 964354660076388445/89767233603312552x_2 - 771093039122806876675 1/212598731583845227320x_3,\\
x_0 + 600953315525715/190786792110254x_1 + 279475735717785218413/195197782743843072 48x_2 - 446956521850320608748851 9/462293415465001676656 80x_3,\\
x_0 + 24850715371714303/5696394486025210x_1 + 382020355755227657280 7/291404756327105642760x_2 - 786876715268942791133399/125480654163883975261 20x_3,\\
x_0 + 903225497/369556365x_1 + 199224827801747/12603350271960x_2 - 6542142470614222261/53728082209365480x_3,\\
x_0 + 1289061985/307910162x_1 + 209545404053987/15751452247272x_2 - 2527971780098556301/37304689405622520x_3,\\
x_0 + 3227297803/826483812x_1 + 90490251893963/7046600981112x_2 - 14336323894698807/202287272609296x_3,\\
x_0 + 57335427860129/11475325450080x_1 + 679202562690930247/65225749858254720x_2 - 259788477508090765984 31/834172114937219614080x_3,\\
x_0 + 6322191013177/3814460277285x_1 + 935124327549320243/65044176648263820x_2 - 3983438390860063284061/30809258339060962740x_3,\\
x_1 - 12646609161011223/21350501266145380x_2 + 3321248368938556955/130959981147593892x_3,\\
x_0 + 5122998713/662005752x_1 + 96913679546351/11288522083104x_2 + 8883742040081694071/240614848201361760x_3,\\
x_0 + 1935440839217/237125656815x_1 + 36305614923105853/4043466700009380x_2 + 2649878320949811823 19/574576618071332898 0x_3,\\
x_0 + 3663575555203/986415103560x_1 + 226684261333339967/16820350345905120x_2 - 2098981181422852332 87/265574642683679728 0x_3,\\
x_0 - 1152767551702/459889427085x_1 + 7025018642918134/280072661094765x_2 - 1161242235470603367/4020032842582435x_3,\\
x_0 + 19960603357/5537568230x_1 + 20324578773181561/1537804847743920x_2 - 1743344773341690593 89/218522068864411032 0x_3,\\
x_0 + 12997908343344/3072843440995x_1 + 1182489526791012001/89825359467165840x_2 - 84150828331893585039 01/12764183580284265864 0x_3,\\
x_0 + 27526310486771/6714783636045x_1 + 31005944979969511/2336744705343660x_2 - 3292097843686002714 1/474359175184762980x_3,\\
x_0 + 601775140562/121781832033x_1 + 76094874659365/5967309769617x_2 - 210266083788915836/4385972680668495x_3,\\
x_0 + 12989495751/3553066880x_1 + 1343532205225249/98670088484352x_2 - 4778774631566269/58847559697920x_3\ ,\\
x_0 + 236687709629/45883182720x_1 + 5324639502755791/434666684300800x_2 - 8883742040081694071/2223580890209172 48x_3,\\
x_0 + 240885426739/27411960735x_1 + 332713529569297/80591164560900x_2 + 4778774631566269/52652894179788x_3,\\
x_0 + 1496363111081/538417805370x_1 + 276048316628067587/18362200834338480x_2 - 285378385570411295515 1/260926873855949800 80x_3,\\
\vdots
\end{gathered}
$$

Labelling based on an Aronhold basis

Let $\rho\colon \operatorname{Pic}(X) \to \operatorname{Pic}(\mathcal{C})$ be the natural restriction map. Let $E_1, \ldots, E_8$ be the exceptional divisors corresponding to the points $P_1, \ldots, P_8$.

- Let κ_X be the canonical divisor of X. Then $\rho(-\kappa_X)$ is an even theta characteristic divisor.

Set $v_i = \rho(\kappa_X + E_i)$ for $i = 1, \ldots, 8$ and $q_9 = q_{\rho(-K_X)}$. For $i = 1, \ldots, 8$, define

$$q_i := q_9 + \sum_{j=1, j \neq i}^{8} v_j,$$

then

$$\{q_1, \ldots, q_9\}$$

is an Aronhold basis for $\mathrm{Q}(\operatorname{Jac}(\mathcal{C})[2]) \sqcup \operatorname{Jac}(\mathcal{C})[2]$.

This means...

$$
\begin{array}{ccccc}
q_1, \dots, q_9 & \longleftrightarrow & \{i\} & \longleftrightarrow & \text{even} \\
q_i + q_j + q_k & \longleftrightarrow & \{i, j, k\} & \longleftrightarrow & \text{odd} \\
q_{i_1} + \cdots + q_{i_5} & \longleftrightarrow & \{i_1, \dots, i_5\} & \longleftrightarrow & \text{even} \\
q_{i_1} + \cdots + q_{i_7} & \longleftrightarrow & \{i_1, \dots, i_7\} & \longleftrightarrow & \text{odd} \\
q_1 + \cdots + q_9 & \longleftrightarrow & \{1, \dots, 9\} & \longleftrightarrow & \text{even}
\end{array}
$$

By that way, we can find all the corresponding theta characteristic divisors and label them.

$\mathcal{C}$	X	$\mathbb{P}^2$
D_{ijk}	$2L - \sum_{l \neq i,j,k} E_l$	conic vanishing simply at $\mathcal{P} \setminus \{P_i, P_j, P_k\}$.
	$4L - \sum_{l \neq i,j,k} E_l - \sum_{l \in \{i,j,k\}} 2E_l$	quartic vanishing at $\mathcal{P}$ and doubly at P_i, P_j, P_k
D_{ij9}	$3L - 2E_i - \sum_{k \neq i,j} E_k$	cubic vanishing doubly at P_i, non-vanishing at P_j, and vanishing simply at $\mathcal{P} \setminus \{P_i, P_j\}$
	$3L - 2E_j - \sum_{k \neq i,j} E_k$	cubic vanishing doubly at P_j, non-vanishing at P_i, and vanishing simply at $\mathcal{P} \setminus \{P_i, P_j\}$

$\mathcal{C}$	X	$\mathbb{P}^2$
$D_{i_1 \ldots i_6 i_7}$	E_i for $i \neq i_1, \ldots, i_6, i_7$	point P_i
	$6L - \sum_{j \neq i}^{8} 2E_j - 3E_i$	sextic vanishing triply at P_i and doubly at the other seven points
$D_{q_{i_1 \ldots i_6} 9}$	$L - E_i - E_j$	line through $\{P_i, P_j\}$
	$5L - \sum_{k \in I_{ij}}^{8} 2E_k - E_i - E_j$	quintic vanishing at all eight points and doubly at the six points in $\mathcal{P} \backslash \{P_i, P_j\}$

Test

Going back to our example

Recall that

$$P_1 = (2 : -3 : 1), \quad P_5 = (1/2 : 0 : 1), \quad P_2 = (3/2 : 1 : 1), \quad P_6 = (2/3 : 2/3 : 1),$$
$$P_3 = (0 : -3/2 : 1), \quad P_7 = (-3 : 2 : 1), \quad P_4 = (3/2 : 3/2 : 1), \quad P_8 = (1/3 : 1 : 1).$$

Let $p_1 = \{1, 2, 3, 4, 5\}$ and $p_2 = \{3, 4, 5, 6, 9\}$, then

$$\left(\frac{\vartheta[p_1]}{\vartheta[p_2]}\right)^4 = 388285435266921829/1618395584522100000$$
$$\approx 0.2399199793798124993931025790953104475687561041468 8.$$

Computing a Riemann matrix τ

$$\begin{bmatrix} 1.07847i & -0.19708i & 0.30983 & 0.50267i \\ -0.19708i & 1.16996i & 0.05607 & 0.24922i \\ 0.30983 & 0.05607 & 1.23052i & -0.16325 \\ 0.50267i & 0.24922i & -0.16325 & 1.42766i \end{bmatrix}$$

$$\left(\frac{\vartheta[p_1]}{\vartheta[p_2]}\right)^4 \approx {\color{red}0.23991997937981249939310257909595}601233140655714802 + 3.7159298539100801602637260320467646858906346912020 \times 10^{-53} i.$$